CENTRO DE POSGRADOS

Tema:

ANÁLISIS DE MALWARE PARA MÓVILES CON SISTEMA OPERATIVO ANDROID. UNA GUÍA DE RECOMENDACIÓN PARA EMPRENDEDORES

Proyecto de investigación previo a la obtención del título de Magíster en Ciberseguridad

Línea de investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

Edgar Fabricio Chacha Chadan

Director:

Mg. Galo Mauricio López Sevilla

Ambato – Ecuador

Diciembre 2024

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **EDGAR FABRICIO CHACHA CHADAN**, con cédula de ciudadanía **1804545232**, autor del trabajo de graduación titulado: "ANÁLISIS DE MALWARE PARA MÓVILES CON SISTEMA OPERATIVO ANDROID. UNA GUÍA DE RECOMENDACIÓN PARA EMPRENDEDORES", previo a la obtención del título de **MAGÍSTER EN CIBERSEGURIDAD**, en el centro de **POSGRADOS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, diciembre 2024

Edgar Fabricio Chacha Chadan

CC. 1804545232

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

ANÁLISIS DE MALWARE PARA MÓVILES CON SISTEMA OPERATIVO ANDROID. UNA GUÍA DE RECOMENDACIÓN PARA EMPRENDEDORES

Línea de investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

Edgar Fabricio Chacha Chadan

Galo Mauricio López Sevilla, Ing. Mg. f._____
CC. 1802836039
CALIFICADOR

Santiago Alejandro Acurio Maldonado, Ing. Mg. f._____
CALIFICADOR

Darío Javier Robayo Jácome, Ing. Mg. f._____
CALIFICADOR

Dayamy Lima Rojas, Lic. Mg. f._____
DIRECTORA CENTRO DE POSGRADOS

Diego Gonzalo Coca Chanalata, Dr. f._____
SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Diciembre 2024

DEDICATORIA

Dedico este logro a las mujeres excepcionales en mi vida, mi madre y mis queridas hermanas. Su amor, apoyo inquebrantable y constante inspiración han sido la luz que me ha guiado a lo largo de este viaje académico. A través de los desafíos y triunfos, su presencia ha sido mi mayor motivación. Este logro es tan suyo como mío, y les agradezco desde lo más profundo de mi corazón por ser mi fuente de fortaleza y perseverancia. Sin ustedes, esto no sería posible. Gracias por ser mi familia y mi apoyo.

Dedico también a mi amada novia, quien ha compartido mis alegrías y tristezas, y ha sido mi roca en los momentos difíciles. Sin su amor y aliento, este logro no sería posible.

Este trabajo es un testimonio de amor y de la importancia que tienen cada uno de ustedes en mi vida. Gracias por estar siempre a mi lado. ¡Este logro es tan vuestro como mío!"

AGRADECIMIENTO

En el culmen de este viaje académico, quiero expresar mi más profundo agradecimiento a las personas que han contribuido significativamente a mi tesis y a mi crecimiento como estudiante en la Maestría en Ciberseguridad de la Pontificia Universidad Católica del Ecuador Sede Ambato.

A mis respetados compañeros de clase, gracias por ser compañeros ejemplares y por compartir este viaje de conocimiento conmigo. Nuestras discusiones, debates y colaboraciones han enriquecido mi comprensión del mundo de la ciberseguridad. Vuestra camaradería y apoyo han sido invaluables.

A nuestros estimados profesores, agradezco profundamente su dedicación a la enseñanza y su generosidad al compartir su experiencia y sabiduría. Vuestras lecciones han sido fundamentales para mi formación en el campo de la ciberseguridad, y valoro su compromiso con nuestra educación.

A mi tutor, el Ing. Galo López, le agradezco por su guía experta, mentoría y apoyo constante en la realización de esta tesis. Sus conocimientos y dirección han sido esenciales en cada paso de este proceso. Su compromiso con mi crecimiento académico y profesional es digno de admiración.

A la coordinadora de la Maestría en Ciberseguridad, agradezco su labor incansable en la gestión de nuestro programa y su apoyo en asuntos académicos. Su contribución ha sido crucial para que esta maestría sea una experiencia exitosa.

Este logro es el resultado del esfuerzo colectivo y de la generosidad de muchas personas. A todos ustedes, les agradezco por su contribución a mi educación y por formar parte de este importante capítulo de mi vida académica.

RESUMEN

En la actualidad, los emprendedores de la ciudad de Ambato se encuentran en una creciente dependencia de los dispositivos móviles para llevar a cabo sus operaciones comerciales. Sin embargo, los convierte en un objetivo potencial para los ciberdelincuentes. Ante esta realidad, es imperativo comprender y mitigar las amenazas de malware en los dispositivos móviles que podrían comprometer la seguridad de sus actividades empresariales.

La guía de recomendaciones proporciona información sobre las mejores prácticas y herramientas disponibles para el análisis de malware en dispositivos Android. Esto incluye el uso de antivirus, cortafuegos, actualizaciones regulares del sistema operativo y la educación de los empleados sobre las amenazas de seguridad.

La seguridad de los dispositivos móviles es fundamental para garantizar la continuidad de las operaciones empresariales y la protección de datos confidenciales. Esta guía busca empoderar a los emprendedores de Ambato con conocimientos y prácticas que les permitan mantener sus dispositivos móviles seguros y protegidos contra las amenazas de malware.

Palabras claves: seguridad de dispositivos móviles, ciberseguridad emprendimiento, innovación tecnológica empresarial, dispositivos móviles, concientización empresarial, análisis de malware

ABSTRACT

Today, entrepreneurs in Ambato increasingly rely on mobile devices to conduct their business operations. However, this makes them a potential target for cybercriminals. Given this reality, it is imperative to understand and mitigate malware threats on mobile devices that could compromiso the security of their business activities.

The recommendations guide provides information on best practices and tools for malware analysis on Android devices. This includes using antivirus, firewalls, regular operating system updates, and educating employees about security threats.

The security of mobile devices is critical to ensure business continuity and the protection of sensitive data. This guide aims to empower entrepreneurs in Ambato with knowledge and practices that will enable them to keep their mobile devices safe and secure from malware threats.

Keywords: *mobile device security, entrepreneurship cybersecurity, business technology innovation, mobile devices, entrepreneurial awareness, malware analysis*

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Las tecnologías de la información, conocidas como TIC´S, son consideradas como las herramientas empleadas para la creación de programas informáticos que permiten procesar, recopilar información a través de sitios web o páginas de acuerdo con el requerimiento de los usuarios. Sin embargo, las continuas trasformaciones que ha realizado la sociedad en base a la ciencia han permitido desarrollar programas que garanticen eficiencia y avance del conocimiento e innovación tecnológica para ser empleados de manera oportuna y adecuada para sistemas operativos.

En octubre de 2005, Andy Rubin, Rick Miner y Chris White crearon el sistema operativo Android con un enfoque claro: introducir al mercado teléfonos inteligentes que pudieran ofrecer contenido avanzado y estuvieran conectados a funciones de servidor de internet. El 5 de noviembre de 2007 marcó un hito en la historia de Android, cuando logró un gran éxito al establecer la *Open Handset Alliance* (OHA), una fundación que impulsó una alianza comercial con 35 miembros para promocionar y vender este sistema. Este paso clave llamó la atención de HTC y cambió el rumbo de la industria de los smartphones.

En octubre del 2008, *Android* crea planes estratégicos para adentrar y vender en el mercado teléfonos de atención HTC, corresponde a la evolución e innovación tecnológica en almacenes para aplicaciones como *play store* la utilizadas en los últimos tiempos.

Por lo tanto, el estudio de Herraiz (2012) con el tema: “Historia de la informática”, realizado en la Universidad de Valencia considera que Google empezó a liderar como fabricante de terminales móviles, operadores de telecomunicaciones fabricantes de chips y desarrollo de software publicando mayor fuente de código para un sistema operativo denominado como *software Apache* con proyectos de códigos abiertos. (p. 20)

Es así que Android, es un sistema operativo de Google para teléfonos inteligentes. Basado en Linux, según Álvarez (2015) con la investigación titulada: “Microprocesadores para Comunicaciones: *Android* Las Palmas de Gran Canarias”, de la Universidad de las Palmas Gran Canarias, considera que es un sistema

gratuito y multiplataforma entendida como el SO que puede ser usado en distintas plataformas (plataforma es una combinación de hardware y software usada para ejecutar aplicaciones) y al ser gratuito se puede instalar de forma fácil en los dispositivos móviles. (p. 52)

Al hablar de un sistema operativo como un conjunto de programas que permiten manejar la memoria de un disco, almacenamiento e información interna de un dispositivo o computadora. Como se analiza en investigación realizada por Pedrozo (2015) con el tema: “Sistemas Operativos en dispositivos móviles”, de la Universidad Nacional del Nordeste, describe que:

> El sistema oprativo basado en Lunix, en conjunto a aplicaciones middleware es utilizado en teléfonos inteligentes, tabletas, Google Tv, que fueron desarrollados por la *Open Handset Alliance* la cual es liderada por Google desde 2005, cuya funcionalidad es un conglomerado de fabricantes para software cuyas unidades vendidas se ubicaron en el primer puesto de Estados Unidos en 2010 con una cuota de mercado de 43,6% en el tercer trimestre. A nivel mundial alcanzó una cuota de mercado del 50,9% durante el cuarto trimestre de 2012, más del doble que el segundo sistema operativo iOS de Apple, Inc. (p.7- 8)

Durante estos últimos años, el desarrollo de *Android* no ha parado y han sido muchas las versiones lanzadas del sistema con mejoras a nivel de rendimiento y seguridad, así como de soporte de muchas tecnología y nuevas funciones. Además, la gran comunidad de desarrolladores detrás del entorno de Google ha permitido extender la funcionalidad de los dispositivos.

El aporte de Ramírez (2020) menciona que a principios de 2018, ya se superaban los dos millones de aplicaciones disponibles en la tienda oficial de aplicaciones para Android, Google Play. Incluso se ha visto cómo han ido apareciendo otras tiendas de aplicaciones no oficiales con gran cantidad de aplicaciones para el sistema operativo de Google. (p. 39)

Sin embargo, el trabajo realizado por Caqueta (2015) con el documento: ”Sistemas operativos”, de la Universidad de las Américas, enfatiza que a nivel mundial “*Apple y Google*” han tomado medidas preventivas como corregir vulnerabilidades, de los

sistemas operativos para adecuar medidas de seguridad en todas las tiendas virtuales. (p. 38)

Por lo tanto, el estudio realizado por *AVG-Comparativesen* citado por Muenas (2018) con el tema:”Malware ára dspositivos máoviles Androit”, de la Universidad Tecnológica de Chile INACAP, integra al sistema “Malware” como un software malicioso identificado como un programa informático creado para perjudicar y amenazar dispositivos, teléfonos inteligentes, computadoras, laptops. Siendo la principal víctima el sistema Android. (p. 4)

En Ecuador, existe una demanda masiva de usuarios que acceden a sitios webs mediante el uso de un dispositivo móvil cuyo estudio realizado por Barrero (2016) con el tema: “Análisis de la eficiencia de los sistemas operativos para servidores web disponibles en el mercado global y su impacto en la aplicación dentro de la Universidad Estatal de Milagro”, empleando una metodología descriptiva menciona que la concientización sobre la utilización de software libre en el país se limita a desarrollarse como buenas bases, debido al desconocimiento de la utilización, capacitación y los beneficios que proveen frente al software tradicional que abarca la mayor parte el mercado comercial. (p. 36)

Bajo este punto de vista, el Estado optó por mejorar el acceso a la tecnología siendo Richard Stallman, fundador del movimiento de Software libre que en el año 2008 mediante el decreto 1014, el Ecuador pasó a ser el tercer país de América Latina en tener políticas en favor del uso del software libre.

Un estudio realizado por Huicamaigua (2017) con el tema: “Aplicación de una metodología para el análisis de los efectos de Malware en dispositivos de sistemas operativos Android en Ecuador”, de la Universidad Politécnica del Litoral, afirma que en el país que el 64% los usuarios no cuenta con herramientas de antivirus instaladas en los dispositivos, permitiendo que se descarguen aplicaciones gratuitas conocidas como antimalware que puede incluir un software malicioso y con fallos de seguridad , estando los dispositivos vulnerables a experimentar pérdida de la información o daño directo en el software del equipo. (p.19)

Por tanto, el problema de estudio tiene por propósito analizar, las repercusiones que puede causar un software malicioso o Malware en los dispositivos móviles y equipos de cómputo. El desarrollo de antivirus y productos para detectar y evitar el software malicioso está en continuo crecimiento, pero el funcionamiento en dispositivos móviles no es a menudo el esperado relegando la mayor parte de la responsabilidad en el usuario, quien debe ser consciente de qué software está instalado, cómo le afecta y el alcance de las consecuencias.

Los emprendedores de la ciudad de Ambato, se han enfrentado a la creciente necesidad de adoptar y desarrollar plataformas digitales para dispositivos móviles que les permitan llegar de manera eficaz y segura a sus clientes, especialmente en tiempos de distanciamiento social. Ejemplos notables incluyen el desarrollo de una aplicación de entrega de comida que conecta restaurantes locales con comensales, así como la expansión de plataformas de *e-commerce* que facilitan la venta de productos y servicios en línea. Estas innovadoras soluciones no solo promueven la continuidad de los negocios locales, sino que también mejoran la experiencia del cliente al ofrecer comodidad y seguridad en el acceso a una amplia gama de productos y servicios.

En este contexto el uso de dispositivos móviles se ha incrementado, así como también los efectos del software malicioso, pudiendo observarse espacios de seguridad vulnerados como perdida de información en este grupo poblacional. Según lo descrito el problema científico se declara en forma de pregunta de la siguiente manera: ¿Cómo disminuir los efectos del Malware en los dispositivos móviles de los emprendedores?

Esta argumentación conduce al investigador a formular las siguientes interrogantes científicas como parte de la investigación:

¿Existe la suficiente fundamentación teórica relacionada con los efectos del Malware en dispositivos móviles de emprendedores con sistema operativo Android?

¿Existe una metodología adecuada que recopile buenas prácticas de seguridad para reducir los efectos de Malware en móviles con sistema operativo Android?

¿Una guía de recomendación para emprendedores permitirá reducir los efectos de Malware en móviles con sistema operativo Android de emprendedores?

El principal objetivo del proyecto de investigación expone la integridad e innovación para analizar los principales problemas tecnológicos que deja un software Malicioso y las repercusiones económicas, sociales de acuerdo con las diferentes modalidades que tiene esta forma dañina para un dispositivo, por tanto, el objetivo general es:

Para resolver el problema señalado se propone como tareas investigativas las mencionadas a continuación:

Como tarea principal se tiene: Analizar los ataques de Malware en dispositivos móviles con sistema operativo Android de emprendedores.

Posterior a ello se detallan las tareas a cumplir para resolver el problema mencionado:

1. Recopilación de la documentación relacionada con los efectos del Malware en dispositivos móviles de emprendedores con sistemas operativos Android.
2. Estudio de perspectivas metodológicas de aplicación de buenas prácticas de seguridad para reducir los efectos del Malware en sistemas operativos Android.
3. Recopilación de buenas prácticas en una guía de recomendaciones de seguridad para emprendedores.

Metodología de la Investigación

Para el desarrollo del presente proyecto se aplica una metodología de campo puesto que se recogerá información necesaria en el lugar de los hechos y así determinar las necesidades de los emprendedores relacionada con los ataques de software malicioso, posteriormente se aplicar una metodología documental, obteniendo información de libros técnicos, informes, artículos que recopile buenas prácticas de seguridad informática. Se utilizará además la modalidad aplicada, poniendo en práctica los conocimientos adquiridos durante los módulos de la Maestría en Ciberseguridad de la Pontificia Universidad Católica del Ecuador Sede Ambato.

Nivel de investigación

De acuerdo con la naturaleza del presente estudio, se realiza una investigación descriptiva y explicativa, se realizará una investigación en base a fuentes documentales que ayudaran a encontrar información para solventar las preguntas científicas que se plasman en la presente investigación, así también con el nivel explicativo se podrá conocer los métodos y guías para analizar los efectos que causan los malwares.

Método

Los métodos que son utilizados en la presente investigación son: inductivo y deductivo. El método inductivo utiliza premisas particulares para llegar a una conclusión general, y el deductivo usa principios generales para llegar a una conclusión específica.

Metodología MAGERIT

Según Ribero (2016) esta Metodología está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

A continuación, se muestra las fases de la metodología MAGERIT

Fase 1 Toma de datos.

Fase 2 Identificar los activos.

Fase 3 Seleccionar las amenazas.

Fase 4 Identificar vulnerabilidades.

Fase 5 Evaluar el riesgo.

Fase 6 Desarrollo de la guía de recomendaciones.

Justificación

Los emprendedores de la ciudad de Ambato no cuentan con un proceso de seguridad para reducir ataques de malware en sus dispositivos, siendo esto por muchas ocasiones un problema muy grande en cuanto al correcto funcionamiento de sus dispositivos móviles, poniendo en peligro la integridad de toda la información importante.

Posterior a la realización de pruebas que ayuden a detectar las diferentes vulnerabilidades en los dispositivos móviles, se realizara una guía que ayude a reducir los diferentes ataques a los que pueden ser expuestas los emprendedores, utilizando la menor cantidad de recursos y tiempo para poder solucionar cualquier inconveniente.

Importancia

La importancia de esta investigación se da porque permite incluir una guía que ayude a reducir los malware en los emprendedores tomando en cuenta la seguridad de estas, con la finalidad de evitar ataques que sean perjudiciales para sus dispositivos y estos no se vean afectados, esta investigación es importante, será de gran ayuda para todos los emprendedores, y de esta manera la información no pueda ser interceptada por algún ciberdelincuente

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Sistema operativo *android*

Android, es un sistema operativo que se utiliza en dispositivos móviles de alta gama, por lo general de pantalla táctil entre ellos; tabletas (*tablets*), teléfonos móviles (celulares) y relojes equipados con Android, aunque el software también se usa en automóviles, televisores y otras máquinas.

Los sistemas operativos son creados para la administración de equipos de cómputo, los mismos que están destinados para quipos de trabajo o de servidores. Bajo el aporte de Cabrera (2018) menciona lo siguiente:

> El pionero en el desarrollo de *Android es Andy Rubin* quien trabajó en firmas como *Apple, WebTv y Danger Inc.* En la última desarrolló un sistema operativo para móviles llamado *Dengueros*. Después de dejar esta empresa y lleno de muchas ideas en el 2003 formó un equipo con ingenieros amigos de empresas pasadas, la compañía se denominó *Android Inc*. Rubin se dedicó a buscar compañías inversionistas, exponiendo los beneficios de la plataforma basada en Linux que estaba desarrollando su equipo. (p. 10)

Sin embargo, Google quien adquirió a Android en 2005 con la intención de adentrase en los dispositivos móviles para ser convertida en la plataforma más popular.

En el año 2007 se estableció el *Open HandSet Alliance* con el objetivo de acelerar la innovación en los dispositivos móviles y ofrecer a los consumidores de forma barata y mejor experiencia móvil. El Android *Open Source Project* (AOSP) es el grupo encargado de desarrollar y mantener las compatibilidades de las distintas versiones de Android.

Arquitectura de Android

Se puede esquematizar cuatro niveles expuestos en la siguiente tabla:

Tabla 1 Niveles de arquitectura de Android

Nivel	Descripción
1.- Kernel	• Es una versión del *Kernel de Linux*, modificada para adaptarlo a las capacidades de un dispositivo móvil, es decir para adaptarse a temas que refieren al consumo de energía y capacidad de cómputo. Donde se encuentran todos los controladores del hardware disponible por el fabricante y las interfaces para la capa superior. • La principal característica es un sistema para multi- usuarios que interfieren entre si denominado *SandBox* o "Caja de Arena". • El servicio de middleware que utiliza el sistema conocido como *IPC-Binder (InterProcess Communications),* que es otra de las modificaciones que se le ha agregado al K*ernel* original de *Linux.*
2.- Middleware	• Consistente en un conjunto de librerías escritas en C/C++, una versión optimizada de *Java Virtual Machine* conocida como *Dalvik Virtual Machine DVM*, y una librería central (core libraries) escrita en Java. • Las aplicaciones son entregadas en forma de códigos de *bytes Dalvik, y el DVM* se encarga de ejecutarla. • Son Utilizados por los frameworks de aplicaciones, provee soporte para base de datos, programación 3D. • Se ejecuta como Usuario corriendo sobre el propio *Dalvik Virtual Machine.*
3.- Framework	• Provee diferentes servicios para las aplicaciones. • La capa es controlada a la necesidad de la información. • Facilita la tarea de la programación para las aplicaciones.
4.- Capa de aplicaciones	• Contiene todas las aplicaciones que corren sobre el sistema.

Fuente: Cabrera (2018)

En la actualidad, *Android* se ha convertido en el sistema operativo para dispositivos móviles más potente, creciente y demandado junto a *iOS,* que es el que poseen los dispositivos que pertenecen a la compañía *Apple*. Por tal razón, se hace referencia a los siguientes componentes según Muenas (2018):

Núcleo Linux. - El núcleo del sistema es *Linux* y actúa como una capa de abstracción entre el hardware del dispositivo y las aplicaciones instaladas y depende de otras funciones para el almacenamiento de la memoria.

Runtime. - El sistema operativo de *Google* para dispositivos móviles incluye un conjunto de bibliotecas que proporcionan la mayor parte de las funciones disponibles en las bibliotecas base del lenguaje de programación Java y esta ejecutada a la versión 5.0 en formato dex.

Bibliotecas. - En el sistema operativo Android, se incorporan diversas bibliotecas en C o C++ que desempeñan un papel fundamental en el funcionamiento de varios componentes del sistema. Entre estas destacan System C, bibliotecas de medios, gráficos, 3D y SQLite, las cuales son esenciales para garantizar la eficiencia y el rendimiento de las aplicaciones y servicios en la plataforma**.**

Marco del trabajo de aplicaciones. – Permite tener un acceso a las API, y está diseñada para simplificar la reutilización de componentes.

Aplicaciones. - Sirve para el uso de funciones básicas de un dispositivo como son, correo electrónico, mensajes de texto SMS, calendario, mapas, navegador, contactos y otros.

Carpeta IPC.- El mecanismo *Binder Inter-Process Communication (IPC*) permite que el marco de la aplicación cruce los límites del proceso y llame al código de servicios del sistema Android.

Servicios del sistema. - . La funcionalidad expuesta por las API del marco de aplicación se comunica con los servicios del sistema para acceder al hardware subyacente, incluyendo en los grupos de servicios: sistema (como *Window Manager y Notification Manager*) y medios (servicios relacionados con la reproducción y grabación de medios).

Capa de abstracción de hardware (HAL). - Una HAL define una interfaz. (p. 45)

Versión y actualización

El sistema operativo Android, ha recibido varias actualizaciones en vista que en algunas versiones se han detectado fallos para posteriormente ir añadiendo varias funciones de acuerdo con el soporte en las nuevas tecnologías Según Aveda (2021) identifica las distintas versiones de Android, a través de la asociación con nombres de postres, cuyas iniciales se ordenan alfabéticamente. Así, la primera versión de Android se llamó Apple Pie, la segunda Banana Bread y así sucesivamente. Esto permite reconocer las versiones y determinar cuáles son las más recientes de acuerdo con la letra inicial. (p. 22)

Además, se describe las cinco últimas versiones de Android:

- *Android Nougat:* versión 7.0-7.1.2 y fecha de lanzamiento 15 de junio de 2016.
- *Android Oreo:* versión 8.0-8.1 y fecha de lanzamiento 21 de agosto de 2017.
- *Android Pie: versión* 9.0 y fecha de lanzamiento 6 de agosto de 2018.
- *Android 10: versión* 10.0 y fecha de lanzamiento 3 de septiembre de 2019.
- *Android 11: versión* 11.0 lanzado el 8 de septiembre de 2020.

Sin embargo, la plataforma *Android* se ha convertido en el sistema operativo más propagado según el diseño y fabricación de nuevos smartphones bajo este contexto la empresa estadounidense de investigación y mercados *IDC*, presentó datos en el tercer trimestre del 2019 *Android*, lideró el mercado en un 86,6%.

Para Gonzáles (2018) la naturaleza del código abierto del sistema operativo brinda una facilidad para crear nuevas aplicaciones y la variedad de mercados para aplicaciones no oficiales influenciando así la seguridad. (p. 52).

Aplicaciones

Las aplicaciones se desarrollan habitualmente en el lenguaje *Java con Android Software Development Kit (Android SDK),* pero están disponibles otras herramientas de desarrollo, incluyendo un *Kit* de Desarrollo Nativo para aplicaciones o extensiones en *C o C++, Google App Inventor,* un entorno visual para programadores novatos y varios cruz aplicaciones de la plataforma web móvil

marcos. y también es posible usar las librerías Qt gracias al proyecto *Necessitas SDK.* Entre las cuales Pedrozo (2015) destaca:

> **Google Play.-** Es la tienda en línea de software desarrollado por Google para dispositivos Android. Una aplicación llamada "play store" que se encuentra instalada en la mayoría de los dispositivos Android y permite a los usuarios navegar y descargar aplicaciones publicadas por los desarrolladores. Google retribuye a los desarrolladores el 70% del precio de las aplicaciones. Por otra parte, los usuarios pueden instalar aplicaciones desde otras tiendas virtuales (tales como *Amazon Appstore o SlideME*) o directamente en el dispositivo si se dispone del archivo APK de la aplicación.
>
> **Privacidad. –** Se ha detectado comportamientos en dispositivos que limita la privacidad del usuario, activando la opción “Usar redes inalámbricas” en el menú “Ubicación y seguridad”, avisando que se guardarán estos datos, y borrándose al desactivar esta opción, pues se usan como caché y no como log tal como hace iPhone.
>
> **Seguridad. -** Según un estudio de *Symantec* de 2017, comparado con el iOS, Android es un sistema más vulnerable, debido principalmente a que el proceso de certificación de aplicaciones es menos, riguroso que el de Apple se debe al esquema de gestión y permisos, por tanto, el usuario debe tener en cuenta los riesgos que se expone un dispositivo a los ataques de la ingeniería cibernética. (p.63)

1.2. Virología móvil

La virología móvil tuvo su auge en los años 2004 al 2006, en vista de un mundo más cambiante los ciberdelincuentes han desarrollado variedad de virus para dañar y amenazar dispositivos móviles, archivos y equipos de cómputo. Como lo interpreta *Unucheck* (2015) con la aparición de toda una gama de amenazas para los teléfonos móviles, casi idénticas a las de los ordenadores: *virus, gusanos, troyanos, espías, backdoors* y programas publicitarios. Surge la necesidad de crear programas que generen que protejan este tipo de dispositivos. Entre los cuales se derriba las siguientes características:

- El número de aplicaciones maliciosas no se pueden eliminar por sí mismas.
- El uso activo de ventanas phishing que se ubican encima de las aplicaciones legítimas.
- Se evidencia un número de programas para la extorción o *ransomwarew*
- Su identifica como un super usuario para enseñar publicidad agresiva
- Existe un crecimiento de número de software malicioso o malware para IOS (p. 41)

Por tanto, la virología móvil es un programa nocivo cuya función es la reproducción y descarga de archivos de una red externa para la inhibición ante un sistema de protección que daña y expone en peligro de espionaje los archivos de un dispositivo móvil como de cómputo en base a una forma disfrazada que es efectiva en ciertas aplicaciones.

Base tecnológica

La base tecnológica de los teléfonos inteligentes o smartphone han sufrido un ataque masivo de virus, en base al desconocimiento de los usuarios por acceder a sitios de la web pueden afectar directamente a la información interna del dispositivo. Un hecho importante es que la plataforma Symbian lideraba un montón de programas nocivos, posteriormente fue desplazado por Nokia adentrándose con el 45% de smartphones en el mercado.

Es aquí donde Microsoft ha permitido realizar contribuciones contra la lucha de Malware para su plataforma. Según *Maslennikov* (2015) identifica que:

> Windows Mobile 5, soportaba muchos fabricantes de acuerdo con la versión acertada de las políticas de uso, posteriormente apareció la sexta versión con códigos iniciales del SO, cuya penetración en el mercado mundial de smartphone sería del 15%, siendo una empresa líder la misma que firmó licencias con cuatro fabricantes de teléfonos a excepción de Nokia cuyo volumen de venta superaron los 20 millones de móviles al año. (p. 36)

Apple en 2008, cumplió con el objetivo de vender 10 millones de dispositivo debido al lanzamiento de *iPhone* cuya versión móvil de *Mac OS X,* incluye un diseño propio siendo el teléfono más vendido a nivel mundial. Actualmente esta empresa ha

obtenido ventas más de 21 millones con diferentes modelos para i*Phone* alcanzando un total de ventas 37 millones para 2020.

Familias y modificaciones de cambio

La primera parte de programas maliciosos para telefonía móvil tuvo indicio con el primer catálogo denominado “virología móvil”, desarrolladas en 2006 las mismas que contenía 5 plataformas sujetas al contagio. *Maslennikov* (2015) menciona que con los tre años posteriores se ha añadido tan solo una plataforma al número de plataformas atacadas por los virus móviles.

Es la plataforma *S/EGOLD (SGold, según la clasificación del Kaspersky Lab*), en la que funcionan los teléfonos *Siemens*. (p. 18)

Tabla 2 Plataformas sujetas al contagio

Plataforma	Número de familias	Número de modificaciones
Symbian	62	253
J2ME	31	182
WinCE	5	26
Python	3	45
SGold	3	4
MSIL	2	4

Fuente: M*aslennikov* (2015)

Los creadores del virus han podido resolver los problemas de selección de una plataforma, sin embargo, al haber rechazado la creación de aplicaciones para una plataforma determinada, prestaron atención a *Java 2 Micro Edition.*

Como es el caso de smartphones, soportan Java permitiendo ejecutar aplicaciones Java descargadas directamente desde internet, Sin embargo, los ciberdelincuentes han optado por crear aplicaciones nocivas para Java con el propósito de dañar o robar información siendo la gran amenaza los teléfonos inteligentes los mismos que poseen datos financieros como información de tarjetas de crédito, débito, correos etc.

Según los datos obtenidos sobre la aparición de familias nocivas de virus bajo el criterio de Barrero (2016) a finales de agosto de 2006 había 31 familias y 170 modificaciones. A mediados de agosto de este año hemos detectado 106 familias y 514 modificaciones de objetos detectables para dispositivos móviles. (p.18)

En los últimos tres años han aparecido nuevas tecnologías y métodos en el software nocivo móvil:

- Propagación en los dispositivos intercambiables (tarjetas flash)
- Deterioro de los datos del usuario
- Inhabilitación de los sistemas de protección incorporados en el sistema operativo
- Descarga de otros archivos de Internet
- Llamadas a números de pago
- Polimorfismo

Tecnología y métodos de empleo del virus

Los creadores de virus móviles han decidido seguir creando las últimas tendencias, empezado a usar este método en los programas maliciosos. Un ejemplo de un programa nocivo de este tipo es Worm.WinCE.InfoJack. Este gusano se copia a sí mismo en el disco E. En smartphones equipados con el sistema operativo Windows Mobile esta letra alude a la tarjeta de memoria de un dispositivo móvil de acuerdo con los siguientes pasos. Maslennikov (2015)

1.- El programa nocivo se propaga en el instalador que, además de la copia del gusano, contiene varias aplicaciones y juegos legales.

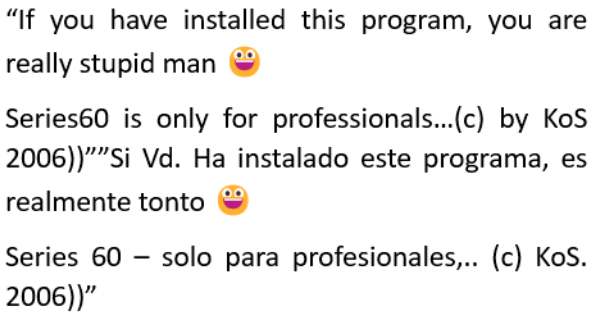
2.- I*nfoJack* deshabilita el análisis de firmas de aplicaciones (un método de seguridad del *SO Windows Mobile).* Lo que decir que si un usuario intenta instalar una aplicación sin firma que puede resultar nociva, el sistema operativo no notificará sobre la ausencia de firma del archivo ejecutable.

3.- Cuando el smartphone se conecta a Internet, el gusano intenta descargar de la red los módulos complementarios para su trabajo. De esta forma, *InfoJack*

> contiene la funcionalidad de descarga. Finalizando con el envío de la información del smartphone de forma nociva. (p. 31)

Se ha tomado como ejemplo *Trojan.SymbOS.Delcon.a.* Es un troyano para smartphones con *SO Symbian de sólo 676 bytes*. Cuya función inicia en el archivo *sis,* el archivo contacts.pdb, donde se almacenan todos los contactos del usuario, se cambia por un archivo con el mismo nombre proveniente del archivo malicioso. En donde aparece el siguiente mensaje.

Figura 1 Mensaje de software malicioso



Fuente: *Maslennikov* (2015)

Antes de la aparición de *not-a-virus:Porn-Dialer.SymbOS.Pornidal.a,* que hace llamadas a números de pago internacionales, los programas de este tipo tan solo eran una realidad informática.

Principales amenazas en virología móvil

Troyanos SMS. - Los Troyanos-SMS son malware líder en el mundo móvil de hoy. Las causas de esta situación se describen en el informe analítico sobre el desarrollo de amenazas en el primer semestre del año.

Herraiz (2012) considera que Rusia, se ha convertido en la capital para la creación de nuevos virus móviles como es el Troyanos-SMS siendo una cadena de producción. El modo más popular de difusión de programas nocivos es a través de los portales *WAP*, donde al usuario se le ofrece la descarga de varias melodías,

imágenes, juegos y aplicaciones para el teléfono móvil. La mayoría absoluta de los troyanos se disfrazan bien como aplicaciones que pueden enviar SMS gratis. (p.64)

Estafas de SMS. - Los programas nocivos móviles no son la única fuente de amenazas, las estafas de SMS son cada vez más populares entre los ciberdelincuentes. Y es que esta amenaza adquirió un carácter internacional hace ya tiempo.

En Rusia los malhechores usan otros esquemas como lo enfatiza Maslennikov (2015):

> **Versión 1:** El malhechor crea un mensaje SMS de semejante contenido: “Hola. Tengo problemas, no puedo contártelo todo. Ingresa el dinero en este número o en el número +79xx-xxx-xx-xx, el dinero te lo devolveré dentro de poco”. Observamos que los mensajes de este tipo no tienen saludos ni firmas, y cada receptor puede creer que le han sido enviados personalmente.
>
> **Versión 2:** En otro esquema se usan los SMS de pago a números cortos. Los textos de los mensajes de estafa pueden ser diferentes. Por ejemplo: “Hola. Manda un SMS con el texto *** al número 3649, ¡recibirás un bono de 150 euros en tu cuenta! Este SMS es gratis, lo he comprobado y me funciona” O: “Hola. Su número ha ganado. Para recibir el premio, mande un SMS con el texto *** al número 1171. El precio del SMS”. (p. 40)

Worm.SymbOS. Beselo.- El modo de funcionamiento del gusano clasificado como Worm.SymbOS. Beselo tiene mucho en común con *ComWar* y es clásico en gusanos de este tipo. La difusión se realiza a través del envío de los archivos SIS infectados mediante MMS y Bluetooth. Una vez iniciado en el dispositivo atacado, el gusano empieza a enviarse a sí mismo a los contactos del libro de direcciones del smartphone, así como a todos los dispositivos accesibles en el área de funcionamiento de Bluetooth.

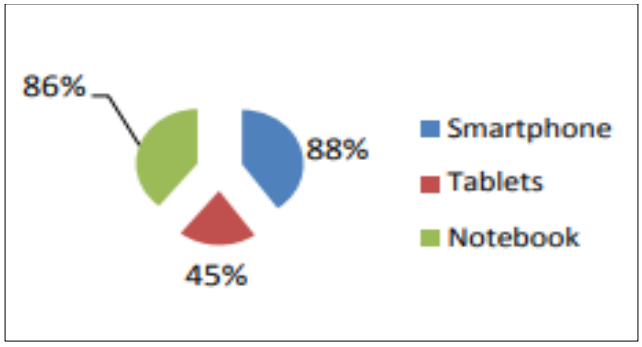
Worm.WinCE.InfoJack.- El blanco principal de los hackers chinos eran los usuarios que jugaban a juegos on-line en las PC. Pero el incidente con InfoJack demostró que en China existe la posibilidad de organizar epidemias masivas y virus móviles.

1.3. Malware para dispositivos móviles

Se denomina Malware a un software malicioso que amenaza dañar el sistema de computadoras, laptops y dispositivos inteligentes y ha sido creado para perjudicar especialmente a teléfonos inteligentes siendo la principal víctima el sistema operativo Android. Para Cabrera (2018) el concepto de Malware viene de las fusiones de las palabras en inglés "*Malicious* + *software*" y cualquier *software* que sin el conocimiento del usuario realiza acciones consideradas poco éticas. (p. 44)

Actualmente, la mayoría de población cuenta con un dispositivo móvil el mismo que necesita de un servidor de internet, para poder realizar las diversas actividades o necesidades de conexión de un usuario. Para Jumbo (2017) realiza un análisis sobre los principales dispositivos de alta demanda correspondientes al 88% de la población utiliza smartphone, en vista que poseen información sobre fotos, contactos, videos, acceso a cuentas bancarias, correos electrónicos y redes sociales. Mientras que el 45% de personas a nivel mundial usa tablets y el 86% notebooks. (p.18) Como se muestra en la siguiente figura:

Figura 2.Acceso a internet



Fuente: Muenas (2018)

Bajo este punto de vista, se debe tener encuenta que un software malicioso o malware aprovecha estas ventajas tecnológicas de sistemas operativos como el Andoit o IOS para Iphone y windows, para ser nocivo, rápido y sutil a través de una forma de engaño a cualquier acceso para un determinado usuario de internet.

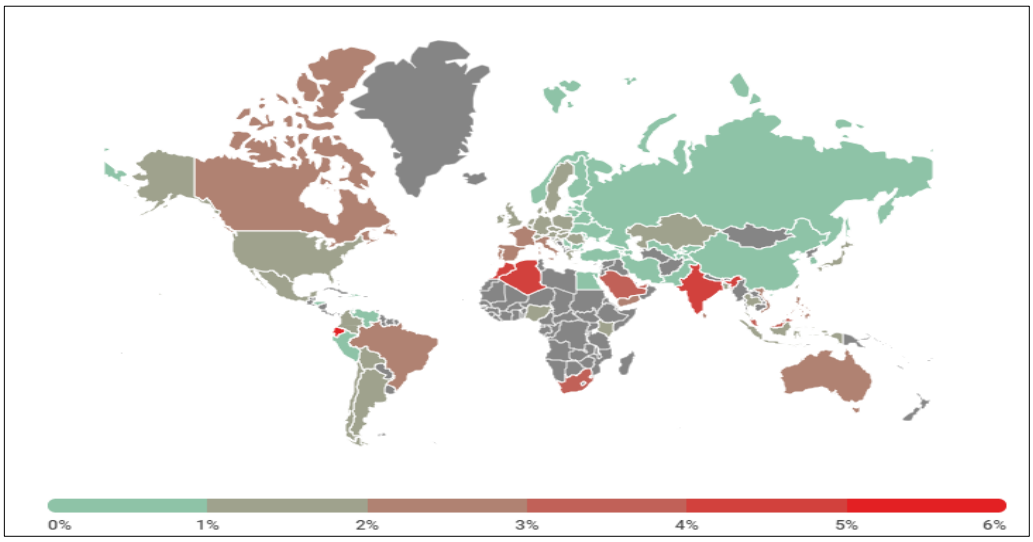
Técnicas de propagación de malware

- Redes sociales involucra la técnica de la ingeniera social para atraer a los usuarios es aquí donde los delincuentes usan este tipo de información para propagarse.
- Correos electrónicos para engañar a los usuarios con el fin de compartir correos basura, direcciones de páginas falsas.
- Sistemas operativos que busca las vulnerabilidades en los sistemas.

Además, *KasperskyLab* detalla los principales tipos de malware que existen entre ellos los *Bonet* que reúne un conjunto de equipos infectados cuya función se centra en realizar operaciones ilegales.

Según *Chebyshev* (2021) menciona que las amenazas *web* contienen los veredictos de detección del módulo del antivirus web proporcionados por los usuarios de los productos de *Kaspersky*, que dieron el consentimiento para el envío de datos estadísticos durante el tercer trimestre del año 2020, se muestra los países con mayor riesgo de infección por medio del uso de recursos web. (p. 45) Como se describe a continuación:

Figura 3. Países en riesgo de infección a través de recursos web, tercer trimestre de 2020



Fuente: *KasperskyLab* (2020)

Sin embargo, el informe presentado *por Kaspersky* en el segundo trimestre del 2020, los residentes de Ecuador correspondiente al (6,33%), Marruecos al (4,51%)

y Argelia con (4,27%) se enfrentaron con mayor frecuencia a varias amenazas web expuesto en la siguiente tabla:

Tabla 3 Los 10 países con mayor riesgo de infección

País	Porcentaje de usuarios atacados
Ecuador	6,33
Marruecos	4,51
Argelia	4,27 Kaspersky
India	4,11
Arabia Saudita	3,78
Singapur	3,69
Kuwait	3,66
Malasia	3,49
Sudáfrica	3,31
Emiratos Árabes Unidos	3,12

Fuente: KasperskyLab (2020)

Clasificación de malware

Virus. - Son códigos que se puede auto- replicar y se redistribuye entre si a diferentes programas informáticos y se instala sin el consentimiento del usuario infectado en archivos existentes. Ribero (2016) este software malicioso que puede llegar a través de archivos adjuntos de correos electrónicos, enlaces maliciosos en internet, compartición de archivos, entre otras formas. (p.20)

Gusanos. - Es un código que puede auto replicar, pero la diferencia es que no afecta los archivos existentes sino en los que se instalan y se ejecutan en la memoria RAM. Según Gonzáles (2019) menciona que infectan un equipo, intenta obtener las direcciones de otros equipos para enviar copias de sí mismo, pudiendo enviar cientos o miles de estas, por lo que su propagación es mucho más rápida y pueden causar daños a grandes escalas. (p.13)

Troyanos. - Son un tipo de malware que se presentan al usuario como software legítimo que al ser ejecutado cumplen funciones destructivas como controlar el dispositivo sin ser advertido. Bustos (2018) Son programas que no se difunden solos, pero generan gran número de infecciones usando herramientas del Internet. (p.25) y se dividen en:

- *Downloader* como descarga y ejecución de códigos maliciosos
- *Banker* cuyo objetivo es el acceso a credenciales de acceso financiero
- *Dropper* se ejecuta en paralelo como un programa legítimo
- *Cliker* que busca beneficio económico por medio de la publicidad
- *Keyllogger* que registra actividades que se realizan en un sistema
- *Backdoor* que abre puertos en el sistema sin autorización
- *Bot* que convierte el programa en zombi

Malware más usual en smartphone

Troyano xHelper. - Herraiz (2012) menciona que son programas que contienen información o código que puede tomar ventaja de vulnerabilidades del software de una aplicación que se está ejecutando en un computador. (p.14)

El propósito de este tipo de troyano es ejecutar, desde fuera, comandos en remoto en el dispositivo y así, instalar aplicaciones no autorizadas.

***Hummingbad*. -** González (2019) menciona que este malware, descubierto en 2016, es uno de los programas maliciosos que más afectan a los usuarios de Android. Su objetivo principal es descargar todas las aplicaciones maliciosas que pueda en ese el dispositivo infectado. Para ello, intenta engañar a la víctima y obtener acceso *root*. (p.35)

Una vez consigue instalar las aplicaciones maliciosas, llena el dispositivo de anuncios difíciles de cerrar y que además pueden instalar otras aplicaciones. Un bucle que resulta complicado de eliminar sin la restauración completa del dispositivo.

Troyanos bancarios o phishing. - González (2019) Los troyanos bancarios en Android se están convirtiendo en el principal ataque para la obtención de información bancaria de los usuarios. Un método que tuvo un considerable crecimiento en 2018. (p.35)

Un troyano o phishing bancarios es un tipo de malware que se hace pasar por una aplicación, página de inicio o software de tu banco para hacerte creer que estás introduciendo tus datos en un sitio oficial y seguro, pero en realidad no es así.

***Trojan-SMS*. -** González (2019) Los programas *Trojan-SMS* envían mensajes de texto desde el teléfono móvil infectado hacia número de tarifa premium, lo cual representa al usuario pérdida de dinero. (p.35)

Una vez ejecutado, *Trojan-SMS.J2ME* intenta mandar un SMS con un texto determinado un número de pago

Herramientas para el análisis de malware

Hoy en día los desarrolladores de malware utilizan técnicas de ofuscación, como paquetes binarios, encriptación o código automodificable por lo cual una gran cantidad de investigación se ha centrado en desarrollar herramientas para el seguimiento y monitoreo de los programas maliciosos.

Según Zapata et, al. (2015) proponen un modelo el análisis dinámico del comportamiento del malware utilizando las técnicas de preparación (en herramientas software y hardware), detección y análisis (detectar, analizar e identificación), confinamiento, erradicación y recuperación (reglas en dispositivos sistemas de detección de intrusos, IDS/IPS sistemas de prevención de intrusiones, firewall entre otros) estos dispositivos ofrecen un alto nivel en la capa de seguridad, diseñados para proteger los activos críticos de las amenazas cibernéticas para destacar las siguientes herramientas de gestión (p.25):

Herramientas de gestión y administración en tiempo real. - Corresponden a monitorización avanzada, ayudan a facilitar la administración, diagnóstico de sistemas y aplicaciones en ejecución. Las características es la solución de problemas del sistema, localización de problemas DLL, y visualización rápida para encontrar procesos, funciones y aplicaciones en la búsqueda de malware.

Herramientas de análisis y gestión de binarios. - Están orientadas a depuradores de código binario, el objetivo fundamental de este tipo de herramientas es proporcionar una solución para organizar fácilmente una colección de malware y explotar las muestras, para facilitar la investigación.

Herramientas para análisis de entornos de red. Son analizadores de protocolos o paquetes de red, de fácil administración en infraestructura TCP/IP, entornos gráficos que ayudan a controlar o iniciar conexiones entrantes y

salientes, estas herramientas son de gran utilidad para la captura del tráfico de red que se genera en el análisis de malware.

Herramientas de análisis de memoria. - Las herramientas de análisis de memoria se utilizan para buscar, remplazar y volcado de memoria de procesos en ejecución, para extraer los archivos DLL inyectados, realizar detección de *rootkits*, encontrar procesos ocultos, entre otros.

Herramientas de *string*. - Las herramientas de análisis de cadenas *string* nos permite analizar *malware* basados en textos o patrones binarios, la mayoría de las herramientas para el análisis de *string* son de código abierto lo cual nos permite modificar el malware.

Herramientas forenses. - Las herramientas para análisis forense suelen ser un conjunto de herramientas de línea de comandos para el análisis que se pueden utilizar para encontrar secuencias de datos alternativos, analiza procesos y extrae información, muestra archivos ocultos por *rootkits*, algunas solo funcionan para sistemas de archivos de tipo Unix, y requiere que la plataforma de análisis sea igual a la del sistema analizado.

Herramientas para virtualización y *sandboxing*. - Esta técnica permite aislar un programa en este caso, malware proporcionando entornos de ejecución confinados, que pueden ser utilizados para ejecutar programas no fiables desde el entorno principal.

Malware para Android

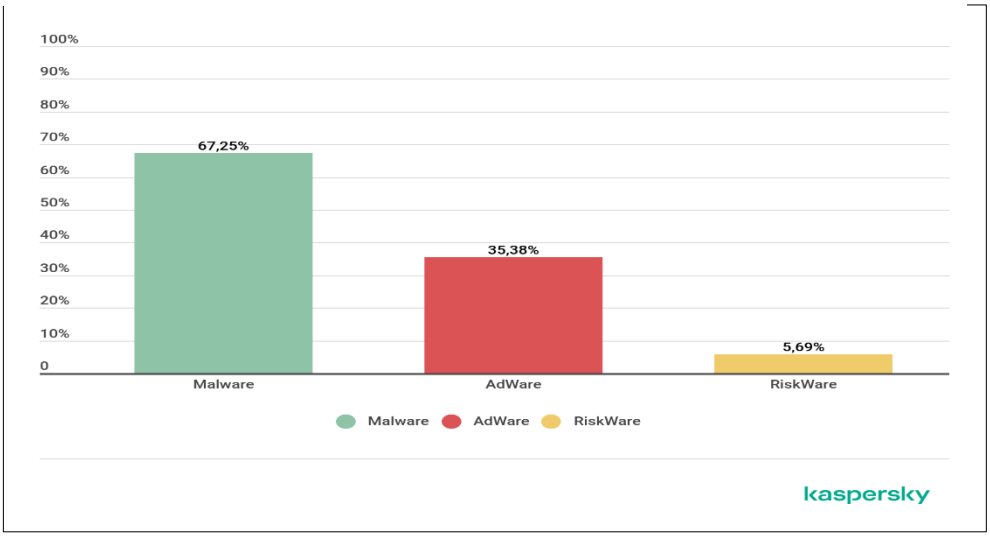
De acuerdo con las políticas de privacidad *Google y Apple* han recurrido a corregir vulnerabilidades de los sistemas operativos o implantar medidas de seguridad en las tiendas oficiales de aplicaciones, Evitando así el software malicioso o malware en dispositivos móviles *IOS y Android.* Sin embargo, el impacto de malware en estos equipos cada vez es más significativo. Según Kaspersky *Security Network*, en el primer trimestre del 2021: Se Detectó un total de 1´ 451. 660 paquetes de instalación maliciosos, de los cuales:

- 25. 314 pertenecían a troyanos bancarios móviles;
- 3.596 resultaron ser troyanos r*ansomware* móviles.

La mayoría (61,43%) de las amenazas detectadas pertenecía a la clase de aplicaciones publicitarias (*Adware).*

Por tanto, Chebyshev (2021) dio a conocer que, durante el primer trimestre de 2021, *Kaspersky* detectó 1´ 451. 660 paquetes de instalación maliciosa, 655 .020 menos en comparación con el trimestre anterior y 298. 998 más que en el primer trimestre de 2020. Además, se puede observar que el software malware ocupa el 67,25% como principal amenaza de un dispositivo y su sistema, mientras que el 35,38% *Adware y 5,69% RisWare*. Como se presenta a continuación (p. 22):

Figura 4. Primer lugar del software malware



Fuente: *KasperskyLab* (2020)

Malware para IOS

De acuerdo con la innovación de la tecnología el sistema iOS, dispuesto para teléfonos inteligentes como IPhone en donde se ha expuesto al software malware para iOS detectado en el año 2015, en comparación hasta el año 2020, se multiplicó por 2,1.

La reciente aparición de aplicaciones malintencionadas en *App Store* una vez más puso de manifiesto y a pesar de la creencia popular, el sistema operativo iOS no es invulnerable al malware. Los atacantes no hackearon *App Store*, sino que publicaron en Internet una versión maliciosa de *Xcode de Apple*, un conjunto de herramientas gratuitas con las que los desarrolladores crean aplicaciones para iOS.

Para Gonzáles (2019) menciona que *Apple* difunde de forma oficial *Xcode*, pero extraoficialmente también lo difunden terceros. Algunos programadores chinos prefieren descargar estas herramientas de desarrollo desde servidores locales. Alguien puso en un servidor web externo en China una versión de *Xcode* que contenía el código malicioso *XcodeGhost*. En cualquier aplicación compilada por este *Xcode*, se integraba código malicioso. (p. 49)

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la institución

Para el desarrollo del estudio se ha seleccionado al grupo de Semilleros Empresariales de la Universidad Técnica de Ambato “Seuta”, que surgió bajo la necesidad de apoyar emprendimientos desde una perspectiva social, económica y tecnológica. Esta idea innovadora parte de la organización de 67 estudiantes pertenecientes a los últimos semestres de la carrera de Marketing y Gestión de Negocios, bajo el propósito de reactivar económicamente a 58 mico empresas siendo partícipes de asesoría con servicios de tele- emprendimiento técnico y desarrollo comercial para los previstos negocios.

Según el Boletín UTA (2021) este espacio ha sido creado para la generación y consultas de emprendimiento para el mejoramiento en los procesos técnicos para el desarrollo productivo de los negocios. Por tanto, promueve el empleo e impulsa la cultura empresarial entre estudiantes y docentes con la finalidad de ofrecer una vinculación hacia la colectividad mediante el servicio y capacitación para fomentar negocios innovadores que generen eficiencia, rentabilidad y sostenibilidad para los micronegocios enfatizando que: “La importancia de fomentar en los jóvenes una cultura empresarial se centra en la capacidad de crear y llevar a cabo proyectos que ayudan a impulsar una sociedad emprendedora e innovadora”. (pág. 3)

Para alcanzar esta meta se ha predispuesto un trabajo conjunto y de convenios dispuestos por el Ministerio de Producción y Comercio del Exterior, Inversiones y Pesca, Corporambato y la Cámara de Emprendimiento e Innovación de Tungurahua.

La Cámara de Emprendimiento e Innovación de Tungurahua “CEIT”, inició las actividades comerciales el 16 de octubre del 2020, dedicada a actividades de organizaciones cuyas necesidades se enfoca en el desarrollo y prosperidad de las empresas que se dedican a la producción o comercio en que incluye el sector agropecuario o de característica del crecimiento económico para una zona específica.

Por tanto, la importancia del apoyo de esta institución para los emprendedores radica en que no hay innovación sin que se ofrezca una asesoría sobre la protección para un sistema informático previsto para estos negocios o sector, siendo un limitante el progreso de los entornos para emprendedores al mismo tiempo el desconocimiento por aplicar procesos técnicos y legales que van a la mano de las competencias de profesionales de área, que pueden trabajar bajo el bienestar y capacitación de estas amenazas para los negociantes, cuya mejora y consolidación es incrementar emprendimientos de esta índole por medio del foro Tungurahua Aprende y Emprende.

De acuerdo con el Honorable Concejo Provincial de Tungurahua “HCPT” (2020) de la ciudad de Ambato menciona que es necesario emprender de manera profesional, porque el emprendedor debe resolver problemas, satisfacer necesidades, no debe enamorarse del producto sino de la necesidad y enfocarse a los 17 objetivos de desarrollo sostenible. En donde el emprendedor debe validar “si no hay innovación no hay emprendimiento”.

Así mismo se incluye contar con un prototipado para ayudar a validar las ideas antes de lanzarlas al mercado a fin de ahorrar tiempo y recursos y evitar errores o al menos no cometerlos, cuya necesidad sea contar con un modelo de negocio importante para la capacitación de manera transversal.

El propósito fundamental de BanEcuador, una entidad bancaria pública, es proporcionar productos y servicios financieros inclusivos que tengan un impacto positivo en la productividad y la calidad de vida de sus clientes. A través de su enfoque en la inclusión financiera, la institución ofrece información detallada sobre diversas opciones de financiamiento para emprendimientos. Esto incluye créditos productivos para microempresas con montos que oscilan entre 50 y 150,000 dólares, créditos productivos para PYME que varían desde 5,000 hasta 3 millones de dólares, créditos de consumo que van desde 50 hasta 10,000 dólares, junto con los respectivos requisitos, modalidades de pago y demás detalles pertinentes.

2.2. Metodología de la investigación

Tipo de investigación: Dentro de la investigación, se utilizan diferentes tipos de enfoques de estudio, que son:

Investigación exploratoria: El tipo de investigación es exploratoria, en vista que permite realizar un estudio sobre la detección de un software maliciosos que afecta directamente en las aplicaciones de los dispositivos móviles como Android, por tanto, este tipo de indagación abraca información real que es puesta en práctica como un problema de contenido tecnológico y social.

Investigación descriptiva: Permite recopilar la información en base de fuentes de información primaria como secundaria, las mismas que ayudan a realizar un análisis y síntesis de las diferentes características que se suscitan en el momento del fenómeno de estudio.

Métodos de investigación: Para la presente investigación se utilizará el método Inductivo, según Ever (2018) Es una forma de razonar partiendo de una serie de observaciones particulares que permiten la producción de leyes y conclusiones generales. Se basa en la observación de hechos, fenómenos y tiene el objetivo de generar nuevo conocimiento, es decir que empieza de conocimientos básicos de un tema en particular y hechos específicos que fueron parte de una investigación.

Método deductivo, permite analizar e indagar las diferentes causas y efectos que intervienen en el problema según Figueroa (2018) permite presentar conceptos, reglas, principios definiciones a partir de las cuales se analiza, se sintetiza compara, generaliza y demuestra.

Modalidad de investigación: La presente es una investigación de campo, según Arias (2020) recopila los datos directamente de la realidad y permite la obtención de información directa en relación con un problema, tomando en cuenta que para la investigación del problema planteado se recurre al lugar de los hechos.

Otra modalidad de investigación es la una revisión bibliográfica la cual permite recopilar información ordenada y documentada de revistas científicas, artículos científicos e internet, y así poder sustentar de manera teórica la investigación del presente proyecto.

Cualitativo. Tiene por objeto de estudio el comportamiento en su ámbito natural, y se propone desvelar el significado del comportamiento más que su cuantificación.

Instrumentación: Para la presente investigación para la recolección de datos se utilizará el instrumento y técnica de la encuesta, la cual contendrá preguntas que se enfocan al tema de estudio.

Población y muestra

La población total por considerar en la realización del presente estudio contempla a 67 emprendedores que conforman el grupo de Semillero Empresarial de la Universidad Técnica de Ambato de la ciudad de Ambato. Al contar con una población reducida, no se procede a calcular la muestra, por lo que se trabajara con la población total.

2.3. Metodología de desarrollo

Se ha tomado como referencia la metodología *Magerit V3. 0*, cuyo sustento permite la implementación para el "Proceso de Riesgos y de Gestión" que una empresa u organización debe llevar para un marco de trabajo de acuerdo, a las decisiones tomadas para el control y verificación sobre el uso de las tecnologías de la información en beneficio del emprendimiento.

En el trabajo realizado por Morales (2017) cita a *Santiso, Kloter y Bisarro* para ser énfasis en la propuesta de estudio de seguridad para entornos virtuales para describir la importancia del uso de esta herramienta informática con la finalidad de detectar incidentes comunes en ciberseguridad para aplicaciones web por tanto: "Este proceso permite plantear medidas de corrección para las bases de controles sugeridos en Norma *ISO 27032* para la protección de los sistemas en relación a la seguridad, disponibilidad y confiabilidad de la información". (p. 11)

Según Rodríguez (2016) considera que *Magerit V3.0* permite detectar a tiempo los incidentes más comunes que puedan presentarse a través de software malicioso, tanto para un dispositivo móvil como para un equipo de cómputo por medio de esta metodología permite: "Seguir un proceso partido en fases con la finalidad de llegar a la elaboración o identificación de los riesgos informáticos para una empresa". (p. 1)

Bajo este mismo aporte de Rodríguez (2016) la aplicación de *Magerit V3. 0* se sustenta en el estudio del "Concejo de Administración Electrónica de España" cuya

metodología parte de un proceso sistémico que identifica los riesgos para ser evaluados en el uso de las tecnologías de la información, permitiendo definir medidas de mitigación para prevención de aplicaciones dañinas o maliciosas. La norma más utilizada en esta organización de ciberseguridad es la a I*SO27032*, siendo la principal característica garantizar el marco de seguridad para incidentes y coordinación para evitar sistemas informáticos libre de virus.

Sin embargo, los procedimientos y estrategias que se han tomado en cuenta para el desarrollo de la investigación metodológica, parte de la identificación de un sistema seguro y oportuno que garantice el bienestar informático para los usuarios o emprendedores. López (2019) Este fin permite a consideración la Gestión y buenas prácticas de seguridad considerando: “El equipamiento de red, *software*, Interconexión de redes, personas, servicios de internet. En donde la norma *ISO27032* abarca los siguientes controles: Aplicaciones (Validación, Autenticación), Servidores (guías de instalación, monitoreo), usuario final (Antivirus, seguridad *web, firewall*)”. (p. 11)

Magerit V3.0, es una de las metodologías más utilizadas para el control y seguridad informática de para las empresas en donde los usuarios generan confianza por este servicio informático que se ofrece. Por tanto, en la investigación se divide en las siguientes fases de acuerdo con la siguiente figura 5 para el posterior análisis e interpretación de datos.

Figura 5. Fases de la metodología Magerit V3.0

Elaborado por: El investigador

Fase 1. Toma de los datos

Para el desarrollo de la investigación, al respecto de la fase 1 se enfoca a la creación de la encuesta prevista en el anexo 1, la cual cumple con los parámetros establecidos por la metodología *Magerit V3.0* para evitar posibles daños y problemas en un sistema operativo cuya validez de la información se obtendrá en la aplicación de la población objeto de estudio. Cuyo propósito es analizar los principales riesgos y vulnerabilidades que pueden afectar al sistema informático de cada emprendimiento.

Además, se puede realizar el análisis completo en vista de validación del nivel de confiabilidad mediante la técnica e instrumento de la investigación. Para la recopilación de la información mediante los datos obtenidos por los requerimientos del grupo de Semilleros UTA, se aplicará como técnica la encuesta bajo el criterio de López y Fachelli (2015) servirá como: “Instrumento de apoyo para recopilar la información de manera versátil y fidedigna para el posterior análisis e interpretación”. (p. 16) También se aplicará un instrumento correspondiente a un cuestionario estructurado el mismo que abarca un banco de 10 preguntas previsto en el anexo 1. Para Meneses (2017) considera al “Cuestionario como un instrumento estandarizado que se emplea para recoger datos de campo, de investigaciones cuantitativas con el propósito de agregar respuestas precisas”. (p. 9)

Fase 2. Identificación de activos

Esta fase sirve para identificar los activos que poseen los emprendedores en base a las actividades diarias que realicen teniendo al *hardware* como factor externo y factor interno el uso de *software*. Además, se ha identificado los siguientes aspectos para el constructo en la metodología *Magerit*:

1.- Activos Físicos

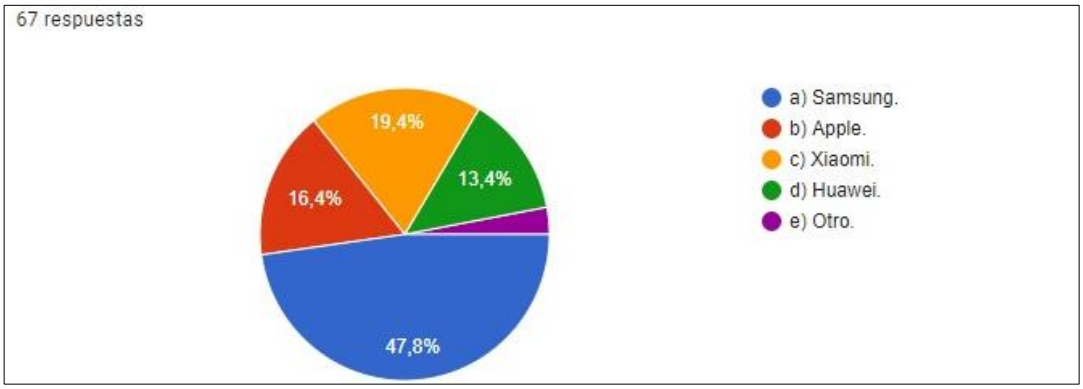
2.- Activos Lógicos

3.- Activos Intangibles

Por tanto, se ha identificado las siguientes preguntas 1,2,3,4 para destacar las respuestas por la aceptación por parte de los usuarios o emprendedores:

1.- ¿Qué marca de dispositivo móvil utiliza?

Figura 6 Marca del dispositivo móvil

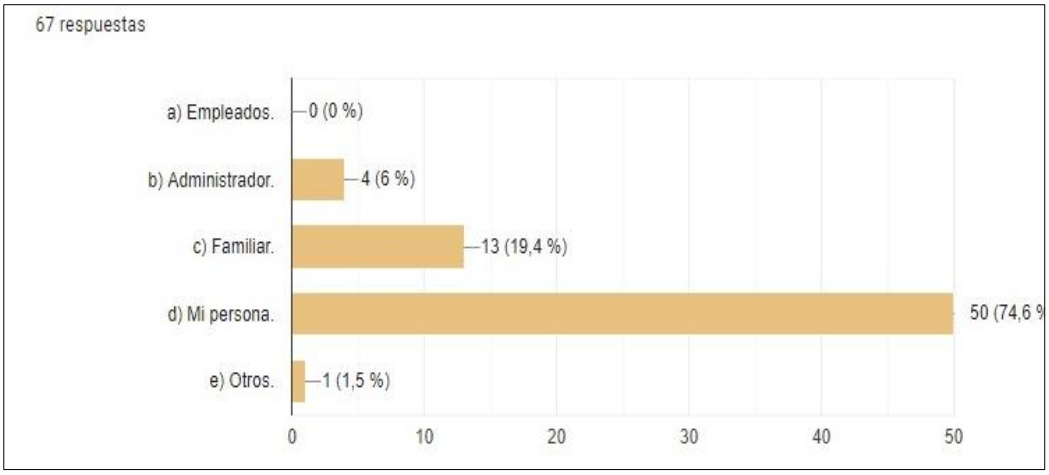


Fuente: El investigador

Análisis e interpretación: De los 67 emprendedores encuestados cuyas respuestas fueron propositivas el 47,8% opina que usan un dispositivo móvil de marca *Samsung* entre tanto el 16,4% usa *Apple,* el 19,4% *Xiaomi* en minoría el 13,4% tienen *Huawei* y el 0% otros. Es decir, los emprendedores han adquirido dispositivos móviles cuyas características técnicas e informáticas corresponden a sistema operativos como: *Android (Samsung, Huawei, Xiaomi) IOS (Apple).*

2.- ¿Quién es responsable de instalar sus aplicaciones y dar mantenimiento a su dispositivo móvil?

Figura 7 Personal de instalación de aplicaciones

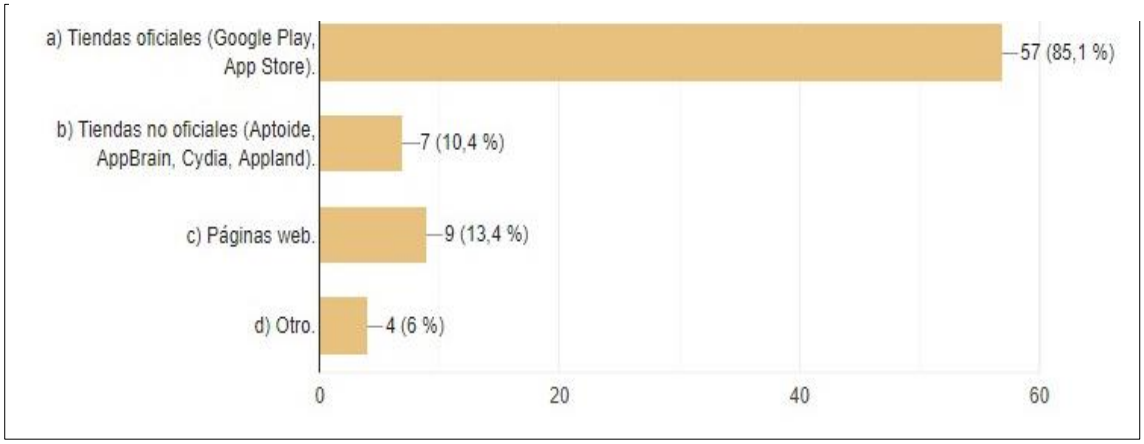


Fuente: El investigador

Análisis e interpretación: De las 67 personas encuestadas el 6% manifiesta que los encargados de instalar aplicaciones y dar mantenimiento a los dispositivos móviles corresponde al administrador, mientras que el 19,4% menciona que lo realiza un familiar y en mayoría el 74,6% afirma que los mismos emprendedores o propietarios los realizan y el 15% otras personas. Lo que quiere decir que para este tipo de acciones se realiza un trabajo empírico cuyo desconocimiento es que un virus malicioso genere daños en los dispositivos.

3.- ¿Cómo descarga sus aplicaciones?

Figura 8 Descarga de aplicaciones



Fuente: El investigador

Análisis e interpretación: Del grupo de los 67 emprendedores consideran que el 85,1% descargan las aplicaciones en base a las tiendas oficiales de *Google Play y App Store,* el 10,4% de tiendas no oficiales como *Aptoide, AppBrain, Cydia, Appland,* y el 6% de otras tiendas.

La información obtenida a través de la pregunta 1,2,3,4 cuyos resultados son que los emprendedores, utilizan dispositivos móviles en base a sistemas operativos *Android* y *IOS*, los mismos que ofertar los productos al cual su emprendimiento se dedica, actuando como factores recurrentes para el uso de aplicaciones digitales y de descarga en la tienda de aplicaciones como: *Play store* y *App Store*.

De acuerdo con la problemática de estudio, la identificación de los activos para los emprendedores se puede destacar la clasificación según los valores que se han obtenido mediante la encuesta y se describen en la siguiente tabla resumen.

Activos Físicos: Representan los activos de tipo hardware que son utilizados por los emprendedores para el uso entre ellos se destaca: dispositivos móviles, computadores, servidores portátiles, etc.

Activos Lógicos: Corresponde al *software* y elementos que se utilizan en los sistemas operativos, aplicaciones propias, paquetes cerrados de mercado, etc.

Activos intangibles. - Corresponden a aquellas acciones que están fuera de la empresa, pero son importantes para la sostenibilidad en el mercado es decir el posicionamiento de la marca, credibilidad innovación o el conocimiento.

Tabla 4 Clasificación de los activos para los emprendedores

Grupo de Activos	Tipo de Activos
Activos Físicos	Dispositivos móviles
Activos Lógicos	Aplicaciones móviles
	Sistemas operativos
	Tienda de aplicaciones
Activos Intangibles	Whatsapp corporativo (Marca)
	Logo empresarial
	Solgan empresarial

Fuente: El investigador

Fase 3. Seleccionar las amenazas

De acuerdo con Rodríguez (2016) la metodología *Magerit* sirve en esta fase 3 para el análisis de las amenazas que afectan directamente a los dispositivos o computadoras y se clasifican en tres grupos entre los cuales un emprendedor debe tener en cuenta al momento de instalar alguna aplicación, descargas, anuncios en sitios o páginas web, o mensajes.

1.- Accidentes

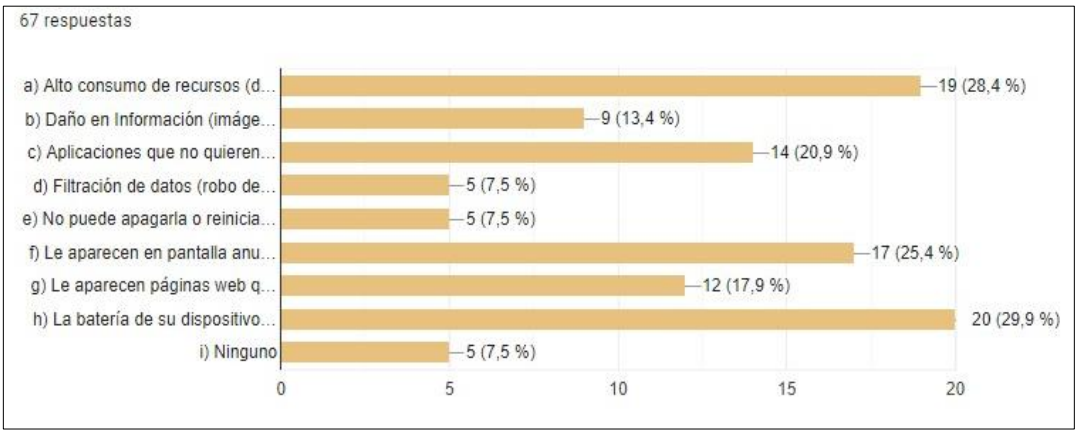
2.- Errores

3.- Amenazas intencionales remotas

Por tanto, se ha seleccionado para la fase de amenazas a las preguntas 7,8,9 en donde se ha obtenido la siguiente información:

6.- ¿Seleccione los problemas que usted ha tenido en su dispositivo móvil?

Figura 9 Problemas en los dispositivos móviles

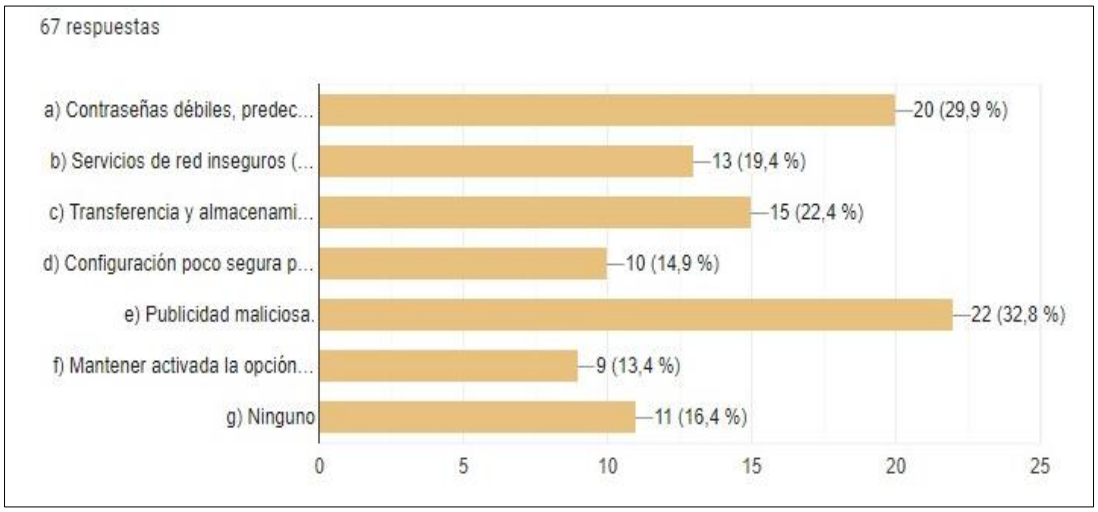


Fuente: El investigador

Análisis e interpretación: Del 100 % de las personas encuestadas correspondientes a los 67 emprendedores mencionan que han observado tener problemas en los dispositivos móviles siendo el 28.4% se refiere al alto consumo de recursos (dispositivo lento), el 13,4% daño en Información (imágenes dañadas, aplicaciones, archivos), entre tanto el 20,9% piensa que las aplicaciones que no quieren desinstalarse, el 7,5% existe filtración de datos (robo de credenciales, contraseñas, cuentas bancarias) y no puede apagarla o reiniciar su dispositivo, mientras que 25,4% le aparecen en pantalla anuncios inapropiados o anuncios que interfieren con el contenido de la página, 17,9% le aparecen páginas web que usted no tenía intención de visitar, o envía mensajes de correo electrónico que usted no escribió finalmente el 29,9% la batería de su dispositivo se agota más rápido de lo normal y el 7,5% considera que ninguna de estas alternativas.

9.- ¿Qué problemas relacionados a temas de seguridad ha experimentado?

Figura 10 Problemas relacionados a la seguridad

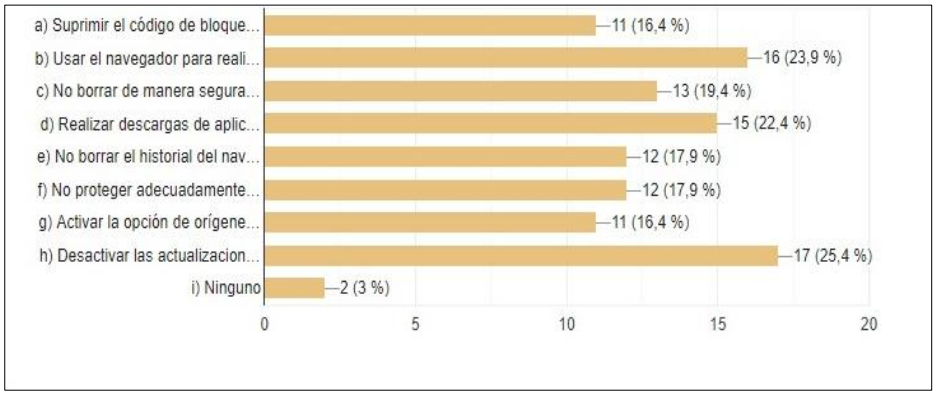


Fuente: El investigador

Análisis e interpretación: Los resultados obtenidos de los 67 emprendedores que conforman el grupo de Semilleros UTA, mencionan que 29,9% han obtenido problemas relacionados a la seguridad de contraseñas débiles, predecibles (contraseñas sencillas y comunes) el 19,4% correspondientes a servicios de red inseguros (wifi gratis). Mientras que el 22.4% han realizado por transferencia y almacenamiento de datos de manera poco seguro (envió por bluetooth, wifi directo), entre tanto, el 19,4% menciona la configuración que es poco segura por defecto, el 32, 8% menciona a la publicidad maliciosa, finalmente el 13. 5% considera que mantener activada la opción de conexión automática a redes inalámbricas, bluetooth, ubicación. Y el 16,4% ninguna.

8.- ¿Cuál de las siguientes acciones las ha realizado en algún momento?

Figura 11 Accionares



Fuente: El investigador

Análisis e interpretación: Los datos obtenidos de los 67 emprendedores encuestados se manifiesta que el 16,4% considera que han realizad acciones en base a suprimir el código de bloqueo del móvil, el 23,9% usar el navegador para realizar actividades que pueden ser realizadas a través de apps, el 19,14% no borrar de manera segura los datos del dispositivo cuando dejamos de usarlo, el 22,4% realizar descargas de aplicaciones que no procedan de un sitio confiable entre tanto el 7,5% no borrar el historial del navegador regularmente y no proteger adecuadamente datos sensibles guardados en el dispositivo, el 16,4% activar la opción de orígenes desconocidos y el 25,4% 3esactivar las actualizaciones automáticas de aplicaciones y sistema operativo, finalmente el 3% aleja esta posibilidad.

Por tanto, el análisis de las peguntas para esta fase 3 sobre las amenazas se obtienen los hallazgos que las principales causas para que exista un daño o perjudique el sistema operativo de un dispositivo se ve a los comunes errores en que los usuarios o propietarios acceden a portales web como páginas, que no son seguras y que propiamente el dispositivo no tiene un sistema antivirus para detectarlo.

Para ser descritos en la siguiente tabla resumen en donde se clasifica por cada pregunta aplicada de la encuesta a los emprendedores este tipo de amenazas que se haya presentado en las actividades diarias.

Accidentes: Se trata de situaciones provocadas involuntariamente y que la mayoría de las veces no pueden evitarse, pueden provocarse, por ejemplo, por efectos naturales.

Errores: Se trata de situaciones cometidas de manera involuntaria por el propio desarrollo de las actividades diarias.

Amenazas intencionales remotas: Se trata de situaciones provocadas voluntariamente por personas ajenas a la empresa. (p. 5)

Tabla 5 Clasificación de las amenazas para los emprendedores

Grupo	Tipo
Accidentes	Transferencia y almacenamiento de datos de manera poco seguro Activar la opción de orígenes desconocidos Contraseñas débiles, predecibles No borrar de manera segura los datos del dispositivo cuando dejamos de usarlo Realizar descargas de aplicaciones que no procedan de un sitio confiable
Errores	Suprimir el código de bloqueo del móvil Aplicaciones que no quieren desinstalarse Usar el navegador para realizar actividades que pueden ser realizadas a través de apps. No borrar el historial del navegador regularmente Activar la opción de orígenes desconocidos
Amenazas intencionales remotas	Aparición de publicidad engañosa en la pantalla del dispositivo Filtración de datos Mantener activada la opción de conexión automática a redes inalámbricas, bluetooth, ubicación. Realizar descargas de aplicaciones que no procedan de un sitio confiable

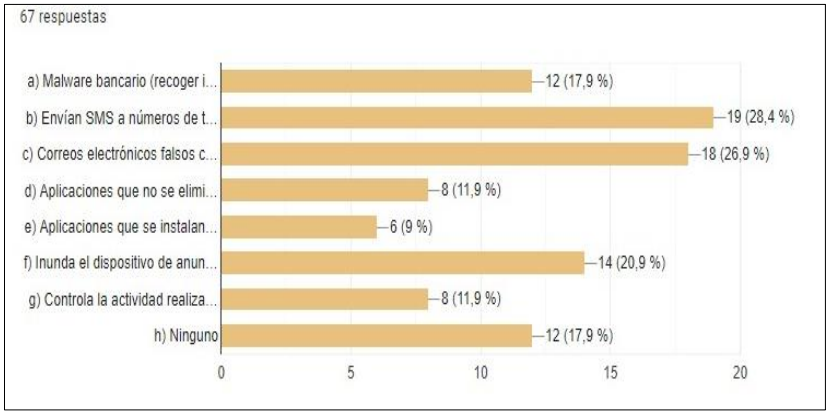
Fuente: El investigador

Fase 4. Establecimiento de las vulnerabilidades

En esta fase se van a identificar los puntos débiles que pueden afectar directamente a los dispositivos de los emprendedores, cuando exista riesgo de publicidad maliciosa, el uso de aplicación para descargar archivos y pueden afectar la memoria y batería de los teléfonos, mensajes o correos electrónicos. Por tanto, se ha seleccionado la pregunta 10 para establecer las posibles vulnerabilidades:

9.- De la lista siguiente seleccione alguna situación que le ha afectado

Figura 12 Afectaciones en los dispositivos móviles



Fuente: Semilleros Uta (2021)

Análisis e interpretación: De las 67 personas encuestadas el 17,9% opina que se ha visto afectado su dispositivo móvil en base de un *malware* bancario (recoger información sobre contraseñas bancarias e inicios de sesión), mientras que 28,4% afirman que envían SMS a números de tarificación especial incrementando las facturas de los usuarios (Troyano-SMS), el 26,9% identifican que han recibido correos electrónicos falsos con avisos importantes de los bancos, aplicaciones falsas de bancos (Troyanos bancarios o *phishing*). El 11,9% han descargado aplicaciones que no se eliminan fácilmente (Troyano *xHelper*) entre tanto, el 9% aplicaciones que se instalan automáticamente (*Hummingbad*) el 20,9% consideran que estos programas dañinos inundan el dispositivo de anuncios publicitarios (*Hiddad*) y el 11,9% piensan que se controla la actividad realizada por el dispositivo, localiza la ubicación y roba importante información (*Spyware* móvil), finalmente el 17,9% ninguno.

Tabla 6 Vulnerabilidades

Grupo	Tipo
Malware Android	Malware bancario Troyanos bancarios Troyano xHelper Hummingbad Hiddad Suprime el código de bloqueo

Fuente: El investigador

Fase 5. Evaluar los riesgos

Para esta fase en el desarrollo de investigación se pretende, mitigar las medidas correctivas que generan este tipo de software malicioso en el sistema operativo de los dispositivos móviles del grupo de personas tomadas como población de estudio, para ello se ha tenido que implementar los siguientes riesgos con los siguientes elementos:

1.- Intervalo de activos

2.- Vulnerabilidades asociadas a cada activo

3.- Conjunto de medidas implementadas

Con estos elementos se requiere identificar las probabilidades de amenaza con el objetivo de mitigar el riesgo de aquellos factores maliciosos para los dispositivos móviles, por tanto, se ha tomado los siguientes criterios de cualitativos como cuantitativos:

Tabla 7 Cálculo de la probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año
Medio	2	La amenaza se materializa a lo sumo una vez cada mes
Alta	3	La amenaza se materializa a lo sumo una vez cada semana

Fuente: El investigador

TABLA 8 Cálculo de impacto

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Fuente: El investigador

Cálculo del riesgo

Para el cálculo del riesgo se ha optado por realizar un análisis cualitativo, haremos uso de una matriz de riesgo como la que se muestra a continuación:

Tabla 9 Probabilidad e impacto

	Impacto		
Probabilidad	**Bajo**	**Medio**	**Alto**
Bajo	Medio	Alto	Muy alto
Medio	Bajo	Medio	Alto
Alto	Bajo	Muy bajo	Medio

Fuente: El investigador

Tabla 10 Análisis

	Cálculo de la probabilidad			Cálculo del impacto			Resultado
Riesgo	**Bajo**	**Medio**	**Alto**	**Bajo**	**Medio**	**Alto**	
Recogen información sobre contraseñas bancarias e inicios de sesión.(Malware bancario)			x			x	Muy alto
Envían SMS a números de tarificación especial incrementando las facturas de los usuarios (Troyano-SMS).			x			x	Muy alto
Correos electrónicos falsos con avisos importantes de los bancos, aplicaciones falsas de bancos (Troyanos bancarios o phishing).			x			x	Muy alto
Aplicaciones que no se eliminan fácilmente (Troyano xHelper).		x				x	Alto
Aplicaciones que se instalan automáticamente (Hummingbad).		x			x		Medio
Inunda el dispositivo de anuncios publicitarios (Hiddad).			x			x	Muy alto
Controla la actividad realizada por el dispositivo, localiza la ubicación y roba importante información (Spyware móvil).	x			x			Muy bajo

Fuente: El investigador

Por tanto, para evaluar el riesgo se ha procedido hacer énfasis bajo los mismo datos de la pregunta 10 de la encuesta la misma que permitió llevar a cabo el análisis de

riesgo en base a las amenazas ya identificadas, para ser interpretadas en las vulnerabilidades con el propósito de evaluar los riesgos siendo el malware bancario (Mensajes bancarios o correos electrónicos, publicidad maliciosa) que se materializa una vez por semana siendo una realidad en el uso de los dispositivos móviles de los emprendedores cuya probabilidad de riesgo es alta.

Fase 6. Guía de recomendaciones

Al ser la última fase, que permite el constructor de una guía de recomendaciones en base a los criterios establecidos y necesidades del grupo de Semilleros Emprendedores de la Universidad Técnica de Ambato. Se identificaron todos estos procesos para ser evidenciado en el anexo 2.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Para el desarrollo de este apartado, se describe la importancia sobre la validación de los resultados debido a los principales criterios y opiniones del grupo de emprendedores, en donde se obtuvo resultados reales y fidedignos sobre el uso de aplicaciones móviles para el uso y manejo del sistema *Android,* cuyos principales hallazgos se evidenciaron de acuerdo con las aplicaciones que son descargadas para el manejo en cada dispositivo móvil de los encuestados.

Teniendo en cuenta que las personas en mayoría desconocen ciertas páginas de contenido de virus entre ellos los troyanos que son los que más predominancia tienen, en vista que suelen aparecer entre publicidad de juegos, anuncios de páginas, mensajes multimedia, bancarios y en correos electrónicos etc. Por tanto, el estudio permite relacionar los posibles ataques que se den mediante un *malware* que debido a la fata de educación informática para los emprendedores pueden desencadenar daños y perjuicios para las actividades de emprendimiento que realizan porque en instancia necesitan de equipos o denominados activos fijos que en la investigación se ha catalogado como; computadoras, laptops, dispositivos móviles.

Entre los dispositivos móviles que poseen los encuestados, se menciona que la mayor parte de descargas se lo realiza en la *play store* porque al ser un sistema *Android,* tiene el riesgo de que la memoria interna se perjudicada por este tipo de software malicioso afectando así el almacenamiento, memoria, y funcionalidad de los mismos. Por tanto, se tiene como evidencia que los emprendedores han adquirido celulares entre ellos Huawei, Xiaomi, Samsung.

En este apartado, demuestra el proceso de gestión mediante el estudio comparativo de las variables, dentro del marco de la metodología Margeit, la misma que ayuda a ordenar, clasificar, calificar y cuantificar la información para que sea factible la aplicación de una guía de recomendaciones. Entendiendo que este instrumento ayudará a los emprendedores a tener un conocimiento y formación empresarial de lo que se debe y no se debe realizar para evitar ataques de un malware, sobre el

uso de los dispositivos y equipos de cómputo debido a la importancia que tiene crear un programa informático o antivirus aplicable en cada equipo.

Bajo este aspecto la guía de recomendaciones describe ciertos aspectos al considerar la aparición de virus desde un contexto macro y entre cual fueron los primeros ataques hacia la plataforma Google, es por eso por lo que los emprendedores deben están en constante capacitación y vanguardia sobre estos temas, que en mayor de los casos roban información personal, cuentas bancarias e inactividad financiera traduciéndose como asaltos cibernéticos.

3.1. Proceso de validación

Para el proceso de validación se ha realizo la aplicación de una segunda encuesta cuyo instrumento se aplicó un cuestionario de 6 preguntas cerradas la misma que tuvo una vigencia de 30 días, y estuvo dirigía a 54 personas cuyo objetivo fue recopilar la información relacionada a la adecuada aplicación y uso de los dispositivos frente a los daños operativos para Android que pueden tener en vista de un software malicioso, proporcionado en una guía de recomendaciones.

En base a esta problemática estudiada se ha propuesto para los modelos de gestión y emprendimiento una guía de recomendaciones para detectar a tiempo posibles robos o daños a los dispositivos mediante los virus informáticos. En un entorno empresarial globalizado y competitivo como el existente en la actualidad, las empresas o emprendimientos dependen cada vez más de sus sistemas de información y de la información que estos administran, pues se ha demostrado que tienen una enorme influencia en la toma de dediciones estratégicas para aumentar el nivel de competitividad y protección de tipos de software maliciosos.

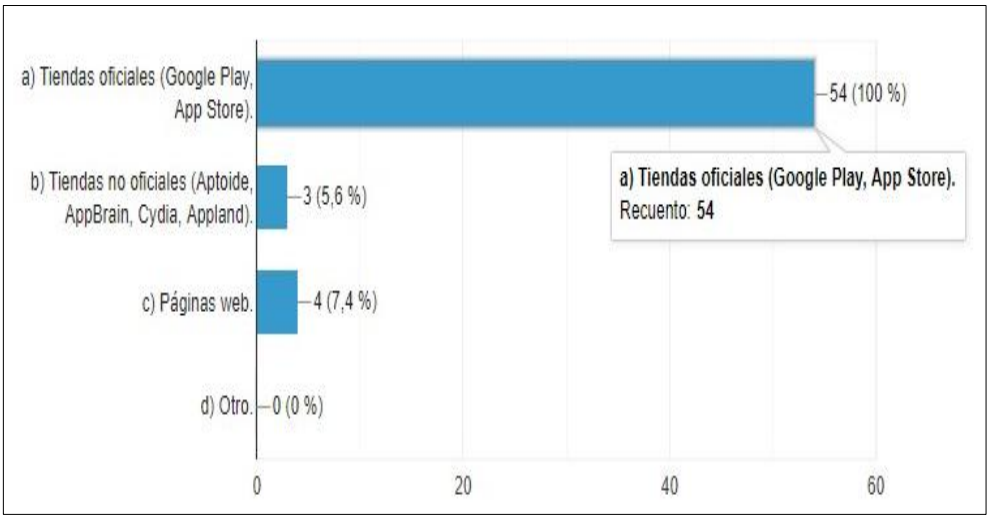
Por tanto, la importancia de la aplicación de la guía ha sido recibida de forma propositiva para los emprendedores, porque a través de este instrumento se puede tener en cuenta de posibles ataques informáticos mediante, anuncios, sitios web que no son seguros, SMS, correos electrónicos. La idea principal de la guía se centra en que las personas conozcan en sentido general lo que es un virus y el grado de afectación que puede desencadenar para ello, se explica lo siguiente:

Los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

Resumen de los resultados

1. **¿Cómo descarga sus aplicaciones después de utilizar la guía de recomendaciones?**

Figura 13 Descarga de aplicaciones a través del uso de la guía

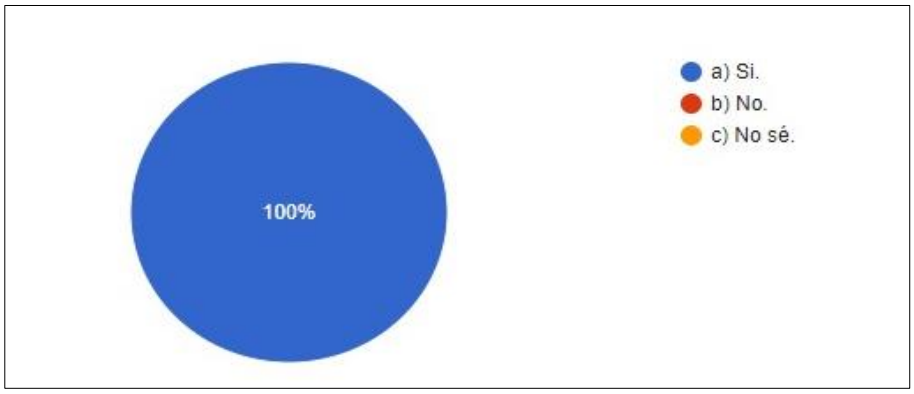


Fuente: El investigador

De acuerdo con los criterios obtenidos, se considera en totalidad que la mayor parte de las personas encuestadas usan tiendas oficiales entre ellas; *Google Play, App Store,* cuyo aporte es propositivo debido a que las personas pueden realizar distintas actividades relacionadas a la búsqueda de información, en vista que la guía de recomendaciones pone a disposición una serie de acciones para el correcto uso y manejo de apps móviles en el sistema operativo *Android*.

2. ¿Considera que es importante tener instalado un antivirus en su dispositivo?

Figura 14 Instalación de antivirus

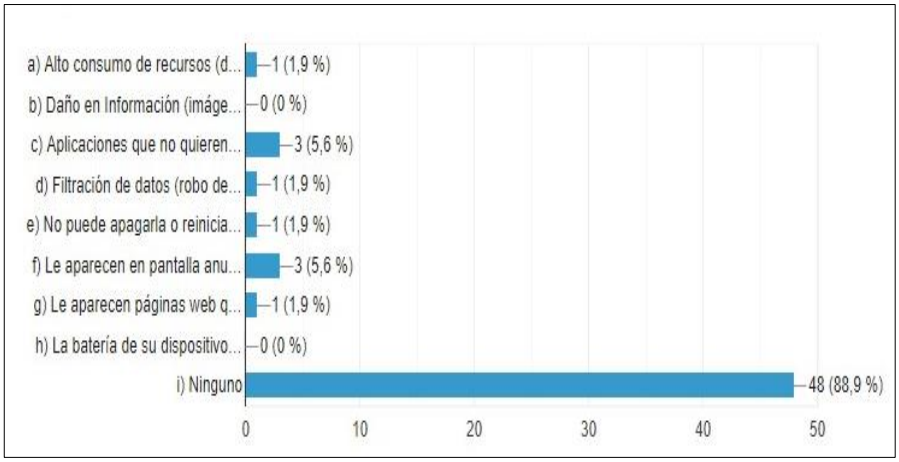


Fuente: El investigador

De las 54 personas encuestadas, consideran en totalidad que si es importante insatalar un antivirus correspondiente al 100% de los datos obnetidos, en vista que esta herramienta ayuda a prevenir ciertos ataques informáticos en las aplicaciones para *Android*.

3. ¿Seleccione los problemas que usted ha tenido en su dispositivo móvil después de utilizar la guía de recomendaciones?

Figura 15 Problemas en los dispositivos



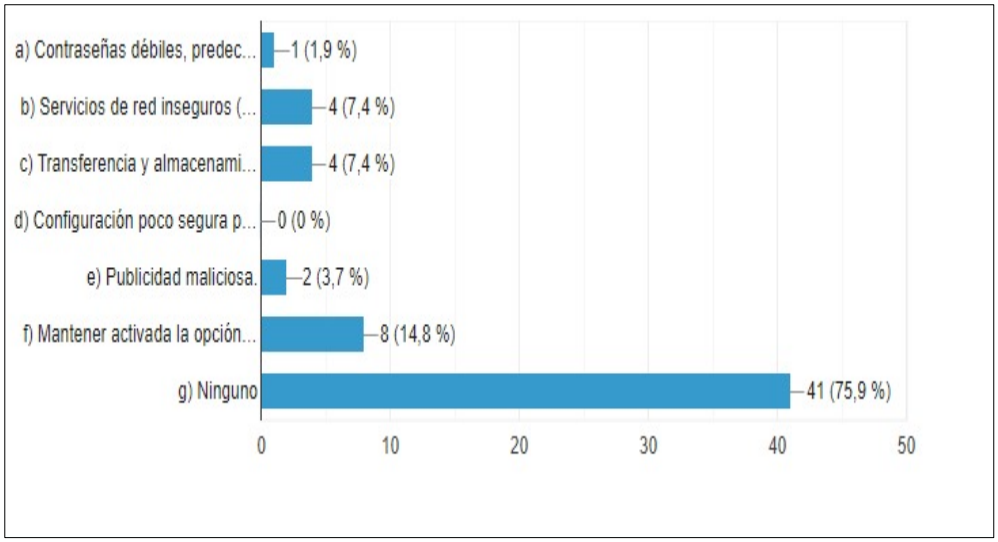
Fuente: El investigador

En base a los datos obtenidos, los encuestados manifiestan que debido a la socialización de la guía de recomendaciones se ha podido solucionar ciertos

inconvenientes que se han presentado con anterioridad, así como las causas de fallos, problemas en los dispositivos móviles. Por tanto, las personas consideran la importancia de adquirir conocimiento sobre el adecuado manejo de apps como anuncios, mensajes de textos o de email, para evitar posibles robos de información, especialmente de cuentas bancarias y afectaciones físicas a los dispositivos, por tal motivo la aplicación de la guía de recomendaciones es factible porque permite ser una estrategia de cambio y de prevención contra virus de software malicioso. Además, de ser vista como una herramienta para el uso y manejo de la información se integra de forma eficaz y eficiente en los contenidos para ser puestos en práctica sobre el adecuado manejo responsable de las apps móviles.

4. **¿Qué problemas relacionados a temas de seguridad ha experimentado después de utilizar la guía de recomendaciones?**

Figura 16 Problemas de seguridad en los dispositivos

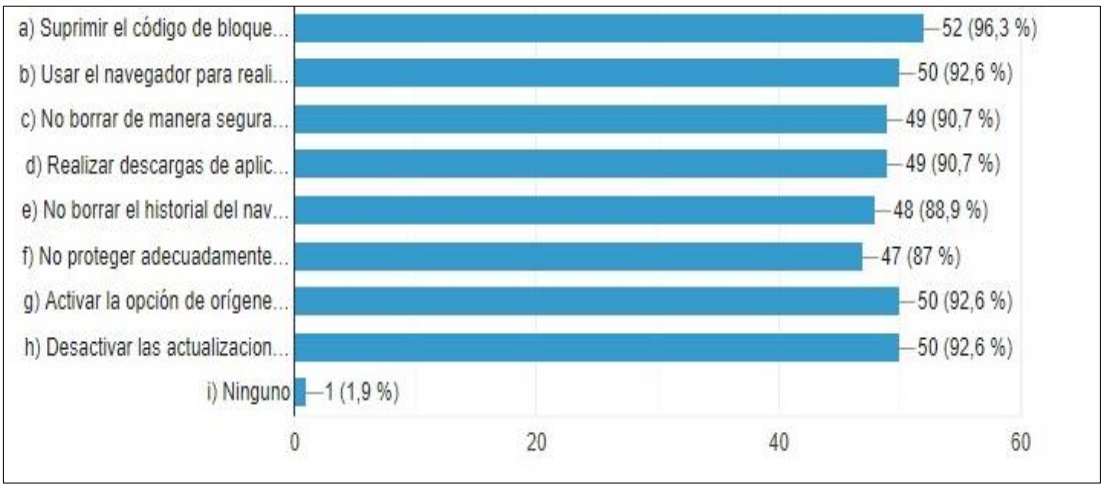


Fuente: El investigador

Mediante la integración de la guía de recomendaciones se ha obtenido que las personas han acoplado esta información de forma positiva, siendo esta herramienta de máxima ayuda para la prevención de daños en los dispositivos móviles. Bajo este aspecto los encuestados han integrado los temas de seguridad de manera proactiva, siendo positivo para el desarrollo investigativo en donde se ha puesto en práctica la serie de recomendaciones para el uso de plataformas, sitios web, descargas, y publicidad maliciosa.

5. **¿Cuál de las siguientes acciones ha dejado de realizar después de utilizar la guía de recomendaciones?**

Figura 17 Acciones

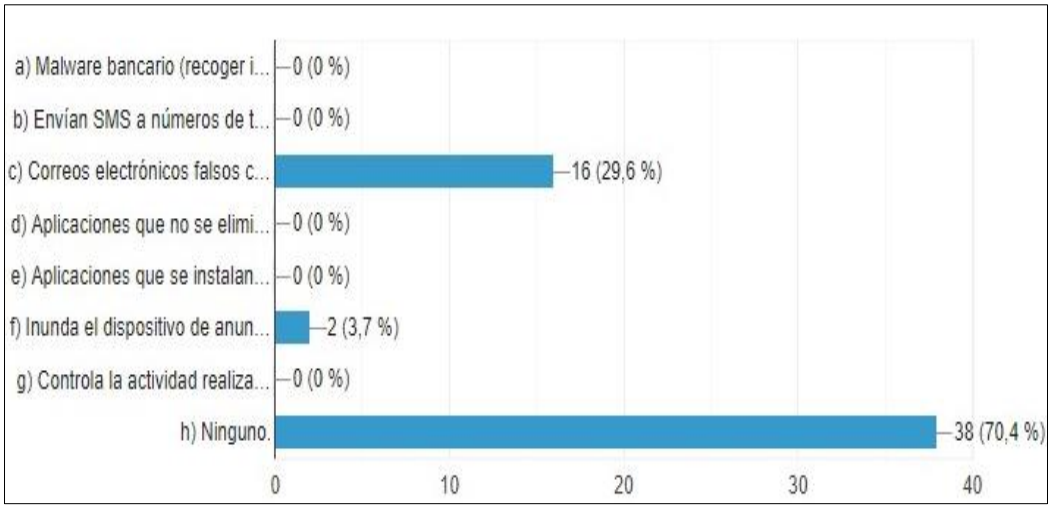


Fuente: El investigador

Los entrevistados consideran que entre las principales acciones que han dejado de realizar luego de la utilización por medio de la práctica de la guía de recomendaciones es; suprimir el código de bloqueo, uso del navegador y borrar adecuadamente los datos del dispositivo e historial. Mediante estas sugerencias las personas opinan que han mejorado la funcionalidad de los dispositivos móviles en este sentido la guía sirve para identificar cuales aspectos informáticos se puede realizar o no con el fin de conocer de mejor manera el uso de aplicaciones móviles.

6. **De la lista siguiente seleccione alguna situación que le ha afectado después de utilizar la guía de recomendaciones**

Figura 18 Lista de afectación



Fuente: El investigador

La mayor parte de encuestados consideran que luego de la aplicación de la guía de recomendaciones, ha sido muy favorable debido a que definen los que es un malware bancario, publicidad maliciosa, aplicaciones que no pueden desinstalarse. Estas características asociadas a los peligros y riesgos que incurre para los dispositivos móviles se encuentran en la guía de recomendaciones cuyo impacto es positivo para los encuestados como para el investigador porque después de esta socialización las personas no han registrado ningún problema que haya afectado a los dispositivos móviles.

3.2. Cuadro comparativo

Después de analizar la guía de recomendaciones, y su incidencia en las actividades que realizan los encuestados en base del uso de aplicaciones apps, para los dispositivos móviles, se manifiesta que la práctica de la misma es eficaz porque a través de estos aspectos de carácter informático las personas pueden adquirir conocimiento y capacitarse frente a los problemas y causas de un software malicioso. Por tal razón, se procede a realizar la siguiente comparación sobre los principales hallazgos, datos y resultados que se han encontrado en la investigación partiendo de la aplicación de las encuestas.

Tabla 11 Comparación de las encuestas

ENCUESTA 1	ENCUESTA 2
1.- ¿Cómo descarga sus aplicaciones?	**1 ¿Cómo descarga sus aplicaciones después de utilizar la guía de recomendaciones?**
a.- Tiendas oficiales (Google Play, App Store). 85.1% b.- Tiendas no oficiales (Aptoide, AppBrain, Cydia, Appland). 10.4% c.- Páginas web. 13.4% d.- Otro. 6%	a.- Tiendas oficiales (Google Play, App Store). 100% b.- Tiendas no oficiales (Aptoide, AppBrain, Cydia, Appland). 0% c.- Páginas web.0% d.- Otro. 0%
Comparación: De acuerdo con los datos se observó que en la encuesta 1, la mayor parte de entrevistados ha ocupado tiendas oficiales como la Google play, app store y luego de la aplicación de la guía de recomendaciones en la encuesta 2, se confirma que en mayoría siguen utilizando esta alternativa.	
2.- **¿Considera que es importante tener instalado un antivirus en su dispositivo?**	**2. ¿Considera que es importante tener instalado un antivirus en su dispositivo?**
a.- Si. 68.7% b.- No. 17.9% c.- No sé. 13.4%	a.- Si. 100% b.- No. 0% c.- No sé. 0%
Comparación: En la encuesta 1, el 68,7% de las personas mencionaron qué si tienen instalado un antivirus mientras que en la encuesta 2, luego de la socialización de la guía de recomendaciones ya hubo mayormente el 100% de las personas que ya instalaron un antivirus.	

3.- ¿Seleccione los problemas que usted ha tenido en su dispositivo móvil?	**3. ¿Seleccione los problemas que usted ha tenido en su dispositivo móvil después de utilizar la guía de recomendaciones?**
a.- Alto consumo de recursos (dispositivo lento). 28.4% b.- Daño en Información (imágenes dañadas, aplicaciones, archivos). 13.4% c.- Aplicaciones que no quieren desinstalarse. 20.9% d.- Filtración de datos (robo de credenciales, contraseñas, cuentas bancarias). 7.5% e.- No puede apagarla o reiniciar su dispositivo. 7.5% f.- Le aparecen en pantalla anuncios inapropiados o anuncios que interfieren con el contenido de la página. 25.4% g.- Le aparecen páginas web que usted no tenía intención de visitar, o envía mensajes de correo electrónico que usted no escribió. 17,9% h.- La batería de su dispositivo se agota más rápido de lo normal. 29,9% i.- Ninguno 7.5%	a.- Alto consumo de recursos (dispositivo lento).1,9% b.- Daño en Información (imágenes dañadas, aplicaciones, archivos). 0% c.- Aplicaciones que no quieren desinstalarse. 5,6% d.- Filtración de datos (robo de credenciales, contraseñas, cuentas bancarias). 1,9% e.- No puede apagarla o reiniciar su dispositivo. 1,9% f.- Le aparecen en pantalla anuncios inapropiados o anuncios que interfieren con el contenido de la página. 5,6% g.- Le aparecen páginas web que usted no tenía intención de visitar, o envía mensajes de correo electrónico que usted no escribió. 1,9% h.- La batería de su dispositivo se agota más rápido de lo normal. 0% i.- Ninguno. 88,9%
Comparación: En la encuesta 1, se puede observar que las personas han tenido problemas relacionados en mayoría a la lentitud de los dispositivos, problemas con la batería, aplicaciones que no se desinstalan, aparición de anuncios. Sin embargo, en la aplicación de la encuesta 2, mediante el uso de la guía las personas conocieron más a fondo estos	

<table>
<tr><td colspan="2">problemas y pusieron en práctica las recomendaciones descritas en el documento posterior dejaron de tener problemas en un 88,9%.</td></tr>
<tr><td>7. ¿Qué problemas relacionados a temas de seguridad ha experimentado?</td><td>4. ¿Qué problemas relacionados a temas de seguridad ha experimentado después de utilizar la guía de recomendaciones?</td></tr>
<tr><td>a.- Contraseñas débiles, predecibles (contraseñas sencillas y comunes ejemplo 12345678). 29,9%

b.- Servicios de red inseguros (wifi gratis). 19.4%

c.- Transferencia y almacenamiento de datos de manera poco seguro (envió por bluetooth, wifi directo). 22.4%

d.- Configuración poco segura por defecto. 14.9%

e.- Publicidad maliciosa. 32.8%

f.- Mantener activada la opción de conexión automática a redes inalámbricas, bluetooth, ubicación. 13,4%

g.- Ninguna. 16.4%</td><td>a.- Contraseñas débiles, predecibles (contraseñas sencillas y comunes ejemplo 12345678). 1.9%

b.- Servicios de red inseguros (wifi gratis). 7.4%

c.- Transferencia y almacenamiento de datos de manera poco seguro (envió por bluetooth, wifi directo). 7.4%

d.- Configuración poco segura por defecto. 0%

e.- Publicidad maliciosa. 3.7%

f.- Mantener activada la opción de conexión automática a redes inalámbricas, bluetooth, ubicación. 14,8%

g.- Ninguna. 75.9%</td></tr>
<tr><td colspan="2">Comparación: De acuerdo con los datos de la primera encuesta las personas si han experimentado problemas en cuento al tema de seguridad entre ellas el tema de códigos de seguridad, almacenamiento del dispositivo, publicidad maliciosa, sin embargo en la segunda en cuesta posterior a la aplicación de la guía de recomendaciones se ha reducido estos riesgos debido a que las personas han centrado en identificar estas causas sobre un mal uso en los dispositivos por tanto, con la aplicación de la misma se redujo en un 75,9% en vista que los encuestados ya no presentan estos problemas.</td></tr>
</table>

5.- **¿Cuál de las siguientes acciones las ha realizado en algún momento?**	**5. ¿Cuál de las siguientes acciones ha dejado de realizar después de utilizar la guía de recomendaciones?**
a.- Suprimir el código de bloqueo del móvil. 16.4% b.- Usar el navegador para realizar actividades que pueden ser realizadas a través de apps. 23.9% c.- No borrar de manera segura los datos del dispositivo cuando dejamos de usarlo. 19.4% d.- Realizar descargas de aplicaciones que no procedan de un sitio confiable. 22.4% e.- No borrar el historial del navegador regularmente. 17.9% f.- No proteger adecuadamente datos sensibles guardados en el dispositivo. 17.9% g.- Activar la opción de orígenes desconocidos. 16.4% h.- Desactivar las actualizaciones automáticas de aplicaciones y sistema operativo. 25.4% g.- Ninguno. 3%	a.- Suprimir el código de bloqueo del móvil. 96,3% b.- Usar el navegador para realizar actividades que pueden ser realizadas a través de apps. 92, 6% c.- No borrar de manera segura los datos del dispositivo cuando dejamos de usarlo. 90,7% d.- Realizar descargas de aplicaciones que no procedan de un sitio confiable. 90,7% e.- No borrar el historial del navegador regularmente. 88,9% f.- No proteger adecuadamente datos sensibles guardados en el dispositivo. 87% g.- Activar la opción de orígenes desconocidos. 92,6% h.- Desactivar las actualizaciones automáticas de aplicaciones y sistema operativo. 92,6% g.- Ninguno. 1,9%
Comparación: En la encuesta 1 se denota los encuestados si han realizado acciones en caso que se le haya presentado un problema entre ellos han suprimido el código de bloqueo, usar el navegador para descargarse aplicaciones, han desactivado las aplicaciones de manera automática, mientras que en luego a la aplicación de la guía de recomendaciones estas acciones si se han mantenido pero la disminución para realizarlas por cuenta propia es mínima correspondiente al 1,9%.	

6.- **De la lista siguiente seleccione alguna situación que le ha afectado**	**6.- De la lista siguiente seleccione alguna situación que le ha afectado después de utilizar la guía de recomendaciones**
a.- Malware bancario (recoger información sobre contraseñas bancarias e inicios de sesión). 17.9% b.- Envían SMS a números de tarificación especial incrementando las facturas de los usuarios (Troyano-SMS). 28,4% c.- Correos electrónicos falsos con avisos importantes de los bancos, aplicaciones falsas de bancos (Troyanos bancarios o phishing). 26.9% d.- Aplicaciones que no se eliminan fácilmente (Troyano xHelper). 11.9% e.- Aplicaciones que se instalan automáticamente (Hummingbad). 9% f.- Inunda el dispositivo de anuncios publicitarios (Hiddad). 20.9% g.- Controla la actividad realizada por el dispositivo, localiza la ubicación y roba importante información (Spyware móvil). 11.9% h.- Ninguno. 17.9%	a.- Malware bancario (recoger información sobre contraseñas bancarias e inicios de sesión). 0% b.- Envían SMS a números de tarificación especial incrementando las facturas de los usuarios (Troyano-SMS). 0% c.- Correos electrónicos falsos con avisos importantes de los bancos, aplicaciones falsas de bancos (Troyanos bancarios o phishing). 26,9% d.- Aplicaciones que no se eliminan fácilmente (Troyano xHelper). 0% e.- Aplicaciones que se instalan automáticamente (Hummingbad). 0% f.- Inunda el dispositivo de anuncios publicitarios (Hiddad). 3.7% g.- Controla la actividad realizada por el dispositivo, localiza la ubicación y roba importante información (Spyware móvil). 0% h.- Ninguno. 70,4%
Comparación: De acuerdo al listado en la encuesta 1, las personas han tenido problemas porque han desconocido términos como malware bancario, algunos desconocen la afectación y robo de la información bancaria mediante el envió de SMS, correos electrónicos, y publicidad como el Hiddad, mientras que en la encuesta 2, mediante el uso de la guía de recomendaciones las personas pudieron capacitarse en estos términos de robo cibernético y en totalidad del 70,4% ya tienen los conocimientos sobre estos problemas y robos de información.	

Fuente: El investigador

CONCLUSIONES

- Se concluye mencionando que un malware es denominado un software malicioso, siendo un programa informático que es creado para dañar y perjudicar los datos de un sistema operativo en este sentido la investigación ha destacado a la publicidad y anuncios e internet, mensajes bancarios, llamadas de larga distancia, envió de correo electrónico siendo el causante de un robo de información y cuentas bancarias.

- Por medio de los datos obtenidos en la encuesta número 1, se obtiene que entre los principales problemas que se suscitan cuando se ingresa a una sitio web o página de contenido de anuncios los dispositivos móviles tienden a que las funciones sean lentas y se almacene rápidamente la memoria incluyendo que el daño en Información se de en imágenes dañadas, aplicaciones, archivos además, existe filtración de datos robo de credenciales, contraseñas, cuentas bancarias en este sentido los dispositivos no responden si se apaga o se reinicia.

- Las formas para persuadir a las personas se han destacado los SMS como números de tarificación especial incrementando las facturas de los usuarios (Troyano-SMS). Y aquellos que envían un virus por medio de mensajes bancarios como el *Pishining*, o los usuarios pueden acceder a la *play store* para descargarse aplicaciones encontrándose también con aquellas que se instalan solas y se denominan (Hummingbad),

- Al hablar de los problemas que se han encontrado los entrevistados se tiene que cuando han ingresado a páginas web de contenido de virus troyano, no pueden suprimir el código de bloqueo, se han su citado problemas y daños en la batería, memoria, al ingresar a correos electrónicos falsos la información es robada y los causa la pérdida de archivos, entre ellas documentación, fotos, videos.

- La investigación se centró en la importancia de diseñar una guía de recomendaciones para malware para que las personas o grupos de empresarios se socialicen con este tipo de software malicioso y las consecuencias que puede traer a los dispositivos móviles, perdida de información, robo de datos bancarios y archivos, entre otros.

RECOMENDACIONES

- Es necesario que los emprendedores, deban conocer las consecuencias que deja los softwares maliciosos al visitar páginas en un navegador que no sean seguras dependiendo el dispositivo que tenga, debe considerar los lineamientos que se presenta en la guía de recomendaciones descrita en el presente estudio.

- Para evitar que un malware dañe las funciones de un dispositivo móvil especialmente Android, computadora o laptop es necesario que las personas o administradores contraten a un profesional en informática para la correcta instalación de un antivirus que ayude a reducir estos problemas.

- Evitar, instalar programas que no se consideren seguros para los dispositivos en vista a los virus especialmente el troyano que afecta al 90%, a la memoria interna y almacenamiento dañando así información.

- A través de la guía se pretende formar a los emprendedores mediante la puesta en marcha sobre los efectos que afecta a los sistemas operativos Android, o equipos de cómputo, por esta razón la guía es muy propositiva para adquirir más conocimiento sobre el cuidado que se deba tener ante estas funciones como; SMS, correos electrónicos, llamadas de larga distancia etc.

BIBLIOGRAFÍA

Álvarez , M. (2015). Microprocesadores para Comunicaciones: Android Las Palmas de Gran Canaria (Primera ed., Vol. Dos). México: Trillas.

Aveda, R. (03 de 03 de 2021). adslzone. Obtenido de adslzone: https://www.adslzone.net/reportajes/software/que-es-android/

Barrero, G. (2016). ANÁLISIS DE LA EFICIENCIA DE LOS SISTEMAS OPERATIVOS PARA SERVIDORES WEB DISPONIBLES EN EL MERCADO GLOBAL Y SU IMPACTO EN LA APLICACIÓN DENTRO DE LA UNIVERSIDAD ESTATAL DE MILAGRO. Milagro: Universidad Estatal de Milagro. Obtenido de http://repositorio.unemi.edu.ec/bitstream/123456789/1783/1/An%C3%A1lisis%20de%20la%20eficiencia%20de%20los%20sistemas%20operativos%20para%20servidores%20web%20disponibles%20en%20el%20mercado%20global%20y%20su%20impacto%20en%20la%20aplicaci%C3%B3n%20dentro

Boletín Semilleros Universidad Técnica de Ambato UTA. (14 de Abril de 2021). Semilleros UTA. Obtenido de file:///C:/Users/Usuario1/Downloads/BOLETIN_104.pdf

Cabrera, F. (21 de Agosto de 2018). Andoit Malware. Obtenido de http://jeuazarru.com/wp-content/uploads/2014/10/android_malware.pdf

Caqueta, F. (2015). Sistemas operativos. Obtenido de http://www.udla.edu.co/documentos/docs/Programas%20Academicos/Tecnologia%20en%20Informatica%20y%20sistemas/Compilados/Compilado%20Sistemas%20Operativos.pdf

Cazau, P. (2017). Tipos de investigación: Exploratoria, Descriptiva, Explicativa, Correlacional (Primera ed.). México: Trillas.

Chebyshev, V. (31 de 05 de 2021). Securelist. Obtenido de https://securelist.lat/it-threat-evolution-q1-2021-mobile-statistics/93855/

Dávila , G. (2016). El razonamiento inductivo y deductivo dentro del proceso investigactivo en ciencias experimentales y sociales. Laurus, 27. Obtenido de https://www.redalyc.org/pdf/761/76109911.pdf

Gonzáles , D. (2019). Estudio de dispositivos móviles, vulnerabilidades y auditoría de seguridad de aplicaciones móviles. openaccess.uoc.edu, 77.

Herraiz, A. (6 de Noviembre de 2012). História de la informática. Obtenido de https://histinf.blogs.upv.es/files/2012/12/ANDROID-Gabriel-Herraiz-Ant%c3%b3n.pdf

Honorable Concejo Provincial de Tungurahua. (27 de Octubre de 2020). Si no hay innovación no hay emprendimiento. Obtenido de https://www.tungurahua.gob.ec/index.php/informativo-hgpt/principales/5301-si-no-hay-innovacion-no-hay-emprendimiento1-4

Huicamaigua, S. (2017). Aplicación de una metodología pra el análisis de los efectos de Malware en dispositivos de sistemas operativos Andorit en Ecuador. Quito: Universidad Politécnica Nacional. Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/17495/1/CD-7996.pdf

Jumbo, T. (2017). Metodología para el análisis de Malware en un Ambiente controlado. Cuenca: Universdad Politécnica Saleciana Sede Cuenca. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/14202/1/UPS-CT006985.pdf

López, C. (2019). Desarrollo de una guía de controles ciberseguridad para la protección integral de la pyme. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/95026/6/cjlopezTFM0619memoria.pdf

López, P., & Fachelli, S. (01 de Febrero de 2015). Metodología de la investigación social cuantitativa. Obtenido de https://ddd.uab.cat/pub/caplli/2016/163567/metinvsoccua_a2016_cap2-3.pdf

Maslennikov, D. (2015). Introducción a la virología móvil. Obtenido de https://securelist.lat/virologa-mvil/67382/

Mejía, T. (2018). Investigación descriptiva: características, técnicas, ejemplos. Obtenido de https://www.lifeder.com/investigacion-descriptiva/

Meneses, J. (19 de Agosto de 2017). El cuestionario. Obtenido de https://femrecerca.cat/meneses/publication/cuestionario/cuestionario.pdf

Morales, P. (2017). Ciberseguridad en las paltaformas educativas institucionales de educación superior de la Provinvia de Tungurahua - Ecuador. Obtenido de file:///C:/Users/Usuario1/Downloads/Art%C3%ADculo%20-%20Pablo%20Morales%20-%203ciencias%20(1).pdf

Muena, B. D. (2018). MALWARE PARA DISPOSITIVOS MÓVILES. Premio Universitario Eset, 12.

Muenas, D. (12 de Junio de 2018). Malware para dispositivos móviles Androit. Recuperado el 18 de Junio de 2021, de https://premios.eset-la.com/universitario/pdf/malaware_para_dispositivos_moviles_android.pdf

Prieto, J. (21 de Abril de 2017). El uso de los métodos deductivo e inductivo para aumentar la eficiencia del procesamiento de adquisición de evidencias digitales. Obtenido de http://www.scielo.org.co/pdf/cuco/v18n46/0123-1472-cuco-18-46-00056.pdf

Ramírez, I. (05 de 2020). xatakandroid. Obtenido de xatakandroid: https://www.xatakandroid.com/sistema-operativo/parches-seguridad-android-que-que-importante-instalarlos

Ribero, M. (2016). Inofospywzre. Obtenido de https://www.infospyware.com/articulos/que-son-los-malwares/

Rodríguez, L. (2016). Metodología de análisis de riesgo. Obtenido de file:///C:/Users/Usuario1/Downloads/liziyoTFM0617-ANEXO%20F%20(1).pdf

Ulin, P. (2016). Investigación Aplicada (Primera ed., Vol. 2). Madrid: Pearson.

Unucheck, R. (2015). Virología movil. Obtenido de https://securelist.lat/mobile-malware-evolution-2015/82669/

Zapata, C., Cubides, I., & Murcia, M. (2015). TÉCNICAS DE DETECCIÓN Y ANÁLISIS DE MALWARE EN ENTORNOS CORPORATIVOS CON SISTEMAS OPERATIVOS WINDOWS. Medellín: Universidad de San Buenaventura seccional Medellín. Obtenido de http://bibliotecadigital.usbcali.edu.co/bitstream/10819/4208/1/Tecnicas_Deteccion_Analisis_Zapata_2015.pdf

ANEXOS

Anexo 1. Encuesta

Pontificia Universidad Católica del Ecuador | Sede Ambato

OFICINA DE POSGRADOS

ENCUESTA DIRIGIDA A EMPRENDEDORES

Propósito: Recabar datos para Analizar los ataques de Malware en dispositivos móviles con sistema operativo Android de emprendedores.

Instrucciones: Lea detenidamente cada pregunta y responda con toda libertad. Seleccione la alternativa que considere pertinente.

1. **¿Qué marca de dispositivo móvil utiliza?**

a) Samsung.
b) Apple.
c) Xiaomi.
d) Huawei.
e) Otro.

2. **¿Quién es responsable de instalar sus aplicaciones y dar mantenimiento a su dispositivo móvil?**

a) Empleados.
b) Administrador.
c) Familiar.
d) Mi persona.
e) Otros.

3. **¿Cómo descarga sus aplicaciones?**

a) Tiendas oficiales (Google Play, App Store).
b) Tiendas no oficiales (Aptoide, AppBrain, Cydia, Appland).
c) Páginas web.
d) Otro.

4. **¿Considera que es importante tener instalado un antivirus en su dispositivo?**

a) Si.
b) No.
c) No sé.

5. **¿Conoce usted sobre la importancia de la seguridad en los dispositivos móviles?**

a) Si.
b) No.

6. **¿Seleccione los problemas que usted ha tenido en su dispositivo móvil?**

a) Alto consumo de recursos (dispositivo lento).
b) Daño en Información (imágenes dañadas, aplicaciones, archivos).
c) Aplicaciones que no quieren desinstalarse.
d) Filtración de datos (robo de credenciales, contraseñas, cuentas bancarias).
e) No puede apagarla o reiniciar su dispositivo.
f) Le aparecen en pantalla anuncios inapropiados o anuncios que interfieren con el contenido de la página.
g) Le aparecen páginas web que usted no tenía intención de visitar, o envía mensajes de correo electrónico que usted no escribió.
h) La batería de su dispositivo se agota más rápido de lo normal.

7. **¿Qué problemas relacionados a temas de seguridad ha experimentado?**

a) Contraseñas débiles, predecibles (contraseñas sencillas y comunes ejemplo 12345678).
b) Servicios de red inseguros (wifi gratis).
c) Transferencia y almacenamiento de datos de manera poco seguro (envió por bluetooth, wifi directo).
d) Configuración poco segura por defecto.
e) Publicidad maliciosa.
f) Mantener activada la opción de conexión automática a redes inalámbricas, bluetooth, ubicación.

8. ¿Cuál de las siguientes acciones las ha realizado en algún momento?

a) Suprimir el código de bloqueo del móvil.
b) Usar el navegador para realizar actividades que pueden ser realizadas a través de apps.
c) No borrar de manera segura los datos del dispositivo cuando dejamos de usarlo.
d) Realizar descargas de aplicaciones que no procedan de un sitio confiable.
e) No borrar el historial del navegador regularmente.
f) No proteger adecuadamente datos sensibles guardados en el dispositivo.
g) Activar la opción de orígenes desconocidos.
h) Desactivar las actualizaciones automáticas de aplicaciones y sistema operativo.

9. De la lista siguiente seleccione alguna situación que le ha afectado

a) Malware bancario (recoger información sobre contraseñas bancarias e inicios de sesión).
b) Envían SMS a números de tarificación especial incrementando las facturas de los usuarios (Troyano-SMS).
c) Correos electrónicos falsos con avisos importantes de los bancos, aplicaciones falsas de bancos (Troyanos bancarios o phishing).
d) Aplicaciones que no se eliminan fácilmente (Troyano xHelper).
e) Aplicaciones que se instalan automáticamente (Hummingbad).
f) Inunda el dispositivo de anuncios publicitarios (Hiddad).
g) Controla la actividad realizada por el dispositivo, localiza la ubicación y roba importante información (Spyware móvil).

10. ¿considera que una guía de recomendaciones le serviría para prevenir riesgos?

a) Si.
b) No.

Anexo 1.1 Encuesta

OFICINA DE POSGRADOS

ENCUESTA DIRIGIDA A EMPRENDEDORES

Propósito: Recabar datos para Analizar los ataques de Malware en dispositivos móviles con sistema operativo Android de emprendedores después de utilizar la guía de recomendaciones.

Instrucciones: Lea detenidamente cada pregunta y responda con toda libertad. Seleccione la alternativa que considere pertinente.

1.- ¿Cómo descarga sus aplicaciones después de utilizar la guía de recomendaciones?

a) Tiendas oficiales (Google Play, App Store).
b) Tiendas no oficiales (Aptoide, AppBrain, Cydia, Appland).
c) Páginas web.
d) Otro.

2.- ¿Considera que es importante tener instalado un antivirus en su dispositivo?

a) Si.
b) No.
c) No sé.

3.- ¿Seleccione los problemas que usted ha tenido en su dispositivo móvil después de utilizar la guía de recomendaciones?

a) Alto consumo de recursos (dispositivo lento).
b) Daño en Información (imágenes dañadas, aplicaciones, archivos).
c) Aplicaciones que no quieren desinstalarse.
d) Filtración de datos (robo de credenciales, contraseñas, cuentas bancarias).
e) No puede apagarla o reiniciar su dispositivo.

f) Le aparecen en pantalla anuncios inapropiados o anuncios que interfieren con el contenido de la página.
g) Le aparecen páginas web que usted no tenía intención de visitar, o envía mensajes de correo electrónico que usted no escribió.
h) La batería de su dispositivo se agota más rápido de lo normal.
i) Ninguno

4.- ¿Qué problemas relacionados a temas de seguridad ha experimentado después de utilizar la guía de recomendaciones?

a) Contraseñas débiles, predecibles (contraseñas sencillas y comunes ejemplo 12345678).
b) Servicios de red inseguros (wifi gratis).
c) Transferencia y almacenamiento de datos de manera poco seguro (envió por bluetooth, wifi directo).
d) Configuración poco segura por defecto.
e) Publicidad maliciosa.
f) Mantener activada la opción de conexión automática a redes inalámbricas, bluetooth, ubicación.
g) Ninguno

5.- ¿Cuál de las siguientes acciones ha dejado de realizar después de utilizar la guía de recomendaciones?

a) Suprimir el código de bloqueo del móvil.
b) Usar el navegador para realizar actividades que pueden ser realizadas a través de apps.
c) No borrar de manera segura los datos del dispositivo cuando dejamos de usarlo.
d) Realizar descargas de aplicaciones que no procedan de un sitio confiable.
e) No borrar el historial del navegador regularmente.
f) No proteger adecuadamente datos sensibles guardados en el dispositivo.
g) Activar la opción de orígenes desconocidos.
h) Desactivar las actualizaciones automáticas de aplicaciones y sistema operativo.

6.- De la lista siguiente seleccione alguna situación que le ha afectado después de utilizar la guía de recomendaciones

a) Malware bancario (recoger información sobre contraseñas bancarias e inicios de sesión).
b) Envían SMS a números de tarificación especial incrementando las facturas de los usuarios (Troyano-SMS).
c) Correos electrónicos falsos con avisos importantes de los bancos, aplicaciones falsas de bancos (Troyanos bancarios o phishing).
d) Aplicaciones que no se eliminan fácilmente (Troyano xHelper).
e) Aplicaciones que se instalan automáticamente (Hummingbad).
f) Inunda el dispositivo de anuncios publicitarios (Hiddad).
g) Controla la actividad realizada por el dispositivo, localiza la ubicación y roba importante información (Spyware móvil).
h) Ninguno.

ANEXO 2. GUÍA DE RECOMENDACIONES "SOFTWARE MALCIOSO" https://guia.fchsecurity.com/

Descripción general

Esta guía de seguridad cibernética, diseñada específicamente para el grupo de emprendedores "SEUTA", aborda la creciente amenaza del software malicioso en el mundo actual, ofreciendo una visión detallada de qué es el malware y sus variadas formas. Además, se centra en prevenir su impacto, proporcionando consejos prácticos, desde políticas de seguridad y soluciones de protección. Aprenderán a detectar y responder a posibles infecciones de malware, y garantizar la integridad de sus negocios en un mundo digital interconectado.

CONTENIDO

Introducción a los tipos de software malicioso

Métodos de propagación del software malicioso

Medidas de protección contra el software malicioso

Estudios de Caso

ÍNDICE

Definición y tipos de software malicioso

1

Introducción a los tipos de software malicioso

El software malicioso, también conocido como malware, se refiere a cualquier programa o código diseñado con la intención de dañar, perjudicar o acceder de manera no autorizada a un sistema informático. Este tipo de software puede tomar diversas formas y tener diferentes objetivos, por lo que es importante conocer los distintos tipos de malware para poder prevenir su aparición y proteger nuestros sistemas y datos.

Virus Informáticos

Los virus informáticos son programas maliciosos que se adhieren o copian en archivos. Cuando se ejecuta el archivo infectado, el virus se activa y se propaga, dañando datos, ralentizando el sistema y robando información. Ejemplos incluyen el gusano ILOVEYOU y el virus de la Policía.

Gusanos informáticos

Los gusanos informáticos son programas maliciosos que se difunden a través de redes sin depender de archivos huéspedes y pueden replicarse automáticamente. Aprovechan vulnerabilidades en sistemas para infiltrarse, robar información o causar daños.

Troyanos

Los troyanos son programas maliciosos que se hacen pasar por software legítimo para engañar a los usuarios y permitir el acceso no autorizado al sistema. Pueden robar información confidencial o permitir el control remoto del sistema. Suelen distribuirse a través de correos electrónicos con archivos adjuntos o descargas engañosas en sitios web.

Spyware

El spyware es un programa malicioso que recopila información de los usuarios sin su consentimiento, instalándose de manera oculta en los sistemas. Puede obtener datos personales, como hábitos de navegación o información financiera, y se utiliza generalmente para publicidad no deseada o robo de identidad.

Ransomware

El ransomware es un malware que cifra archivos o bloquea sistemas, exigiendo un rescate para restaurar el acceso. Puede causar graves problemas al hacer que los datos y sistemas sean inaccesibles. Ejemplos incluyen WannaCry y Petya.

Botnets

Las botnets son redes de computadoras controladas por un atacante (botmaster) a través de malware. Se utilizan para realizar ataques DDoS, enviar spam y robar datos confidenciales. Suelen infectar dispositivos sin el conocimiento de los usuarios, utilizando métodos como el phishing y la explotación de vulnerabilidades.

Los troyanos son programas maliciosos que se hacen pasar por software legítimo para engañar a los usuarios y permitir el acceso no autorizado al sistema. Pueden robar información confidencial o permitir el control remoto del sistema. Suelen distribuirse a través de correos electrónicos con archivos adjuntos o descargas engañosas en sitios web.

Métodos de propagación del software malicioso

El malware es un programa informático diseñado para dañar sistemas o dispositivos. Importante entender cómo se propaga e infiltra en los sistemas

5

Ingeniería social

La ingeniería social es un método común para distribuir malware, engañando a los usuarios a través de phishing, enlaces maliciosos y mensajes falsos

Exploits y vulnerabilidades

Los ciberdelincuentes explotan vulnerabilidades en sistemas, aplicaciones y dispositivos para instalar malware sin que el usuario lo detecte, ya sea aprovechando vulnerabilidades desconocidas o sin actualizar.

Descargas no autorizadas

La descarga de contenido no autorizado es una vía común de propagación de malware, ya que los archivos piratas pueden contener software malicioso. Es esencial usar fuentes legítimas y confiables al descargar en línea.

Dispositivos extraíbles

Los dispositivos extraíbles, si están infectados, pueden propagar malware al conectarse a otros sistemas sin que el usuario lo sepa. Es esencial escanearlos antes de usarlos en una computadora.

Redes P2P y transferencias de archivos

Las redes P2P, como BitTorrent, son usadas por ciberdelincuentes para propagar malware al compartir archivos. Las transferencias por correo electrónico y mensajería también pueden contener malware.

Anuncios y pop-ups maliciosos

Los anuncios maliciosos redirigen a sitios infectados o descargas de malware; deben evitarse y se puede usar software de bloqueo de anuncios. La conciencia de los métodos de propagación y la seguridad cibernética son esenciales para proteger sistemas y dispositivos.

Medidas de protección contra el software malicioso

El malware es software dañino que puede infiltrarse en sistemas sin consentimiento, incluyendo virus, gusanos, troyanos, ransomware y spyware. Se explorarán medidas de protección para prevenir y mitigar estos riesgos.

8

Actualiza Regularmente tu Sistema Operativo y Aplicaciones

Mantén tu sistema operativo (iOS, Android) y todas las aplicaciones actualizadas. Las actualizaciones suelen incluir parches de seguridad que protegen contra amenazas conocidas.

Utiliza una Contraseña Fuerte o un Método de Desbloqueo Seguro

Configura una contraseña sólida, un PIN o utiliza una autenticación biométrica (huella dactilar o reconocimiento facial) para proteger tu dispositivo. Evita patrones de desbloqueo predecibles.

Descarga Aplicaciones Solo de Fuentes Confiables

Utiliza las tiendas oficiales de aplicaciones, como la App Store (iOS) y Google Play Store (Android). Evita instalar aplicaciones desde fuentes desconocidas o enlaces no verificables.

9

Investiga las Aplicaciones antes de Descargarlas

Lee las reseñas y calificaciones de otras personas antes de instalar una aplicación. Desconfía de las aplicaciones con pocas descargas o comentarios negativos.

Concede Permisos con Cautela

Revisa y limita los permisos que otorgas a las aplicaciones. No permitas que una aplicación acceda a datos o funciones innecesarios.

Activa el Antivirus y Anti-Malware

Instala una aplicación antivirus confiable en tu dispositivo y manténla actualizada. Esto te ayudará a detectar y eliminar software malicioso.

10

Habilita el Bloqueo Remoto y la Localización

Configura las funciones de "Encontrar mi dispositivo" o "Buscar mi iPhone" para poder rastrear y bloquear tu teléfono en caso de pérdida o robo.

Evita Redes Wi-Fi Públicas No Seguras

No te conectes a redes Wi-Fi públicas no seguras, ya que pueden ser un blanco fácil para ataques. Utiliza una red privada virtual (VPN) cuando sea necesario.

Desconfía de Mensajes y Correos Electrónicos no Solicitados

No hagas clic en enlaces ni descargues archivos adjuntos de mensajes o correos electrónicos desconocidos o no solicitados. Estos pueden contener malware.

Realiza Copias de Seguridad Frecuentes

Realiza copias de seguridad de tus datos de forma regular en un lugar seguro, como la nube o un dispositivo externo. Esto garantiza que puedas recuperar la información en caso de un ataque de malware.

Educa a tu Equipo

Si tienes empleados que utilizan dispositivos móviles para el trabajo, asegúrate de que estén informados sobre las mejores prácticas de seguridad y de que sigan estas recomendaciones.

Monitorea tu Cuenta Bancaria y Actividad Financiera

Mantén un ojo en tus transacciones bancarias y actividad financiera. Si notas actividades sospechosas, toma medidas inmediatas para proteger tus cuentas.

Considera la Seguridad Móvil en tu Plan de Continuidad de Negocio

Incluye medidas de seguridad móvil en tu plan de continuidad de negocio para asegurarte de que tu empresa pueda seguir operando en caso de un incidente de seguridad.

Contrata a un Experto en Seguridad

Si puedes, consulta con un experto en seguridad informática para evaluar y fortalecer la seguridad de tus dispositivos y sistemas empresariales.

Mantén un Registro de Dispositivos

Lleva un registro de todos los dispositivos móviles utilizados en tu empresa y realiza un seguimiento de las actualizaciones y medidas de seguridad implementadas en cada uno.

13

Recuerda que la protección contra el software malicioso es un proceso continuo. Mantén tus sistemas y dispositivos actualizados, sigue las mejores prácticas de seguridad y mantente informado sobre las últimas amenazas para asegurar una protección adecuada contra el malware.

14


15
Estudios de Caso

16

Identificación de software malicioso

Objetivo: Aprender a identificar diferentes tipos de software malicioso. 1. Investiga y describe brevemente 5 tipos de software malicioso, como virus, gusanos, troyanos, ransomware y spyware. 2. Crea una lista de características comunes que ayuden a identificar cada tipo de software malicioso. 3. Comparte tu lista con tus compañeros y discutan los diferentes tipos de software malicioso y cómo se pueden identificar.

Investigación sobre métodos de propagación de software malicioso

Objetivo: Investigar y comprender los diferentes métodos de propagación de software malicioso. 1. Investiga sobre los métodos más comunes utilizados por los creadores de software malicioso para propagarlo, como spam, descargas no seguras, archivos adjuntos de correo electrónico, etc. 2. Crea una lista de al menos 5 métodos de propagación y describa cómo funcionan. 3. Comparte tus hallazgos con tus compañeros y discutan las implicaciones de estos métodos de propagación y cómo se pueden evitar.

Implementación de medidas de protección

Objetivo: Aprender a implementar medidas de protección contra el software malicioso. 1. Investiga y describe al menos 3 medidas de protección efectivas contra el software malicioso, como la instalación de un software antivirus, la actualización regular del sistema operativo y el uso de cortafuegos. 2. Detalla paso a paso cómo implementar cada medida de protección en un equipo. 3. Comparte tus instrucciones con tus compañeros y discutan la importancia de estas medidas de protección y cómo pueden proteger contra el software malicioso.

Conclusión

En un mundo digital, la ciberseguridad es esencial. Al seguir las recomendaciones presentadas en esta guía, los emprendedores de "SEUTA" pueden proteger sus negocios de amenazas de software malicioso y garantizar la continuidad de sus operaciones.

Agradecimientos

Extendemos nuestro agradecimiento a los miembros del grupo de emprendedores "SEUTA" por su compromiso con la seguridad de la información y su voluntad de salvar sus negocios ante las amenazas cibernéticas.