PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE ESMERALDAS

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

ESCUELA DE INGENIERIA EN SISTEMAS

TESIS DE GRADO

TEMA:

ESTUDIO DE VULNERABILIDADES EN LOS SISTEMAS OPERATIVOS DISEÑADOS PARA LOS SMARTPHONE BASADO EN ESTÁNDARES DE SEGURIDAD

PREVIO A LA OBTENCIÒN DEL TÌTULO DE INGENIERIA EN SISTEMAS Y COMPUTACIÓN

NOMBRE DEL AUTOR

ERIKA GABRIELA SANTOS CEDEÑO

ASESOR:

ING. KLEBER VERA

MES Y AÑO

Esmeraldas, Septiembre 2017

TRIBUNAL DEL GRADUACIÓN

Trabajo de Tesis aprobado luego de haber dado cumplimiento a los requisitos exigidos por el Reglamento de Grado de la PUCESE previo a la obtención del título de Ingeniera en Sistemas y Computación.

Mgt. Xavier Quiñónez Ku
PRESIDENTE TRIBUNAL DE GRADUACIÓN

Mgt. Cesar Godoy Rosero
LECTOR 1

Mgt. Fabián Martínez
LECTOR 2

Mgt. Kleber Vera
DIRECTOR DE TESIS

Esmeraldas, Septiembre 2017

AUTORIA

Yo, Erika Santos Cedeño, declaro que la presente investigación enmarcada en el actual trabajo de Tesis es absolutamente original, auténtica y personal.

En virtud declaro que el contenido de esta investigación es de exclusiva responsabilidad legal y académica del autor y de la PUCESE.

Erika Santos Cedeño
C.I.: 0802656785

DEDICATORIA

El presente trabajo de investigación se lo dedico a Dios quién supo guiarme e inspirarme para efectuar el presente trabajo de investigación, darme fuerzas para seguir adelante y no desmayar en los problemas que se presentaban, enseñándome a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento.

A mi familia quienes me apoyaron en este largo camino de preparación académica.

A mis padres por su ayuda incondicional, consejos, comprensión, amor, quienes me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos. A mis hijos quienes han sido mi motivación, inspiración, y felicidad en mi vida. A mi esposo por su ayuda moral e incondicional.

Erika Santos Cedeño

AGRADECIMIENTO

El presente trabajo de tesis primeramente me gustaría agradecerle a Dios por derramar sobre mi sus bendiciones y darme la oportunidad de cumplir este sueño anhelado.

Agradezco a mis padres, por darme la confianza y el apoyo moral, por sus incondicionales consejos que me empujaron a seguir adelante.

A mi asesor de tesis, Kleber Vera, por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado que pueda terminar mis estudios con éxito.

Son muchas las personas que han formado parte de mi vida profesional a las que me encantaría agradecerles su amistad, consejos, apoyo, ánimo y compañía en los momentos más difíciles de mi vida, muchas gracias.

Erika Santos Cedeño

INDICE DE CONTENIDOS

Portada i
Tribunal del graduación ii
Autoria iii
Dedicatoria iv
Agradecimiento v
Índice de contenidos vi
Índice de gráficos viii
Resumen ix
Abstract x

Introducción 1
Presentación de la investigación 1
Planteamiento del problema 2
Justificación 3
Objetivos 4

Capítulo I
Marco de referencia

1.1. Antecedentes (estudios previos) 5
1.2. Bases teóricas científicas 6
1.2.1. Sistema operativo 6
1.2.2. Modelo y arquitectura de seguridad de los sistemas operativos iOS 8
1.2.3. Modelo y arquitectura de seguridad del sistema operativo Android 9
1.2.4. Modelo y arquitectura de seguridad del sistema operativo Windows Phone 12
1.2.5. Vulnerabilidades comunes en software 13
1.2.6. Mecanismos de prevención ante amenazas 14
1.2.7. Dispositivos móviles 16
1.2.8. Teléfonos móviles inteligentes 17
1.2.9. Asistentes digitales personales (pda) 18

1.2.10. Tabletas 18
1.3. Marco legal 19

Capítulo II
Materiales y métodos

2.1. Descripción y caracterización del lugar 21
2.2. Métodos y técnicas 21
2.3. Población y muestra 22
2.4. Técnicas de procesamiento y análisis 23
2.5. Normas éticas 23

Capítulo III
Resultados

3.1. Análisis e interpretación de resultados. 24
3.1.1. Encuesta aplicada a la ciudadanía esmeraldeña 24
3.1.2. Encuesta aplicada a técnicos de la ciudad de esmeraldas 28

Capítulo IV
Discusión

4.1. Discusión de los resultados 32
4.2. Conclusiones 34
4.3. Propuesta 35
4.3.1. Tema 35
4.3.2. Justificación 35
4.3.3. Descripción de la propuesta 35
4.3.4. Explicación formal del modelo 37
4.3.5. Análisis del modelo de amenazas 38

5. Referencias 40
5.1. Referencias bibliográficas 40
5.2. Anexos. 42

ÍNDICE DE GRÁFICOS

Gráfico N° 1: Conocimiento de mecanismos de seguridad 24
Gráfico N° 2: Dispositivo móvil según las edades 25
Gráfico N° 3: Mecanismos de seguridad más utilizados según las edades de los usuarios. 26
Gráfico N° 4: Sistema operativo más utilizado 27
Gráfico N° 5: Desbloqueo de dispositivos smartphone 28
Gráfico N° 6: Sistema operativo fácil de vulnerar 29
Gráfico N° 7: Recomendaciones de configuración de seguridad 30
Gráfico N° 8: Confiabilidad de las aplicaciones descargadas del internet. 31

RESUMEN

El definir las vulnerabilidades que existen en los sistemas operativos utilizados por los Smartphone basándose en los estándares de seguridad se constituyó en el objetivo principal de la presente investigación, se analizó la base legal y tecnológica que la sustenta, empleando una metodología cualitativa, mediante el análisis estadístico se identificó cuáles son los sistemas operativos más utilizados por los Smartphone, así como también se indicaron los mecanismos de seguridad con que cuenta cada sistema. A esto se añade la arquitectura de seguridad tanto de iOS, Android y Windows Phone que fueron los sistemas operativos analizados por su gran demanda y aceptación, también se detallan las vulnerabilidades a la que se encuentran expuestos. Como investigación de campo se aplicaron encuestas a usuarios y técnicos especializados en la configuración, reparación y manejo de Smartphone. Como resultado de la investigación se determinó que las vulnerabilidades que se presentan en los sistemas operativos de los dispositivos móviles en su mayoría son por la falta de conocimiento de los usuarios que tienen poca precaución al instalación de aplicaciones obtenidas del Internet y en las configuraciones de seguridad de los equipos.

Palabras claves: Sistema Operativo, Android, iOS, Windows Phone, vulnerabilidades, estándares de seguridad.

ABSTRACT

The definition of the vulnerabilities that exist in the operating systems used by the Smartphones based on the security standards was constituted in the main objective of the present investigation, analyzed the legal and technological base that supports it, using a quantitative methodology, through the analysis Statistic was identified which are the operating systems most used by Smartphones, as well as indicated the security mechanisms that each system has. To this is added the security architecture of both iOS, Android and Windows Phone that were the operating systems analyzed for their high demand and acceptance, also detail the vulnerabilities to which they are exposed. As a field investigation, surveys were carried out for users and technicians specialized in the configuration, repair and management of Smartphone. As a result of the investigation it was determined that the vulnerabilities that are presented in the operating systems of the mobile devices are mostly due to the lack of knowledge of the users who have little caution when installing applications obtained from the Internet and in the security configurations of the teams.

Keywords: Operating System, Android, iOS, Windows Phone, vulnerabilities, security standards.

INTRODUCCIÓN

Presentación de la investigación

En la actualidad, la forma de trabajar y de comunicarse a través de la creación de los dispositivos móviles y de las tecnologías inalámbricas ha mejorado. La evolución constante de estas tecnologías coloca a los dispositivos móviles como uno de los objetivos principales de las ciberamenazas.

La creciente demanda de los Smartphone, requiere se realice una evaluación a fondo en la seguridad que ofrecen estos dispositivos, de igual manera debe hacerse con las herramientas de protección de la información que gestionan, enmarcados en los entornos de las TIC (Tecnologías de la Información y las Comunicaciones). Al hablar de seguridad en los dispositivos móviles se hace referencia a las normas, procedimientos, métodos y técnicas destinados para obtener un sistema seguro y confiable (Prieto, 2012).

Antiguamente los teléfonos inteligentes estaban exentos de riesgos inherentes a su seguridad, puesto que los mismos no tenían conexión alguna con el Internet; pero, con las innovaciones en el campo tecnológico que han permitido a dichos dispositivos conectarse y descargar información de la red, en la actualidad, estos se encuentran expuestos a las mismas amenazas de seguridad que los equipos informáticos.

El desarrollo de este tipo de dispositivo ha permitido también la proliferación del número de aplicaciones que se crean para los Smartphone; tal es el caso que la tienda de aplicaciones de Apple, el appStore, alberga alrededor de 500.000 aplicaciones, mientras que la tienda oficial del sistema operativo Android, Google Play contiene más de 600.00 aplicaciones.

De acuerdo a un informe presentado por Canalys (2011), se indica que el beneficio directo obtenido de las aplicaciones, ya sea por compra directa, compras dentro de la aplicación o suscripción, pasará de los 7.300 millones de dólares de 2013 a 36.000 millones en el 2016, lo que implica un incremento del 500% aproximadamente (Párr.1).

Estos datos permiten evidenciar el impacto que ha tenido este tipo de tecnología. Sin embargo, dentro de este acelerado crecimiento, no se ha tenido en cuenta un aspecto importante como lo es la seguridad. A consecuencia de esto, en los últimos años han surgido nuevas amenazas y nuevos vectores de ataque que serán analizadas más a fondo en el presente estudio.

Planteamiento del problema

En el desarrollo de sistemas operativos, aplicaciones web y de escritorio, la seguridad ha sido siempre un problema relevante; para lo cual se ha desarrollado varias tecnologías para disminuir las fallas y ataques que a diario son detectados.

Los dispositivos móviles no están ajenos a estos ataques, la mayoría de los sistemas operativos desarrollados para estos equipos poseen muchas de las tecnologías de protección potentes en la actualidad. Algo que es importante acotar es que muchas veces la principal línea de defensa ante estos ataques suele ser el propio usuario.

Un factor que hace vulnerables a los dispositivos móviles es el desconocimiento por parte de los usuarios de los mecanismos de seguridad con que cuentan los diferentes sistemas operativos, como es el caso de la configuración de las aplicaciones para que se ejecuten en procesos aislados. Cambiar las claves de autentificación de usuario y contraseña que trae predeterminado el sistema operativo, respaldar la información al actualizar las aplicaciones, buscar páginas confiables para descargar los ROM, e instalar antivirus en los equipos. Todas estas alternativas varían dependiendo del sistema Operativo que utilice el dispositivo móvil (Vulnerabilidad en los sistemas informáticos, 2011).

Sin embargo al hablar de seguridad en los sistemas operativos se hace referencia a uno de los campos más amplios y complejos de las ciencias de la computación. Según Salter, existen 9 áreas principales de investigación de la seguridad de los sistemas operativos, entre ellas tenemos: ejercicio de penetración del sistema, estudio de las interfaces de usuario, Prueba de correctitud, modelos matemáticos de protección del núcleo, mecanismos de protección, seguridad en la comunicación de los datos, recursos de bases

de datos, Mecanismos de autenticación y problemas operacionales del departamento de defensa.

Muchos de estos elementos se encuentran vigentes en la seguridad de los sistemas operativos de hoy en día. Así mismo existen herramientas desarrolladas para caracterizar las amenazas, muchas de las cuales se han especializado en el sector de la informática, entre ellas tenemos, STRIDE, T-MAP, Trike y Chen.

Por lo antes expuesto, se puede indicar que la experiencia adquirida en otro tipo de plataformas sirve para aplicarla en estos nuevos dispositivos. Sin embargo, estos equipos tienen una serie de características que los hace especiales. Se pretendió como resultado de la investigación tener una visión clara de cuál ha sido el recorrido que se ha seguido en otros dispositivos más comunes como los PCs y otros equipos móviles en cuanto a estándares de seguridad. También se analizaron otros estudios realizados en la misma área, resaltando los resultados más relevantes obtenidos en los mismos.

Justificación

En la actualidad existen un sinnúmero de amenazas y vulneraciones relacionadas con los Smartphone que afecta a la seguridad tanto del dispositivo como a la información que este maneja. Para estos casos se han desarrollado contramedidas que consisten en un sistema diseñado para prevenir que un ataque consiga su objetivo. Las contramedidas pueden convertirse en una lista de consejos y buenas prácticas.

Mientras un Smartphone no se encuentre conectado a una red, su sistema operativo es seguro. El problema que se pretende abordar a través de la presente investigación es el riesgo que tiene la información y los datos almacenados en un teléfono inteligente. Identificar cuáles son las protecciones que ofrece el sistema operativo ante las diversas amenazas como los virus y los hackers así como también los casos de pérdida de los equipos.

Además se analizarán los diversos estándares de seguridad desarrollados para la protección de la información en base a la configuración de los sistemas operativos incluyendo también la seguridad en la conexión a la red. Siendo este el principal riesgo que tienen los equipos inteligentes de estar expuesto a vulneraciones. Para dar un realce a la investigación, se realizó un experimento que consistió en la instalación de los sistemas operativos más utilizados y comunes en el mercado de los Smartphone, activando todos los mecanismos de seguridad que posee cada uno, con el propósito de evaluar la vulnerabilidad del sistema, haciendo intentos por violentar la protección de seguridad activada.

El presente estudio tiene su importancia porque ha permitido identificar una gran cantidad de ataques, vulnerabilidades y amenazas a las que son expuestos los Smartphone cada día. De igual manera a través de la investigación se analizó la importancia que tienen las amenazas físicas, tal como lo es la pérdida o extravío del dispositivo o el ingreso al dispositivo por parte de otras personas mediante los canales de transmisión o utilizando redes wifi no seguras.

Objetivos

Objetivo General

Determinar las vulnerabilidades que existen en los sistemas operativos utilizados por los Smartphone basándose en los estándares de seguridad.

Objetivos Específicos

- Establecer los mecanismos de seguridad en los sistemas operativos de los dispositivos Smartphone.
- Identificar el conocimiento que tienen los técnicos y los usuarios locales acerca de la seguridad que ofrecen los diferentes sistemas operativos móviles.
- Describir un modelado de amenazas en los Smartphone, para obtener una visión más amplia de cuáles son las problemáticas que desde el ámbito de la seguridad deben afrontar estos equipos.

CAPÍTULO I
MARCO DE REFERENCIA

1.1. Antecedentes (Estudios Previos)

Estudios realizados han demostrado que Android es el Sistema Operativo más instalado en teléfonos inteligentes esto se debe a que una gran variedad de Smartphone con diversas características pueden soportar el sistema. Pero de igual forma es el más expuesto a sufrir ataques informáticas (Albarracin, Parra, & Camargo, 2013). Estas investigaciones han enfatizado que los usuarios de estos equipos deben revisar cada una de las aplicaciones que se instalan en los Smartphone, a fin de evitar que se infecte o contamine con virus troyanos.

Otras investigaciones presentan un estudio de los sistemas operativos más populares en la actualidad como lo son Android, iOS y Windows Phone. Incluyen un análisis de las características principales, las ventajas y desventajas que cada uno implementa en la seguridad y otros aspectos importantes. También se identifica cuáles son los ataques más frecuentes en dispositivos móviles y, además, se realiza una comparación en los niveles de seguridad que ofrece cada sistema operativo. Finalmente, se indican que para virus más potentes, como el adware y el exploits se recomiendan la instalación de antivirus en los equipos. (Albarracin, Parra y Camargo, 2013; Fabbiani, Sanz, y Vidal, 2010; Lagunes, 2012).

Otros estudios también han proporcionado una lista de recomendaciones de seguridad para la configuración de dispositivos móviles, previo a una evaluación y análisis de los riegos, amenazas y vulneraciones a las que se encuentran expuestos los Smartphone en la actualidad (Siles, 2014; Mendoza, 2016).

En efecto, algunas teorías como la de Siles (2013) sobre seguridad en dispositivos móviles se enfatizaron en caracterizar los sistemas operativos más utilizados en los Smartphone, resaltando las amenazas más comunes a las cuales son expuestos por encontrarse conectados a la red. Se expresa también que la seguridad en los sistemas operativos está garantizada por las modificaciones que se realicen en la configuración que viene por

defecto en los teléfonos inteligentes, para aumentar los niveles de protección de los mismos.

Entre las características que poseen los Smartphone, existen limitaciones de compatibilidad establecidas por los mismos fabricantes de los equipos, lo que a su vez, imposibilita que los sistemas operativos diferentes al suyo puedan ser instalados en los teléfonos inteligentes, logrando de esta manera que sus sistemas operativos sean los más utilizados. Lo mismo sucede con las aplicaciones que, por lo general, deben ser desarrolladas para un equipo en particular, alcanzando así la funcionalidad y el atractivo del teléfono (Bermúdez y López, 2011).

En resumen, todos los estudios anteriormente analizados, presenta un enfoque comparativo entre los diferentes sistemas operativos, indicando sus características y la evolución de los mismos, sus riesgos y amenazas más comunes, sin embargo se ha excluido el análisis de las vulnerabilidad que se presentan inherentes a la configuración de los estándares de seguridad para la protección de la información materia de estudio relevante para la presente investigación.

1.2. Bases teóricas científicas

1.2.1. Sistema Operativo

Prieto (2012), define a los sistemas operativos como:

La capa que se encuentra entre el hardware y las aplicaciones de programas. Es el que gestiona los recursos de hardware del dispositivo y brinda servicios comunes para hacer más fácil la programación de aplicaciones (Prieto, 2012, p.24).

En la actualidad, la complejidad de los S.O. (Sistemas Operativos) de los equipos móviles se ha desarrollado considerablemente. Se han creado sistemas muy simples, a otros similares a los de un ordenador. Este crecimiento ha permitido que su seguridad se

transforme en un requisito fundamental. Pero el conseguir esta seguridad en los S.O. se hace cada vez más difícil.

Al comienzo, cuando los dispositivos móviles no manejaban multimedia ni entretenimiento, los S.O. para móviles eran simples; como aquellos que poseían la función primordial de llamar o enviar mensajes, su sistema operativo en estos casos tenía poca importancia. Pero por ser sistemas limitados en recursos físicos y en funcionalidad, no eran de interés a los atacantes.

Seguridad de los Sistemas Operativos: La rápida evolución de los equipos informáticos y de las telecomunicaciones en los últimos años, ha vuelto más accesible a los sistemas informáticos, incrementado los riesgos relacionados con la seguridad.

El sistema operativo como administrador de los recursos del sistema realiza una función importante en la instrumentación de la seguridad, no encierra a todos los aspectos de la seguridad, y debe ser complementado con medidas externas al sistema operativo (Loor, 2002, p. 31).

Únicamente la seguridad física es insuficiente ante el riesgo de que equipos remotos conectados tengan acceso a la información. Se pretende que los sistemas sean cada vez más fáciles de utilizar, pero esta favorabilidad hacia el usuario ocasiona un aumento en la vulnerabilidad de los sistemas (Morales, Gómez y Camargo, 2016, p. 18).

Se debe identificar cuáles son las amenazas potenciales que afectan a los sistemas operativos, las mismas pueden proceder de fuentes maliciosas así como también de fuentes que aparentan ser confiables. En el Internet existen un sin número de aplicaciones que se promocionan con el propósito de ayudar a mejorar el rendimiento del equipo, pero en muchas ocasiones estas aplicaciones suelen estar infectadas con virus como es el caso de los malware, que facilitan la obtención de datos privados del usuario almacenados en el dispositivo móvil.

Principales ataques a los Sistemas Operativos: Una de las principales amenazas que podrían afectar a un sistema operativo es la causada por errores en el aislamiento de los recursos, esto debido a su diseño, errores en el programa o por alguna configuración errónea de sus servicios.

Un ejemplo que se podría suscitar es el caso de que un proceso podría alterar los parámetros ya verificados el otro proceso, pero que aún este no ha utilizado. Las consecuencias de tal ataque son imprevisibles, debido a que el proceso realizará operaciones empleando parámetros para los cuales no ha sido diseñado. Todas estas vulnerabilidades podrían ser empleadas para ejecutar ataques, ya sea desde los servicios que ofrece el propio sistema operativo como desde la capa de aplicaciones (Fleizach, Liijenstam, Johansson, Volker y Mehes, 2007, p. 37).

Por otra parte, en el Internet también circulan versiones no oficiales de los sistemas operativos para dispositivos móviles, también conocidos como ROM. Estos son copias de versiones oficiales de los sistemas operativos pero personalizados. Además estos ROM pueden contener códigos maliciosos.

1.2.2. Modelo y arquitectura de seguridad de los Sistemas Operativos iOS

iOS ha basado la arquitectura de seguridad en el sistema operativo UNIX, compuesta por componentes como gestores de arranque, procesador criptográfico, sistema operativo con Kernel y sus extensiones, las librerías compartidas y el software del sistema. También, proporciona herramientas de protección en cuatro áreas diferentes: seguridad del dispositivo, seguridad en la información que se almacena y que se transmiten mediante las redes de comunicación y finalmente la seguridad en las aplicaciones que se descargan e instalan.

Su integridad en el proceso de arranque se encuentra protegido a posibles alteraciones, permitiendo la instalación de iOS exclusivamente en dispositivos validados por Apple. Es decir que el sistema es exclusivo de los equipos que pertenecen a esta marca. Los cuales suelen ser más costosos, motivo por el cual a pesar de ser un sistema confiable es menor utilizado que el Android.

Control de acceso y privacidad: Se basa en un mecanismo muy básico de permisos que imponen restricciones en las operaciones que un proceso puede llevar a cabo sobre ciertos elementos. Estos controles han experimentado una evolución en las últimas versiones. Los permisos eran muy limitados, solo posibilitaban la gestión del acceso a la información localizada, las notificaciones push y la integridad con twitter, pero no se disponía de permisos para operaciones críticas tales como: gravar audio empleando el micrófono, o acceder a la cámara.

Security enclave: Consiste en un coprocesador criptográfico que se encarga de procesar los datos biométricos del sensor Touch ID, y verificar si la huella dactilar coincide con una huella previamente registrada, comunicándose a través de un canal interno cifrado empleando una clase de sesión.

Sandbox: establece una política de control de acceso para cada aplicación o proceso a nivel del sistema operativo, restringiendo el acceso a ficheros, preferencias, recursos de red, hardware, etc. El objetivo de sandbox es evitar que las aplicaciones tengan accesos a los datos y recursos de otras aplicaciones o del sistema, por causa de un mal comportamiento de la misma o porque sea vulnerable y posibilite a un hacker o software malicioso la ejecución de código en el dispositivo móvil.

1.2.3. Modelo y arquitectura de seguridad del sistema operativo Android

Android se caracteriza por tener como objetivo el convertirse en el sistema operativo más útil y seguro diseñado para los Smartphone, brindado para tal efecto controles de seguridad en el sistema como protección de la información almacenada por el usuario, protección de los recursos del sistema (incluyendo la red) y proporcionar aislamiento de las aplicaciones.

Para lograr la consecución de estos fines, el sistema operativo Android posee las siguientes características de seguridad que se consideran son las más relevantes:

Seguridad a través del kernel de Linux: Es un tipo de seguridad que Android ofrece desde hace años, se emplea en la seguridad de millones de ambientes sensibles. El kernel de Linux ofrece alternativas de seguridad que trabaja con un modelo basado en permisos,

incluye aislamiento de procesos, posee un sistema de seguridad extensible que permite eliminar partes innecesarias e inseguras.

Mecanismo de seguridad sandbox obligatorio para todas las aplicaciones: Se destaca por que en Linux cada aplicación se ejecuta en un proceso con identificadores particulares de grupo y usuario. Lo que posibilita definir políticas de acceso para cada aplicación de acuerdo a los requerimientos y propósitos. Tales permisos son abalados por el usuario a través de la aceptación del manifiesto.

Partición del sistema y modo seguro: Cuenta con una partición solo de lectura que contiene el kernel de Linux, las librerías, el tiempo de ejecución, el framework de aplicaciones y las aplicaciones. Cuando se inicia en modo seguro, se inicia únicamente la partición del sistema, haciendo disponible únicamente las aplicaciones básicas de Android, lo que garantiza que el usuario inicia su teléfono en un ambiente libre de aplicaciones de terceros y por lo tanto en un modo seguro.

Permiso del sistema de archivos: La utilización de Linux afirma que un usuario no pueda leer ni escribir archivos de otro usuario. Debido a que en Android las aplicaciones se ejecutan como su propio usuario, es decir que una aplicación no tiene la posibilidad de leer ni escribir archivos desarrollados por otra aplicación, con la excepción de que el creador los exponga de forma explícita.

Sistema de cifrado: Android a partir de la versión 3.0 ofreció un cifrado completo de los ficheros. Siendo estos datos cifrados en el núcleo o kernel empleando una clave derivada de la contraseña del usuario y a fin de evitar vulneraciones. Para protección contra ataques de diccionario, Android posee cuenta con reglas de complejidad de contraseña las cuales pueden ser configuradas por el administrador del dispositivo y son ejecutadas por el S.O. (sistema Operativo).

Protección por contraseña: El sistema Operativo Android puede ser programado para que pida una contraseña de usuario antes de permitir el acceso al equipo móvil, esto hace más fácil que se prevenga el uso no autorizado del dispositivo y como se indicó anteriormente la contraseña es utilizada por el algoritmo de encriptación.

Administrador de dispositivo: Android posee una interfaz de programación de aplicaciones (API) para la administración del Smartphone, el mismo que cuenta con funciones a nivel del sistema. Empleando esta API se logra configurar funcionalidades tales como borrar la información de manera remota o restaurar los valores de fábrica, lo que resulta útil cuando se pierde o se roban el equipo.

Mejoras de seguridad en la administración de la memoria: Android incluye características de seguridad que dificultan el aprovechamiento a causa de los problemas comunes generados por la corrupción de memoria. Siendo una de estas características el seleccionar de manera aleatoria los lugares de importancia de la memoria, disminuir problemas de desbordamiento y evitar ejecución de código en la pila y el heap.

Permiso del root en los dispositivos: Si un usuario modifica los permisos del equipo y brinda servicios del root a las aplicaciones, está incrementando el riesgo de seguridad de aplicaciones maliciosas. Sin embargo Android posibilita la configuración de los permisos del root siendo esta una propiedad trascendental para los desarrolladores y para que los usuarios puedan instalar un sistema operativo alternativo.

APIs protegidas: Algunas APIs requieren permisos especiales para poder ser empleadas, estas son: las de acceso a la información personal, el uso de dispositivos de entrada que son sensibles como la cámara el micrófono, GPS y la de metadatos del equipo, que a pesar de ser datos que intrínsecamente no son sensibles, indirectamente podrían develar características del usuario en cuanto a la utilización del dispositivo.

Firma de las aplicaciones: Android solicita la firma del código de la aplicación con el propósito de identificar al autor y responsable de la misma, pero las aplicaciones que se pretendan instalar sin ser firmadas no podrán instalarse. Las firmas se realizan a través de certificados que son verificados en el momento de la instalación **(Sanchez, Acuña, & Sánchez, 2015, págs. 6-7)**.

1.2.4. Modelo y arquitectura de seguridad del sistema operativo Windows Phone

El módulo de seguridad que ofrece Windows Phone permite controlar al accesoal dispositivo, ofrece seguridad en los datos almacenados tanto del usuario como del sistema de archivos y además securiza las conexiones de red e internet. Para conseguir toda esta protección emplea 4 herramientas básicas: Autenticación, autorización, encriptación y repudio.

Las aplicaciones interactúan con el sistema operativo Windows Phone a través de Winsock, que permite identificar las conexiones seguras y las no seguras, Wininet que emplea muchos protocolos seguros siendo uno de ellos DLL de seguridad, API de criptografía, y la API de almacenamiento protegido. Logrando de esta forma establecer un filtro entre las aplicaciones y el kernel del sistema protegiendo al núcleo en todo momento **(Monjo, Febrer, & Sans, 2010, pág. 23)**.

La gran mayoría de los usuarios desean un sistema operativo que permita la recuperación de la información almacenada en el dispositivo y no permita el acceso de la misma al usuario no autorizado, esto en caso de pérdida o robo del equipo. Al respecto Windows Phone ha implementado una contraseña fuerte para evitar este tipo de acceso no deseado. A más de ello si cualquier usuario no autorizado repite muchas veces logins incorrectos el equipo nos hace esperar un tiempo de back – off más largos en cada intento, e incluso se puede llegar a borrar de forma permanente la información del dispositivo de forma remota.

Windows Phone ofrece la encriptación de datos almacenado en la tarjeta de memoria. En el caso de comunicaciones entre dispositivos y el servidor de correo, se emplea SSL con un cifrado de 128 a 256 bits. De igual forma para el acceso no autorizado a la red local, se utiliza un cliente de autentificación flexible SSL, TLS, Exchange ActiveSync, Cerficate-based, RSA SecurID-Protected (Monjo, Febrer, & Sans, 2010, pág. 24).

1.2.5. Vulnerabilidades comunes en software

Las vulnerabilidades son errores de programación cometidos durante el desarrollo de un software que pasan desapercibidos al programador y que Inicialmente no representan un problema desde el punto de vista del usuario final, pero que los cibercriminales son capaces de detectar y que potencialmente permiten realizar un sin número de actividades no deseadas en los sistemas operativos corriendo estos software vulnerables; como acceder al sistema de archivos, alterar el comportamiento normal del sistema y en el caso más grave controlar el dispositivo atacado remotamente.

Pero las vulnerabilidades no solo se manifiestan por errores de programación, en algunos casos el propio diseño de estos programas es la causa de ellas. A veces simplemente no se consideró la validación de un dato o archivo de entrada y que al ser procesado, genera un comportamiento inesperado que termina siendo una vulnerabilidad explotable

A continuación se enlistan y explican a groso modo algunas vulnerabilidades comunes encontradas en los sistemas operativos de los dispositivos móviles modernos.

Desbordamiento de búfer: Sucede cuando un programa no valida el tamaño de los datos de entrada y al superar el tamaño en memoria reservado para ellos, se sobre escribe la dirección de memoria que el procesador utiliza para ejecutar la próxima instrucción del programa, permitiendo a un atacante tomar el control del flujo del mismo y ejecutar código arbitrario

Desbordamiento de entero: En programación existen diferentes tipos de datos para representar valores numéricos enteros y almacenarlos en memoria y éstos tienen un rango de valores posibles limitado. Cuando se trata de almacenar un valor o realizar una operación matemática que excede la capacidad de los tipos de datos, se genera un desbordamiento de entero, que por sí solo no es muy peligroso, pero sí de ese entero depende una operación con memoria, se puede propiciar un desbordamiento de búfer.

Usar después de liberar: En la mayoría de los programas se realizan reservas de memoria en tiempo de ejecución, utilizando datos llamados punteros que referencian a las localidades de memoria reservadas. La vulnerabilidad, usar después de liberar, es el resultado de acceder al contenido de la dirección de memoria reservada después de que ésta ha sido liberada, si un atacante es capaz de escribir datos en dicha localidad, se puede llegar a ejecutar el código arbitrario plantado por el atacante.

Condición de carrera: Esta vulnerabilidad existe cuando el cambio en el orden de dos o más eventos puede causar un cambio de comportamiento en un programa.

Se crea en escenarios donde diferentes procesos acceden a datos compartidos al mismo tiempo; como archivos, bases de datos, memoria, etc. En estas circunstancias un atacante podría insertar código malicioso en regiones compartidas de memoria y en otros casos tomar ventaja de pequeños lapsos de tiempo entre operaciones para interferir con la secuencia en que se éstas se realizan

1.2.6. Mecanismos de prevención ante amenazas

De acuerdo a lo indicado por INTECO (2012):

Todos los recursos y la información que maneja el sistema operativo podrían estar en riesgo. Es por ello fundamental identificar los mecanismos de seguridad que poseen los sistemas operativos para dispositivos móviles; entre los más importantes se encuentran: los privilegios de usuarios, el aislamiento de procesos y las actualizaciones.

Por lo general en los dispositivos móviles todas las aplicaciones se ejecutan con los privilegios de usuario normal, lo que limita los cambios y los desperfectos que el usuario puede causar al sistema. Esto es relevante en el caso de que exista una vulnerabilidad, por cuanto los daños estarían limitados por los privilegios que el usuario posea. Pero como contraparte esto es un limitante para el usuario, debido a que solamente podría realizar las acciones que el Sistema Operativo le permita realizar con los privilegios actuales (Fleizach et al, 2007)

Es importante recalcar que los sistemas operativos móviles emplean una autentificación basada en usuario y contraseña. Razón por la cual se debe cambiar la contraseña con la que viene por defecto.

De igual manera se debe activar solamente los servicios que se necesiten en un momento dado, de esta forma se está evitando posibles ataques a los dispositivo. También se recomienda precaución ante las aplicaciones que se instalan en los equipos. Además es aconsejable cambiar las contraseñas cada cierto periodo de tiempo.

El aislamiento de procesos es una medida de protección que se está implementado en los sistemas operativos móviles, y consiste en limitar los permisos que tiene cada aplicación, aislándola. De esta forma, cada aplicación tendrá un solo acceso a los recursos y no podrá alterar el funcionamiento de ninguna otra (Albarracin, Parra, & Camargo, 2013).

Este aislamiento de procesos, por lo general, se lo implementa utilizando un lenguaje de programación que lo habilite, como java, y haciendo para cada aplicación un usuario nuevo con privilegios bastante restringidos, que les permita únicamente acceder a los recursos a los que haya solicitado el acceso. Como ejemplo, si una aplicación solicita únicamente acceso a la posición mediante el uso del GPS, este no podrá conectarse al Internet. Pero en el caso de que varias aplicaciones compartan un mismo servicio, se debe emplear un sistema de permisos más complejo. La correcta implementación de este aislamiento y el manejo de los recursos compartidos son importantes para que esta medida sea efectiva.

Los sistemas operativos hoy en día disponen de actualizaciones periódicas. En el caso de actualizaciones menores, estas por lo general se dan para solucionar algunos errores detectados en el software y que presentan un riesgo para su seguridad (Prieto, 2012).

En el caso de actualizaciones mayores, se añaden nuevas funcionalidades y mejoran el rendimiento, pero estas actualizaciones realizan grandes cambios en el sistema, a tal punto que algunas veces llevan a cabo un borrado completo del dispositivo.

Por lo expuesto es fundamental antes de realizar una actualización hacer una copia de seguridad de todo el sistema, y en especial de los datos personales, para luego restaurarlos en el nuevo sistema, También es aconsejable hacer respaldos de la información a través de

la creación de una cuenta de correo que permita almacenar información relevante y disponer de ella cada vez que se resetee el equipo a su estado de fábrica.

Es importante mencionar también que los ROM de los sistemas operativos para los dispositivos móviles deben ser descargados de sitios seguros, ya que algunas de estas ROM son personalizadas y pueden contener código malicioso (Prieto, 2012). En concreto estas aplicaciones pueden venir acompañadas de los siguientes ataques: suplantación (spoofing), alteración (tampering), repudio, divulgación de la información, denegación de servicios y elevación de los privilegios.

1.2.7. Dispositivos móviles

La definición de lo que se denomina como «dispositivo móvil incluye una gran variedad de dispositivos. Si bien actualmente esta definición suele relacionarse con los tablets y los smartphones, son muchos los dispositivos que, aún hoy, pueden acogerse a esta definición. Así, los ordenadores portátiles o las Personal Digital Assistants (PDAs), también podría entrar en esta definición.

Para Lagunes (2012), los dispositivos son:

Equipos de tamaño pequeño, cuya característica es poseer capacidades de procesamiento, memoria limitada y una conexión de red permanente o interrumpida; son dispositivos que se han creado con el propósito específico, pero puede llevar a cabo otras funciones más generales.

Otra característica importante de este dispositivo es que son pequeños de tal manera que pueden ser fácilmente transportados y empleados durante su traslado, de forma fácil; de igual manera posee gran capacidad de comunicación, que le permite acceder a la información y a los servicios desde cualquier lugar.

Por lo general se relaciona al dispositivo móvil con los teléfonos celulares, pero en la actualidad existe una gran variedad de estos dispositivos.

1.2.8. Teléfonos Móviles Inteligentes

Los teléfonos celulares se han convertido en un medio innovador que surgió con el propósito de mejorar las comunicaciones entre las personas. Desde su aparición estos dispositivos han evolucionado en cuanto al tamaño, aplicaciones y funciones. La utilización de los teléfonos celulares se ha incrementado con el paso del tiempo, para satisfacer las necesidades de los usuarios y sus exigencias se han desarrollado los llamados dispositivos móviles inteligentes o Smartphone, los cuales se han convertido en la mayor evolución alcanzada por los teléfonos móviles.

Un dispositivo móvil es un equipo electrónico que posibilita a su usuario llevar consigo un objeto de dimensiones pequeñas, que realiza funciones similares a las de un computador personal, y no solo realiza transferencia de voz como los dispositivos de la antigüedad sino que también atrae la atención de los usuarios mediante la navegación por Internet, reproducción de datos multimedia, realizar transferencias bancarias, orientación mediante GPS, descargas de juegos, conexión a redes sociales, etc. (Malave, Beauperthuy, 2011, pp. 79 – 96)

Para Speckmann (2008) "una de las características más relevantes de los dispositivos móviles es su conectividad e interacción con las redes de datos, como es el Internet el mismo que se ha convertido en un elemento fundamental para las comunicaciones".

Pero lo que convierte atractivo a un dispositivo móvil es su sistema operativo que en conjunto con el equipo permiten desarrollar operaciones que posibilitan ejecutar cierta cantidad de procesos que son traducidos en importantes y atractivas aplicaciones, transformándose en dispositivos más competitivos que otros.

Los teléfonos inteligentes o Smartphone cumplen con las siguientes características:

Funcionalidad avanzada: los Smartphones son aquellos teléfonos cuya funcionalidad va más allá de llamar o recibir mensajes SMS. Este tipo de teléfonos son capaces de realizar tareas más complejas como la gestión del correo personal o la reproducción de contenidos multimedia, entre otros.

Hardware especializado: estos dispositivos cuentan con hardware dedicado necesario para la realización de las tareas avanzadas de las que son capaces. De esta manera, este tipo de dispositivos suele contar con chip GPS (Global Positioning System), giroscopio, acelerómetro o procesador gráfico.

Alta capacidad de cómputo: la capacidad de procesamiento de información que poseen estos dispositivos es la que hace posible toda esa funcionalidad avanzada.

Con estas características se puede considera el término Smartphone desde diferentes puntos de vista, es decir desde la evolución natural de distintos dispositivos existentes como desde la descripción de sus capacidades.

1.2.9. Asistentes Digitales Personales (PDA)

Según Guachun (2013), los PDA son agendas electrónicas personales cuya característica principal es la capacidad de almacenamiento de datos, esto debido a la cantidad de memoria que posee para realizar esta función; su principal uso es en el ámbito empresarial, razón por la cual todavía continúa presente en el mercado. Es muy útil debido a su aplicación de información geográfica, paquetes ofimáticos, clientes de correo electrónico, navegadores web entre otros.

1.2.10. Tabletas

Su nombre se deriva del término en inglés Tablet, en la actualidad se han convertido en un gran porcentaje de dispositivos móviles existentes en el mercado, su nombre hace referencia a un computador portátil.

Su característica principal es la integración de pantallas táctiles que proporcionan facilidad de interacción con tan solo el contacto con los dedos. También permite ejecutar aplicaciones populares en el mercado actual. Las principales marcas proveedoras de esta tecnología son Apple y Samsung, que emplean en sus dispositivos los sistemas operativos iOS y Android respectivamente (Mediasmash, 2013).

1.3. Marco Legal

En la Resolución JB-2012-2148 emitida por la Superintendencia de Bancos y Seguros del Ecuador, indica en las medidas de seguridad en canales electrónicos que las instituciones del sistema financiero deben implementar y acoger los estándares y prácticas favorables internacionales de seguridad vigentes a nivel internacional para la utilización de canales electrónicos, los mismos que deben ser constantemente supervisados para asegurar su cumplimiento.

De igual manera se establece los mecanismos para realizar un monitoreo periódico de la efectividad de los niveles de seguridad incorporados en hardware, software, redes y comunicaciones, así como en cualquier otro equipo electrónico o tecnológico empleado en los canales electrónicos, con el fin de garantizar de manera permanente la seguridad y calidad de la información.

La información que se transmite a través de los canales electrónicos y sitios en donde se realice el procesamiento de la entidad, se deberá proteger mediante la implementación de técnicas de encriptación y deberá examinarse regularmente la efectividad y vigencia de la herramienta de encriptación empleada.

Así mismo se establecen mecanismos de monitoreo y control que emitan alarmas en línea oportunas que identifiquen eventos inusuales o de fraude que pueden aparecer en algunos sitios del canal electrónico (Solines, 2012).

Por lo antes expuesto, se indica que dentro de los reglamentos constitucionales y normativos existentes en el Ecuador no se encuentra artículos que regulen o aborden el tema de la seguridad de los sistemas operativos en los dispositivos móviles. Solo especifican la seguridad de la información en los canales electrónicos como lo expresa la resolución emitida por la Superintendencia de Bancos y Seguros del Ecuador.

Sin embargo, dentro de las reformas aplicadas al COIP (Código Orgánico Integral Penal) en su artículo 191 se sanciona con la privación de la libertad de uno a tres años, a las personas que se dediquen a la reprogramación o modificación de información de identificación de equipos terminales móviles.

En la misma ley el artículo 192 expresa que la persona que intercambie comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, se sancionará privándolo de su libertad por el tiempo de 1 a 3 años.

En cuanto al remplazo de identificación de terminales móviles, el artículo 193, indica que el individuo que reemplace las etiquetas de fabricación de los equipos móviles que contienen información de identificación de dichos equipos y coloquen otras etiquetas en su lugar con identificación falsa, será sancionado con la privación de su libertad de 1 a 3 años.

Finalmente, el en artículo 195 se expone la sanción por el caso de la infraestructura ilícita, es decir quien posea programas, equipos, base de datos o etiquetas que permitan la reprogramación, modificación o alteración de información de identificación de un equipo terminal, será privado de su libertad de 1 a 3 años (COIP, 2014, pp.8 -9).

CAPÍTULO II
MATERIALES Y MÉTODOS

2.1. Descripción y caracterización del lugar

La presente investigación se llevó a cabo en la ciudad de Esmeraldas, que está situada en el noroccidente del Ecuador, cuenta con una población 189,504 habitantes de los cuales el 49,02% son hombres y el 50,98% son mujeres (INEC, 2010).

2.2. Métodos y técnicas

La presente investigación se inscribe en el paradigma de la metodología cualitativa. Esto se debe a que mediante un análisis bibliográfico se identificó cuáles son los sistemas operativos más utilizados por los Smartphone, así como también se detallan los mecanismos de seguridad con que cuenta cada sistema.

Así, para realizar este estudio se empleó: en primer lugar, una encuesta (Anexo 1) a usuarios para determinar el grado de conocimiento que tienen con respecto a la seguridad que ofrecen los sistemas operativos en los Smartphone; y, en segundo lugar, se encuestó (Anexo 2) a técnicos especializados para identificar cuáles son las violaciones de seguridad más comunes en los sistemas operativos de los equipos inteligentes y, además, para obtener recomendaciones y proteger los dispositivos móviles de estas amenazas.

Para la aplicación de los instrumentos en el caso de los usuarios se utilizó el método no probabilístico, mientras que para los técnicos se utilizó el método de bola de nieve ya que no se cuenta con registros o estudios que indique el número de técnicos especializados en la configuración y manejo de los Smartphone en la ciudad de Esmeraldas.

Se adquirió información bibliográfica, ya que se estudiaron algunos libros, revistas, artículos, ensayos que posibilitaron conocer más acerca del tema, de esta manera se organizaron los datos, de tal manera que se emplearon de acuerdo a los avances de la

investigación, con el propósito de elaborar un excelente análisis de los objetivos planteados.

2.3. Población y muestra

Para el desarrollo de la presente investigación se ha considerado a 15 técnicos especializados en la configuración de Smartphone, y a usuarios que posean dispositivos móviles inteligentes. Para el último grupo de personas se consideró el censo poblacional realizado en el año 2010 por el INEC el cual establece a la población esmeraldeña con una cantidad de 189504 personas aproximadamente; mientras que a nivel nacional se determinó que el 37,7 % de los ecuatorianos poseen Smartphone, estableciendo una relación entre estos dos valores se obtuvo que en Esmeraldas aproximadamente existen 71443 personas con teléfonos inteligentes (INEC, 2015).

Por ser un universo de grandes dimensiones se procedió aplicar la fórmula que permitió obtener una muestra representativa de la población a encuestar.

$$n = \frac{N\sigma^2 Z^2}{(N-1)e^2 + \sigma^2 Z^2}$$

Donde:
n: Tamaño de la muestra
N: Tamaño de la población (71443)
σ: Desviación estándar de la población 0,5
Z: Niveles de confianza en relación al 95% equivalente a 1,96
e: Límite aceptable de error muestral 7% equivalente a 0,07

Reemplazando valores en la formula se tiene:

$$n = \frac{71443 \cdot 0{,}5^2 \cdot 0{,}09^2}{(71443-1)\cdot 0{,}09^2 + 0{,}5^2 \cdot 1{,}96^2}$$

n= 195 habitantes

Tabla N° 1: Muestra

POBLACIÓN	Nº DE ENCUESTADOS
USUARIOS	195
TECNICOS	15
TOTAL	**210**

Elaborado por la Autora

2.4. Técnicas de procesamiento y análisis

Los datos investigados se tabularon y ordenaron de acuerdo a los indicadores establecidos en cada uno de ellos. En la encuesta se realizaron cuadros de frecuencia y porcentaje que posibilitaron realizar un análisis sobre la vulnerabilidad de los sistemas operativos de los dispositivos móviles con respecto a los estándares de calidad.

De igual forma se emplearon las herramientas informáticas, mediante el uso de programas o recursos como Microsoft Word que permitió desarrollar el informe escrito y Microsoft Excel que se utilizó para la elaboración de cuadros y gráficos estadísticos.

2.5. Normas éticas

Toda la información que contiene el presente estudio es de exclusiva responsabilidad de la autora, es decir que todas las citas e ideas incluidas en el presente análisis se encuentran debidamente referenciadas teniendo en cuenta sus autores y los años de publicación según lo estipula la normativa APA en su séptima edición.

Cabe recalcar también que al momento de realizar las encuestas se mantuvo en el anonimato la identidad de las personas encuestadas ya que la información verdaderamente relevante es su pensamiento y opinión más no su identidad.

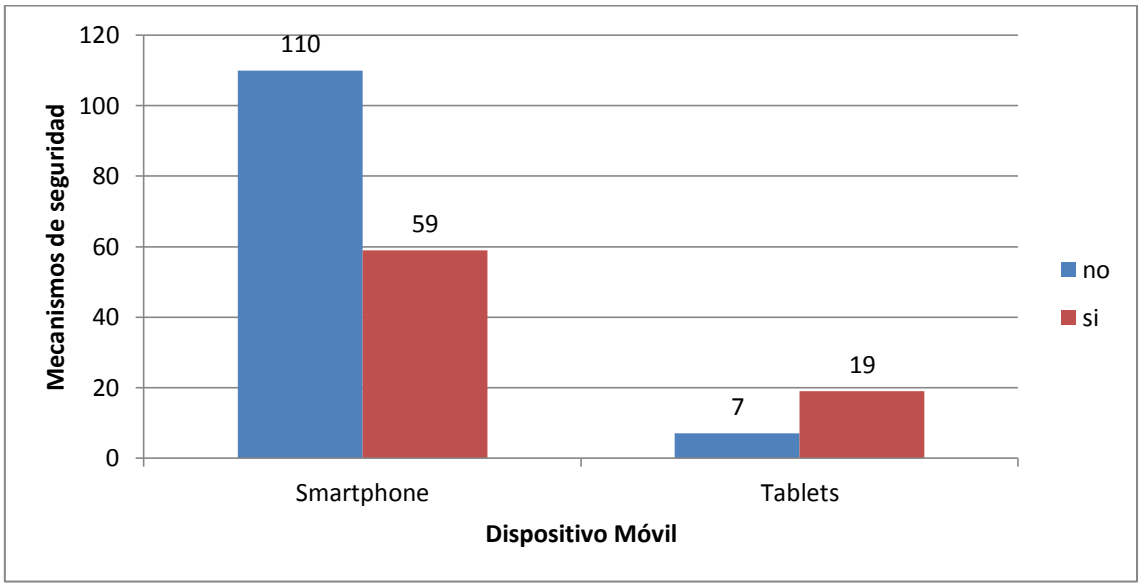
CAPÍTULO III
RESULTADOS

3.1. Análisis e interpretación de resultados.

3.1.1. Encuesta aplicada a la ciudadanía esmeraldeña

El resultado que se reflejan en la figura N° 1, permite evidenciar que la mayoría de los usuarios encuestados sí tienen conocimiento acerca de los mecanismos de seguridad que poseen los sistemas operativos de los dispositivos móviles, sobre todo aquellos ciudadanos que poseen teléfonos inteligentes (Smartphone).

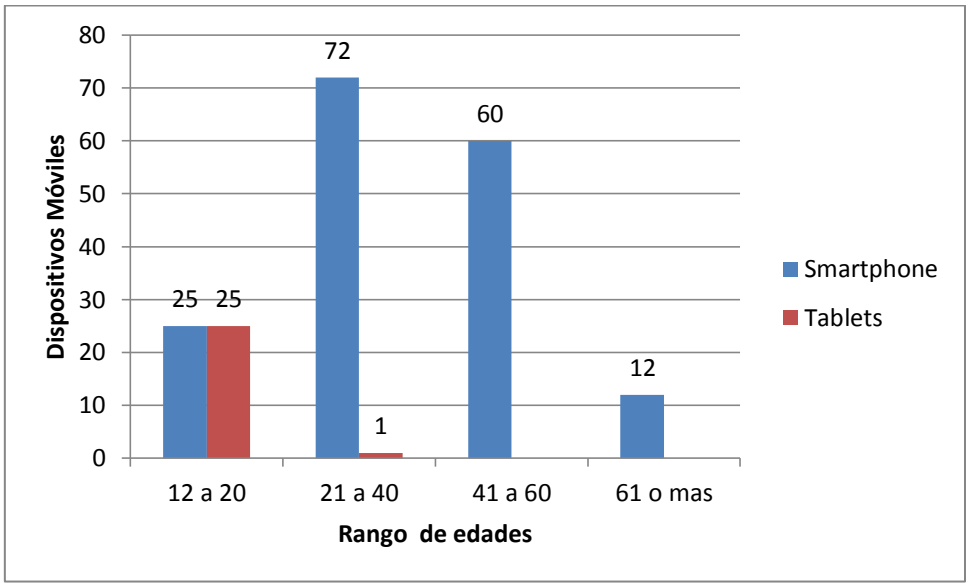
Gráfico N° 1: Conocimiento de mecanismos de seguridad



Fuente: usuarios de la ciudad de Esmeraldas

De acuerdo a los grupos de edades establecidos en la encuesta (Ver Figura Nº 2), se evidencia que la mayor parte de los usuarios tiene preferencia por los Smartphone, sobre todo la población adulta; a diferencia de los adolescentes que por lo general poseen Tablet. Otro grupo de personas son los adultos mayores que en menor porcentaje poseen equipos inteligentes.

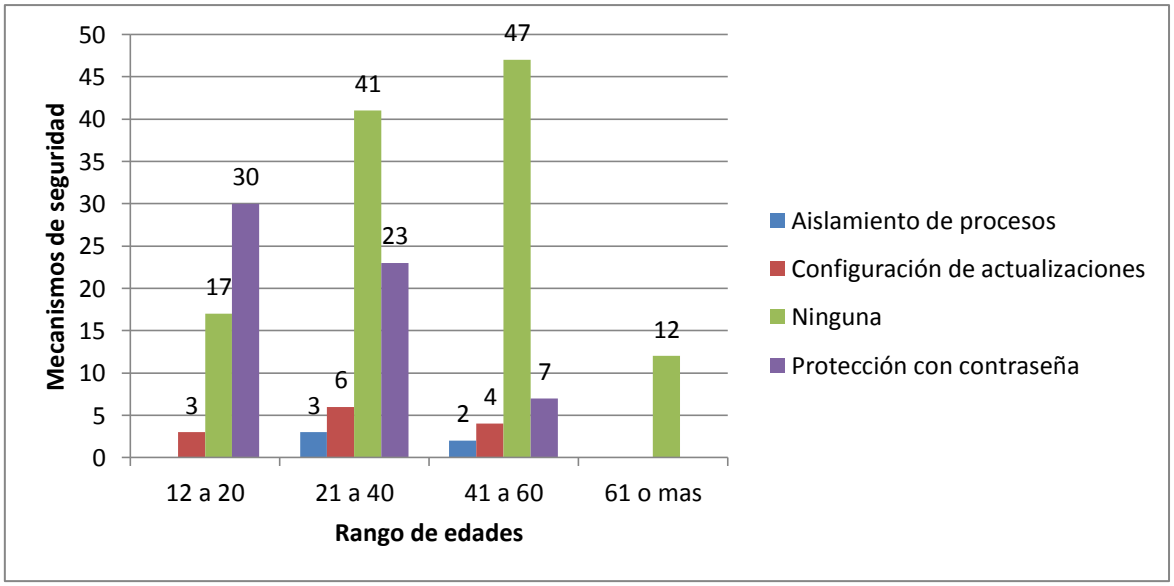
Gráfico N° 2: Dispositivo móvil según las edades



Fuente: usuarios de la ciudad de Esmeraldas

La gran mayoría de la población entre jóvenes y adultos utiliza el mecanismo de protección de contraseña (Ver Figura Nº 3). Mientras que los adultos mayores indican nunca haber configurado algún mecanismo de protección. Sin embargo una pequeña parte de la población encuestada tiene preferencia por los aislamientos de procesos y la configuración de las actualizaciones para una protección más eficaz de sus equipos, sobre todos aquellos que utilizan los canales electrónicos estos últimos mecanismos ofrecen mayor seguridad.

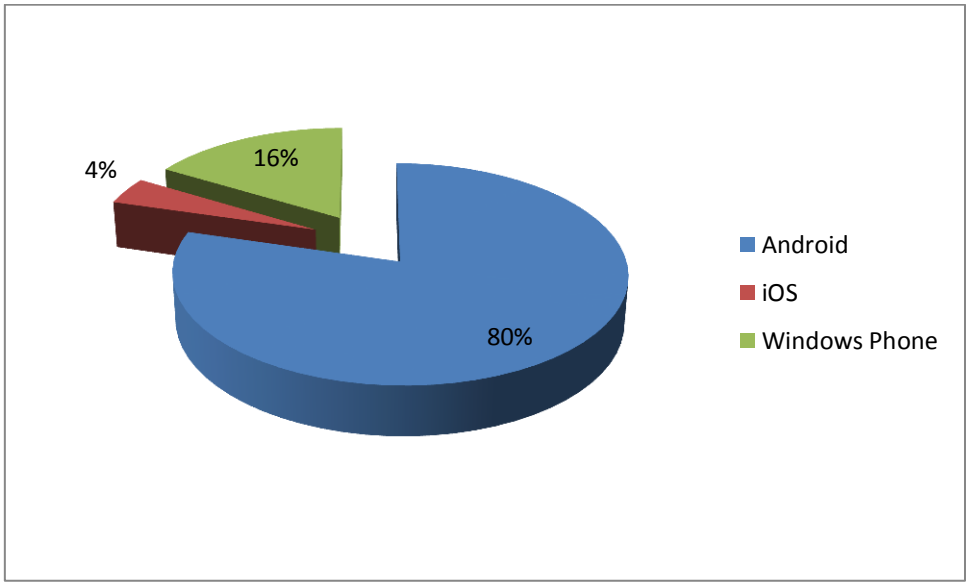
Gráfico N° 3: Mecanismos de seguridad más utilizados según las edades de los usuarios.



Fuente: usuarios de la ciudad de Esmeraldas

Como resultado de la encuesta aplicada se pudo evidenciar que la mayoría de los usuarios poseen equipos con sistema operativo Android. Sin embargo, un grupo reducido tiene preferencia por los equipos con sistema operativo iOS, que se caracterizan por ser más costos pero ofrecen mayores seguridades en cuanto a accesibilidad y protección de la información.(Ver Figura Nº 4)

Gráfico N° 4: Sistema Operativo más utilizado

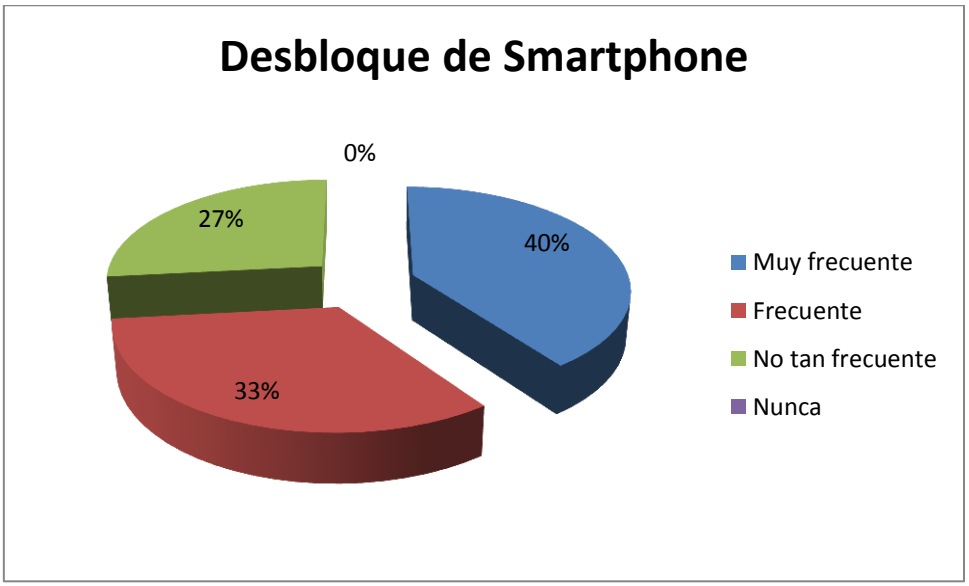


Fuente: usuarios de la ciudad de Esmeraldas

3.1.2. Encuesta aplicada a técnicos de la ciudad de Esmeraldas

En la figura Nº 5, se puede evidenciar que la mayoría de los técnicos especializados en reparación y manejo de los Smartphone indican que muy frecuentemente tienen solicitudes de desbloqueo de este tipo de dispositivos móviles, un menor porcentaje afirman que frecuentemente, mientras que un mínimo porcentaje señala que no tan frecuentemente le han solicitado realizar este tipo de trabajos.

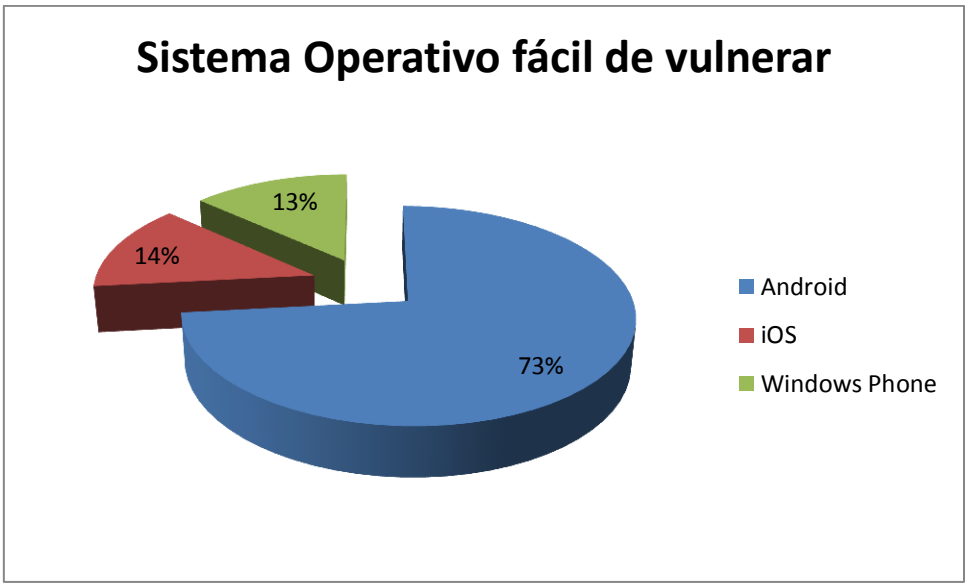
Gráfico N° 5: Desbloqueo de dispositivos Smartphone



Fuente: Técnicos de la ciudad de Esmeraldas

La mayoría de los técnicos encuestados manifiestan que el Sistema Operativo Android es el más fácil de recuperar tanto la información como el equipo en casos de pérdida o robo, un menor porcentaje afirma que es el sistema operativo iOS, finalmente un mínimo porcentaje consideran que es el Windows Phone. Aunque todos los sistemas poseen aplicaciones antirrobo y encriptación de los datos estas opciones de seguridad varían dependiendo el modelo del equipo y la configuración de los mismos.

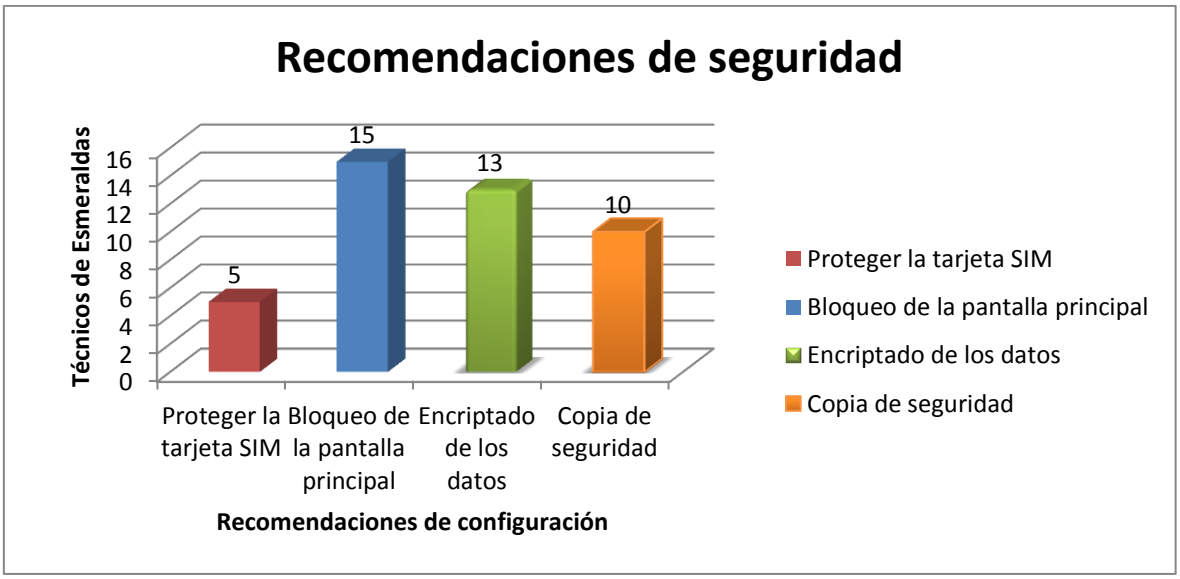
Gráfico N° 6: Sistema Operativo fácil de vulnerar



Fuente: Técnicos de la ciudad de Esmeraldas

De acuerdo a los datos recabados en la encuesta aplicada a los técnicos, se pudo evidenciar que la mayoría considera que es importante el bloque de la pantalla principal del dispositivo móvil, seguido de la encriptación de los datos, también consideran importante hacer copia de seguridad y finalmente la protección de la tarjeta SIM. Todas estas recomendaciones de configuración los técnicos consideran esenciales para poder recuperar el equipo y los datos en caso de robo o pérdida del equipo.

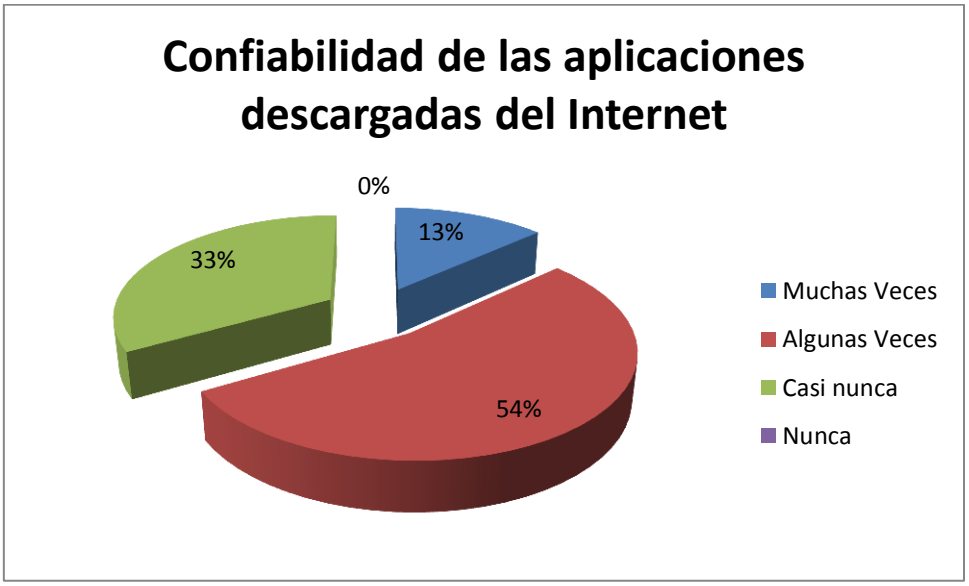
Gráfico N° 7: Recomendaciones de configuración de seguridad



Fuente: Técnicos de la ciudad de Esmeraldas

En la gráfica 8 se puede evidenciar que de la encuesta aplicada a los técnicos especializados en el manejo y configuración de los Smartphone, la mayoría considera que algunas veces son confiables y seguras las aplicaciones que se descargan del Internet, Sin embargo un menor porcentaje considera que casi nunca son confiables, por último un bajo porcentaje consideran que muchas veces son seguras las aplicaciones.

Gráfico N° 8: Confiabilidad de las aplicaciones descargadas del Internet.



Fuente: Técnicos de la ciudad de Esmeraldas

CAPITULO IV
DISCUSIÓN

4.1. Discusión de los resultados

Los resultados obtenidos han demostrado que en su mayoría las personas que poseen equipos móviles inteligentes tienen conocimiento de los mecanismos de seguridad que ofrecen los sistemas operativos de estos dispositivos. Con el avance de estas tecnologías se hace necesario proteger la información que se maneja o almacena en estos medios.

Dentro de los mecanismos de seguridad más empleados por los usuarios de los Smartphone para la protección de la información, se destaca el uso de contraseñas, seguido por la configuración de las actualizaciones y el aislamiento de procesos respectivamente. Sin embargo, existen dispositivos modernos según Siles (2013) que puede incluir opciones de autentificación alternativos como mecanismos biométricos o autentificación por proximidad. Así mismo es posible combinar múltiples factores de autentificación simultánea, aumentado el grado de protección de acceso al equipo.

Gran parte de las aplicaciones maliciosas y de los ataques apuntan al sistema operativo Android (Fabbiani, Sanz y Vidal, 2010). Al respecto existen dos razones fundamentales que conllevan a que esto suceda, la primera es por qué según los resultados de las encuesta aplicadas se destaca que el 80% de los usuarios de dispositivos móviles han elegido Android, convirtiéndose en un mercado más atractivo para quienes desarrollan aplicaciones maliciosas. Además como la seguridad depende de los mecanismos de protección que el usuario utilice, muchas de las fallas pueden ocasionarse por la incorrecta configuración o las malas decisiones.

Finalmente, de la bibliografía revisada (Fabbiani et al., 2010; Morales et al., 2016) podemos indicar que los tres sistemas operativos como Android, iOS, Windows Phone poseen ventajas y desventajas frente a los otros, por lo que es difícil indicar cuál de ellos tiene un mejor sistema de seguridad. Dependiendo de los requerimientos de cada usuario se escoge el que mejor se adapte a sus necesidades.

Uno de los mecanismos de seguridad que más recomiendan los técnicos para protección de los dispositivos móviles es el bloque de la pantalla principal con lo que se garantiza que nadie puede acceder a la información almacena en nuestro teléfono si no dispone de la forma de desbloquearlo. Aunque se debe tener en cuenta que esté método es menos seguro que el establecimiento de un código de acceso.

En el mercado existen diferentes formas de bloque entre ellos tenemos: bloqueo por deslizamiento, movimiento, desbloqueo facial, cara y voz, Patrón, PIN, contraseña, entre otros; los cuales varían dependiendo el sistema operativo y el modelo del equipo Smartphone (Todotech, 2016).

La encriptación delos datos es otro método recomendado por los técnicos para reforzar la seguridad de nuestro teléfono inteligente, este proceso de encriptación es irreversible esto quiere decir que una vez ejecutado para poder quitarlo es necesario restaurar el equipo a su estado inicial, perdiéndose toda la información almacenada en el mismo.

Las aplicaciones que se encuentran en el internet se han convertido hoy en día en otra amenaza para la seguridad de los Smartphone, debido a que es una manera utilizada frecuentemente por los ciber delincuente para camuflar virus bajo la apariencia de programas que simulan ser aplicaciones o juegos. Para no ser víctima de este tipo de amenazas se recomienda descargar las aplicaciones de páginas oficiales como Google Play, Apple Store, Windows Phone, Black BerryWorld. Pero aun así es importante también consultar la información sobre la aplicación antes de descargarla, debido a que a pesar de los esfuerzos que hacen las compañías desarrolladoras de las diferentes plataformas móviles se filtran en ocasiones aplicaciones maliciosas en estos markets.

Por lo antes expuesto la presente investigación resaltar la importancia de cambiar la configuración de fábrica de los equipos Smartphone; además de emplear alguno o varios mecanismos de seguridad a fin de evitar la vulneración del sistema por robo o por el hecho de estar conectado a una red; así mismo es fundamental la instalación de aplicaciones que detecten software maliciosos como es el caso de los antivirus y por último, escoger sitios confiables en la red de los cuales se puedan efectuar descargas de aplicaciones que sean seguras para el equipo.

4.2. Conclusiones

- Al analizar los diferentes sistemas operativos desarrollados para los equipos Smartphone, se ha identificado que todos están expuestos a vulneraciones las cuales por lo general están siendo corregidas por los fabricantes, razón por la cual se han generado una serie de versiones de las mismas aplicaciones, a pesar de todo esto los usuarios deben tener precaución en el manejo de los datos y la información almacenada en los dispositivos con el propósito de evitar posibles daños y pérdida de los mismos.

- Las vulnerabilidades que se presentan en los sistemas operativos de los dispositivos móviles en su mayoría son por la falta de conocimiento de los usuarios que tienen poca precaución al instalar aplicaciones y en las configuraciones de seguridad de los equipos.

- En el mercado existen múltiples aplicaciones que son consideradas herramientas para analizar el sistema operativo, siendo útiles como técnicas de pent-testing, y como analizador de datos almacenado en el dispositivo, busca virus y fallas en archivos del sistema, limpieza de software entre otros servicios que ofrecen, pero estas herramientas pueden tener una procedencia no confiable que mal utilizadas permiten modificar, dañar o filtrar la información del dispositivo.

- En el presente estudio se han analizado los diferentes modelos en las arquitectura de seguridad de los sistemas operativos iOS, Android y Windows Phone; así como también se han analizado sus vulnerabilidades, lo que permitió concluir que cualquier sistema operativo por más avanzado que sea presenta vulnerabilidades; por lo que es necesario tomar medidas preventivas y sensibilizar a los usuarios para ser conscientes sobre el uso seguro de este tipo de equipos móviles.

4.3. Propuesta

4.3.1. Tema

Descripción de un modelado de amenazas existentes en dispositivos inteligentes para la identificación de problemas en el ámbito de la seguridad de los Smartphone.

4.3.2. Justificación

El modelado de amenazas es importante de realizar para abordar el tema de la seguridad en los Smartphone, con el objetivo de conocer a fondo las vulnerabilidades y riesgos que se presentan en esta clase de equipos y así contribuir la adquisición de forma ágil de estos conocimientos.

Para lograr el propósito planteado se analizaron las ventajas que otros modelos similares han aportado a los Smartphone. Luego, se detallaron una serie de amenazas, vulnerabilidades y ataques que se podrían aplicar, a lo que se denominará banco de ataques. Incluyendo puntos vulnerables que se podrían aprovechar en el futuro. Por último se evaluaron los posibles resultados, que permitirán tener una visión más clara de cuáles son los aspectos más débiles de la seguridad de los Smartphone.

4.3.3. Descripción de la propuesta

Para llevar a cabo la propuesta planteada se identificó todos aquellos elementos que forman parte del ámbito de la seguridad en los teléfonos inteligentes. Se empleó una categorización similar al modelado de redes sociales SLAB10, puesto que este se asemeja y se ajusta a las necesidades identificadas.

En el modelado de amenazas, existen 4 elementos importantes sobre los cuáles se desarrollará el modelo como son: los activos, las amenazas, los ataques y las vulnerabilidades. Los cuales se relacionan porque los ataques buscan perjudicar al usuario o a alguno de los activos, que se encuentran comprometidos por distintas amenazas a través de las vulnerabilidades que existen en el sistema operativo.

La finalidad del modelado es evaluar el riesgo de los dispositivos Smartphone identificando las posibles amenazas a las que se encuentra expuesto.

En la presente investigación se estableció una metodología cuantitativa en el modelado de amenazas, clasificando las amenazas de seguridad en relación a la suma de los pesos que tienen los caminos de ataque que son relevantes. Basado en esta idea se empleará un método que facilite clasificar las amenazas en función a la importancia otorgada a cada uno de los activos, para tal efecto se empleará la propagación del peso de cada uno de los elementos por los diversos caminos existentes, siendo estos valores otorgados a cada activo los que debemos tener en cuenta a la hora de evaluar las amenazas.

A continuación, definiremos cómo es el camino, así como las partes que lo componen y la forma de calcular cada uno de los valores en cada una de las etapas.

Definimos el banco de ataques. Este banco está compuesto por todos aquellos accesos, ataques, vulnerabilidades, amenazas y activos identificados en el área en concreto, así como su relación entre los mismos. De esta manera, se define una parte de los valores que se utilizarán más adelante para calcular el valor de cada uno de los elementos dentro del modelado de amenazas.

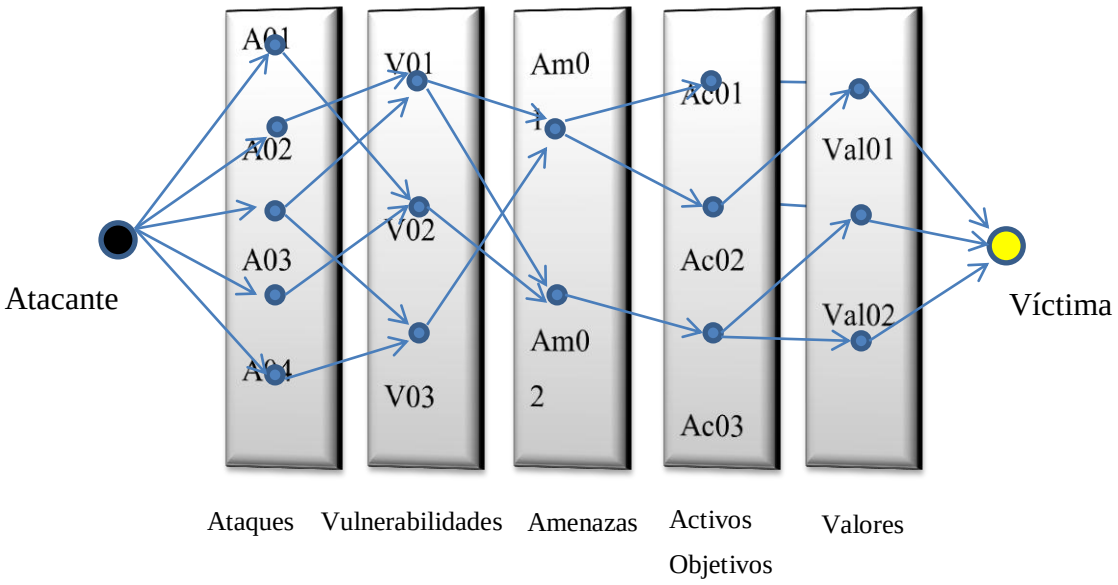
Una vez completado el banco de ataques, se generó el grafo correspondiente, el mismo que estuvo compuesto por todos los elementos definidos anteriormente, también se incluye las relaciones existentes entre los mismos.

Luego, se calcularán los valores de cada uno de los nodos del grafo. Posteriormente, evaluamos la importancia que tiene cada uno de ellos en la propagación de los mismos.

Otorgamos el peso de cada uno de los valores. Durante esta etapa se determina el peso que cada uno de los elementos debe tener en la valoración de cada una de las amenazas. Para ello, el usuario introduce el peso que se le quiere otorgar a cada uno de ellos.

4.3.4. Explicación formal del modelo

Con la utilización de los caminos de ataque se pretende determinar cuáles son las vías por las que el atacante consigue el acceso a la víctima, que vulnerabilidades se explotan y cuál es el impacto en los activos de dichos ataques. Para alcanzar este propósito, se trazan diversos caminos que un atacante puede recorrer para llegar a su víctima, en cada paso el atacante tiene múltiples opciones. Como por ejemplo, el atacante que accede a los datos de un contacto en un Smartphone, puede borrarlos o modificarlos. Cada uno de estos ataques genera un escenario distinto. Mediante esta metodología se busca generar un mapa con los posibles ataques, así como la relación existente entre ellos.



En la representación gráfica se puede observar que partiendo de un nodo atacante, el cual pretende acceder al sistema mediante alguno de los accesos que se encuentra disponibles, se lleva a cabo el ataque, el cual explota algunas vulnerabilidades existentes, estas a su vez son representadas por amenazas concretas a los diversos activos de la víctima del ataque. Así, por ejemplo, se puede ver que el ataque A03 explota dos vulnerabilidades distintas, mientas que el A02 solamente 1. Mediante este modelo, se explota la información obtenida para clasificar las amenazas existentes.

Base de datos con los ataques, amenazas y vulnerabilidades identificadas en los Smartphone.

Como fuente de alimentación de este modelo se proyecta el desarrollo de una base de datos o biblioteca de ataques. En ella se almacenarán una gran cantidad de ataques, amenazas y vulnerabilidades encontradas y a las que se enfrentan este tipo de dispositivos cada día.

En esta sección se identifican todos los activos que hay que proteger, también las amenazas a las que se enfrentan y las vulnerabilidades encontradas. La estructura que se diseñará es agrupando todos los elementos para facilitar la comprensión de los mismos. Las amenazas se clasificarán en tres categorías que se relacionan con las aplicaciones, las redes de comunicaciones y los aspectos físicos de los dispositivos Smartphone.

4.3.5. Análisis del modelo de amenazas

Con el desarrollo de un modelo que posibilitará caracterizar las situaciones de riesgo que se producen sobre los equipos Smartphone. Basado en diversos caminos de ataque que se producen, obteniendo como resultado la clasificación de las amenazas a las que se enfrentan los usuarios que utilizan este tipo de dispositivo móvil.

El modelo a desarrollarse está enfocado en evaluar cuáles son las principales amenazas a las que se enfrentan los Smartphone, haciendo énfasis aquellos aspectos que los usuarios consideran importantes, como por ejemplo la privacidad frente a la disponibilidad. También se pretende reflejar la importancia que tiene las amenazas físicas, tales como el extravío, pérdida o el acceso al mismo por parte de otras personas. Otra parte trascendental es la importancia de los elementos software como es el caso de la modificación de datos del equipo y la transmisión de la información personal sin conocimiento expreso del usuario.

Una falencia del modelo a desarrollarse es la dependencia de la biblioteca de ataques y limitaciones de la misma. Sin embargo esto puede superarse incorporando una herramienta que posibilite a la comunidad alimentar esta biblioteca para de esta manera mejorar los resultados obtenidos. Contribuyendo de esta manera con la sociedad, tanto investigadora como civil a identificar las amenazas a las que se enfrentan a la hora de usar estos dispositivos.

5. REFERENCIAS

5.1. Referencias Bibliográficas

Vulnerabilidad en los sistemas informáticos. (2011). Obtenido de http://inf-tres-quince.blogspot.com/2011/04/vulnerabilidades-de-los-sistemas.html

Albarracin, J., Parra, L., & Camargo, J. (2013). *Seguridad en dispositivos móviles con sistemas operativos Android y iOS.* Colombia: Universidad Pedagógica y Tecnológica de Colombia.

Canalys. (2011). *App stores' direct revenue to exceed $14 billion next year and reach close to $37 billion by 2015*. Obtenido de http://www.canalys.com/newsroom/app-stores-direct-revenue-exceed-

COIP. (2014). *Nuevos delitos incluidos en el Código Orgánico Integral Penal*. Obtenido de http://www.justicia.gob.ec/wp-content/uploads/2014/08/TIPOS-PENALES-COIP.pdf

Fabbiani, E., Sanz, C., & Vidal, S. (2010). *Seguridad en Dispositivos Móviles.* Udelar.

Fleizach, C., Liijenstam, M., Johansson, P., Voelker, G., & Mehes, A. (2007). *"Can You Infect me now? Malware propagation in Mobile Phone Networks.* EE.UU.: ACM Press.

Guachun, A. (11 de Mayo de 2013). *Programas para tu PDA Palm OS*. Obtenido de http://www.pdaexpertos.com/Articulos/Experiencias_de_Usuarios/42-programas-pda-palm-os.shtml

INEC. (2010). *Institu Nacional de Estadísticas y Censo*. Obtenido de http://www.ecuadorencifras.gob.ec//wp-content/descargas/Manu-lateral/Resultados-provinciales/esmeraldas.pdf

INEC. (2015). *Tecnologias de la información y comunicaciones* . Obtenido de http://www.ecuadorencifras.gob.ec//documentos/web-inec/Estadisticas_Sociales/TIC/2015/Presentacion_TIC_2015.pdf

INTENCO. (2012). *Estudio sobre seguridad en dispositivos móviles smartphone.* España.

Kaspersky. (2012). *Seguridad en dispositivos móviles en España*. Obtenido de http://webcache.googleusercontent.com/search?q=cache:CCbX6tJY878J:https://www.inteco.es/file/pEdja0pwhXbAyyRDEuknZg+&cd=1&hl=es&ct=clnk&gl=co.

Lagunes, J. (2012). *Seguridad en dispositivos móviles. Facultad de Contaduría y Administración.* Veracruz: Universidad Veracruzana.

Loor, D. (2002). *Seguridad de los Sistemas Operativos.* Obtenido de http://exa.unne.edu.ar/informatica/SO/SO14.htm#UTTS

Malave, K., & Beauperthuy, J. (2011). *"ANDROID" GOOGLE'S OPERATING SYSTEM FOR MOBILE DEVICES.* Obtenido de www.revistanegotium.org.ve 19 (7)

Mediasmash. (2013). *Qué tipo de dispositivos móviles hay*. Obtenido de http://smash-media.blogspot.com/2012/04/que-tipos-de-dispositivos-moviles-hay.html.

Mendoza, E. (2016). *Permisos de aplicaciones. ¿Hasta dónde llega la seguridad?* Obtenido de https://tabletzona.es/2016/02/10/permisos-de-aplicaciones-hasta-donde-llega-la-seguridad/

Monjo, C., Febrer, L., & Sans, G. (2010). *Arquitectura de Windows CE 6.0.* Obtenido de http://studies.ac.upc.edu/EPSC/PSE/documentos/Trabajos/Archivo/Trabajo_Windows_CE_6.pdf

Morales, Y., Gómez, J., & Camargo, J. (2016). Evaluación comparativa de accesibilidad para sistemas Android, iOS y Windows Phone. *Revista Virtual de la Universidad Catolica del Norte*, 76.

Prieto, M. (2012). *Seguridad en dispositivos móviles.* Universidad Abierta de Catalunya.

Sanchez, D., Acuña, S., & Sánchez, C. (2015). *Estudio al modelo de seguridad de Android y de lo que se ha hecho para mejorarlo*. Obtenido de http://paradigma.uniandes.edu.co/images/sampledata/PARADIGMA/ediciones/Edicion7/Numero1/Articulo1/mendez-sanchez_ed7-1.pdf

Siles, R. (2013). *Seguridad en dispositivos móviles.* España: Nipo.

Siles, R. (2014). Seguridad de dispositivos móviles: iPhone (iOS 7x). https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/13-ccn-stic-455-seguridad-en-iphone/file.html.

Solines, P. (2012). *Superintendencia de Bancos y Seguros del Ecuador.* Obtenido de Resolución JB-2012-2148: http://www.sbs.gob.ec/medios/PORTALDOCS/downloads/normativa/2012/resol_JB-2012-2148.pdf

Todotech. (2016). *Como proteger tu teléfono ante una eventual pérdida*. Obtenido de https://www.todotech.com/android/apps/como-proteger-telefono-perdida_r75.html

5.2. Anexos.

PONTIFICA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE EN ESMERALDAS

ENCUESTA DIRIGIDA A LA POBLACIÒN ESMERALDEÑAQUE POSEE ALGUN TIPO DE DISPOSITIVO MOVIL

Por medio de la presente me dirijo a usted respetuosamente con la finalidad de solicitar su colaboración para responder la siguiente encuesta que es un requisito fundamental para realizar la investigación cuyo tema es "ESTUDIO DE LAS VULNERABILIDADES DE LOS SISTEMAS OPERATIVOS DE LOS SMARTPHONE BASADOS EN ESTÀNDARES DE SEGURIDAD"

Instrucciones:

Lea detenidamente cada pregunta y seleccione la categoría que más se ajusta a su opinión marcándola con una (X).

1. **¿A qué rango de edad de edad pertenece usted?**
   (12 – 20) _____
   (21 – 40) _____
   (41 – 60) _____
   (61 o más) _____

2. **¿Qué tipo de dispositivo móvil posee usted?**

Teléfonos móviles inteligentes.	**( )**
Asistentes Digitales Personales (PDA)	( )
Tablets	( )

3. **¿Cuál es el Sistema Operativo qué posee su dispositivo Móvil?**

   Android ( )

   iOS (iPhone) ( )

   RIM (Blackberry) ( )

   Symbian ( )

   Windows Phone ( )

4. **Actualmente los sistemas operativos de los dispositivos móviles poseen mecanismos de seguridad, ¿conoce alguno de ellos?**

   Si ( )

   No ( )

5. **¿Qué mecanismo de seguridad ha configurado en el sistema operativo de su dispositivo móvil para la protección del mismo?**

   Protección con contraseña o patrón de bloqueo ( )

   Aislamiento de Procesos. ( )

   Configuración de las actualizaciones. ( )

   Ninguna. ( )

PONTIFICA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE EN ESMERALDAS

ENCUESTA DIRIGIDA A TÉCNICOS LOCALES ESPECIALIZADOS EN CONFIGURACIÓN, MANEJO Y REPARACIÓN DE SMARTPHONE

Por medio de la presente me dirijo a usted respetuosamente con la finalidad de solicitar su colaboración para responder la siguiente encuesta que es un requisito fundamental para realizar la investigación cuyo tema es "ESTUDIO DE LAS VULNERABILIDADES DE LOS SISTEMAS OPERATIVOS DE LOS SMARTPHONE BASADOS EN ESTÀNDARES DE SEGURIDAD"

Instrucciones:

Lea detenidamente cada pregunta y seleccione la categoría que más se ajusta a su opinión marcándola con una (X).

1. **¿Algún usuario le ha solicitado desbloquear un Smartphone cuya seguridad se encuentra activada y no se posee clave alguna?**
   Muy frecuente…….
   Frecuente……
   No tan frecuente……
   Nunca…….

2. **¿En cuál de los sistemas operativos considera que es más fácil recuperar el dispositivo o la información almacenada en él?**
   Android……
   iOS……
   Windows Phone……..

3. **¿Cuáles son sus recomendaciones en cuanto a la configuración de la seguridad en los sistemas operativos de los Smartphone a fin de evitar se violente o se pierda la información?**

   ……

   ……

   …….

4. **Existen aplicaciones en el Internet que se promocionan como software seguros para garantizar la protección de los Smartphone ¿Considera que estas aplicaciones son eficaces y confiables?**

   Muchas veces……..

   Algunas veces…….

   Casi nunca…….

   Nunca…….