UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN SISTEMAS
Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

TRABAJO DE INVESTIGACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS

Estudio de seguridad lógica informática aplicada en dispositivos móviles para la protección de sus datos.

LOOR CAMPOSANO ANGÉLICA ESTEFANÍA

AUTORA

A.S. MARÍA SORAIDA ZAMBRANO QUIROZ, MSc.

TUTORA

EL CARMEN, ENERO DEL 2020

UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ
EXTENSIÓN EN EL CARMEN

DECLARACIÓN DE AUTORÍA

Yo, **Angélica Estefanía Loor Camposano**, con número de cédula **131442684-0**, estudiante de la carrera de Ingeniería en Sistemas de la Universidad Laica Eloy Alfaro de Manabí extensión El Carmen, en calidad de autora del presente Trabajo de Titulación del periodo 2019(1)-2019(2), declara que asume la originalidad de dicho trabajo cuyo tema es: "**ESTUDIO DE SEGURIDAD LÓGICA INFORMÁTICA APLICADA EN DISPOSITIVOS MÓVILES PARA LA PROTECCIÓN DE SUS DATOS**" entendido en el sentido que no ha utilizado fuente sin citarlas previamente.

Además, cedo los derechos a la Universidad Laica Eloy Alfaro de Manabí en extensión El Carmen con fines académicos.

_____

Angélica Estefanía Loor Camposano

CI. 131442684-0

CERTIFICADO DEL TUTOR

Uleam	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A).	CÓDIGO: PAT-01-F-010
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO.	REVISIÓN: 1 Página 1 de 1

CERTIFICACIÓN

En calidad de docente tutor(a) de la Extensión El Carmen, de la Universidad Laica "Eloy Alfaro" de Manabí, certifico:

Haber dirigido y revisado el trabajo de titulación, cumpliendo el total de 400 horas, bajo la modalidad de proyecto de investigación, cuyo tema del proyecto es **"Estudio de Seguridad Lógica Informática aplicada en Dispositivos Móviles para la protección de los datos"**, el mismo que ha sido desarrollado de acuerdo a los lineamientos internos de la modalidad en mención y en apego al cumplimiento de los requisitos exigidos por el Reglamento de Régimen Académico, por tal motivo CERTIFICO, que el mencionado proyecto reúne los méritos académicos, científicos y formales, suficientes para ser sometido a la evaluación del tribunal de titulación que designe la autoridad competente.

La autoría del tema desarrollado, corresponde al señor/señora/señorita LOOR CAMPOSANO ANGÉLICA ESTEFANÍA, estudiante de la carrera de Ingeniería en Sistemas, período académico 2019-2020(2), quien se encuentra apto para la sustentación de su trabajo de titulación.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

El Carmen, 10 de enero del 2020.

Lo certifico,

A.S. María Soraida Zambrano Quiroz, Mg.
Docente Tutor(a)
Área: Sistemas

UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ
EXTENSIÓN EN EL CARMEN
CARRERA DE INGENIERÍA EN SISTEMAS
Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

APROBACIÓN DE PROYECTO DE INVESTIGACIÓN

Los miembros del tribunal examinador han aprobado el informe del proyecto de investigación con el tema. **ESTUDIO DE SEGURIDAD LÓGICA INFORMÁTICA APLICADA EN DISPOSITIVOS MÓVILES PARA LA PROTECCIÓN DE SUS DATOS**, con autoría de Loor Camposano Angélica Estefanía, estudiante de la carrera de Ingeniería en Sistemas.

El Carmen, 20 de febrero del 2020

Ing. Rocío Mendoza, Mg

Ing. Patricio Quiroz, Mg

Ing. René García

DEDICATORIA

El presente trabajo está dedicado a mi familia que me han apoyado moral y económicamente, mi madre que me apoyado mucho y ha estado para mí en todo momento, mi padre brindándome sus consejos y apoyo para continuar sin rendirme, mis hermanas que me han acompañado en este camino, mis maestros que me han brindado muchos conocimientos académicos para mi formación y mis compañeros que de alguna u otra manera me han apoyado.

Angélica

AGRADECIMIENTO

Agradezco a todos los que han estado conmigo en estos años, en especial a la Universidad Laica Eloy Alfaro de Manabí Extensión en EL Carmen, por haberme permitido formarme como profesional y haberme brindado los conocimientos para mi formación.

También a los maestros por haberme enseñado tanto con su excelente manera de expresar sus conocimientos y experiencias para que aprendiera mucho de ellos desde el principio de mis estudios.

Autora

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de investigación trató un estudio de seguridad lógica informática en dispositivos móviles para la protección de los datos, la población que se tomó en consideración fueron 74 docentes de la universidad Laica “Eloy Alfaro” de Manabí Extensión en El Carmen, de los cuales para el presente estudio se tomó una muestra discrecional de 18 docentes de la carrera de Ingeniería de Sistemas y Tecnologías de la Información. Los métodos utilizados para la recolección e interpretación de la información en esta investigación fueron el análisis que es utilizado para recolectar la información y saber cómo avanza la tecnología, y los métodos de protección de datos, también está la inducción-deducción que es empleado en las tabulaciones e interpretaciones de los datos recogidos para formular un estudio de lo ya existente para encontrar nuevos métodos de seguridad y demostrarlos teóricamente. También se constató la falta de información para los usuarios acerca la protección que brindan las aplicaciones de seguridad y el dispositivo, se recopilo información acerca de que pocas de las personas encuestadas tienen cierto conocimiento de seguridad en dispositivos y la mayoría no lo tiene, esto indica que existe una problemática, analizando cualitativamente que la seguridad lógica no está siendo usada adecuadamente para proteger la información.

SUMMARY

The present research paper dealt with a study of computer logic security in mobile devices for data protection, the population that was taken into consideration were 74 teachers from the Laica “Eloy Alfaro” University of Manabí Extension in El Carmen, of which For the present study, a discretionary sample of 18 teachers from the Systems and Information Technology Engineering degree was taken. The methods used for the collection and interpretation of the information in this investigation were the analysis that is used to collect the information and know how the technology advances, and the data protection methods, there is also the induction-deduction that is used in the tabulations and interpretations of the data collected to formulate a study of what already exists to find new security methods and demonstrate them theoretically. There was also a lack of information for users about the protection provided by security applications and the device, information was collected about the fact that few of the people surveyed have some knowledge of security in devices and most do not have it, this indicates that there is a problem, qualitatively analyzing that logical security is not being used properly to protect information.

INTRODUCCIÓN

En el mundo actualmente hay muchas personas que cuentan con un dispositivo que contiene información la cual hay que proteger, la seguridad informática es la encargada de hacer esta protección. Es la rama en la que se utilizan varias herramientas de protección contras malware, virus, robos, etc. También previene y detecta el mal uso de la información.

La seguridad lógica está dentro de la seguridad informática, esta es la que se encarga de la protección del software. Se asegura que la conexión a las redes sea segura para la información, con un conjunto de medidas de protección como las contraseñas, también garantiza que solo la persona autorizada tenga acceso a la información con políticas de privacidad.

Se cerciora de garantizar la integridad de los datos, que estos estén disponibles para la persona autorizada en el sistema del dispositivo sin que éste sea rechazado de alguna manera, también se asegura de que sólo el usuario autorizado tenga acceso a la manipulación de la información y que sea de una manera confidencial.

En este estudio se tomó en cuenta la problemática que es la poca importancia de parte de los usuarios para proteger su información, para ello se consideró el área de sistemas porque se relaciona con la investigación. Se utilizó metodología de investigación, tales como la población y muestra también las técnicas para recolectar los datos y así dar uso de toda la información en conjunto con herramientas que va a permitir obtener información de las personas que usan dispositivos Smartphone y aplicaciones de seguridad.

Un manual de usuario es para que las personas que tienen conocimientos básicos y avanzados de como resguardar su información teniendo en cuenta ciertos principios de seguridad para sus datos que estarán aquí registrados. También estará detallado el cómo activar la seguridad en su dispositivo de modo que este lo más protegido posible y así no tenga perdida o fuga de información.

CAPÍTULO I

1 MARCO TEÓRICO

1.1 Principios de la seguridad lógica informática

La mayoría de los daños que reciben los sistemas informáticos es contra los datos; la información es lo más importante, y por esto existen técnicas para protegerla. Las técnicas para proteger los datos, consisten en aplicaciones de barreras para resguardar la información, y dar acceso a las personas autorizadas. También es importante recalcar que la mayoría de los daños se dan más al software (sistemas) que al hardware (medios físicos), porque ésta es la más importante para los delincuentes informáticos, los dispositivos tienen mucha información almacenada también la procesan a diario con cada acción que realizan. Así como la seguridad lógica es importante para proteger la información, también lo es la seguridad física que es la responsable de proteger los equipos informáticos. Se deben tener en cuenta mucho las técnicas de seguridad que hoy en día existen, más allá de la seguridad física, ya que con el paso del tiempo se actualizan para mayor seguridad de los datos. (Costas, 2014)

La seguridad lógica es un conjunto de medidas de protección de datos y aplicaciones informáticas; consiste en aplicar barreras y procedimientos para resguardar el acceso a los datos, garantizando el paso a la información únicamente a las personas autorizadas en el dispositivo. (Escrivá, 2013)

1.1.1 Se deben plantear objetivos tales como:

- La restricción desde el BIOS, al sistema, programas y archivos.
- Asegurar que los usuarios puedan trabajar sin una supervisión y que no puedan modificar los programas ni los archivos que no correspondan a su cargo.

- Asegurar que se estén utilizando los datos, archivos y programas correctamente también actualizando periódicamente los mismos. (Costas, 2014)

1.2 Controles de acceso

Este tipo de controles se hacen en el BIOS o en cualquier otro de los sistemas de las aplicaciones del equipo. Este control es muy importante para la protección de los sistemas operativos de la red y de todos los sistemas que se utilizan o modifican de un modo no autorizado para resguardar la información. También es conveniente tener en cuenta todas las consideraciones posibles para la seguridad lógica, como puede ser el acceso a los datos. Hay varias técnicas para la autenticación de los usuarios una de las más utilizadas son los servidores de autenticación este hace una identificación y autenticación de todos los usuarios de cada equipo en una organización. Estos servidores son independientes y son de acuerdo a los equipos que se utilizan en las organizaciones. Hay diferentes tipos de ataques que son comunes en la actualidad como son los ataques de fuerza bruta que estos son los que intentan recuperar las contraseñas haciendo comprobaciones con todas las posibles; también está el ataque de diccionario este se basa en comprobar una contraseña con todas las palabras de un diccionario ya que las personas usan palabras comunes. (Costas, 2014)

1.2.1 Identificación y autenticación.

La identificación y autenticación es la primera línea de defensa de los sistemas computarizados, ya que con esto se pueden prevenir los ingresos no permitidos de personas no autorizadas. El control de los accesos son la base de los controles de acceso y el seguimiento de las actividades de las personas en los dispositivos. (Costas, 2014)

1.2.2 Limitaciones a los servicios

La limitación se refiere a restricción de controles del uso de las aplicaciones o los servicios del sistema. Podría ser se dispongan licencias a los usuarios de una organización para permitir el uso de ciertos sistemas a ciertos usuarios, es decir, aun cierta cantidad de personas dentro de la organización. (Costas, 2014) & (Lescano & Elisa, 2017)

1.2.3 Roles

Mediante esta función también se puede controlar el acceso a la información, considerando la función que se requiera. Algunos de los ejemplos de roles serian: programador, líder de proyecto, operador, jefe de área de usuario, etc. Los derechos y los recursos se restringen de acuerdo a los roles, ya que cambiar de rol implica salir del sistema. el uso de los roles es una manera de implementar control de acceso. (Costas, 2014) & (Lescano & Elisa, 2017)

1.2.4 Modalidad de acceso

Aparte de considerar cuando se permite un acceso, también se debe tener en cuenta el tipo de acceso que se permite es por esto que la modalidad de acceso permite al usuario el acceso a la información con algunos de los siguientes modos:

- **Lectura:** que permite leer o visualizar la información.
- **Escritura**: permite agregar datos, modificar y borrar también.
- **Ejecución:** da acceso al usuario de ejecutar programas.
- **Borrado:** permite borrar recursos del sistema, también es considerado una forma de modificación. (Costas, 2014) & (Lescano & Elisa, 2017)

También existen otras modalidades como: creación y búsqueda. Estos criterios pueden ser usados de manera conjunta.

1.2.5 Ubicación y horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. permite establecer tipos de control de horarios que puede ser a determinadas horas del día (horario de oficina), así como a determinados días de la semana, de esta forma el control es más restringido. (Costas, 2014) & (Lescano & Elisa, 2017)

1.2.6 Control de acceso interno

Este determina lo que el usuario puede hacer con los recursos del sistema, a continuación, se mencionan cinco métodos de control de acceso interno:

- **Palabra clave:** Está asociada con la autenticación del usuario y sirve para proteger datos.
- **Encriptación:** la información encriptada solo puede ser desencriptada por quien tenga la clave.
- **Lista de control de acceso**: para ver a que usuario no se le permite el acceso.
- **Limite sobre la interface de usuario:** va en conjunto con listas de control de acceso, estos límites restringen a los usuarios a funciones específicas.
- **Etiquetas de seguridad**: una forma efectiva de control de acceso, se usan para varios propósitos. (Costas, 2014) & (Lescano & Elisa, 2017)

1.3 Política Screen-look (Bloqueo de Pantalla)

Una de las caracteristicas comunes de los dispositivos es la capacidad de configurar un bloqueo de pantalla ya sea un PIN, patrón, contraseñas o biometrías para aumentar la seguridad, así como la privacidad de los usuarios con mecanismos de autenticación para evitar ataques directos a la información del dispositivo. Generalmente las diferentes plataformas contienen métodos de bloqueos de pantalla de esta manera el usuario escoge cual desea usar. Una política de bloqueo de pantalla no debe ser demasiado simples o fáciles de predecir, está configurada para definir el nivel de longitud de las contraseñas implementando entropía. La

entropía mide la seguridad y la resistencia de la contraseña contra ataques de la fuerza bruta. (Pacheco, Piazza Orlando , & Carlos , 2016)

1.4 Sistemas de autenticación biométricos en la seguridad lógica

Los sistemas biométricos están bien vistos en la actualidad y se proyectan como los favoritos para la protección de datos en el futuro, facilitan mucho al ingresar al sistema y la seguridad, aunque todavía tiene algunas limitaciones. Consiste en la verificación de la identidad de una persona, basándose en los elementos morfológicos que son esenciales y que solo se dan en esa persona. Se puede decir que se recopila información acerca de un rasgo distintivo de esa persona como la voz, las huellas dactilares, el iris del ojo, y más. Esto es para hacer comparaciones de las personas y ver su autenticidad dentro del sistema. Hay algunos pasos para poder evaluar los sistemas biométricos, como las tazas de falso rechazo esto muestra a las personas que son rechazas por el sistema biométrico activado, también están los falsos positivos que son aceptados de forma incorrecta por el sistema de seguridad biométrico. Estas fases están relacionadas es por ello que a la hora de diseñar el sistema hay que tenerlas muy en cuenta y que ambas estén comprometidas. Luego está la taza de error de cruce que se trata de verificar la fiabilidad del sistema. (Gómez, 2014)

1.5 Verificación de contraseñas

Este es el mecanismo más usado para identificar a los usuarios basándose en los nombres y contraseñas que las personas utilizan. Cada persona utiliza un usuario que le es asignado con el cual viene asociada su determinada contraseña para la verificación de este usuario, así como su respectiva autenticación, para verificar la autenticación de la contraseña. Con esto a cada usuario se le asigna un nombre o una identificación, esto tiene asociada una contraseña como ya se había mencionado antes y esta debe ser autentica y confidencial. Existen ciertas políticas para que una contraseña se defina como segura; así como el tamaño para que se componga, es recomendable un mínimo de 6 caracteres. La autenticación basada en contraseñas es un mecanismo ampliamente extendido, soportado por prácticamente todos los sistemas del mercado. Por otra parte, se tendría que

cambiar todas las contraseñas por defectos de los sistemas y se procede a la desactivación de las cuentas genéricas. (Vieites, 2017)

1.6 Gestores de contraseñas

En los últimos años se ha propagado mucho el uso de las contraseñas en los sistemas y en el servicio de internet, es por ello que los usuarios deben recordar todas las contraseñas que utilizan a diario para todos los servicios (correos, usuarios a distintos sitios webs, pin de tarjetas de crédito, contraseña de los celulares, computadores, acceso a la oficina, etc.) por esto se recomienda usar distintas contraseñas para cada servicio. Los gestores de contraseñas son aplicaciones para resguardar la identificación de un usuario y su contraseña en una base de datos, así simplifica el manejo de estas y también mejora la seguridad. El trabajo de estas aplicaciones es guardar los usuarios en forma cifrada, de esta manera no son vistas por intrusos, también se incorporan generadores de contraseñas complejas sin la necesidad de que el usuario tenga que memorizarlas. Aquí se encuentran unos cuantos ejemplos de gestores de contraseñas disponibles en la web, tales como: Password Safe, SplashID, PasswordVault, Just1Key, Aurora Password Manager, Handy Password, Keepass Password Safe, etc. Es una pequeña lista ya que éstos son los más conocidos. (Vieites, 2017)

1.7 Identificación de los usuarios remotos

Este tipo de identificación es mucho más compleja porque su proceso de autenticación tiene que ser realizado mediante redes inseguras por esta misma razón es más complejo. Por esto que se han propuesto algunos protocolos de autenticación de acceso remotos que se emplearon inicialmente en conexiones basadas en accesos telefónicos o un módem, pero en la actualidad este tipo de protocolos se los utiliza en lo que son conexiones de redes locales inalámbricas. Para este tipo de conexión existen algunos protocolos de autenticación de acceso remotos. Los principales protocolos de autenticación de acceso remoto son los siguientes:

- **PAP** (Password Authentication Protocol RFC 1334): Este no es muy robusto, ya que la contraseña es enviada a través de la red.
- **CHAP** (Challenge Handshake Authentication Protocol, RFC 1994): Es de autenticación tipo desafío/respuesta, con este protocolo no es necesario enviar la contraseña ya que es de tipo secreto compartido, es por ello que utiliza algoritmo de digestión MD4.
- **EAP** (Extensible Authentication Protocol, RFC 2284): es de tipo capa superior que facilita también la autenticación mutua, utiliza distintos tipos de algoritmos de autenticación. para el proceso de autenticación tiene como respuesta cuatro tipos de mensajes que intervienen en el proceso, que son: request, response, success y failure. (Vieites, 2017)

1.7.1 Servidores de autenticación

Para no implantar protocolos de seguridad en los servidores de red, se puede utilizar un servidor de autenticación centralizado en todo el sistema informático, así como en la red. Este ofrece un servicio de autenticación mutuo tanto para el servidor como para el usuario. para poner en marcha este servidor se puede utilizar sistemas basados en criptografía. (Vieites, 2017)

1.8 La seguridad lógica en las redes

En la actualidad existen varias formas de atacar los dispositivos ya sea por la red, internet (que es el medio más común de hoy en día), de forma directa que es instalando virus o robando información de forma manual; estas son solo algunas de las formas de robar o suplantar información en los equipos. (Baca, 2016)

1.8.1 Suplantación de la dirección ip.

La suplantación es una de las técnicas para robar información, esta consiste en enviar paquetes de una dirección ip a otra enviando información maligna de forma anónima. Pero también existen formas de proteger estos paquetes enviados de una dirección ip a otra, por ejemplo, está el proxi que este protege las direcciones ip de los equipos dando la posibilidad de ocultar las direcciones ip. La otra forma de

proteger es el firewall, éste no puede interpretar los paquetes enviados, los deja pasar por la identificación de la ip, éste solo rechaza los que no están autorizados por el equipo. Para suplantar una ip se modifica desde el origen, para que parezca que el paquete provenga de otra dirección ip. (Baca, 2016)

La vía de ataque más común es por internet, pero este tipo de ataque utiliza protocolos TCP por esto es que parecen confiables y se abren los archivos, aunque se pueden identificar por los datagramas que se generan. (Baca, 2016) afirma: “En el formato de un datagrama, la suplantación de la dirección IP implica modificar el campo Dirección IP origen, para simular que el paquete proviene de otra dirección IP. Los datagramas IP agrupan paquetes TCP llamados segmentos, que tienen dentro de su formato un número de acuse de recibo, de modo que antes de aceptar un paquete, el receptor del datagrama, genera el número de acuse de recibo enviado por la computadora que envía el paquete” (p.154)

1.9 Políticas de seguridad.

Cuándo se implanta un sistema de seguridad también hay que aplicar políticas de seguridad complementadas a la seguridad. Estas requieren de mucha información de la empresa a la que se aplicaran, tales como: amenazas, recursos, origen de la información. De nada sirve proteger los equipos de amenazas externas (virus), si también existen internas (aplicaciones. (Velazco, 2018) nos dice que: “La política de seguridad es "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos". Los documentos de una política de seguridad deben ajustarse y mejorarse continuamente según los cambios que se presentan en los ambientes donde se crearon.” (p. 4). Las políticas de seguridad son creadas para preservar la información y los sistemas de una empresa, garantizando así la integridad, confidencialidad y disponibilidad de la información.

Entre los documentos que pueden citarse son los siguientes:

- Copias de respaldo
- Software legal

- Uso del servicio de Internet y del correo electrónico
- Seguridad en las comunicaciones
- Protección física
- Sanciones por incumplimientos. (Velazco, 2018)

1.10 Herramientas para la realización de las copias de seguridad

Las copias de seguridad son fundamentales en los sistemas, también existen herramientas preinstaladas en los propios sistemas operativos de los equipos, así como existen aplicaciones específicas para realizar las copias de seguridad; las opciones para analizar son las siguientes:

- **Compresión:** es el método para disminuir el espacio de almacenamiento.
- **Duplicación:** se puede realizar un duplicado en un soporte diferente o extraíble como un USB.
- **Cifrado:** ayuda a que la información no se pierda o sea robada, aunque es un proceso que consume mucho tiempo y baja la velocidad.
- **Nombre del archivo**: suele incluir el tipo de copia, la fecha de los datos o la carpeta que contiene. (Costas, 2014)

1.11 Amenazas lógicas

Para evitar amenazas posibles es importante que se tenga especial conocimiento y conciencia del cuidado que deben tener para que no se materialicen posibles daños en el equipo. Además, es fundamental implementar sistemas de prevención, protección ante posibles amenazas lógicas que con frecuencia pueden dañar bienes tanto en una empresa como en un dispositivo. Los softwares maliciosos son los que más daños causan a los sistemas y a las personas, existen varios de ellos como:

- **Virus:** este programa es creado para dañar a un dispositivo, cada uno de estos son particulares para cada ataque y se reproducen solos.

- **Gusano:** este es un programa que está diseñado para multiplicarse y autoprogramarse infectando los dispositivos, se infiltra a través de los correos, mensajes, transferencia de archivos por USB.
- **Troyanos:** estos son códigos maliciosos que se ocultan dentro de archivos importantes para un usuario, estos son activados por medio de activación del usuario tienen varias funciones dependiendo de cómo sean utilizados y son muy variados. (Paz, 2010)

Existen muchos más softwares maliciosos como: **spyware**: que es un programa espía que almacena información; **adware:** este sistema se instala en el sistema al instalar otras aplicaciones; **ransomware**: esta es una aplicación que secuestra la información con el dispositivo incluido y también solicita pagos para liberarlos; y muchos sistemas más que aparecen día a día para provocar fraudes, robos de información y mucho más. (Davitic, 2017)

1.11.1 Malware

Se refiere a la clasificación general de software maliciosos ya que son algunos en la lista, son mas relacionados con el robo de datos. su definición se puede clasificar en dos categorías que son la tradicional se refiere a infectar y propagarse al mayor número posible de dispositivos causando el mayor daño sin motivo especifico. la categoría moderna son los ataques más actualizados y sofisticados en estrategias de planificación como un ataque APT que es el más conocido. Los creadores de los malware modernos se enfocan en los dispositivos móviles y sistemas operativos como la plataforma Android; un ejemplo de un ataque con APT contra Android tuvo lugar en el 2013 consistió en enviar un correo electrónico con un archivo .apk malicioso, con esto robaron mucha información desde contactos, registros de llamadas, mensajes, etc. (Pacheco, Piazza Orlando , & Carlos , 2016)

1.12 Correos Spam

Estos correos son de tipo basura que son más publicitarios y también se diría que son de remitente anónimo. Desde que se empezó a utilizar este tipo de correos se han envido a foros, blogs, redes sociales, y por otra parte cada vez más aumenta el uso de los correos y también a los celulares por este último se pueden enviar a través de mensajes de textos. Ejercer el envío de los correos spam es sustentado con las deficiencias de los protocolos en la red. Existe un protocolo de transferencia de correos el cual es el SMTP (Simple Mail Transfer Protocol) éste es utilizado para el intercambio de correos entre computadores, así como entre dispositivos móviles. Este protocolo es un estándar de internet RFC 2821. El protocolo SMTP es muy útil, pero tiene ciertas limitaciones en cuanto a recepción en el servidor de destino, es por esto que se han asociado otros protocolos, como el POP (Post Office Protocol), es un protocolo de correos de oficina, se encuentra en su versión 3. (Baca, 2016)

Otro de los protocolos asociados es el IMAP (Internet Message Access Protocol), por medio de este se puede acceder a mensajes almacenados en un servidor de internet, también se puede acceder al correo desde cualquier equipo ya que se visualizan los mensajes sin necesidad de descargarlos; este intercambio de información está conformada por tres secuencias de comandos que son:

- **MAIL**: que es para establecer la dirección de retorno.
- **RCPT:** establece un destino para el mensaje
- **DATA:** este se encarga de enviar el mensaje, es decir se convierte en el mensaje; compuesto por la cabecera y el cuerpo del mensaje. (Baca, 2016)

1.13 Los dispositivos móviles

Los dispositivos móviles (celulares) no son tan antiguos, aunque han evolucionado mucho durante todo este tiempo, desde que la voz era inalámbrica hasta que los dispositivos móviles se usan cotidianamente. La evolución ha permitido que nos comuniquemos con cualquier persona en cualquier lugar del mundo. Las primeras ideas de la comunicación fueron planteadas hace muchos años por el matemático Maxwell, quien al formular las ecuaciones de soluciones para la propagación de las ondas electromagnéticas a la velocidad de la luz. Pasaron más de 40 años para que se creara la primera aplicación móvil. Los dispositivos con el paso del tiempo se hacen más pequeños ya que cuando recién aparecieron eran de gran tamaño, costosos y la batería de muy poca duración; ahora son tan pequeños que se usan en la muñeca, están al alcance del bolsillo del usuario y la batería dura bastante. (Dominguez, Paredes, & Santacruz, 2014)

También aparecido lo llamado computación ubicua que es definida para poner la computadora dentro del mundo real. Esta trabaja con cuatro paradigmas fundamentales que son:

Descentralización: aparece en la era mainframe; es caracterizada por ayudar a definir la arquitectura cliente-servidor. con este paradigma aparece la sincronización para mantener datos actualizados.

Diversificación: permite actualizaciones en diferentes dispositivos, ya que existen muchas herramientas para cada uno de estos.

Conectividad: con la aparición de nuevos dispositivos aparece la necesidad de conectarse, este permite ejecutar cualquier sistema sobre cualquier plataforma.

Simplicidad: centralizado en diseño de dispositivo con interface intuitiva. (Dominguez, Paredes, & Santacruz, 2014)

1.13.1 Características y limitaciones en el desarrollo de aplicaciones para dispositivos móviles

Las características de los dispositivos son de acuerdo a la compañía que los fabrica y basándose en los estudios de sus encuestas a sus clientes. Las aplicaciones móviles son creadas para dispositivos pequeños con pantallas pequeñas y su teclado también, estas son diferentes desde las interfaces que son aptas para estos equipos y son diferentes de las de ordenadores o portátiles, también en la comunicación son diferentes ya que incorporan mensajerías, videos conferencias, geolocalización, capacidades de voz. También ofrecen conectividad en redes inalámbricas y banda ancha esto depende de la capacidad de las señales y la conectividad. (Dominguez, Paredes, & Santacruz, 2014)

1.14 Visualización

Dependiendo del tamaño de la pantalla del dispositivo se visualiza el contenido mediante el sentido de la vista, el tamaño de las pantallas varía según la oscilación de las pulgadas que mide el dispositivo también se tiene en cuenta la lectura del contenido y el diseño del sitio web. Aunque los actuales dispositivos tiene muy buena resolución en la imagen y la pantalla es grande casi del tamaño del equipo, aunque no en comparación con una Tablet que su pantalla es de mayor tamaño y una lectura se puede hacer con mayor comodidad. (Dominguez, Paredes, & Santacruz, 2014)

1.15 Limitaciones en la ejecución de aplicaciones para dispositivos móviles

Existen limitaciones al crear aplicaciones para dispositivos móviles que tiene que ver con el hardware (tamaño de las pantallas, iluminación, tamaño del dispositivo) y las conexiones. Las aplicaciones deben diseñarse evitando sobrecargas para no exigir mucho al dispositivo. Lo más importante es ofrecer interfaces intuitivas y naturales, es decir, fácil de usar de modo que el usuario pueda acceder a su información en cualquier momento. Hay que tener en cuenta que cuando accedemos a internet descargamos varios bytes de información, es necesario que el envío y la recepción de los datos este en un tiempo de espera aceptable para el

dispositivo. Hay que tener presente que las funciones de telecomunicación, es decir, llamadas tienen mayor prioridad que cualquier otra función; también hay que tener presente que las conexiones pueden fallar en ciertas ocasiones lo que significa que no siempre tendremos internet. (Dominguez, Paredes, & Santacruz, 2014)

1.15.1 Programación y aplicación para dispositivos móviles

Las herramientas y fases de construcción, así como también, el proceso de compilación, pre verificación, empaquetado y ejecución de cada aplicación. Antes de crear una primera aplicación en Android, es necesario verificar que el entorno de desarrollo ha sido configurado correctamente. Para esto, se recomienda como primera medida, añadir al entorno Eclipse un ejemplo de aplicación de los proporcionados por el SDK y ejecutarlo en un emulador Android para verificar su funcionalidad. Después, estaremos listos para interactuar con la aplicación a través del emulador y finalmente a través del dispositivo físico. El crear estas aplicaciones requiere de mucho esfuerzo ya que tienen que ser seguras y que sean fáciles de usar para los usuarios. (Dominguez, Paredes, & Santacruz, 2014)

1.15.1.1 Utilización de librerías multimedia

Estas son más para almacenar información de todo tipo, involucra varias áreas como telecomunicaciones y edición de documentos. Se refiere a cualquier objeto o sistema con el objetivo de presentar información utilizando múltiples medios de expresión ya sean físicos o lógicos. Estos múltiples medios pueden ser imágenes, sonido, videos, etc., con esto el usuario puede escoger con mayor libertad que tipo de información es la que desea y cuando la quiere ver y en el orden que quiere. Ya que la multimedia es interactiva y la soportan los sistemas informáticos interactivos. A la multimedia el usuario la usa con estructuras de navegación que le permiten definir la presentación de la información. (Dominguez, Paredes, & Santacruz, 2014)

1.16 Herramientas y fases de construcción para el desarrollo de códigos

Hablaremos de los códigos de configuración y creación de las aplicaciones para los dispositivos, veremos el cómo se usan las herramientas en cada fase de construcción de estas, usando los paquetes que integran los programas, como los emuladores de comprobación, los procesos de compilación, las verificaciones para su creación. (Dominguez, Paredes, & Santacruz, 2014)

Para crear aplicaciones se tiene que tener permisos para la ejecutar las aplicaciones con el sistema operativo que se desee y de acuerdo a las versiones que los sistemas operativos posean, estas aplicaciones deben ser compatibles con las actualizaciones que estas tengan. Tomaremos como ejemplo el sistema Android, antes de crear cualquier aplicación en el sistema Android hay que verificar la configuración, es decir, que este correcta. A continuación, se describen las fases de cómo construir una aplicación en Android:

1.16.1 Creación del proyecto

Este se crea en Eclipse que viene con un paquete de herramientas bastante completo para crear aplicaciones. También se pueden crear mediante comandos, en diferentes lenguajes de programación. (Dominguez, Paredes, & Santacruz, 2014)

1.16.2 Definición del nivel de la API

Cuando se crea un proyecto se tienen que ir midiendo los niveles de soporte que tendrá en la aplicación. De esta manera se podrá ver si la aplicación puede ser ejecutada. (Dominguez, Paredes, & Santacruz, 2014)

1.16.3 Creación de la configuración de lanzamiento para el proyecto

En este paso se configuran las aplicaciones para saber en cual plataforma serán aplicadas en Eclipse. Podremos ver en qué entorno serán ejecutadas, primero probando en el emulador del programa así veremos si las aplicaciones se pueden ejecutar. (Dominguez, Paredes, & Santacruz, 2014)

1.16.4 Máquina virtual

Es una incorporación de sistemas de una computadora que hace ejecuciones como una maquina normal, es decir física. Están diseñadas para ejecutar un único programa, quiere decir que soporta un único proceso de ejecución, un ejemplo claro y conocido es una máquina virtual que utiliza Java, en un sistema operativo para celulares como Android que se podría ejecutar una aplicación como Dalkit. (Jaramillo & Eraso, 2015)

1.16.5 Kernel

También conocido como núcleo se podría definir que es el corazón de los sistemas operativos ya que se encarga de que el software y el hardware se comuniquen y trabajen en equipo dividiendo las tareas de los distintos servicios y aplicaciones, también gestionando la memoria para un servicio más eficiente. Las funciones más importantes son las siguientes:

- Administración de memoria para programas y procesos de ejecución.
- Administración del tiempo de procesos de programas y ejecución.
- Se encarga que se pueda acceder a los periféricos del dispositivo. (Jaramillo & Eraso, 2015)

1.16.6 Aplicación nativa

Esta viene instalada en el mismo dispositivo por defecto se desarrolla utilizando lenguajes de programación obviamente compatible con el sistema operativo del equipo. (Jaramillo & Eraso, 2015)

1.16.7 ADB

Depurador bridge de Android es una herramienta que viene incluida en Android, permite hacer cambios en el dispositivo con un emulador mediante comandos compatibles con el sistema operativo. (Jaramillo & Eraso, 2015)

1.16.8 NFC

Comunicación de campo cercano, es un estándar de comunicación sin cable de corto alcance para realizar pagos de corto alcance a través de dispositivos móviles mayormente. (Jaramillo & Eraso, 2015)

1.16.9 Rootear

Permite modificar el sistema para poder disfrutar de permisos de superusuario, es imprescindible para usar aplicaciones; es similar al Jailbreak de Apple para controla los dispositivos en su totalidad. (Jaramillo & Eraso, 2015)

1.16.10 SDK

Es un paquete de programas de desarrollo de software. es un conjunto de herramientas de desarrollo para crear aplicaciones Android, lo pueden usar desarrolladores de conocimiento básico, así como expertos. (Jaramillo & Eraso, 2015)

1.17 Introducción a la web móvil

Los dispositivos se han integrado desde hace poco en nuestras vidas y nos la han cambiado mucho ya que fue una revolución. La tecnología móvil ha cambiado desde que hizo su aparición en el mundo, en este tiempo ha ganado mucho terreno y juega un papel importante. Hay una lista de los dispositivos más vendidos en el mundo como son: netbook, tablets, handhelds y Smartphone. La mayoría de estos dispositivos tienen una gran aceptación, mientras que otros no tanto porque no son una buena alternativa en el mercado para el usuario final. Aunque las tablets hicieron su aparición en los 90 no fue muy aceptada en aquel entonces como lo es en la actualidad; esta dio un surgimiento a nuevas ideas que han tomado mucho interés por parte de las personas. (Luna, 2016)

Los primeros dispositivos móviles aparecieron de la mano de CASIO y COMPAQ, estos fueron los primeros en buscar aceptación en el mercado de las computadoras. Uno de los primeros Smartphone que llego al mercado fue de la mano de Nokia que

fue el nokia9000 Communicator, unos años después apareció Sony Ericson. La primera versión tuvo algunas evoluciones en su existencia, la última fue en 2004 con el modelo Nokia 9500 Communicator. El primer modelo de Sony Ericsson fue p990 que tenía la función de manejar las aplicaciones en la pantalla. Podemos decir que los fracasos del pasado se pudieron haber dado porque no existían aplicaciones que acompañaran a la creación de los dispositivos. Aunque algunos tuvieron sus propias tiendas de aplicaciones, pero estas tenían limitaciones para su desarrollo en las empresas o de los socios cercanos a las empresas. (Luna, 2016)

1.18 El mundo móvil web

IPhone cambio el concepto de la web en los dispositivos móviles modificando su navegador con determinadas características propias de su pantalla, aunque la web ya existía a precios de este siglo. Muchos teléfonos ya imponían su navegador desde que aparecieron con una versión reducida que no era muy buena en la época. Esto no era impedimento para que la web se impusiera en su totalidad en los equipos. Aunque con el pasar del tiempo los Smartphone han ganado mucho terreno con la modificación de sus pantallas. (Luna, 2016)

1.18.1 ¿Cuándo se conjugaron la web y la móvil web?

Las nuevas tecnologías y la configuración wi-fi hicieran que los móviles explotaran en su esplendor iPhone provoco las primeras investigaciones de nuevas opciones de conexiones de equipos de un modo normal a una conexión móvil. Empezaron a implementar nuevas propiedades para combinar tecnologías y así lograr mejores productos basados en la web. (Luna, 2016)

1.18.2 Plataformas móviles

En la actualidad existen varias plataformas móviles tanto para Smartphone como para tablets y otros dispositivos que existen en el mercado, ya que hay muchos modelos y marcas. La web móvil se enfoca en el software encargado de interactuar con el equipo físico es por ellos que hay que conocer los sistemas operativos de cada equipo incluyendo las limitaciones de estos. (Luna, 2016)

A continuación, mostramos algunas de las plataformas más conocidas:

1.18.2.1 iOS

Este sistema es de Apple, fue desarrollado para ser integrado en el lanzamiento de iPhone. Al principio este sistema no tenía nombre, pero fue oficializado en 2008 cuando Apple lanza una nueva versión de este. Con el paso del tiempo iOS se adaptó a las versiones táctiles. (Luna, 2016)

1.18.2.2 Android

Empezó como un sistema operativo móvil independiente. en la actualidad es propiedad de Google, esta cuando vi que iPhone se lanzó al mercado también lo hizo y por ello adquirió el sistema Android para adecuarlo acorde a sus necesidades y tener una herramienta sólida para entrar al mercado. Android ha tenido varias versiones desde la primera que fue la (1.5) desde allí ha avanzado mucho, empezó a ganar popularidad con su segunda versión (2.1); este sistema es de código abierto por ello es uno de los más populares en la actualidad. Desde que saco su versión 4 este sistema es adaptable tanto en Smartphone como en tablets, es por ello que en la actualidad cualquier aplicación desarrollada para esta plataforma puede ser instalada sin problema. (Luna, 2016)

1.18.2.3 Windows Phone

Microsoft también entro al mercado de la telefonía móvil en el 2010 con el sistema operativo Windows Phone, que fue recreado del sistema Windows Mobile que no era muy aceptado y también había sido abandonado. por ello ingreso al mercado empezando desde cero con un nuevo desarrollo. (Luna, 2016)

1.18.2.4 BlackBerry

Es un sistema operativo que en la actualidad se encuentra en su versión 10.2.1, tomando a QNX como base de su creación. garantiza un correcto funcionamiento multitareas, en tiempo real a nivel mundial, aunque perdió aceptación por no

actualizar el sistema operativo a tiempo, esta es una empresa desarrolladora de hardware y sistemas operativos móviles. (Luna, 2016)

1.18.2.5 Otros sistemas operativos

Como hemos mencionado hay muchos sistemas operativos móviles en el mercado las cuales se disputan la hegemonía de campo. aparte de los ya mencionados hay algunos otros que no son muy conocidos, pero buscan serlo, como Firefox OS. (Luna, 2016)

1.19 Protección de datos

Para la empresa DEBITOOR que es una de las que protegen los datos de las empresas que confían en ella; la protección de los datos es lo más importante que hay que hacer hoy en día ya que es un derecho también y es muy fundamental porque así se pueden identificar personalmente los datos que ingresan en su equipo. es un derecho proteger sus datos más que todo los personales y estos derechos son obligatorios para todas las empresas y deben estar en las políticas de todas las entidades. Esta es una empresa de facturación en la nube y los términos de protección de datos y privacidad son muy importantes ya que su relación con los clientes es muy confiable entonces tienen que proteger muy bien los datos de las empresas que confían ellos para administrar sus datos. su prioridad es proteger los datos como el reglamento lo exige; esta empresa también informa a sus clientes todos los procesos de los datos. (debitoor, 2017)

Testimonios de empresas que utilizan los reglamentos y protocolos de la protección de datos. Hoy en día es de vital importancia proteger nuestros datos es por ellos que existen leyes y normas certificadas desde hace años para proteger los datos que generamos cada día, que en la actualidad son millones de datos generados por segundo. La Agencia Española de protección de datos ha desglosado algunos de los derechos de privacidad y protección, a continuación:

- Derecho de información y sobre cómo se recopilan sus datos, así como sus derechos sobre ellos.

- Derecho de rectificación sobre aquellos datos inexactos, equívocos o falsos.
- Derecho de cancelación o supresión de aquellos datos que puedan ser perjudiciales al interesado (dentro de los límites de la ley).
- Derecho de oposición, permite que un ciudadano pueda rechazar que se recopilen sus datos.

Estos derechos son establecidos por la Ley Orgánica de Protección de Datos y son obligatorios para todas las instituciones que recopilan información. El Reglamento General de Protección de Datos (RGPD), ha escalado desde que fue aprobada en el 2016 y es obligatorio llevarla a cabo en las instituciones desde el 2018. Esta regulación permite a los usuarios mantener sus datos protegidos en todo momento. (debitoor, 2017)

1.19.1 ¿Qué son datos personales?

Cualquier información sobre una persona que sirva como su identidad, tales como: nombres, apellidos, domicilio, correos electrónicos, documentos de identidad, datos de localización, etc. Por ejemplo, hay empresas que necesitan mucha información personal de sus clientes, como Debitoor que es una empresa de facturación en la nube y como empresa que trabaja con datos importantes debe proteger estos datos de modo que no puedan ser vistos por nadie que no sea el cliente y el programador de la empresa. Esta empresa trabaja con el sistema de protección de datos RGPD, debitoor tiene un acuerdo de procesamiento de datos para enviar los procesos de los datos a cada uno de sus clientes para que estos estén informados de todo lo que sucede con su información. (debitoor, 2017)

1.20 Valor económico y social de los datos personales

En la actualidad los datos personales tienen un valor muy alto, tan alto como el valor de un software o el nombre de un dominio. Pero no es la información en si la que tiene tanto valor si no la asociación con otros datos y como se utilicen estos. También se permite el ingreso de un lucro mediante explotación comercial, orientados al consumo, interesados en predicciones de conducta y patrones de

comportamiento. Mediante este sentido se podría afirmar que la economía digital se ha convertido en una moneda de cambio de un valor elevado permitiendo que muchos modelos de negocio se puedan sustentar. Según estudios se ha visto que las empresas como Google o Facebook, basan sus modelos de negocios en la información de los usuarios, podemos decir que con los avances tecnológicos se pueden guardar grandes cantidades de datos generadas a diario en tiempo real. (Enriquez, 2018)

1.21 Importancia de proteger los datos

Es muy importante porque hay muchas personas que comparten la información con otras personas y esto implica riesgos, fácilmente pueden utilizar esta información de manera maliciosa, es por esto que la información debe ser protegida estrictamente. Desde que aparece el internet el modo de manejar datos ha cambiado mucho ahora los negocios se hacen por internet (comercio electrónico). Las empresas creen que por la red pueden tener mayor venta en sus negocios. Los datos en la red corren mucho peligro ya que es difícil el protegerlos, entre los peligros más destacados tenemos: ataques de malware, robo de identidad, fuga de información, es por esto que es importante la protección de los datos. La información es importante para la toma de decisiones por es considerado un activo económico muy importante, también es fundamental para las operaciones de todos los días, es por esto que los ciberdelincuentes están pendiente de encontrar la forma de adueñarle los datos de distintas formas. (Enriquez, 2018)

1.22 Aplicaciones multimedia

Este término apareció en los 90 y se involucran diferentes áreas de la informática, telecomunicaciones y edición de documentos. Significa múltiples medios. Actualmente en el escenario hay múltiples medios de almacenamiento, transmisión, mostrar y recibir información, en cualquier momento o sistemas desde cualquier medio con el objetivo de mostrar la información que pueden ser audio, video, texto, imagen, grafico, etc. el usuario tiene la opción de elegir qué información quiere ver y cuando. (Dominguez, Paredes, & Santacruz, 2014)

CAPÍTULO II

2 DIAGNÓSTICO

2.1 Método de investigación

2.1.1 Cuantitativa

La investigación cuantitativa se basa en el estudio y análisis de la realidad a través de diferentes procedimientos basados en la medición. Permite un mayor nivel de control e inferencia que otros tipos de investigación, siendo posible realizar experimentos y obtener explicaciones contrastadas. Los resultados de estas investigaciones se basan en la estadística y son generalizables. (Castillero, 2010)

2.2 Enfoque de investigación

2.2.1 Inductivo – Deductivo

Para el proyecto es aplicable este método porque se relaciona con las técnicas a utilizar, que es la observación de los datos ya existentes de otras investigaciones, la entrevista y la encuesta, estos datos ayudan mucho para completar una investigación de un estudiante, este método ayudará a sacar buenas conclusiones de la investigación hecha mediante las técnicas que se aplicaran. (Rodriguez E. , 2005)

En este proceso de estudio se obtuvieron conclusiones para la explicación de este estudio. Se alcanzaron buenos resultados de toda la información recogida en la investigación realizada, y así se hizo el análisis de los datos.

2.2.2 Analítico

Las técnicas y métodos a aplicar a este proyecto sirven mucho para lo que es el análisis porque hay que revisar y analizar detalladamente cada información y cada conocimiento que adquiera mientras se realiza la investigación, además la relación que existe entre los métodos se da mucha ayuda mientras se realizan los avances. (Rodriguez E. , 2005)

Con este método se analizó la entrevista, así como la encuesta donde se identificaron los problemas a resolver del proyecto.

2.3. Tipos de investigación.

2.2.3 Descriptiva

El objetivo de la investigación descriptiva es comprender y describir registros, análisis e interpretación de datos reales, así como considerar la población del objeto de la investigación, también incluye el diseño de la investigación, tipos de datos a estudiar y las variables del estudio. (Castillero, 2010)

2.3 Técnicas de investigación

2.3.1 La encuesta.

Es una recopilación de opiniones por medio de cuestionarios o entrevistas en un universo o muestras específicas, con el propósito de aclarar un asunto de interés para el encuestador. Se recomienda buscar siempre agilidad y sencillez en las preguntas para que las respuestas sean concretas y centradas sobre el tópico en cuestión. (Ledesma, 2017).

Se escogió esta técnica por el hecho de ser fácil de aplicar para recolectar datos, y lo sencillo que es para el encuestado la resolución de las preguntas, además de que recolectar la información en muy poco tiempo a varias personas; ésta fue aplicada a los profesores de la carrera de Ingeniería en Sistemas de la ULEAM Extensión El Carmen.

2.3.2 Entrevista

Una entrevista es una conversación que persigue un propósito. Dicho propósito depende del o de los temas que se investigan. Es decir, es una interacción entre el entrevistado y el entrevistador, donde el entrevistador realiza una serie de preguntas a la otra persona para obtener información específica sobre el tema tratado. (Mendez & Rodriguez , 2016)

Se escogió esta técnica porque se puede interactuar con la persona entrevistada, de una manera más cómoda, como una conversación donde las preguntas ya están previamente escogidas de acuerdo al tema de la investigación. Esta entrevista fue realizada el coordinador de la carrera de Ingeniería en Sistemas de la ULEAM Extensión El Carmen.

2.4 Instrumentos de investigación

2.4.1 Cuestionario

El cuestionario es considerado un procedimiento clásico para obtener y registrar datos. Es muy utilizado como instrumento de investigación y evaluación de personas, ya que puede registrar la información solicitada de una forma impersonal contrario a la entrevista, y en menos tiempo. Es muy utilizado para recoger información de campo en alguna investigación. Se podría decir que es el instrumento que permite plantear un conjunto de preguntas para obtener la información deseada. (Meneses & Rodriguez, 2014)

Se escogió este instrumento para la investigación de campo, de esta manera se pudo realizar las preguntas que me permitieron aplicar la encuesta como la entrevista y así recolectar los datos necesarios para la investigación del proyecto. Tener más claro lo que los usuarios están necesitando para la protección de sus datos con la información obtenida mediante este instrumento.

2.4.2 Guía de la entrevista.

Se puede manifestar que la entrevista se guía por ciertos argumentos limitadas por el propio investigador, no obstante, hay una ventaja muy significativa, la cual es ofrecer ciertas conformidades para aclarar, pulir o ilustrar las preguntas, no solamente eso, sino también profundizar aún más la investigación a través de las respuestas adquiridas por el entrevistado. (Mediano, 2014)

2.5 Validación de Instrumentos.

Es una técnica o conjunto de técnicas que permitirán una asignación numérica que cuantifique las manifestaciones que son medibles. Los instrumentos de investigación son herramientas de recolección de datos, para elaborar estos instrumentos se debe tener claridad de los conceptos teóricos, medición, confiabilidad y validez. (Rodriguez A. m., 2014)

2.5. Población y muestra

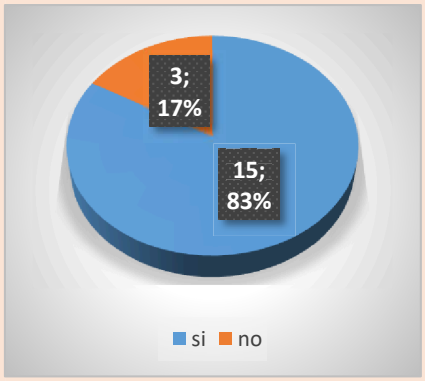
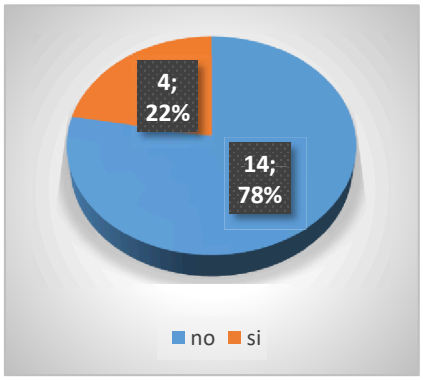
2.5.1. Población

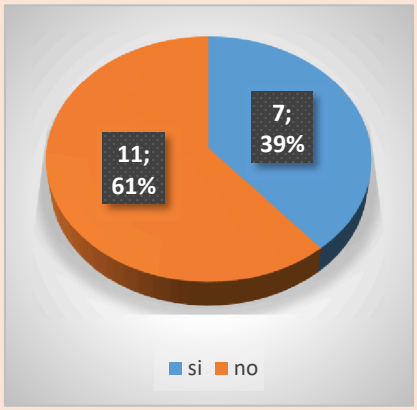
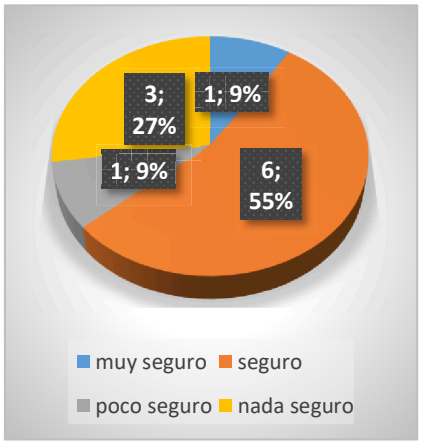
La universidad Laica Eloy Alfaro de Manabí Extensión El Carmen cuenta con un total de 74 maestros que laboran en las cuatro carreras correspondientes las cuales son: Ingeniería en Sistemas y Tecnologías de la Información, Ingeniería Agropecuaria, Ingeniería en Contabilidad y Auditoría, Ciencias de la Educación, los cuales será tomados en la presente investigación.

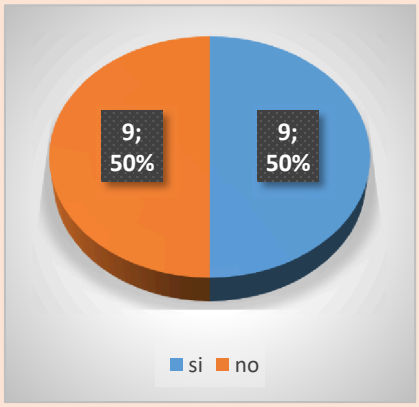
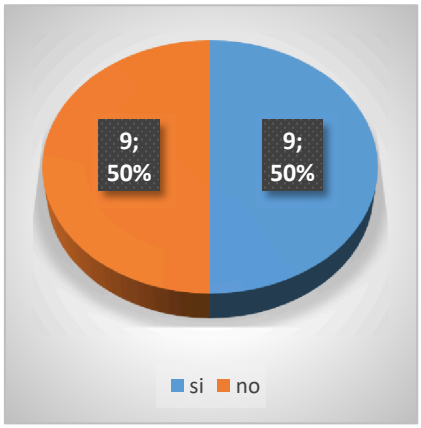
2.5.2. Muestra

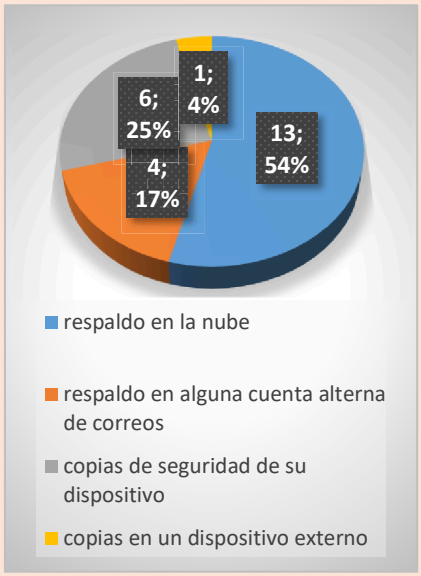
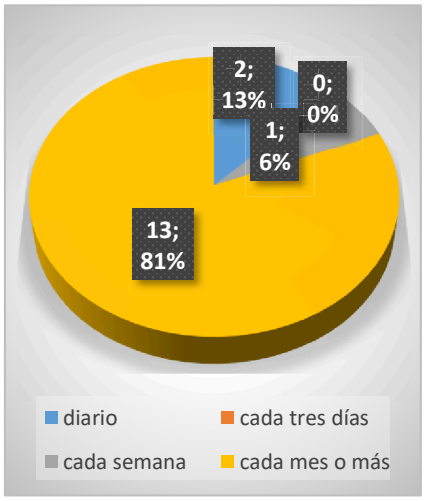
La muestra para la presente investigación se basó en una muestra discrecional donde se tomó como referencia a los docentes que dominan la tecnología que son 18 docentes de la carrera de Ingeniería en Sistemas y Tecnologías de la Información para realizar la respectiva encuesta. Para la entrevista se seleccionó al coordinador de la carrera.

2.5.3. Tabulación de la encuesta realizada a los docentes de la Universidad Laica Eloy Alfaro de Manabí extensión en El Carmen.

PREGUNTAS	GRÁFICAS	ANÁLISIS
1. **¿Utiliza un dispositivo Smartphone?**		En base a los resultados obtenidos, nos damos cuenta que no todos los docentes utilizan Smartphone.
2. **¿Utiliza contraseñas para ingresar a su dispositivo móvil?**		Basándonos en las respuestas de la encuesta realizada, nos damos cuenta que la mayoría de los encuestados no utilizan contraseñas para proteger su equipo y sus datos.

3. **¿Tiene algún antivirus instalado en su dispositivo móvil?**		En base a las respuestas obtenidas de la encuesta realizada nos damos cuenta que la mayoría de los docentes no instalan antivirus en sus equipos. Mientras que el otro porcentaje cree que es seguro tener un antivirus instalado en su equipo.
4. **¿Qué tan seguro considera el antivirus instalado en su dispositivo móvil?**		En base a los datos obtenidos de las personas que han instalado un sistema de seguridad, este es seguro para ellos y protege la información almacenada, resalta también que los demás encuestados no confían en sistemas de seguridad para instalar en sus equipos y proteger sus datos.

5. **¿Cuándo va a instalar una aplicación en su dispositivo lee las políticas de privacidad de la aplicación previo a la instalación?**		En base a los resultados obtenidos mediante la encuesta nos damos cuenta que la mitad de los encuestados no leen las políticas de privacidad de las aplicaciones antes de instalarlas, mientras que la otra mitad de los encuestados si lee estas políticas.
6. **¿Conoce algún tipo de seguridad para proteger los datos de su celular?**		Basándonos en los resultados obtenidos mediante la encuesta realizada, la mitad de los encuestados tienen conocimiento de la existencia de otras formas de proteger la información en los equipos, mientras que los demás no tienen conocimiento.

7. **¿Cuál de las siguientes opciones utiliza para la protección de sus datos?**		Basándonos en los resultados de las encuestas realizadas nos damos cuenta que la mayoría usan más de un método de protección para sus datos y la mayor cantidad hacen respaldos en la nube y confían en las copias de seguridad de sus equipos.
8. **¿Cada que tiempo hace respaldo de seguridad de sus datos?**		En base a la encuesta realizada se determinó, que la gran mayoría hace respaldos cada mes o más tiempo. Mientras que los otros porcentajes varían por muy poco. Pocas personas encuestadas realizan sus respaldos a diario mientras que unas seis personas los realizan cada semana.

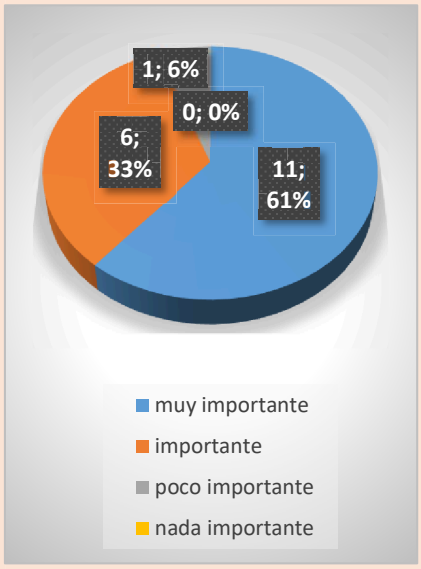
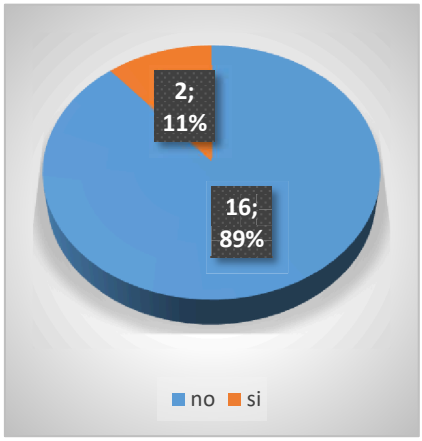
9. **¿Qué tan importante considera proteger los datos de su dispositivo?**		En base a los datos obtenidos mediante la encuesta realizada, nos damos cuenta que es muy importante para las personas encuestadas la protección de sus datos. Para el otro porcentaje es importante el proteger sus datos ya que tienen información que no desean perder o que sea robada.
10. **¿Conoce alguna aplicación o herramienta que le permita medir la seguridad lógica de su dispositivo para lograr proteger sus datos?**		En base a los datos obtenidos en la encuesta realizada, nos damos cuenta que la gran mayoría de las personas encuestadas, no tienen conocimiento de herramientas que valoren la seguridad de sus equipos, para saber qué tan protegidos están sus datos. Las otras dos personas si tienen conocimiento de estas herramientas.

Tabla 1 Resultado de encuesta realizada a docentes

2.5.4. Análisis de las encuestas realizadas a los docentes de la ULEAM Extensión El Carmen

De las encuestas aplicadas es evidente que para la mayoría es importante el proteger los datos, sin embargo, no utilizan aplicaciones o métodos para proteger su información. La mayoría solo aplica las herramientas de protección que vienen incorporadas en su dispositivo o hace respaldos en la nube que es uno de los métodos más conocidos y seguros de protección de datos. Aunque hay un porcentaje que no tienen conocimiento de herramientas que miden la seguridad en los dispositivos para conocer si su información está bien protegida con el método que utilizan.

2.5.5. Entrevista realizada al coordinador de la carrera de Ingeniería en Sistemas

PREGUNTAS	RESPUESTAS	ANÁLISIS
1. **¿Conoce algunos métodos o aplicaciones para proteger los datos de su celular?**	Si, solamente lo que es contraseñas, en algunas aplicaciones o incorporadas en el mismo celular como son lectores de huellas.	Basándonos en la respuesta del entrevistado él tiene basto conocimiento de aplicaciones de seguridad para proteger la información del equipo.
2. **¿Utiliza algunos de los métodos o aplicaciones mencionados anteriormente**	Si, para ingresar el celular uso una contraseña, para ingresar al WhatsApp uso otra, también uso una contraseña para ingresar al telegram, pero en	En su respuesta menciona que solo utiliza la configuración de seguridad de su equipo para proteger sus aplicaciones de comunicación y toda la

para proteger su celular?	general lo que me brinda el celular.	información que contenga el dispositivo.
3. ¿Qué tan segura en para usted la aplicación que usa para proteger sus datos?	Es seguro, porque es de parte del fabricante que en este caso es Huawei que tiene un lector de huellas que viene incorporado, y se supone que sin mi huella no se puede acceder.	Basándonos en su respuesta la configuración de seguridad de su equipo, él la considera muy segura por lo que es un lector de huella dactilar que viene incorporado en el equipo.
4. ¿El método que utiliza para proteger su celular lo considera seguro?	Yo creo que es muy seguro, para proteger los datos	Supo mencionar que el método de seguridad que él utiliza es muy seguro para proteger su información, también dijo que puede ser vulnerable en ciertos aspectos, por ejemplo en la conectividad a una red abierta.
5. ¿Considera que, con la aplicación de protección de su celular, éste podría ser hackeado?	Creo que no, porque es segura la protección que utilizo.	Basándonos en su respuesta, él está muy seguro que su equipo no puede ser hackeado, aunque no cuente con una aplicación de

		seguridad extra en su equipo.
6. ¿Por qué es importante para usted el proteger sus datos?	Proteger los datos es importante, porque muchas veces hay fuga de información de pronto uno tiene información que es personal (fotos, audios, etc.), y progresivamente se le pudo dar un mal uso, por eso es necesario tener los datos protegidos con contraseña, patrones de seguridad, por eso es muy necesario el proteger.	Según lo manifestado, la protección de los datos es importante y tener el celular protegido también lo es, por ello recomienda que se proteja la información de la mejor manera posible para que esta no sea robada y se le dé un mal uso.
7. ¿Cree que sus datos están bien protegidos con la aplicación que utiliza?	Solo utilizo la que viene incorporada en el celular, no uso aplicación para proteger mis datos.	Según su manifestación la configuración de seguridad del sistema operativo de su celular protege bien su información que no necesita de una aplicación de seguridad en su equipo.

8. ¿Cree que respaldar los datos en la nube es seguro?	Hasta el momento yo creo que sí, supo mencionar, siempre y cuando se tenga una cuenta en un lugar seguro, por ejemplo, drive, servidor virtual. Donde me permita almacenar información, incluso el que se pueda pagar por ese servicio garantiza que la información se mantenga segura, aun teniendo información de hace muchos años.	Manifestó que confía mucho en la seguridad de la nube para respaldar su información, porque hay mucho espacio para almacenar toda la información que se desee, también dijo que la información en esta plataforma puede estar guardada por mucho tiempo sin ser vulnerada.
9. ¿Utiliza antivirus en su celular?	No, porque talvez el tiempo no me ha dado para hacerlo, aunque los celulares tienen una vulnerabilidad, por ejemplo, al conectarse en una red libre permite que los datos puedan ser robados por cualquier intruso que pueda obtener la información guardada.	Supo manifestar que no confía en las aplicaciones de antivirus o seguridad para instalarlas en su equipo, es decir, no las considera seguras se podría vulnerar la información a través de ellas.

10. ¿Cree que los antivirus protegen bien a los celulares de los virus?	No en un cien por ciento, porque eso depende también del sistema operativo que utilice como Android, Windows Phone. La seguridad también depende del sistema operativo, el antivirus que use el sistema, aunque también usan imágenes de pánico para que usen el antivirus, aunque no sea seguro.	Manifiesta que no son seguros y usan imágenes de pánico para que los usuarios confíen ellos y descarguen la aplicación aunque esta no sea nada segura.

Tabla 2 Resultados de entrevista realizada al coordinador de la carrera

2.5.1 Análisis de resultados de la entrevista.

Por lo manifestado por el coordinador de la carrera de Ingeniería en Sistemas, él conoce mucho de seguridad lógica y como se debe aplicar para proteger los datos, aunque menciona que son muy vulnerables dependiendo del uso que se les dé y como se resguarden.

Según lo manifestado, la protección de los datos es importante y tener el celular protegido también lo es. Sin embargo, hay ciertos aspectos que supo manifestar como, por ejemplo: él en lo personal no ha instalado un antivirus en su celular. También supo decir que no los considera muy seguros y que a través de una conexión de wifi libre los datos pueden ser vulnerados.

De los métodos de protección de datos solo usa los incorporados en su celular y confía que su sistema operativo le ayuda a proteger los datos. Su celular cuenta con lector de huellas dactilares que según su opinión personal es uno de los mejores

métodos para proteger los equipos, ya que solo permite el ingreso a los datos a la persona autorizada. Refiriéndose a otros dispositivos mencionó que cada equipo tiene un sistema de protección diferente que viene incorporado en el sistema operativo.

En la entrevista se mencionó que uno de los mejores métodos y formas de respaldar datos es en la nube ya que cuenta con suficiente espacio para almacenar toda la información que se desee de todo tipo desde fotos hasta archivos de suma importancia que necesiten ser protegidos.

2.6. Triangulación de resultados de la encuesta y la entrevista.

A partir de lo declarado por los resultados obtenidos, mediante las técnicas de investigación hay variación de datos. Según las respuestas de la entrevista de las preguntas 9 y 10, y las encuestas en las preguntas 3 y 4. No utilizan mucho los antivirus porque no les parecen lo suficientemente seguros para la protección de los celulares por ende los datos o por desconocimiento de éstos.

Mediante los resultados obtenidos, la protección de los datos es de vital importancia, puesto que puede existir fuga de información o algún intruso puede forzar la seguridad del dispositivo por medio de la red para sustraer información muy importante de las personas, información que solo el usuario puede manipular.

Los resultados obtenidos por la entrevista y las encuestas, muestran que al utilizar un dispositivo inteligente (Smartphone) la información guardada en ellos corre riesgos de ser burlada todo el tiempo, con el solo hecho de conectarse a internet, es decir, a la red hay riesgo de vulnerabilidad en los datos y estos pueden ser robados.

Recalcando la respuesta señalada hay varias personas que no tienen conocimiento de herramientas que les permitan mantener seguro su equipo, si el tipo de protección que utilizan para su celular y sus datos logra proteger lo suficiente su información. Según el testimonio de la entrevista los datos están bien protegidos

con el sistema de protección de huellas dactilares, él lo considera uno de los más seguros existentes en la actualidad.

CAPÍTULO III

3. MANUAL DE SEGURIDAD LÓGICA INFORMÁTICA APLICADA EN DISPOSITIVOS MÓVILES PARA LA PROTECCIÓN DE SUS DATOS.

3.1. Introducción

Como lo explican varios autores y expertos en seguridad informática, el proteger los dispositivos es importante porque cada día aparecen nuevas formas de burlar la seguridad y robar la información de los usuarios. Es por ello que los creadores de aplicaciones de seguridad pruebas nuevas estrategias de protección de la información como por ejemplo es el iris, es decir, lector de retina incorporada en las aplicaciones que crean.

En esta investigación se ha realizado un manual de usuario ya que los usuarios no tienen en cuenta la protección de sus dispositivos e información, con este manual podrán proteger su dispositivo siguiendo las indicaciones de como activar las configuraciones de fábrica del dispositivo incluyendo una aplicación de seguridad para aumentar la protección, siguiendo estos pasos se demostrará que protegiendo bien el equipo no podrá ser hackeado con facilidad.

3.2. Objetivos

3.2.1. General

Desarrollar un manual de seguridad lógica informática aplicada en dispositivos móviles para la protección de sus datos.

3.2.2. Específicos

- Fundamentar teóricamente la seguridad lógica informática, y dispositivos móviles.
- Obtener información sobre seguridad lógica informática de los dispositivos móviles.

- Comparar y seleccionar una herramienta de seguridad lógica informática para teléfonos inteligentes.
- Diseñar un manual de usuario sobre seguridad lógica informática de los teléfonos inteligentes.

3.3. HERRAMIENTAS DE SEGURIDAD LÓGICA INFORMÁTICA PARA TELÉFONOS INTELIGENTES.

3.3.1. Antecedentes

En la actualidad el mundo gira en torno al uso del internet para muchas acciones cotidianas como leer las noticias, hacer consultas, enviar y recibir correos, acceder a redes sociales, hacer compras en línea, pagos de servicios, etc. Todo esto es información confidencial que se relaciona con la web por lo cual no tiene que ser de fácil acceso para otras personas, esto genera posibles intrusiones y amenazas de seguridad lo cual vulnera el acceso a los servicios y uso de la información.

En esta investigación, el tema a tratar son los datos de autenticación del usuario, específicamente los nombres de usuarios y contraseñas; mientras una persona más utilice el servicio de identificación con una contraseña es más difícil memorizarla.

Con el desarrollo de esta investigación se mostrará el funcionamiento de tres de las aplicaciones de seguridad escogidas las cuales protegen la información con gestores de contraseñas en función del almacenamiento de las contraseñas y la información que estas protegen con el fin de determinar las ventajas y desventajas de cada una, apreciando al final del estudio que características son más seguras para el uso y poder solucionar los problemas encontrados.

La encuesta realizada para este trabajo fue dirigida a los docentes de la carrera de Ingeniería en Sistemas y Tecnologías de la Información porque interactúan con servicios que requieren autenticación a través de internet; al final del estudio se muestran los resultados correspondientes.

3.3.2. Comparación de las funciones de herramientas según su versión

Las herramientas cuentan versiones gratuitas, así como de pago, esta información es de varias aplicaciones de seguridad, todas las encontradas tienen las versiones gratuitas tienen funciones como:

- Número ilimitado de entradas
- Agrupar y filtrar entradas
- Generador de contraseñas segura
- Sincronización gratuita

Las versiones de pago cuentan con:

- Sincronizar todos los dispositivos
- Realizar y restaurar las copias de seguridad
- Plantillas personalizadas
- Centro de seguridad
- Autenticación de huellas dactilares

Cada herramienta tienes estas funciones integradas, aunque cada una aumenta otras funciones acordes a cada actualización que le realice el programador estas se le realizan en cierto tiempo con peticiones de los usuarios.

Las herramientas a utilizar serán versiones finales no versiones de pruebas que se enlistan a continuación:

- **mSecure:** En este estudio se analiza la funcionalidad de la herramienta.
- **Bitwarden:** En este estudio se analiza la funcionalidad de la herramienta.
- **LastPass:** En este estudio se analiza la funcionalidad de la herramienta.
- **SplashID Safe:** En este estudio se analiza la funcionalidad de la herramienta.
- **Myki:** En este estudio se analiza la funcionalidad de la herramienta.

3.4. Análisis de gestores de contraseñas

- Para analizar los gestores de contraseñas se establecieron subcaracterísticas para determinar pros y contras de cada una de las herramientas seleccionadas. Los aspectos evaluados se describen a continuación:
- **Confidencialidad**. Capacidad de protección contra el acceso de datos e información no autorizados, ya sea accidental o deliberadamente. Se va a evaluar por cada herramienta: tipo de algoritmo para cifrar los datos, ingreso a la herramienta, generador de contraseñas, protección del ingreso a la herramienta.
- **Integridad.** Capacidad del sistema o componente para prevenir accesos o modificaciones no autorizados a datos o programas de ordenador. Se va a evaluar por cada herramienta que el BD de contraseñas no pueda ser alterada o modificada.
- **No repudio.** Capacidad de demostrar las acciones o eventos que han tenido lugar, de manera que dichas acciones o eventos no puedan ser repudiados posteriormente.se va a evaluar la integridad de los datos, origen de los datos.
- **Facilidades de uso**. En este contexto, a evaluar por cada herramienta la sencillez de uso, idiomas, plataformas e integración con navegadores, y si cuentan con un medidor de calidad de contraseñas.

3.5. Estudio técnico

3.5.1. Lista de aplicaciones de seguridad para realizar las pruebas.

	APLICACIONES DE SEGURIDAD CON GESTORES DE CONTRASEÑAS				
	mSecure	**SplashID Safe**	**Bitwarden**	**LastPass**	**Myki**

Funciones principales	Proteger toda la información del equipo con un cifrado **AES-256** y autenticación por huella dactilar.	Cuenta con una caja fuerte para almacenar toda la información personal. Permite que el dispositivo se sincronice con su ordenador, cuenta con cifrado de **AES-256** bits también cuenta con reparación y restauración de contraseñas	Esta cuenta con una bóveda sellada con cifrado **AES-256** bits y **PBKDF2 SHA-256** con acceso personal, además es de código abierto.	Cuenta con una extensión desplegable en tu navegador y un número ilimitado de claves. También cuenta con el cifrado **AES-256** bits.	Cuenta con un gestor de contraseña y autenticador con cifrado **AES-256** y de grado militar punto a punto, privacidad incorporada e ingreso de huella dactilar, cierre de sesión remota

Tabla 3 Lista de aplicaciones de seguridad para realizar las pruebas.

3.5.2. Comparación técnica de las aplicaciones de seguridad.

A continuación, se realiza un resumen de las subcaracterísticas que se han considerado para la realización del estudio estas son las más relevantes en la comparación de gestores de contraseñas analizados:

3.5.2.1. Compatibilidad de plataformas

Una aplicación multiplataforma es un atributo que se concede a software que implementan y operan entre múltiples plataformas informáticas, es muy importante porque contribuye a la facilidad que tiene el usuario que utiliza diferentes plataformas a la vez.

- **mSecure 5.7.0**

Es multiplataforma

Funciona en Android, iOS, Mac y Windows, esta misma versión funciona en todas las plataformas mencionadas. La versión PRO ofrece una licencia y autenticación con huella dactilar para todas las plataformas.

- **Bitwarden 2.2.8**

Es multiplataforma

Funciona en Android, iOS Mac y Windows, esta versión, así como las anteriores funcionan en todas las plataformas mencionadas. Es de código abierto.

- **LastPass 4.4.2024**

Es multiplataforma

Funciona en Android Oreo y las otras versiones, iOS Mac y Windows, esta misma versión funciona en todas las plataformas mencionadas. La versión PRO ofrece autenticación multifactor Premium como YubiKey y autenticador de huella dactilar en ordenadores

3.5.2.2. Compatibilidad en idiomas

- **mSecure 5.7.0**

Incorpora múltiples idiomas

- **Bitwarden 2.2.8**

Incorpora múltiples idiomas

- **LastPass 4.4.2024**

Incorpora múltiples idiomas

3.5.2.3. Tipo de licencia

Esta característica determina el contrato que concede los derechos de autor en la que están precisados los derechos y deberes de desarrollo.

- **mSecure 5.7.0**

El tipo de licencia es Propietario y no hay información disponible sobre su código fuente.

- **Bitwarden 2.2.8**

El tipo de licencia es Propietario y es de código abierto, el código fuente está alojado en GitHub y puede ser revisado, modificado o auditado por cualquier persona.

- **LastPass 4.4.2024**

El tipo de licencia es Propietario y no hay información disponible sobre su código fuente.

3.5.2.4. Ingreso a la herramienta

Es la característica que describe el ingreso a la herramienta.

- **mSecure 5.7.0**

Acceso rápido y seguro a tu información con tu huella dactilar gracias a Nexus Imprint, principalmente a través de la contraseña maestra para que sea exitosa la autenticación, también existe la posibilidad de asociar la cuenta de usuario Windows para asociar el acceso de los datos.

- **Bitwarden 2.2.8**

Se ingresa principalmente a través de una contraseña maestra, el ingreso es fácil y seguro para guardar todas las contraseñas de manera sincronizada, recomienda tener varias, es decir una contraseña para cuenta, guarda los usuarios en bodegas cifradas con AES-256 sincronizadas a través de los dispositivos de uso.

- **LastPass 4.4.2024**

Se ingresa principalmente a través de una contraseña maestra, también cuanta con un factor de autenticación de huella dactilar para el ingreso, LastPass recuerda todas sus contraseñas y las mantiene seguras. Se sincroniza con todos los dispositivos que utilice con más frecuencia de manera gratuita.

3.5.2.5. Algoritmo Criptográfico

En esta característica se describe el algoritmo criptográfico con el cual se cifran las bases de datos que contiene el usuario.

- **mSecure 5.7.0**

Utiliza cifrado AES-256.

- **Bitwarden 2.2.8**

Utiliza AES-256 bit, con semilla y PBKDF2 SHA-256.

- **LastPass 4.4.2024**

Utiliza cifrado AES-256.

3.5.2.6. Sincronización de datos

En esta característica se describe la forma en la que se sincronizan los datos del usuario especialmente si usa la herramienta en distintos dispositivos.

- **mSecure 5.7.0**

Las bases de datos se sincronizan en cualquier dispositivo a través de vía Dropbox, wifi y el servicio de mSecure Cloud.

- **Bitwarden 2.2.8**

Sincroniza con todos los dispositivos y las bases de datos a través de cualquier navegador por medio de wi-fi o datos.

- **LastPass 4.4.2024**

Sincroniza con todos los dispositivos que utilice al instante a través de cualquier navegador por medio de wi-fi y datos.

3.5.2.7. Generador de contraseñas

Esta característica es útil si la herramienta tiene la facultad de generar las contraseñas.

- **mSecure 5.7.0**

Genera contraseñas para la protección de todas las aplicaciones que utiliza el usuario de forma segura, a través de conjunto de caracteres, dependiendo de la combinación la herramienta genera la fortaleza en bits.

- **Bitwarden 2.2.8**

Protege y genera las contraseñas mientras estés en línea, a través de caracteres generados aleatoriamente, mientras más fuerte la contraseña mayor seguridad para la información. Utiliza conjunto de caracteres para fortalecer las contraseñas.

- **LastPass 4.4.2024**

Genera contraseñas para la protección de todas las aplicaciones, sincroniza todos los dispositivos, 1 giga de almacenamiento de forma cifrada, contraseña maestra y utiliza generador de caracteres para mayor protección.

3.5.2.8. Medidor de calidad de contraseñas

Esta característica indica si la contraseña de ingreso es más o menos robusta.

- **mSecure 5.7.0**

Si incluye medidor de calidad para MASTER PASSWORD.

- **Bitwarden 2.2.8**

Si incluye medidor de calidad para MASTER PASSWORD y para la contraseña de servicio, también analiza las contraseñas para buscar las debilidades.

- **LastPass 4.4.2024**

Si incluye medidor de calidad para MASTER PASSWORD.

3.5.2.9. Ingreso de datos para usar un servicio

En esta característica se describe la forma en la que la herramienta ingresa los datos al formulario donde se contienen los usuarios y las contraseñas requeridas que pueden ser de dos formas manualmente haciendo copias de seguridad o de forma automática con funciones que ofrecen las herramientas. El ingreso de los datos es importante en el término de la confidencialidad, al utilizar el ingreso de datos de forma adecuada se reducen los problemas de ataques.

- **mSecure 5.7.0**

Los datos se guardan en la memoria y también la nube mediante Dropbox por la sincronización que dispone con cada dispositivo. Mientras se la esté usando los datos se están guardando también se generan las contraseñas.

- **Bitwarden 2.2.8**

La información registrada en la herramienta es resguardad en la base de datos de la herramienta, mantiene a salvo la información mientras trabajas en la red para evitar intrusos.

- **LastPass 4.4.2024**

Resguarda los datos en una base de datos sincronizada con todos los dispositivos de su uso ya que cuenta con una bodega cifrada y una página web para cuidar la in formación mientras está conectado en la red.

3.5.2.10. Desventajas

Se describen las principales desventajas detectadas de cada una de las aplicaciones de seguridad:

- **mSecure 5.7.0**
  - Al hacer actualizaciones la información guardada se pierde,
  - No es compatible con ciertas versiones de Android,
  - Cobran dinero de más para cada actualización nueva.
- **Bitwarden 2.2.8**
  - Al ser de código abierto compromete la seguridad de la información.
  - Los datos no se pueden cargar sin conexión a Internet
  - Bitwarden no puede almacenar imágenes de tarjetas de identificación, etc.
  - El navegador web puede pegar sólo un campo a la vez.
- **LastPass 4.4.2024**
  - Se necesita una buena contraseña para el propio gestor de contraseñas
  - La contraseña maestra es la llave que abre todas las cuentas
  - Al sincronizar las contraseñas con la nube estas podrían ser violentadas.

3.5.3. Evaluación de aplicaciones de seguridad con gestores de contraseñas.

Se evaluará a las aplicaciones seleccionadas según propuesta de (Ramirez, 2016)

para analizar en el estudio, cada uno de estos tiene a considerar un equivalente a una calificación de 0 a 3 donde cero es el menor valor y tres es el mayor valor, considerando las subcaracterísticas, ventajas y desventajas que muestra cada una, en la siguiente categoría:

- Confidencialidad
- Disponibilidad
- Integridad
- Resguardo de datos
- Privacidad
- Facilidad de uso

		mSecure	Bitwarden	LastPass	Análisis
Confidencialidad	**Tipos de algoritmo para cifrar los datos**	3	3	3	Estas herramientas cuentan con el mismo cifrado para la protección de la información, pero Bitwarden utiliza un protocolo extra para brindar mucha más seguridad. Este cifrado es muy favorable para estos gestores.
	Ingreso a la herramienta	2	2	3	Todas las herramientas funcionan con un MASTER PASSWORD para acceder a la base de datos, es la opción más favorable en este aspecto.
	Generador de contraseñas	3	2	2	Las aplicaciones usan generadores con conjunto de caracteres, Bitwarden mientras más fuerte la contraseña más eficaz es el generador de esta. LastPass sincroniza los dispositivos y los resguarda aleatoriamente.

Disponibilidad	**Portabilidad de los datos**	2	3	2	Las aplicaciones están disponibles en todo momento, son portables y compatibles con la mayoría de los sistemas operativos y del navegador, la sincronización les facilita el poder ingresar desde cualquier dispositivo a la herramienta y poder llevar los datos todas partes.
Integridad	**Seguridad en bases de datos**	3	2	2	La Base de Datos que almacena las contraseñas se cifran localmente y luego se envían a la nube (se delega la confianza al fabricante).
Resguardo de datos	**Backup de datos**	2	3	2	Bitwarden cuenta con un KeePass para realizar las importaciones de esta manera el usuario no se tiene que preocupar de ingresar las contraseñas más de una vez. Las otras aplicaciones también cuentan con importación de datos seguros y automático para que el usuario este más cómodo y tranquilo.
Privacidad	**Autocompletado**	3	3	3	Todas las aplicaciones ofrecen autocompletado, lo cual minimiza el riesgo de ataques PHISHING.

	Autenticación de doble factor	3	3	3	Las tres funciones cumplen con múltiples alternativas de doble factor. Pueden ser complejas así como ser de diversas soluciones para la integración.
Facilidad de uso	**Sencillez de uso**	2	2	3	Las tres aplicaciones son fáciles de usar pero LastPass es más fácil que las otras ya que es mas intuitiva y esto la hace mejor opción.
	Idioma	2	2	2	Para las aplicaciones multiplataformas involucran manuales y paginas pero la mayoría de las opciones y funciones están en inglés.
	Plataforma	3	3	2	Las tres aplicaciones son multiplataforma, es decir, adaptables a cualquier dispositivo en todas las plataformas. Aunque LastPass no es compatible con algunas versiones anteriores de Android.
	Integración con navegadores	3	3	3	Las tres aplicaciones se pueden integrar a cualquier navegador gracias a sus opciones de integración.
	Medidor de calidad de contraseñas	3	3	3	Todas las aplicaciones cuentan con medidor de contraseñas seguro.

Tabla 4 Evaluación de aplicaciones de seguridad con gestores de contraseñas.

3.5.4. Resultado de la evaluación

A partir de las calificaciones obtenidas en la tabla, se generan los valores de cada grupo definido agrupándolos en ponderado, cada ponderado es el aspecto a evaluar por cada grupo de cada aplicación de seguridad determina la calificación final de las soluciones descritas.

	mSecure	**Bitwarden**	**LastPass**
Ponderador confidencialidad	2,67	2,33	2,67
Ponderador disponibilidad	2	3	2
Ponderador Integridad	3	2	2
Ponderador Resguardo de datos	2	3	2
Ponderador Privacidad	3	3	3
Ponderador Facilidad	2	2	2
TOTAL	**14,67**	**15,33**	**13,67**

Tabla 5 Resultado de la evaluación

3.5.5. Análisis de la tabla

Bitwarden es la herramienta que obtuvo mejor puntaje de acuerdo a que sobresale en la disponibilidad, resguardo de datos y la privacidad quiere decir que posee niveles adecuados de seguridad, aunque tiene que hacer mejoras en las otras subcaracterísticas especialmente en la integridad.

mSecure posee una buena calificación por su integridad, privacidad y confiabilidad de esta manera también tiene que hacer mejoras en el resguardo de los datos, la

disponibilidad y la facilidad de uso ya que la mayoría de sus funciones están en inglés.

LastPass pese a ser la solución más tercera sobresale en la privacidad, para un usuario que no tenga mucho conocimiento de seguridad puede ser la mejor, fácil de usar en ciertos aspectos.

3.5.6. Conclusión

Con esta información se notó que es necesario utilizar un sistema de protección para la información como un gestor de contraseñas, es una opción muy acertada debido a que se puede acceder a la información con un factor de autenticación. Además, la herramienta de protección debería tener protección para controlar el número de intentos de ingreso de contraseñas fallidas para evitar ataques de fuerza bruta o de diccionario. Aunque Bitwarden fue la herramienta más acta para proteger los datos en este estudio, el dispositivo en el cual se realizó la prueba no fue compatible con esta versión de Android como se había mencionado, por ello se realizaron las pruebas con mSecure que también obtuvo buenos resultados y si es compatible.

3.6. Recursos tecnológicos

3.6.1. Análisis técnico del dispositivo móvil a utilizar con una aplicación

Recurso	Función
Dispositivo móvil.	Es un celular el cual es para comunicarse, recibir y enviar todo tipo de información, el cual nos ayudará para realizar la prueba de nuestro estudio a realizar. Existen ciertos dispositivos que no son compatibles con las aplicaciones por su versión del sistema operativo.

Aplicación de seguridad	Una aplicación de seguridad es para proteger un equipo y la información que se almacena en éste, esta función es opcional por el usuario. También existen ciertas aplicaciones que no son compatibles con ciertos dispositivos y versión del sistema operativo que este tenga instalado.

Tabla 6 Recursos Tecnológicos

3.7. Pruebas

3.7.1.1. Validación

3.7.1.1.1. Pruebas de la seguridad del dispositivo sin la aplicación de seguridad y la aplicación de seguridad instalada en el dispositivo.

En el dispositivo que realizó la prueba con la aplicación de seguridad la cual, si cumple con los parámetros evaluados anteriormente aplicados en el equipo, esta cumple con todo, el detalle es que están en inglés ciertas funciones, pero da una muy buena protección a la información por función de autenticación.

El dispositivo sin la aplicación instalada no cuenta con sistema de autenticación, este cuenta con copias de seguridad y bloqueo de pantalla el cual no es fácil de vulnerar si el usuario aplica una contraseña robusta, pero puede ser vulnerado, las aplicaciones no cuentan con protección, así como con la aplicación de seguridad.

3.8. Factibilidad

3.8.1. Técnicas

En base a las pruebas de campo realizadas con mSecure, técnicamente es viable el manual de usuario, en un 50 por ciento de los datos es adecuado instalar una aplicación de seguridad como es un gestor de contraseñas para que en el equipo mejore la seguridad también se activan las opciones de seguridad que viene incorporada en el dispositivo.

3.8.2. Operativa

El manual se encuentra diseñado de tal manera que sea fácil de interpretar tanto para un usuario experimentado como para uno de conocimiento básico, se muestra como se activan las opciones de configuración de seguridad del equipo y como se instala una aplicación de seguridad y como se usa esta aplicación.

3.8.3. Económica

No se calculó debido a que las aplicaciones de seguridad son gratuitas en su mayoría, pero estas también tienen una versión pagada que cuenta con mejores beneficios y hace la aplicación más efectiva en todas funciones también el menú de opciones aumenta brindando mas efectividad en la seguridad.

3.9. Recomendaciones

- Proteger la información configurando el dispositivo para que se bloquee después de un tiempo de inactividad con contraseñas para acceso a la persona dueña de los datos almacenados.
- Buscar programas para cifrar la información de esta manera no puede ser vista o leída por terceras personas, ya que se resguarda mediante un código secreto que solo la persona debe tener.
- Acudir a la oficina de la operadora cuando el dispositivo es perdido o robado para solicitar que sea bloqueado tanto el equipo como la tarjeta SIM para que así nadie pueda acceder a la información que en éste existe, también se puede activar el bloqueo remoto del dispositivo para borrar la información.
- Crear copias de seguridad de la información almacenada en el dispositivo con regularidad para no tener riesgo de pérdida de información importante.
- Activar una aplicación de seguridad para dispositivos móviles para prevenir la infección de malware o virus, ésta debe proceder de una fuente segura y confiable, también es importante que realice actualizaciones a su sistema operativo para corregir anomalías de fábrica.

- Procurar no conectarse a internet de redes libres o públicas ya que estas permiten que una persona maliciosa ingrese a nuestros dispositivos y robe la información que se tiene guardada, es importante tener protección para esto como usar una VPN.

3.10. Discusión

Los profesores de la ULEAM extensión El Carmen, carrera Ingeniería en Sistemas que fueron los encuestados usan sus dispositivos como sus computadores personales para manejar información tanto de los estudiantes como de ellos mismos en el ámbito laboral, información importante de la universidad por ejemplo informes de comisiones, resultados de autoevaluaciones, horarios de reuniones, notas de los estudiantes, información que ningún estudiante debe saber o modificar.

Si por alguna razón ésta información llegase a ser divulgada, la seguridad de los dispositivos debe ser mejorada por cada usuario en su equipo, ya que podrían filtrarse usuarios y claves de sus cuentas de la institución y la información puede ser modificada o borrada, la institución seria perjudicada y la información de los estudiantes también.

3.4. MANUAL DE USUARIO SOBRE SEGURIDAD LÓGICA INFORMÁTICA DE LOS TELÉFONOS INTELIGENTES.

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ

EXTENSIÓN EL CARMEN

- **Objeto del documento**

Este documento pretende mostrar al usuario como proteger su información con la seguridad lógica informática en los dispositivos móviles. Es un manual dirigido a las personas que tienen poco conocimiento de la seguridad incorporada en los dispositivos también la seguridad que brindan las distintas aplicaciones de seguridad.

- **Dirigido a:**

Todas las personas que usan un Smartphone con sistema operativo Android y tiene poco conocimiento de cómo aplicar la seguridad en sus equipos. Para poder obtener este documento se lo puede realizar en Play Store con formato PDF, ya que es más fácil de descargar y no pesa mucho en megas también se lo puede abrir en cualquier dispositivo.

- **Objetivo**

Mostrar de una manera clara y concisa el funcionamiento de la seguridad lógica en los dispositivos móviles para la protección de los datos. Se mostrará como activar la seguridad de su equipo, es decir, la seguridad que viene incorporada en el sistema operativo más la instalación de una aplicación de seguridad.

- **Sistemas operativos para dispositivos móviles**

Tenemos que tener conocimiento acerca de qué sistema operativo tiene incorporado nuestro dispositivo, para poder desenvolvernos bien en el uso del dispositivo. Son varios los sistemas operativos para móviles que existen tales como: Android, iOS, Symbian, BlackBerry y Windows Phone. Los sistemas operativos para dispositivos móviles son un poco más fáciles que los de computadores. (Bustamante, 2016)

Cada uno de los sistemas operativos cuenta con su propia configuración de seguridad incorporada, van mejorando con las actualizaciones creadas para cada versión con el paso del tiempo, esto hace que los equipos brinden mayor protección a los usuarios. Cada sistema operativo realiza sus propias mejoras para destacar de los otros sistemas.

- **Aplicaciones de seguridad**

Cada una de las aplicaciones de seguridad o antivirus cuentan con una característica en particular para destacar de las demás, aunque la mayoría cuenta con limpiadores de archivos, liberadores de espacio, seguridad personal para cada aplicación, ahorro de energía, existen muchas características para herramienta de seguridad. A continuación, se muestra una pequeña lista de algunas aplicaciones de seguridad para el sistema Android:

- **Especializadas en gestores de contraseñas**
    - **LastPass:** es uno de los métodos de almacenamiento y generación de contraseñas más usados.
    - **BitWarden**: se encarga de almacenar toda la información relacionada con nuestras cuentas.
    - **Myki**: es el gestor de contraseñas con una de las opciones más originales y seguras que se pueden usar gracias a su protección de grado militar.
    - **Dashlane:** una de las aplicaciones de almacenamiento y generación de contraseñas más populares que existen.

- **mSecure:** está diseñada para proteger la información con el modelo de cifrado AES contiene generador de contraseñas seguras y autenticador de huella dactilar.
- **SplashID Safe:** se considera una de las mejores ya que permite guardar la información personal en una caja fuerte con cualquiera de los métodos de seguridad, sus funciones añaden el cifrado AES-256 para mayor protección.

Manual de usuario

- **Pantalla inicial**

La pantalla de inicio muestra todas las opciones de aplicaciones en el dispositivo, entre ellas está la opción de ajustes o configuración para activar las configuraciones de seguridad del dispositivo.

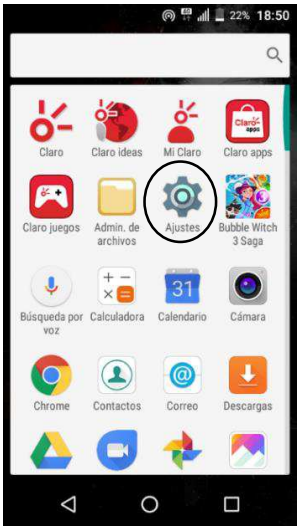


Figure 1 Pantalla de inicio

- **Ingreso a ajustes**

En ajustes se muestran algunas opciones de las cuales seleccionamos la de seguridad y se procede a abrir.

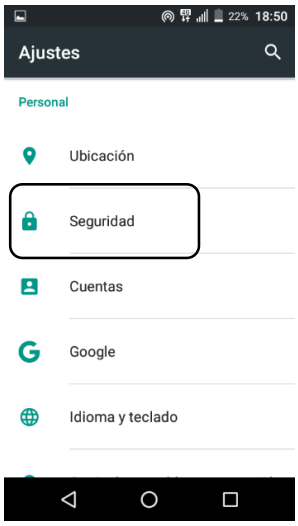


Figure 2 Ingreso a ajustes

- **Lista de opciones de seguridad del dispositivo.**

Se muestran algunas opciones de seguridad las cuales son: bloqueo de pantalla, bloqueo automático, mensaje de pantalla bloqueada, Smart Lock, encriptar teléfono, administradores de dispositivo.

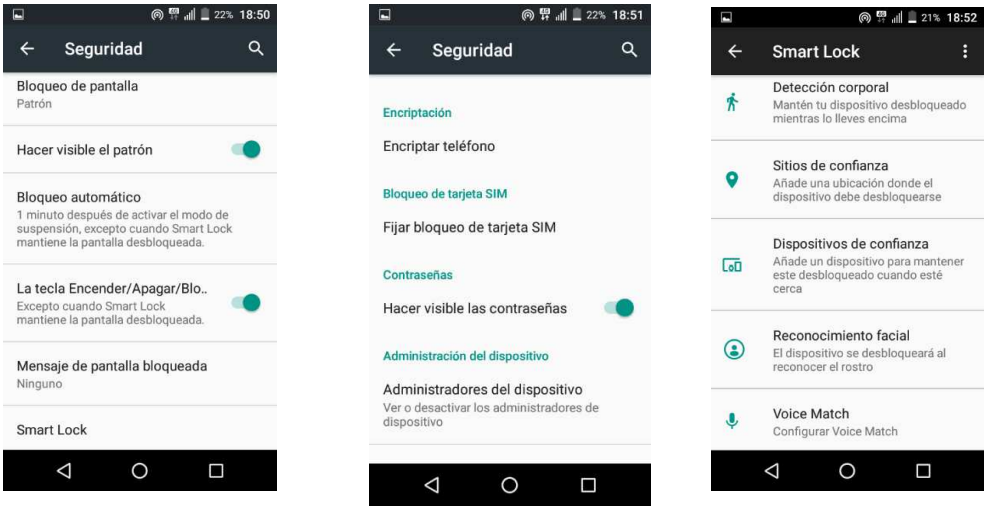


Figure 3 Lista de opciones

- **Selección de opción de seguridad**

Seleccionar la opción que se desea usar para resguardar su equipo;

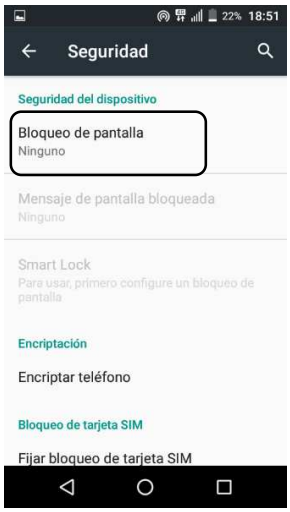


Figure 4 Selección de opciones

Seleccionamos bloqueo de pantalla para escoger una de las opciones de seguridad que se muestran;

Figure 5 Elección de seguridad

Luego de escoger el patrón como tipo de seguridad, dibujamos el tipo de patrón que vamos a usar para proteger el equipo.

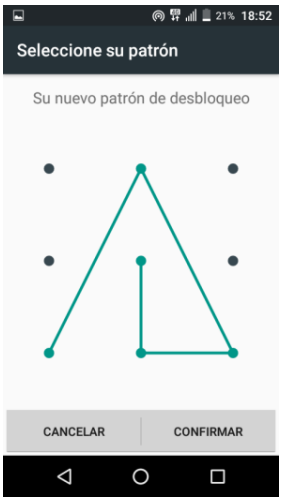


Figure 6 Selección terminada

- **Verificación de seguridad en el dispositivo**

Probará que la opción escogida después de la activación, bloqueando el equipo y desbloqueando ya con la opción de seguridad activada, para comprobar que si funciona la seguridad escogida.

Figure 7 Muestra confirmada

Figure 8 Muestra terminada

- **Respaldos de información**

Se activan las copias de seguridad y respaldos de información del dispositivo automáticamente como contraseñas e historial de llamadas y datos de aplicaciones

de forma remota, para tener respaldos y poder restaurar la información de todo tipo como información sensible, archivos, contactos, fotos, etc. en caso de pérdida del dispositivo.

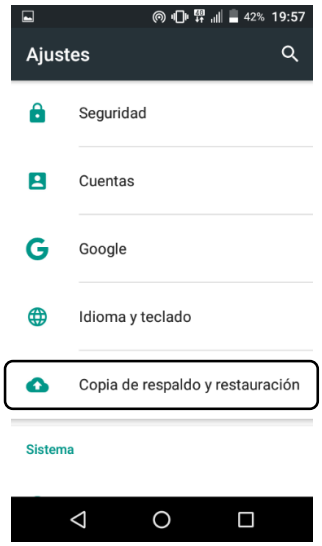


Figure 9 Respaldo de información

También se elige una cuenta de correo electrónico para que guarde en drive la información de las copias de seguridad, es decir, que esta información se guarde en la nube.

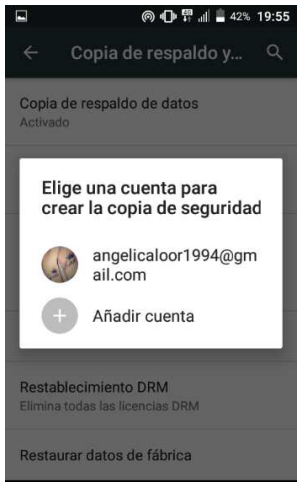


Figure 10 Elección de cuenta

- **Cuentas**

Se crea una cuenta de correo electrónico de google para vincularla con el dispositivo de esta manera se guardarán los datos en esta cuenta de forma automática como los respaldos, contactos, archivos, fotos, restauración de contraseñas, correos y más.

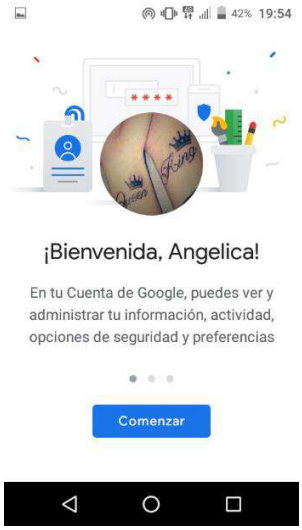


Figure 11 Confirmación de cuenta vinculada

- **Administradores de dispositivo**

Esta opción se activa para encontrar un dispositivo en caso de que se pierda, puede bloquear o borrar la información que éste contenga de forma remota.

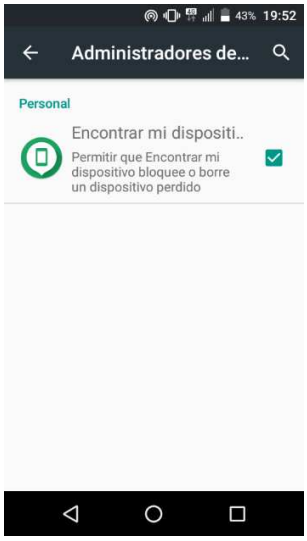


Figure 12 Administrador de dispositivo

- **Actualizar sistema**

Tiene que actualizar el sistema operativo del dispositivo con regularidad para que el dispositivo tenga mejor rendimiento y sea más eficiente con las nuevas versiones.

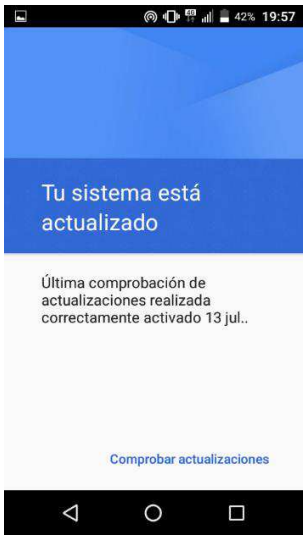


Figure 13 Actualización del sistema operativo

- **Búsqueda e Instalación de aplicación de seguridad**

Para realizar la instalación de la aplicación de seguridad, lo que hay que hacer es algo muy fácil. Se tiene que ingresar a Play Store, escriba en el navegador el nombre de la aplicación deseada para Android como resultado aparece una larga lista de aplicaciones de seguridad, entonces se procede a seleccionar mSecure-Password Manager y se procede a la instalación de la aplicación en el dispositivo.

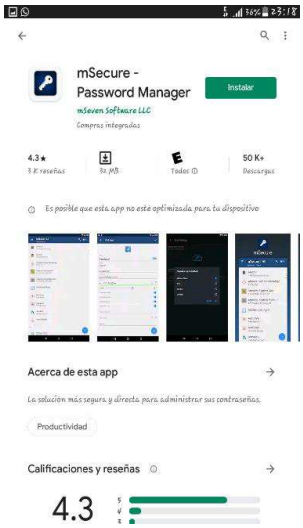


Figure 14 Búsqueda, encuentro e instalación de la aplicación

Una vez instalada la aplicación en el equipo se procede a abrirla entonces se muestra un mensaje de bienvenida con indicaciones y mensajes de las funciones que ofrece la aplicación.

Figure 15 Bienvenida a la aplicación

- **Creación de cuenta para ingresar a la aplicación**

Después de la presentación de la aplicación se presiona en el botón de empezar, entonces aparece el siguiente paso que es crear una cuenta con correo electrónico

y contraseña para ingresar a la aplicación de una manera más segura y única para el usuario.

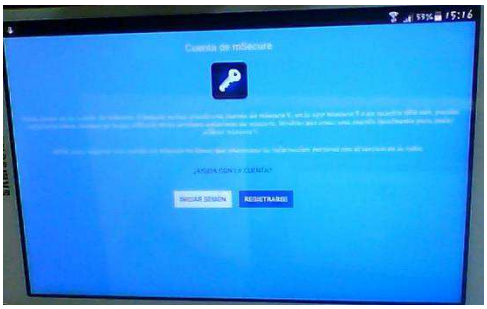


Figure 16 Creación de cuenta para ingresar a la aplicación

Figure 17 Confirmación de ingreso en la aplicación

- **Confirmar en que plataforma guardar la información**

Después de crear la cuenta y la contraseña aparece otra ventana confirmando el ingreso a la aplicación ya con la cuenta creada, después presionamos el botón para continuar entonces aparece otra ventana para confirmar en que plataforma se guardara la información.

En esta sección se escoge en qué lugar se guardará la información del dispositivo desde una cuanta alterna hasta la nube o Dropbox en vinculación con la aplicación.

Figure 18 Confirmación donde guardar la información

- **Interface de la aplicación**

Una vez escogido en qué lugar se resguardará la información aparece la interface de la aplicación, donde una vez guarda información esta aparece aquí en una lista. Con el icono de cada aplicación, en esta parte también se añade una aplicación nueva para proteger en el botón con el signo mas.

Figure 19 Interface de la aplicación

- **Menú de funciones de la aplicación**

Este es el menú de la aplicación donde está distribuida por categorías el tipo de información, como tarjetas de crédito, notas importantes, cuentas bancarias y más. En la parte inferior derecha existe un botón con el signo mas éste es para agregar la información.

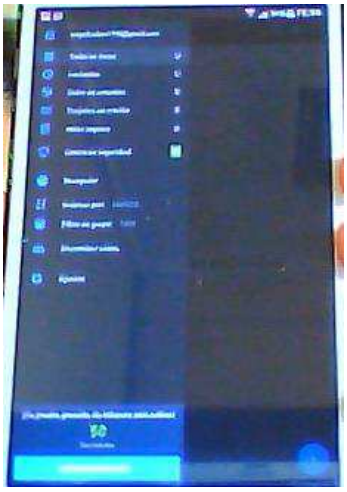


Figure 20 Menú de aplicación

- **Pantalla de inicio de aplicación**

Las funciones de esta aplicación en este dispositivo solo son una prueba de 30 días, ya que es gratuita después de esto hay que pagar un coste por esta aplicación y sus funciones.

Figure 21 Interface de ingreso

Así es la interface de ingreso, ya que necesita una contraseña para ingresar esta aplicación es segura es por ello que no permite hacer capturas de la misma.

Nota: Las aplicaciones son seguras, pero no en un cien por ciento ya que a los programadores se les puede pasar algún detalle por alto, entonces existen las actualizaciones, es por ello que es recomendable e importante actualizar la aplicación de seguridad cada vez que salga una actualización.

Algoritmo AES-128, AES-192, AES-256 o Rijndael: Advanced Encryption Standard, es un algoritmo de encriptación simétrica con un esquema cifrado en bloques, desde el 2006 se convirtió en uno de los más populares y seguros en la seguridad de la información. Estos algoritmos están basados en dificultades de descifrado que presenta cada uno de ellos; para el AES-128 son 10 rondas de llaves, para AES-192 son 12 rondas de llaves, para AES-156 son 14 rondas de llaves, de esta manera, es por esto que no es fácil de descifrar. (MTEK, 2019)

4. CONCLUSIONES

- La fundamentación teórica sobre seguridad lógica informática y dispositivos móviles permitieron obtener información actualizada realizada por varios autores aportando conocimiento para el tema.

- Las metodologías usadas en este estudio ayudaron mucho a realizar la investigación, la obtención de información mediante las técnicas de la encuesta y entrevista permitieron darnos cuenta que los usuarios no protegen adecuadamente sus datos.

- La comparación de las herramientas móviles de seguridad lógica informática para teléfonos inteligentes nos da a entender que para cualquier usuario es necesario utilizar un sistema de seguridad, es decir una herramienta para proteger su información y la más acertada es un sistema de gestión de contraseñas.

- El desarrollo del manual de seguridad lógica informática de los teléfonos inteligentes, con los resultados de la comparación de las aplicaciones de seguridad donde se demostró un gestor de contraseña es una buena opción para proteger la información y el dispositivo.

5. RECOMENDACIONES

- A los usuarios que estén muy pendientes de la protección de sus datos y a quien le permiten acceder a estos realizando un seguimiento de seguridad continuamente a sus dispositivos.

- A los usuarios que vinculan sus celulares con los datos importantes de su trabajo, tengan particionados sus dispositivos para que la información este bien protegida en caso que un intruso ingrese a su dispositivo. Utilizar gestores de contraseñas, para así tener mayor protección de la información.

- A las personas que utilizan varias contraseñas para ingresar a sus aplicaciones de comunicación se recomienda usen un gestor de contraseñas que se ajuste a sus necesidades, estos facilitan la administración de sus contraseñas, aunque tienen pros y contras, son muy buena alternativa.

6. BIBLIOGRAFÍAS

Baca, U. G. (2016). seguridad lógica en las redes. En U. G. Baca, *Introduccion a la seguridad Informatica* (págs. 156-192). España: grupo editorial Patria.

Bustamante, J. J. (2016). los sistemas operativos para dispositivos móviles y para pcs. *wordpress.com*, 2-15.

Castillero, O. (2010). Los 15 tipos de investigación y características. En O. Castillero, *Metodologías de la Investigación* (pág. 5). Mexico: Mexico.

Costas, S. J. (2014). *Seguridad informática.* Sevilla: RA-MA S.A.

Davitic. (2017). seguridad informática. *daviticblog*, 1-4.

debitoor, e. (18 de agosto de 2017). *debitoor*. Obtenido de debitoor: https://debitoor.es/glosario/privacidad-y-proteccion-de-datos-personales

Dominguez, M., Paredes, V., & Santacruz, L. (2014). *Programacion Multimedia y Dispositivos Móviles.* Madrid: RAMA, copyrignht.

Enriquez, O. M. (2018). Marco juridico de la proteccion de datos personales en las empresas de servicios establecidas en mexico. *revista IUS*, 3-4.

Escrivá, G. G. (2013). *Seguridad informática.* españa: macmillan iberia.

Gómez, A. (2014). *Enciclopedia de la seguridad informática.* España: RA-MA.

Jaramillo, O., & Eraso, S. (2015). Seguridad en dispositivos móviles Android. En O. Jaramillo, & S. Eraso, *Seguridad en dispositivos móviles Android* (pág. 46). Universidad nacional UNAD: Universidad nacional UNAD.

Ledesma, R. (2017). Técnicas de investigación. En R. L., *Metodologias de la investigacion* (págs. 92-108). México: A. S.A.

Lescano, M., & Elisa, Z. (2017). Seguridad en el comercio electrónico. *Tesis Digitales UNMSM*, 2-5.

Luna, F. (2016). *Desarrollo web para dispositivos móviles.* Buenos Aires: copyright.

Mediano, C. M. (2014). *Ténicas e instrumentos de recogida y Analisis de Datos.* España.

Mendez, J., & Rodriguez , D. (2016). El cuestionario y la Entrevista. *OUC, universidad de Catalunya*, 8-9.

Meneses, J., & Rodriguez, D. (2014). El cuestionario y la entrevista. *univsantana*, 8-9.

MTEK, G. L. (2019). AES-256, el algoritmo de encriptación que aumenta la seguridad BLOCKCHAIN. *MTEK Labs. All rights reserved.*, 2-8.

Pacheco, V., Piazza Orlando , S., & Carlos , D. (2016). Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las. En P. Veliz, S. Piazza Orlando, & D. Carlos , *Estudio y análisis de seguridad en dispositivos móviles.* (págs. 54-55). La Plata: Universidad Nacional de la Plata.

Paz, M. M. (2010). *Seguridad Lógica y de accesos y su Auditoría.* Madrid: Universidad Carlos III.

Ponce, L. B., Juanes Menéndez, J., & Garcia Peñalvo , F. (2015). *Dispositivos móviles y Apps.* España: Universidad de Salamanca.

Públicos, D. N. (2018). Ley de Proteccion de Datos Personales una oportunidad para el Ecuador. *Datos Puúlicos*, 1-3.

Ramirez, M. A. (2016). *Análisis de Seguridad y Uso de Gestores de Contraseñas.* Buenos Aires: Biblioteca digital de la facultad de Ciencias Económicas.

Resumen de reglamento de Proteccion de Datos. (2019). *Digital Guide*, 1-2.

Rodriguez, A. m. (2014). Diseño y validación de instrumentos de medición. *Dialogos*, 20-21.

Rodriguez, E. (2005). Métodos de Investigacion. En E. Rodriguez, *Motodologías de la Investigacion* (págs. 28-30). Mexico: Universidad de Juarez.

Velazco, W. V. (2018). Políticas y Seguridad de la información. *Fides et Ratio*, 3-4-5.

Vélez, A. (2017). ¿cómo sera la seguridad de tu celular en los proximos años? *parentesis.com*, 1-4.

Vieites, Á. G. (2017). *Enciclopedia de la seguridad informática.* Madrid: RAMA S.A.

7. ANEXOS

7.1. Anexo A

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ
Proyecto de Investigación "Auditoría y Seguridad Informática"

CERTIFICACIÓN

Quien suscribe Ing. Clara Guadalupe Pozo Hernández, Directora del proyecto de Investigación "AUDITORÍA Y SEGURIDAD INFORMÁTICA" tengo a bien CERTIFICAR:

Que la señorita **LOOR CAMPOSANO ANGÉLICA ESTEFANÍA**, portadora de la cédula de ciudadanía N° **1314426840,** ha realizado el trabajo de investigación:**" ESTUDIO DE SEGURIDAD LÓGICA INFORMÁTICA APLICADA EN DISPOSITIVOS MÓVILES PARA PROTECCIÓN DE SUS DATOS"**, como una actividad del proyecto de investigación, "Auditoría y Seguridad Informática" durante el período 2019(1) y 2019(2) según la planificación y documentación que reposa en los archivos del proyecto.

La señorita **LOOR CAMPOSANO ANGÉLICA ESTEFANÍA**, puede hacer uso del presente documento en lo que estime conveniente, dentro del marco legal académico establecido.

El Carmen, 06 de enero del 2020

Ing. Clara Guadalupe Pozo Hernández, Mg.
DIRECTORA DEL PROYECTO

Anexo 1 Certificación de director de proyecto

7.2. Anexo B

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN

CARRERA DE INGENIERÍA EN SISTEMAS

Proyecto de titulación

Encuesta realizada en la universidad LAICA Eloy Alfaro de Manabí Extensión en El Carmen, con la finalidad de conocer si los usuarios tienen en sus dispositivos sistemas de seguridad para proteger sus datos, y de esta manera poder realizar un estudio.

Encuesta

Objetivo:
Conocer el tipo de protección que utilizan los usuarios para sus datos y que tan importante es para ellos el protegerlos.

Dirigido a: Los profesores de la carrera de Ingeniería en Sistemas.

1. **¿Utiliza un dispositivo Smartphone?**

   Si ☐ No ☐

2. **¿Utiliza contraseñas para ingresar a su dispositivo móvil?**

   Si ☐ No ☐

3. **¿Tiene algún antivirus instalado en su dispositivo móvil?**

   Si ☐ No ☐

4. **¿Qué tan seguro considera el antivirus instalado en su dispositivo móvil?**

   Muy seguro ☐

   Seguro ☐

   Poco seguro ☐

   Nada seguro ☐

5. **¿Cuándo va a instalar una aplicación en su dispositivo lee las políticas de privacidad de la aplicación previo a la instalación?**

   Si ☐ No ☐

6. **¿Conoce algún tipo de seguridad para proteger los datos de su celular?**

   Sí ☐ No ☐

7. **¿Cuál de las siguientes opciones utiliza para la protección de sus datos?**

   Respaldo en la nube ☐

   Respaldo en alguna cuenta alterna de correos ☐

   Copias de seguridad de su dispositivo móvil ☐

   Copias en un dispositivo externo ☐

8. **¿Cada que tiempo hace respaldo de seguridad de sus datos?**

   Diario ☐

   Cada tres días ☐

   Cada semana ☐

   Cada mes o más ☐

9. **¿Qué tan importante considera proteger los datos de su dispositivo?**

   Muy importante ☐

   Importante ☐

   Poco importante ☐

   Nada importante ☐

10. **¿Conoce alguna aplicación o herramienta que le permita medir la seguridad lógica de su dispositivo para lograr proteger sus datos?**

    Sí ☐ No ☐

Anexo 2 Formato de encuesta

7.3. Anexo C

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ EXTENSIÓN EL CARMEN

CARRERA DE INGENIERÍA EN SISTEMAS

Proyecto de titulación

Entrevista realizada al coordinador de la carrera de Ingeniería en Sistemas con la finalidad recolectar datos importantes y de esta manera poder realizar el estudio.

Entrevista

1. ¿Conoce algunos métodos o aplicaciones para proteger los datos de su celular?
2. ¿Utiliza algunos de los métodos o aplicaciones mencionados anteriormente para proteger su celular?
3. ¿Qué tan segura en para usted la aplicación que usa para proteger sus datos?
4. ¿El método que utiliza para proteger su celular lo considera seguro?
5. ¿Considera que, con la aplicación de protección de su celular, éste podría ser hackeado?
6. ¿Por qué es importante para usted el proteger sus datos?
7. ¿Cree que sus datos están bien protegidos con la aplicación que utiliza?
8. ¿Cree que respaldar los datos en la nube es seguro?
9. ¿Utiliza antivirus en su celular?
10. ¿Cree que los antivirus protegen bien a los celulares de los virus?

Anexo 3 Formato de entrevista

7.4. Anexo D

	NOMBRE DEL DOCUMENTO: NOTIFICACIÓN DE DESIGNACIÓN DE TUTORES	CÓDIGO: PAT-01-F-007
Uleam	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO	REVISIÓN: 1
		Página 6 de 13

COMISIÓN ACADÉMICA
EXTENSIÓN EL CARMEN

MEMORANDUM No. 006-2019-PCA-TCL-CIS

PARA: **An. Soraida Zambrano, Mg. tutor(a) designado(a)**
DE: **Eco. Tito Cedeño Loor, Mg., Presidente Comisión Académica**
ASUNTO: **Designación para desarrollar tutorías de titulación**
FECHA: **El Carmen, 8 de febrero del 2019.**

En cumplimiento a la distribución de la carga horaria dispuesta dentro de la planificación académica de esta unidad y considerando los artículos 76 y 77 del proceso de titulación del Reglamento de Régimen Académico, la Comisión Académica de la Extensión El Carmen, ha considerado que, de acuerdo con su experticia en el área de conocimiento asignado, usted deberá dirigir y verificar el desarrollo de los trabajos de titulación de los siguientes estudiante

Estudiante/s	Nivel	Modalidad de Titulación	Tema de investigación
Giraldo Cevallos Lenner Arturo	Noveno	Proyecto de Investigación	Estudio informático forense para dispositivos electrónicos de los estudiantes de la "Universidad Laica Eloy Alfaro de Manabí Extensión en El Carmen"
Loor Camposano Angélica Estefanía	Noveno	Proyecto de Investigación	Auditoría informática para la seguridad lógica aplicada en la radio Eco FM. en el cantón El Carmen
Alvia Alava Verónica Cecilia	Noveno	Proyecto de Investigación	Estudio de seguridad lógica informática aplicada en dispositivos móviles para la protección de sus datos

Además, es de vital importancia su aporte profesional en los trabajos de tutorías desarrollados por los demás compañeros tutores, debiendo realizar equipos de trabajo en conjunto, para lo cual le adjunto el informe de designación de tutorías, el mismo que ha sido conocido por el Consejo de Facultad.

Particular que se informa para los fines consiguientes.

Atentamente,

Eco. Tito Cedeño Loor, Mg.
PRESIDENTE COMISIÓN ACADÉMICA
toti_cede01@hotmail.com

08-02-2019

Elaborado por: Patricio Quiroz

Anexo 4 Asignación de Tutor de Titulación

7.5. Anexo E

	Preguntas	profesor 1	profesor 2	profesor	profesor 4	profesor 5	profesor (	profesor 7	profesor (	profesor 9	profesor 1(	profesor 11	profesor 1:	profesor 1:	profesor 1·	profesor 1:	profesor 1	profesor 1	profesor 18	
1	¿Utiliza un dispositivo Smartphone?																			TOTAL
	si	x		x	x	x		x	x	x	x	x	x	x	x	x	x	x		15
	no		x				x												x	3
2	¿Utiliza contraseñas para ingresar a su dispositivo móvil?																			
	si		x		x							x							x	4
	no	x		x		x	x	x	x	x	x		x	x	x	x	x	x		14
3	¿Tiene algún antivirus instalado en su dispositivo móvil?																			
	si	x		x	x		x			x	x					x				7
	no		x			x		x	x			x	x	x	x		x	x	x	11
4	¿Qué tan seguro considera el antivirus instalado en su																			
	muy seguro			x																1
	seguro	x				x		x		x	x							x		6
	poco seguro		x																	1
	nada seguro				x		x		x			x			x				x	6
5	¿Cuándo va a instalar una aplicación en su dispositivo lee las políticas de privacidad de la aplicación previo a la instalación?																			
	si	x			x	x	x			x		x		x			x		x	9
	no		x	x				x	x		x		x		x	x		x		9
6	¿Conoce algún tipo de seguridad para proteger los datos de su																			
	si			x		x	x			x		x	x			x		x	x	9
	no	x	x		x			x	x		x			x	x		x			9
7	¿Cuál de las siguientes opciones utiliza para la protección de sus																			
	respaldo en la nube	x		x	x		x	x		x	x			x	x	x	x	x	x	13
	respaldo en una cuenta alterna de correos		x		x	x			x											4
	copias de seguridad de su dispositivo						x					x	x		x		x		x	6
	copias en un dispositivo externo							x												1
8	¿Cada que tiempo hace respaldo de seguridad de sus datos?																			
	diario			x				x												2
	cada tres días																			
	cada semana											x								1
	cada mes o más	x	x		x	x	x			x	x			x	x	x	x	x	x	13
9	¿Qué tan importante considera proteger los datos de su																			
	muy importante	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	17
	importante																			1
	poco importante							x												
	nada importante																			
#	¿Conoce alguna aplicación o herramienta que le permita medir la seguridad lógica de su dispositivo para lograr proteger																			
	si			x									x							2
	no	x	x		x	x	x	x	x	x	x	x		x	x	x	x	x	x	16

Anexo 5 Resultado de la encuesta