

UNIVERSIDAD CATOLICA DE EL SALVADOR

FACULTA DE CIENCIAS EMPRESARIALES



INFORME FINAL DE INVESTIGACIÓN

**EVALUACIÓN DE LAS APLICACIONES DE SEGURIDAD DE INFORMACIÓN DE
LOS SMARTPHONES DE LOS ALUMNOS DE LA UNIVERSIDAD CATÓLICA DE EL
SALVADOR EN EL AÑO 2015**

PRESENTADO POR

LINARES GARCIA, JOSÉ ERNESTO

TRABAJO DE GRADUACIÓN

PARA OPTAR AL GRADO ACADÉMICO DE

LICENCIADO EN SISTEMAS INFORÁTICOS ADMINISTRATIVOS

MARZO 2016

SANTA ANA, EL SALVADOR, CENTROAMÉRICA

UNIVERSIDAD CATÓLICA DE EL SALVADOR

UNICAES

AUTORIDADES ACADÉMICAS

MONSEÑOR Y LICENCIADO FRAY ROMEO TOVAR ASTORGA

RECTOR

DOCTOR MOISÉS ANTONIO MARTÍNEZ ZALDÍVAR

VICERRECTOR GENERAL

MÁSTER CÁSTULO AFRANIO HERNÁNDEZ ROBLES

SECRETARIO GENERAL

MAESTRA CENIA PATRICIA ORELLANA

DECANA DE LA FACULTAD DE CIENCIAS EMPRESARIALES

DEDICATORIAS Y AGRADECIMIENTOS

A DIOS TODO PODEROSO: Gracias a él es que este sueño de ser una persona de bien a la sociedad se a cumplido, permitiendome haber compluido con satisfacción la carrera que emepece ya hace 10 años, gracias por escuchar mis oraciones y que esto sea el comienzo de un futuro mejor AMEN.

A MI MADRE: a mi querida madre, por brindarme la oportunidad de comenzar un largo camino que me ha ayudado a recorrerlo junto a mi, por haber sacrificado mucho para sacarnos adelante desde los estudio primario hasta este momento que soy profesional.

A MI ESPOSA: por ser una parte muy especial en mi vida esa persona que me alienta día con día, la que me cuida, la que me dio la bendicion de ser padre, gracias por comprenderme y apoyarme en todo mi camino universitario,

A MI HIJA: por ser el motor, mi vida mi bendicion y por siempre resivirme con una sonrisa en los dias de trabajo, por su amor

A MI ASESOR: por guiarme en este proceso de graduación por tenerme paciencia y organizarse con su trabajo y el asesoramiento hacia mi persona gracias a él y a Dios se hace realidad el sueño de toda mi familia

INDICE

INTRODUCCIÓN.....	i
CAPÍTULO I: GENERALIDADES: EVALUACIÓN DE LAS APLICACIONES DE SEGURIDAD DE INFORMACIÓN DE LOS SMARTPHONES DE LOS ALUMNOS DE LA UNIVERSIDAD CATÓLICA DE EL SALVADOR EN EL AÑO 2015	2
1.1 Planteamiento del problema	2
1.2 Justificación de la investigación	4
1.3 Objetivos generales	6
Objetivos específicos.....	6
Hipótesis de la investigación.....	7
CAPÍTULO II: MARCO TEÓRICO Y ANTECEDENTES DE EVALUACIÓN DE LAS APLICACIONES DE SEGURIDAD DE INFORMACIÓN DE LOS SMARTPHONES DE LOS ALUMNOS DE LA UNIVERSIDAD CATÓLICA DE EL SALVADOR EN EL AÑO 2015.....	8
2.1 Teléfonos móviles inteligentes o Smartphone.	8
2.2 Algunas características de los Smartphone.....	9
2.3 Sistemas operativos que existen en los mercados.	10
2.3.1 Android:.....	10
2.3.2 iOS:	11
2.3.3 Windows Phone:	12
2.3.4 BlackBerry OS:.....	13
2.3.5 Symbian:	13
2.4 Aplicaciones móviles.....	14
2.4.1 definición:	14
2.5 Tipos de aplicaciones móviles.	15

2.5.1 App Nativas:.....	16
2.5.2 Web App:	17
2.5.3 Web App Nativas ó Híbridas.	18
2.6 AppStore Donde se descargan aplicaciones según si sistema operativo. ...	19
2.6.1 AppStore	19
2.6.2 Google Play.....	20
2.6.3 Windows phone Store	20
2.6.4 BlackBerry World.....	20
2.6.5 Ovi Store	21
2.7 ¿Qué son las App de seguridad móvil?	21
2.8 APLICACIONES MEJORES EVALUADAS EN LOS DIFERENTES SISTEMAS OPERATIVOS DETALLANDO LA UTILIZACIÓN PARA LA QUE FUERON CREADAS	22
2.8.1 Android:.....	22
2.8.2 iOS:	25
2.8.3 Windows Phone:	27
2.8.4 BlackBerry OS:.....	28
2.8.5 Symbian:	29
2.8.6 Backup	30
2.8.7 Sincronización de datos	31
3. CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN PARA LA EVALUACIÓN DE LAS APLICACIONES DE SEGURIDAD DE INFORMACIÓN DE LOS SMARTPHONES DE LOS ALUMNOS DE LA UNIVERSIDAD CATÓLICA DE EL SALVADOR EN EL AÑO 2015	32
3.1 Tipo de Investigación.	32
3.2 Población y muestra.	32

3.3 técnicas e instrumentos.....	34
Técnica.....	34
Instrumento.....	34
3.4 Procedimientos.....	35
3.5 Análisis Estadístico.....	35
4. CAPÍTULO IV RESULTADO DE LA INVESTIGACIÓN PARA LA EVALUACIÓN DE LAS APLICACIONES DE SEGURIDAD DE INFORMACIÓN DE LOS SMARTPHONES DE LOS ALUMNOS DE LA UNIVERSIDAD CATÓLICA DE EL SALVADOR EN EL AÑO 2015.....	36
4.1 Importancia de tener una App de seguridad.....	36
4.2 Análisis de la investigación de campo realizada a los alumnos de la UNICAES ciclo II 2015.....	37
4.2.1 Análisis de la encuesta dirigida a los estudiantes.....	38
5. CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES.....	46
BIBLIOGRAFÍA.....	50
CRONOGRAMA DE LA INVESTIGACIÓN.....	51
ANEXOS.....	52

INTRODUCCIÓN

El presente trabajo comprende una investigación acerca de la evaluación de las aplicaciones de seguridad además del estudio de las diferentes aplicaciones que brindan los diferentes sistemas operativos en los teléfonos inteligente utilizados por los alumnos de la Universidad Católica de El Salvador.

En la actualidad la importancia de las aplicaciones de seguridad móvil queda ejemplificada si se observan la enorme demanda que hoy en día tienen los Smartphone, las Tablet y cualquier equipo inteligente que permita la entrada al mundo del internet.

La banda ancha móvil continúa ganando adeptos en Latinoamérica. El uso de los teléfonos inteligentes ya a un nivel que alcanza un 70%, y son los jóvenes entre 15 y 29 años, el grupo etario que más utiliza este tipo de servicios, como la mensajería instantánea, WhatsApp y servicios de video. Así lo muestra en el estudio hecho por Ericsson Consumer Lab. Dicho estudio añade también que todavía mantiene un alto potencial de crecimiento especialmente en las redes 4G, ya que los usuarios cada vez más requieren mayor capacidad de datos para servicios avanzados.

La teoría sociológica urbana de la protección de datos, nos permite realizar encuestas a los diferentes tipos de estudiantes de diferentes decanatos pertenecientes a la Universidad Católica de El Salvador. Luego de estas encuestas, se tendrá una estadística de como los estudiantes son capaces de confiar los datos más importantes a las aplicaciones diseñadas a la seguridad de sus cuentas, datos, contraseñas, imágenes y todo lo relacionado a información.

Se demostrara como los estudiantes aseguran la información más importantes dentro de sus equipos inteligentes, que es lo que un estudiante realiza cuando sufre el robo, pérdida o el mal funcionamiento de sus equipos inteligentes, además se utiliza de manera adecuada las herramientas necesarias para la recuperación de información.

CAPÍTULO I: GENERALIDADES: EVALUACIÓN DE LAS APLICACIONES DE SEGURIDAD DE INFORMACIÓN DE LOS SMARTPHONES DE LOS ALUMNOS DE LA UNIVERSIDAD CATÓLICA DE EL SALVADOR EN EL AÑO 1015

1.1 Planteamiento del problema

Los jóvenes actuales, tienen acceso a una amplia gama de tecnología lo cual facilitan la vida del estudiante pero, ¿Qué tan seguras y confiables son las aplicaciones de seguridad en los Smartphone o Tablet de los alumnos de la universidad Católica de El Salvador?

Particularmente, el problema del bajo nivel de seguridad que presenta algunas aplicaciones móviles, así como la falta de información y de manuales para la buena utilización de estas aplicaciones hace que nuestra información y documento sean vulnerables.

La necesidad de seguridad acompaña la evolución de los Smartphone. Al tener más capacidad de almacenamiento y procesamiento, la información estratégica podría perderse o podría ser extraída de manera ilegal a través de hackers en el caso de que un Smartphone se pierda, sea robado o se encuentre desprotegido.

Los usuarios de teléfonos móviles han ido incrementando en los últimos años, debido a la extensa variedad de aplicaciones que pueden instalar. La navegación e intercambio de información en internet se ve beneficiada por la mejora de las redes inalámbricas (Wi-Fi), facilitando el envío y recepción de correos electrónicos en cualquier momento, así como la realización de diversas transacciones online.

Para garantizar el correcto funcionamiento del dispositivo, es esencial estar bien informado sobre las ventajas y desventajas respecto de las prestaciones que ofrece el teléfono. También hay que considerar que al mismo tiempo que nos

mantiene comunicados, nos expone a peligros cuando éste es usado o intervenido sin nuestro permiso. Las conversaciones vía telefónica o por mensajes de texto pueden contener información confidencial y sensitiva, la cual podría ser escuchada o leída por otros a nivel global, cuando el móvil se encuentra conectado al internet. Por eso es importante llevar a cabo algunas medidas de seguridad para proteger el dispositivo y la información contenida en él.

Ante todo, un teléfono inteligente requiere de un manejo inteligente, sobre todo en términos de seguridad. El Smartphone debe recibir el mismo tratamiento que le das a tu propia casa, en cuanto a evitar el acceso de personas ajenas, es por eso que se hará una investigación en donde se podrá verificar que aplicaciones de seguridad poseen y utilizan los estudiantes de la Universidad Católica de El Salvador en el año 2015.

1.2 Justificación de la investigación

Hoy en día, Internet forma parte de nuestras vidas. Dicho de otra forma, nuestra vida cotidiana está compuesta por muchas acciones, y algunas o muchas de estas acciones se relacionan con Internet de alguna forma. Esto es un hecho, la tecnología avanza y nos facilita la vida, por lo que es difícil prescindir de la tecnología.

Cada vez usamos más nuestros dispositivos móviles y, por tanto, intercambiamos información a través de ellos, accedemos a nuestro correo electrónico o a nuestros perfiles en Twitter, Facebook o Instagram. Nuestros Smartphone y Tablet atesoran información de carácter personal, guardan nuestras fotos, nuestros mensajes o nuestra agenda de contactos; información de valor que debemos proteger adecuadamente

Perder nuestro dispositivo móvil puede ocasionarnos bastantes dolores de cabeza, sobre todo si no tenemos una copia de la información que almacenábamos. En este sentido, las copias de seguridad son fundamentales y es una tarea que debemos asumir e implementar para poder recuperarnos ante un desastre como la avería de nuestro dispositivo o su pérdida.

Los ciberdelincuentes han aprovechado la popularización de los llamados teléfonos inteligentes y de las tabletas para tratar de aprovecharse de cada vez más usuarios despreocupados.

El sistema operativo más utilizado en el mundo es Android. Según estudio realizado por Google I/O es sistema Android. A mediados del año 2015 la cantidad de Smartphone superó los mil millones¹, Según Kaspersky Lab, 2015 marcó el momento en que la demanda de nuevos programas maliciosos alcanzó el punto de saturación, cuando el número de nuevos archivos de malware detectados diariamente por sus productos se redujo 15,000 veces -de 325,000 en 2014 a 310,000 en 2015². Además, en los últimos meses se han especializado en camuflar las funciones maliciosas de las apps infectadas de forma más sofisticada y también se han incrementado las operaciones de compra-venta de los llamados “kit de malware”.

Esta investigación ayudara a concientizar a los jóvenes de los riesgos del robo de información almacenada en sus móviles o Tablet, del mismo modo demostrar cuales son las mejores aplicaciones móviles de seguridad ya sea gratuitas o de paga en las diferentes sistemas operativos que manejan los estudiantes de la Universidad Católica de El Salvador. Se trata de ayudar a los jóvenes a mantener a salvo información que puede ser importante y que si cualquier persona tiene acceso a ella puede causar un enorme problema.

¹ <http://elmundo.com.sv/salvadorenos-gastan-1-2-millones-al-dia-en-telefonía-movil/>

² <http://www.hardwaremx.com/forum/topic/302366-kaspersky-lab-registro-de-nuevos-programas-maliciosos-baj%C3%B3-a-310000-por-d%C3%ADa-en-2015-a-la-par-que-ciberdelincuentes-buscan-ahorrar-dinero/>

1.3 Objetivos generales

Identificar las aplicaciones de seguridad en los Smartphone que los estudiantes de la Universidad Católica de El Salvador utilizan para protección de su información en el año 2015.

Objetivos específicos.

- Determinar si los estudiantes de la Universidad Católica de El Salvador hacen uso de aplicaciones de seguridad en sus equipos inteligente.
- Identificar las mejores formas de protección de información almacenada en los diferentes tipos de equipos inteligentes de los estudiantes de la Universidad Católica de El Salvador.
- Describir los tipos de aplicaciones de seguridad en los diferentes sistemas operativos de los Smartphone para que los estudiantes de la Universidad Católica de El Salvador elijan la mejor.
- Identificar cuáles son las aplicaciones preferidas de los estudiantes de la Universidad Católica de El Salvador
- Determinar las ventajas y desventajas de la utilización de las aplicaciones de seguridad en los Smartphone
- Comparar entre aplicaciones de paga y aplicaciones gratuitas que brindan seguridad a los Smartphone
- Demostrar que la información almacenada en los Smartphone robado o extraviado es recuperable siempre y cuando tengan las herramientas necesarias.

Hipótesis de la investigación

- El tiempo que los estudiantes dedican a actualizar sus aplicaciones de seguridad es menor, relacionado al tiempo que emplean para personalizar sus equipos inteligentes.
- Los estudiantes muestran poca importancia en las aplicaciones de seguridad de la información almacenada en sus equipos inteligentes.
- Los diferentes tipos de aplicaciones que cada sistema operativo móvil brinda a cada usuario, que tipo de aplicaciones es más descargable por los estudiantes.
- Los estudiantes que utilizan aplicaciones de seguridad en Smartphone, tienen menor índice de robo de información que aquellos que solo utilizan los Smartphone como un teléfono normal.
- Se puede recuperar información de un equipo Smartphone luego que este se pierde, se lo roban o sufre algún desperfecto

CAPÍTULO II: MARCO TEÓRICO Y ANTECEDENTES DE EVALUACIÓN DE LAS APLICACIONES DE SEGURIDAD DE INFORMACIÓN DE LOS SMARTPHONES DE LOS ALUMNOS DE LA UNIVERSIDAD CATÓLICA DE EL SALVADOR EN EL AÑO 2015

2.1 Teléfonos móviles inteligentes o Smartphone.

Son conocidos como teléfonos inteligentes, es un tipo de teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de almacenar datos y realizar actividades similares a las de una computadora (minicomputadora), diferentes de los teléfonos convencionales que solo se utilizan para llamadas o mensajes de textos, se les llama inteligente por las muchas funciones que brinda la mayoría de los teléfonos con pantalla táctil se les llama inteligentes.

Smartphone en inglés es un término comercial para denominar a un teléfono móvil que ofrece más funciones que un teléfono móvil común. Casi todos los teléfonos inteligentes son móviles que soportan completamente un cliente de correo electrónico con la funcionalidad completa de un organizador personal.

Los primeros Smartphone se diferenciaron de los móviles normales porque se fueron añadiendo funciones extras como organizadores personales incorporados en el teléfono, estos organizadores incluían aplicaciones como un bloc de notas, un calendario donde anotar citas, reuniones y alarmas, un gestor para la recepción y envío de correos electrónicos, un teclado QWERTY que facilitaba la escritura en el teléfono, etc. Estos móviles dieron un paso tecnológico con el objetivo de asemejarse a ciertas funcionalidades que solo las computadoras y portátiles de

Aquella época podían ejecutar, pero con la ventaja de tenerlo en un pequeño dispositivo fácilmente transportable.

2.2 Algunas características de los Smartphone.

- Disponen de una aplicación para el envío y recepción de emails así mismo se pueden gestionar varias cuentas de correo.
- Disponen de una varias aplicaciones enfocadas a realizar funciones de organizador personal como calendarios, recordatorios y alertas, bloc de notas, los cuales pueden comunicarse y sincronizarse con otros ordenadores, tablets o móviles.
- Pueden leer, editar y reproducir una amplia familia de archivos como hojas de cálculo, editores de textos, archivos multimedia de video y música, etc.
- Permiten la descarga y la ejecución de aplicaciones (app) desarrollados por terceros los cuales amplían nuevas funcionalidades, por ejemplo: juegos, retoques fotográficos, lectores de libros electrónicos, navegadores GPS, reproductores de música/videos, mejorar la visualización del equipo, etc.
- La característica más importante dispone de un sistema operativo capaz de desarrollar todas las funcionalidades descritas anteriormente. IOS de la empresa Apple, Android de la empresa Google o Windows phone por parte de la empresa Microsoft son ejemplos de sistemas operativos diseñados y

programados para hacer trabajar a nuestros Smartphone como un ordenador de bolsillo³.

2.3 Sistemas operativos que existen en los mercados.

El sistema operativo es básicamente el motor que hace que tu Smartphone opere con fluidez y maneja tanto el equipo como el software, creando una experiencia de usuario agradable, los sistemas operativos móviles son mucho más simples y están más orientados a la conectividad inalámbrica, los formatos multimedia para móviles y las diferentes maneras de introducir información en ellos.

A medida que los teléfonos móviles crecen en popularidad, los sistemas operativos con los que funcionan adquieren mayor importancia.

2.3.1 Android:

El sistema operativo Android es sin duda el líder del mercado móvil en sistemas operativos, está basado en Linux, diseñado originalmente para cámaras fotográficas profesionales, luego fue vendido a Google y modificado para ser utilizado en dispositivos móviles como los teléfonos inteligentes y luego en tablets como es el caso del Galaxy Tab de Samsung, además se encuentra en desarrollo para usarse en notebooks y PCs, el desarrollador de este S.O. es Google, fue anunciado en el 2007 y liberado en el 2008; Android Inc. es la empresa que creó el

³ <http://www.quees.info/que-es-un-smartphone.html>

sistema operativo móvil, se fundó en 2003 y fue comprada por Google en el 2005 y 2007 fue lanzado al mercado. Su nombre se debe a su inventor, Andy Rubin⁴.

Las aplicaciones para Android se escriben y desarrollan en Java aunque con unas APIS propias por lo que las aplicaciones escritas en Java para PC y demás plataformas ya existentes no son compatibles con este sistema.

Una de las grandes cualidades o características de este sistema operativo es su carácter abierto. Android se distribuye bajo dos tipos de licencias, una que abarca todo el código del Kernel y que es GNU GPLv2, Google también por supuesto tiene otra licencia para el resto de componentes del sistema que se licencia bajo APACHE v2.

Imagen:



2.3.2 iOS:

iOS es el sistema operativo que da vida a dispositivos como el iPhone, el iPad, el iPod Touch o el Apple TV. Su simplicidad y optimización son sus pilares para que millones de usuarios se decanten por iOS en lugar de escoger otras plataformas que necesitan un hardware más potente para mover con fluidez el sistema operativo. Cada año, Apple lanza una gran actualización de iOS que suele traer características exclusivas para los dispositivos más punteros que estén a la venta en ese momento.

⁴ https://es.wikipedia.org/wiki/Sistema_operativo_m%C3%B3vil

Anteriormente denominado iPhone OS creado por Apple originalmente para el iPhone, siendo después usado en el iPod Touch e iPad. Es un derivado de Mac OS X, se lanzó en el año 2007, aumento el interés con el iPod Touch e iPad que son dispositivos con las capacidades multimedia del iPhone pero sin la capacidad de hacer llamadas telefónicas, en si su principal revolución es una combinación casi perfecta entre hardware y software, el manejo de la pantalla multi-táctil que no podía ser superada por la competencia hasta el lanzamiento del celular Galaxy S I y II por parte de Samsung.

Imagen:



2.3.3 Windows Phone:

Anteriormente llamado Windows Mobile es un S.O. móvil compacto desarrollado por Microsoft, se basa en el núcleo del sistema operativo Windows CE y cuenta con un conjunto de aplicaciones básicas, actualmente va por la versión 10. Está diseñado para ser similar a las versiones de escritorio de Windows estéticamente y existe una gran oferta de software de terceros disponible para Windows Mobile, la cual se puede adquirir a través de la tienda en línea Windows Marketplace for MobileS

Imagen:



2.3.4 BlackBerry OS:

BlackBerry es un sistema desarrollado por Research In Motion el cual fue presentado en el WES 2010 junto con un video promocional donde se muestra algunas novedades. RIM apuesta que su BlackBerry 6 estará enfocado en el mercado corporativo y no-corporativo. La mejor experiencia de este sistema se encontrara en los equipos touchscreen (Pantalla Táctil), aunque RIM aseguro que en los equipos que cuenten con un TouchPad o TrackPad podrán ejecutarlo ya que ejerce casi la misma función. Así mismo todavía RIM no ha aclarado cuales son los equipos que se podrán actualizar a esta versión aunque hay muchos rumores al respecto. RIM en el desarrollo de este OS se enfocó en la parte multimedia hacia el usuario, sin dejar a un lado la parte profesional, también se muestra la integración de las redes sociales y la mensajería instantánea en este. Sin duda RIM quiere dar al usuario una nueva experiencia en su equipo BlackBerry que nadie conocía

Imagen:



2.3.5 Symbian:

Fue producto de la alianza de varias empresas de telefonía móvil, entre las que se encuentran Nokia como la más importante, Sony Ericsson, Samsung, Siemens, BenQ, Fujitsu, Lenovo, LG, Motorola, esta alianza le permitió en un momento dado ser unos de los pioneros y más usados. El objetivo de Symbian fue crear un sistema operativo para terminales móviles que pudiera competir con el de Palm o el Smartphone de Microsoft. Técnicamente.

El sistema operativo Symbian es una colección compacta de código ejecutable y varios generalmente, en un circuito flash dentro del dispositivo móvil. Gracias a este tipo de tecnología, se puede conservar información aun si el sistema no posee carga eléctrica en la batería, además de que le es factible reprogramarse, sin necesidad de separarla de los demás circuitos. Las aplicaciones compatibles con Symbian se desarrollan a partir de lenguajes de programación orientados a objetos como C++, Java (con sus variantes como PJava, J2ME, etc.), Visual Basic para dispositivos móviles, entre otros, incluyendo algunos lenguajes disponibles en versión libre. ewrfFirefox OS.

Imagen:



2.4 Aplicaciones móviles.

2.4.1 definición:

Una aplicación móvil es un programa que se puede descargar y al que puede acceder directamente desde su teléfono o desde algún otro equipo inteligente. Una aplicación móvil o App, es una aplicación informática diseñada para ser ejecutada en teléfonos inteligentes, tabletas y otros dispositivos móviles. Por lo general se encuentran disponibles a través de plataformas de distribución, operadas por las compañías propietarias de los sistemas operativos móviles como Android, iOS, BlackBerry OS, Windows Phone, entre otros. Existen aplicaciones móviles gratuitas y otras de pago, donde Google Play es el Marketplace líder del sector, con 900 millones de usuarios activos al mes. Sin embargo, es la App Store la que cuenta con un mayor número de aplicaciones subidas: 1.250.000. Detrás de

ellas hay cerca de 235.000 desarrolladores, a los que Apple les ha pagado en el último año 5.000 millones de dólares. Las aplicaciones para Windows Phone son las que mayor beneficio por descarga registran: 15 centavos, superando así a los 10 centavos de las aplicaciones para iOS y los 2 centavos de las apps para Android. A pesar de que Windows Phone sólo cuenta con 160.000 apps en su store, un importante porcentaje de las mismas son de pago. Por este motivo, a un desarrollador Windows Phone le cuesta menos trabajo obtener dinero de una aplicación que a un desarrollador de Android. El sistema operativo de Google cuenta con 800.000 aplicaciones, pero una inmensa mayoría son gratuitas. Pese a los datos positivos de Windows Phone, Apple sigue siendo la plataforma que mayor importe paga a sus desarrolladores⁵.

¿Qué necesito para descargar y usar una aplicación?

Usted necesita un Smartphone o algún otro aparato móvil con acceso a internet. No todas las aplicaciones funcionan en todos los aparatos móviles. Cuando usted compra uno de estos aparatos debe saber que sistema operativo y el tipo de aplicaciones corresponde a ese aparato. Los sistemas operativos móviles Android, Apple, Microsoft y BlackBerry tienen tiendas de aplicaciones que operan en línea en las cuales usted puede buscar, descargar e instalar las aplicaciones. Para establecer una cuenta, es posible que tenga que suministrar el número de una tarjeta de crédito, especialmente si va a descargar una aplicación que no es gratuita.

2.5 Tipos de aplicaciones móviles.

Existen tipos de app de las cuales se mostrará cada una con un breve resumen.

⁵ <https://www.yeeply.com/blog/beneficio-economico-de-las-apps/>

2.5.1 App Nativas:

Es la que se desarrolla de forma específica para un determinado sistema operativo, llamado Software Development Kit o SDK. Cada una de las plataformas, Android, iOS o Windows Phone, tienen un sistema diferente, por lo que si quieres que tu app esté disponible en todas las plataformas se deberán de crear varias apps con el lenguaje del sistema operativo seleccionado, además las aplicaciones nativas no necesitan conexión a internet para que funcionen.

Por ejemplo:

- Las apps para iOS se desarrollan con lenguaje Objective-C
- Las apps para Android se desarrollan con lenguaje Java
- Las apps en Windows Phone se desarrollan en .Net

Las ventajas y desventajas de estas son:

Ventajas

- Utilización de los recursos tanto del sistema como del hardware.
- Permite ser publicada en tiendas para su distribución.
- En su mayoría, no necesitan estar conectadas a Internet para su funcionamiento.

Desventajas

- Solo pueden ser utilizadas por un dispositivo que cuente con el sistema para el cual fue desarrollada.
- Requiere de un costo para distribuirla en una tienda, y dependiendo el sistema, para el uso del entorno de desarrollo.
- Necesitan aprobación para ser publicadas en la plataforma.

2.5.2 Web App:

Las aplicaciones web o web application. Son aquellas desarrolladas usando lenguajes para el desarrollo web como lo son html, css y JavaScript y un framework

para el desarrollo de aplicaciones web, como por ejemplo jquery mobile, Sencha, Kendo UI, entre otros.. Se podría decir que este tipo de aplicaciones son muy usadas para brindar accesibilidad a la información desde cualquier dispositivo, sin importar el sistema operativo, ya que solo se necesita un navegador web para acceder a dicha aplicación.

Las ventajas y desventajas de estas son:

Ventajas

- Pueden ser utilizadas desde cualquier dispositivo sin importar el sistema operativo.
- Puede que requiera un coste para su desarrollo, peor este puede ser mínimo en comparación con las nativas.
- No requieren de ninguna aprobación para su publicación.

Desventajas

- No pueden ser publicadas en plataformas para su distribución
- No utilizan los recursos del sistema ni del dispositivo de manera óptima.
- Se requiere de una conexión a internet
- Tiempo de respuesta entre el usuario, interacción y navegación es menor que la app nativas.

2.5.3 Web App Nativas ó Híbridas.

Una aplicación híbrida es una combinación de las dos anteriores, se podría decir que recoge lo mejor de cada una de ellas. Las apps híbridas se desarrollan con lenguajes propios de las web app, es decir, HTML, Javascript y CSS por lo que permite su uso en diferentes plataformas, pero también dan la posibilidad de acceder a gran parte de las características del hardware del dispositivo. La principal ventaja es que a pesar de estar desarrollada con HTML, Java o CSS, es posible agrupar los códigos y distribuirla en la appstore.

Algunos ejemplos: phonegap, titanium appaccelerator, Steroids, entre otros. La facilidad que brinda este tipo de desarrollo es que no hay un entorno específico el cual hay que utilizar para su desarrollo y la mayoría de las herramientas que se utilizan son de uso gratuito, también pudiendo integrarlo con las herramientas de aplicaciones nativas.

Ventajas

- Uso de los recursos del dispositivo y del sistema operativo
- El costo de desarrollo puede ser menor que el de una nativa
- Son multiplataforma
- Permite distribución a través de las tiendas de su respectiva plataforma.

Desventaja

- La documentación puede ser un poco escasa y desordenada.
- Diseño visual no siempre relacionado con el sistema operativo con el que se muestra.⁶

2.6 AppStore Donde se descargan aplicaciones según si sistema operativo.

Hasta ahora, muchas veces instalar una aplicación requería conseguir encontrarla (no siempre una tarea fácil), realizar el pago, instalarla, registrarla (un proceso que varía para cada una de ellas). La mayoría de veces resultaba un fastidio que las tiendas de aplicaciones en el móvil quieren resolver, existen appstore donde se pueden encontrar las diferentes aplicaciones para todo lo que se pueda imaginar algunos ejemplos de estas tiendas son:

2.6.1 AppStore



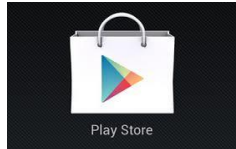
Aunque no fuera la primera de las tiendas en aparecer, la **App Store** es la que ha marcado la pauta a seguir por el resto y ha hecho que estas se popularicen.

⁶ <http://www.lancetalent.com/blog/tipos-de-aplicaciones-moviles-ventajas-inconvenientes/>,

<http://deideaaapp.org/tipos-de-aplicaciones-moviles-y-sus-caracteristicas/>

Está disponible para el iPhone y el iPod touch, y el control por parte de Apple sobre los contenidos de esta, con un sistema de aprobación de aplicaciones el cual tiene la desventaja que se retrasa durante varias semanas.

2.6.2 Google Play



Google Play (anteriormente Android Market) es una plataforma de distribución de software en línea desarrollado por Google Inc. para dispositivos con sistema operativo Android. En la plataforma se encuentran disponibles tanto aplicaciones gratuitas como de pago. Su interfaz es sencilla y rápida.

2.6.3 Windows phone Store



La Windows Phone Store es la plataforma de distribución de Microsoft para los dispositivos que cuentan con el sistema operativo móvil Windows Phone.

2.6.4 BlackBerry World



Las aplicaciones para los dispositivos BlackBerry se encuentran disponibles mediante descarga a través del servicio BlackBerry World (antes BlackBerry App World)⁷.

2.6.5 Ovi Store



Uno de los grandes lanzamientos de Nokia ha sido la **Ovi Store**, su tienda de aplicaciones que va, incluso, un poco más allá de lo que proponen sus competidores. Para ello, aplica conceptos como la geolocalización o las redes sociales a la hora de ofrecernos las aplicaciones.⁸

2.7 ¿Qué son las App de seguridad móvil?

El tema de la seguridad en Android es uno de los más sonados y que más preocupan a muchos usuarios. Debido al auge de los ataques cibernéticos y el robo de información privada de los usuarios de internet, muchas personas utilizan aplicaciones de seguridad que se pueden encontrar en la tienda de aplicaciones del sistema operativo que pertenezca nuestro Smartphone o Tablet.

Estas aplicaciones ayudan a resguardar la información más importante en nuestros móviles, a rescatar información perdida y a bloquear el acceso a personas ajenas a nuestro equipo inteligente.

⁷ https://es.wikipedia.org/wiki/Aplicaci%C3%B3n_m%C3%B3vil#Tiendas_de_aplicaciones:

⁸ <http://www.xatakamovil.com/aplicaciones/ovi-store-la-tienda-de-aplicaciones-de-nokia>

2.8 APLICACIONES MEJORES EVALUADAS EN LOS DIFERENTES SISTEMAS OPERATIVOS DETALLANDO LA UTILIZACIÓN PARA LA QUE FUERON CREADAS

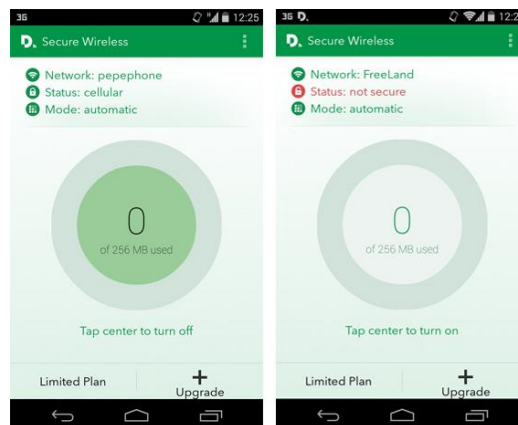
2.8.1 Android:



Secure Wireless 1.1.2: una conexión a prueba de espías

Cuando te conectas a Internet desde una red WiFi pública, la posibilidad de que haya alguien a la escucha y listo para interceptar tus mensajes o claves es real. La solución es usar conexiones seguras de tipo VPN, pero tienen el inconveniente de ser caras.

Secure Wireless ofrece ese nivel de seguridad pero solo cuando lo necesitas, esto es, cuando detecta que estás conectado a una red poco segura. La versión gratuita incluye 256 megabytes de transferencia, como extra, Secure Wireless bloquea las cookies trazadoras al navegar.

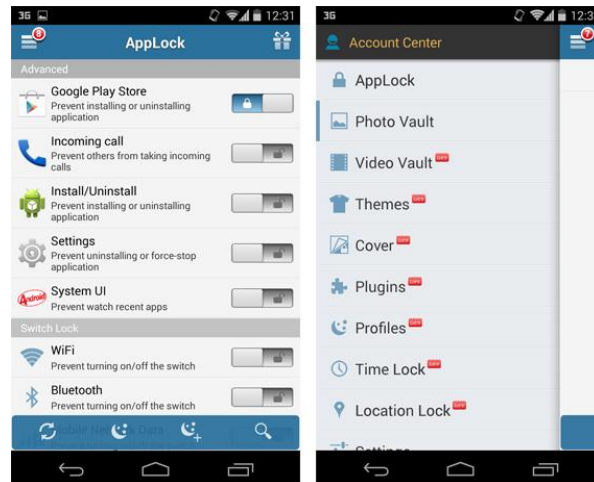




AppLock (Varía según el dispositivo): un candado para tus apps y galerías

Le pasas a alguien tu teléfono porque necesita buscar algo, mirar un mapa. Pero las App están ahí, dispuestas a abrirse ante cualquiera que presione su icono. Tus chats. Tus fotos. Tus correos. Todo expuesto. Tienes dos opciones: confías en ellas, o bien instalas AppLock.

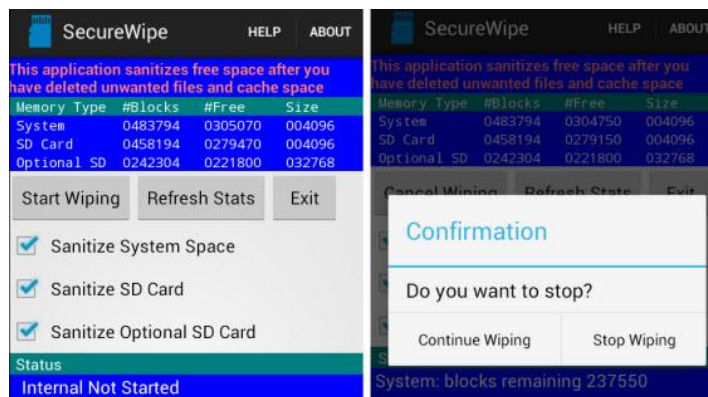
AppLock bloquea con un PIN la apertura de las apps que tú elijas. Y no solo apps, sino también opciones de Android, como la elección de red WiFi o la tienda Play. Es fácil de configurar (solo hay que introducir dos veces el PIN al principio), y si pones una dirección de correo de seguridad, puedes recuperar el código en caso de que lo olvides.



Secure Wipe 1.09: nadie recuperará tus archivos borrados



Cuando borras un archivo en Android, este no desaparece de inmediato: sus restos quedan "flotando" en la memoria del dispositivo y se pueden recuperar. Tanto si quieres borrar archivos para siempre como si deseas preparar el teléfono para venderlo, necesitas una solución de borrado permanente. Secure Wipe limpia el espacio libre de la memoria interna y de la tarjeta SD para que ningún archivo borrado pueda recuperarse con herramientas como Recuva o DiskDigger. Es mejor usarla cuando el teléfono o la Tablet esta en carga, puesto que el proceso de borrado tarda bastante tiempo.

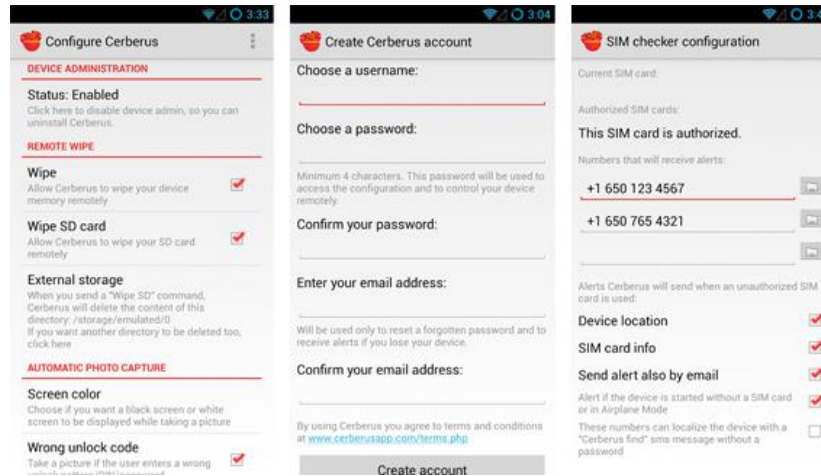


Cerberus 3.3.2: el antirrobo más completo para Android



Robar un teléfono con Cerberus instalado es una imprudencia: no solo el propietario puede localizarlo en el mapa desde cualquier navegador, sino que también puede **controlarlo a distancia** para disparar alarmas, borrar todos los datos, bloquear el dispositivo o grabar audio del

Micrófono

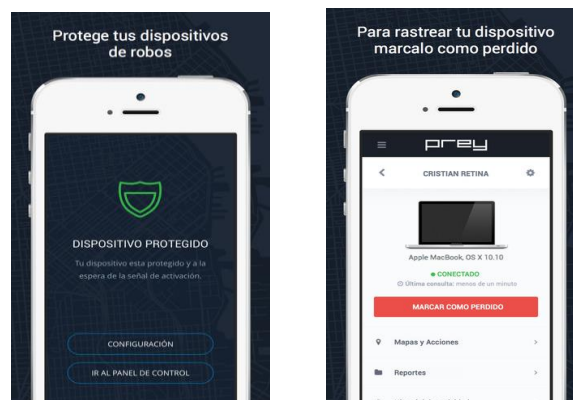


2.8.2 iOS:

Prey 1.3.6 anti robos:



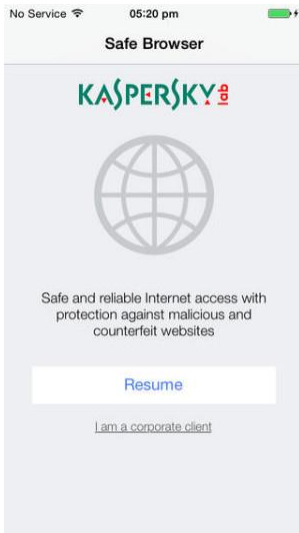
Prey es la aplicación anti robos más completa. Te permite rastrear y ubicar tu teléfono, tableta o laptop en caso de pérdida o robo. Ubica y recupera tu dispositivo con geolocalización y muchas otras opciones. Prey es 100% GRATIS y puede proteger hasta tres dispositivos con una sola cuenta.





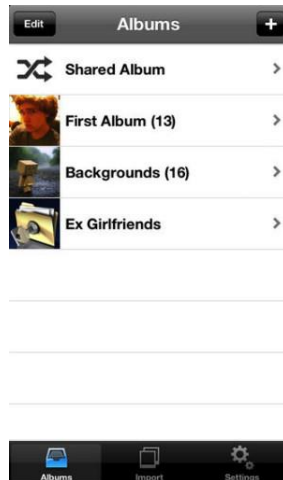
Kaspersky Lab 2016

El navegador de Kaspersky Safe Browser para iOS está diseñado para proteger los dispositivos que funcionan con el sistema operativo móvil de Apple de las últimas amenazas móviles y al mismo tiempo ofrece un conjunto de garantías para padres en pos de restringir las actividades de los niños en Internet



Legendary Software Labs

Con el objetivo de asegurarse de que nadie entrara a tus archivos privados. “Private Photo Vault” hace exactamente eso: protege todas las fotos y videos que quieras con una contraseña. Para poder hacer esto, debes transferir todo el contenido dentro de la aplicación. Por suerte, no es muy complicado.



2.8.3 Windows Phone:



MotionCam:

Es una aplicación de seguridad personal y vigilancia. Una vez está activa, la app detecta el movimiento y ruido de la zona, empieza a grabar un vídeo mp4 y lo envía a nuestra dirección de correo electrónico con una imagen adjunta de alarma.



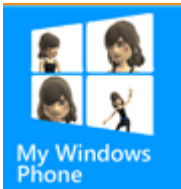
4UrEyesOnly:

Protege los archivos, imágenes, mensajes de texto y de voz a través de un sistema de cifrado. Esta app ofrece la oportunidad de almacenar nuestras fotos de forma encriptado y protegidas mediante un PIN.



SplashID:

Protege nuestras actividades online diarias, inclusive cuentas bancarias y datos de tarjetas de crédito. Además, cifra toda la información e incluye un gestor de contraseñas y un sistema de sincronización con tu PC o Mac.



Microsoft My Phone:

Es una funcionalidad de Microsoft que nos ayuda a encontrar nuestro dispositivo en caso de pérdida. Asimismo, nos permite llamar, bloquear o eliminar la información del terminal, situando su localización en el mapa.

2.8.4 BlackBerry OS:



**BlackBerry
Protect**

BlackBerry Protect:

Para poder localizar tu celular robado tienes que tener activo un plan de datos y tener instalado BlackBerry Protect, con esto se empieza el plan de rastreo. BlackBerry Protect incluye funciones diseñadas para ayudar los usuarios a encontrar su dispositivo BlackBerry y proteger los datos en caso de pérdida o robo. El usuario puede bloquear el dispositivo, cambiar la contraseña o eliminar todos los datos del dispositivo.

Media Lock Pro for BlackBerry:

Es una aplicación de gran alcance que protege la privacidad de su carpeta de multimedia. De inmediato pide una contraseña, si alguien intenta acceder a la cámara, las imágenes, música y vídeos de forma individual le permite bloquear todo lo que está en la carpeta Media. Si sólo desea bloquear las imágenes y no de la cámara, Media Lock Pro te ayudará a hacerlo

2.8.5 Symbian:**F-Secure Mobile:**

Este protector seguridad para Nokia nos ofrece las siguientes ventajas: Permite proteger nuestro teléfono móvil contra virus, contra robo o pérdida, de tal forma que podremos asegurar el móvil con todo lo posible, para que si se nos pierde, no se pueda volver a encender si no es con una contraseña que tú has establecido previamente. Localizar móvil en caso de robo o pérdida. Copias de seguridad Online. También nos permite hacer copias de seguridad del móvil Nokia y del contenido del teléfono móvil, fotos, vídeos, documentos, música, etc. en un espacio Online que nos ofrece la misma aplicación.

MazeLock:

MazeLock te da la opción de bloquear tu teléfono utilizando un determinado movimiento de tus dedos, en lugar de los típicos números. Al estilo del bloqueo opcional en Android, con MazeLock puedes determinar y guardar los movimientos de tus dedos por la pantalla para que sea la única forma de bloquear y desbloquear el teléfono.

ActiveLock:

Es una utilidad que te permitirá proteger mediante una contraseña de acceso cualquiera de las aplicaciones instaladas en tu terminal. Su uso es muy sencillo. Sólo tienes que seleccionar la aplicación que quieres proteger desde el entorno del programa y definir la contraseña de acceso. Sus opciones te permitirán bloquear o desbloquear aplicaciones selectivamente o bloquear o desbloquearlo todo simultáneamente.

2.8.6 Backup

El Backup (copias de seguridad) surge de la necesidad de resguardar la información relevante ya sea de una equipo inteligente, de una computadora o hasta de una empresa, los Backup son fundamentales siempre que te pones configurar, actualizar tu dispositivo, si tienes pensado rootear tú móvil, no te olvides de hacer una copia de seguridad tanto de tus datos como del sistema.

Un Backup de datos consiste en hacer una copia completa de las apps instaladas en tu móvil, sus configuraciones y todos tus datos (mensajes de texto y archivos), de forma que podrá restaurarse en un dispositivo nuevo. Existen muchas app que te ayudan a realizar un buen Backup pero tú decides cual es la mejor, lo aconsejable es que realices una copia de seguridad cada 2 o 3 días para que tenga una información actualizada por cualquier pérdida o robo de equipo

2.8.7 Sincronización de datos

La multiplicación de terminales y dispositivos móviles te permite poder recuperar tus informaciones en cualquier momento. Puedes por ejemplo recibir tus emails en tu tableta, reenviarlos desde tu ordenador y guardar una cita en tu Smartphone. Para que estos usos sean simplemente realizados, pasamos al modo "sincronización" y todas nuestras cuentas son accesibles y actualizadas simultáneamente en todos los terminales.

La sincronización de datos con una cuenta Google es posible desde todos los sistemas operativos. No hay problema, en caso de posesión de un ordenador Apple, de un Smartphone, BlackBerry y de una tableta con Android.

Sincronizar con iCloud:

Reservado para los usuarios Apple, iCloud es también un servicio gratuito que permite sincronizar datos en varios terminales. Si la cuenta iCloud ya existe, con datos guardados, basta una conexión simple. A la inversa, es necesario crear una cuenta y aceptar el compartimiento de datos.

Sincronizar BlackBerry con un ordenador:

BlackBerry posee un programa específico que permite recuperar datos desde un ordenador, el BlackBerry Desktop Manager. Este es descargable desde el sitio web de BlackBerry y disponible para computadora y Mac.

3. CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN PARA LA EVALUACIÓN DE LAS APLICACIONES DE SEGURIDAD DE INFORMACIÓN DE LOS SMARTPHONES DE LOS ALUMNOS DE LA UNIVERSIDAD CATÓLICA DE EL SALVADOR EN EL AÑO 2015

3.1 Tipo de Investigación.

Este estudio de evaluación es una investigación descriptiva, también conocida como investigación estadística, en el cual se sondeará a una parte de la población estudiantil de la Universidad Católica de El Salvador para evaluar que tanto conocen los estudiantes los métodos de seguridad aplicada a sus Smartphone o Tablet, además clasificar alguna aplicaciones de seguridad y determinar la complejidad y la vulnerabilidad de los equipos inteligentes (Smartphone).

3.2 Población y muestra.

La población evaluada que ayudará a verificar que tanto los jóvenes en el año 2015 son responsables de la información almacenada en sus dispositivos móviles inteligentes, más allá de las aplicaciones que existen para brindar los diferentes

tipos de seguridad requerida (seguridad de información, recuperación de datos y restricción de acceso), el objetivo principal consiste en ampliar y profundizar nuestro conocimiento sobre la seguridad de los Smartphone, conocer cuáles son las mejores aplicaciones para ello, de igual manera la mejor forma de recuperar información de un aparato extraviado, o ya con su vida útil terminada.

Cabe destacar que la investigación está enfocada a los jóvenes que cuentan con un teléfono inteligente. En El Salvador un porcentaje elevado de persona cuentan con un teléfono inteligente (Smartphone) sin importar la versión de su sistema operativo, la capacidad de almacenamiento o del tamaño. Muchos de los que poseen estos móviles no saben que tanto pueden facilitar la vida por ejemplo, cuánto cuestan las llamada a Estados Unidos o a otros países como España, Alemania, hoy en día con que tenga cuenta en una red social como Facebook con que active un paquete de navegación de \$1.10 de cualquier compañía la llamada puede durar muchas horas y hasta realizar varias llamadas, las video-conferencias son la manera de estar más cerca de personas que se encuentran en países diferentes y hasta diferentes continentes.

Verificando que hay mucha información importante almacenada en nuestros móviles se ha tomado como referencia de esta investigación a los estudiantes de la Universidad Católica de El Salvador correspondiente al ciclo II 2015.

Esta muestra definida nos proporcionar información sobre que tanto les importa la seguridad de información en su Smartphone, además se realiza un análisis de las mejores aplicaciones a utilizar para el propósito de resguardar nuestra información. Las aplicaciones evolucionan a diario así como la forma de robo de información por ello hay que hacer conciencia de lo importante que es la información y el saber protegerla.

3.3 técnicas e instrumentos.

Técnica

La técnica es el medio en el cual se llevó a cabo esta investigación tomando en cuenta lo que se evaluó, además se verifica si se cumplen las hipótesis realizadas con la información obtenida.

Realizar encuestas online a los diferentes cursos, enfocándonos a los estudiantes del ciclo II del año 2015 de la Universidad Católica de El Salvador.

Examinar cada respuesta proporcionada por cada alumno y evaluar que tanta atención prestan a la seguridad móvil enfocándose a los teléfonos inteligentes.

Instrumento

Los principales instrumentos para la realización de esta investigación serán los alumnos encuestados de la Universidad Católica de El Salvador del ciclo II del año 2015 además de algunos aspectos tecnológicos:

- Computadoras de escritorio
- Navegador Web
- Sistema de encuesta vía web realizadas en Google
- Moodle.
- Sistema de encuestas en línea
- Sistema de tabulación como una hoja de cálculo

3.4 Procedimientos

Este proceso se realizó primeramente gestionando permiso de realizar las encuestas online en los diferentes centros de cómputo de la Universidad Católica de El Salvador en donde se encuentran recibiendo clases los estudiantes de ésta universidad, con el consentimiento del encargado de la clase, se recopila la información necesaria y oportuna para llevar a cabo la investigación.

3.5 Análisis Estadístico

La información obtenida mediante las encuestas realizadas, fue procesada mediante la aplicación de Google en donde muestra detalladamente en una hoja de cálculo, las diferentes respuestas obtenidas, donde se muestra la información necesaria para poder llevar a cabo la investigación.

Para analizar los resultados obtenidos se utilizó matrices de resumen, en las cuales se indica el total del resultado obtenido por pregunta, mostrando en cada interrogante el valor porcentual obtenido la cual se presenta en forma gráfica.

4. CAPÍTULO IV RESULTADO DE LA INVESTIGACIÓN PARA LA EVALUACIÓN DE LAS APLICACIONES DE SEGURIDAD DE INFORMACIÓN DE LOS SMARTPHONES DE LOS ALUMNOS DE LA UNIVERSIDAD CATÓLICA DE EL SALVADOR EN EL AÑO 2015

4.1 Importancia de tener una App de seguridad.

El crecimiento en la venta de celulares y tablets hizo que los piratas depositaran su mirada en esos dispositivos. La mayoría de las apps permiten además rastrear el equipo y borrar información a distancia.

Cada vez es más habitual el uso de aplicaciones y tecnologías móviles en los jóvenes de todo el mundo, en este momento nos enfocaremos en los estudiantes de la Universidad Católica de El Salvador. Su fácil implementación y uso han hecho que sean prácticamente omnipresentes y esenciales en el comercio electrónico y aplicaciones para todos los usos. Por lo tanto, mucha información es manejada a través de aplicaciones móviles por ejemplo: documentos, fotos, contraseñas, canciones, cuentas de bancos, y mucha información personal.

En agosto de 2010 se detectó el primer malware enfocado a Android y hoy ya existen más de 7.000 ejemplares de amenazas.

A pesar de la importancia que está adquiriendo mantener protegido un Smartphone debido al exponencial crecimiento del malware, el peor escenario para el usuario actual es perder su equipo. Los celulares se convirtieron en computadoras de mano, por lo que en su interior no sólo hay acceso a fotos sino

también al correo electrónico y demás datos privados. Un usuario común cuenta con varias opciones para mantener a salvo su equipo, no sólo de malware sino también en caso de pérdida o robo de un Smartphone, borrado a distancia de datos y ubicación mediante el GPS del equipo son algunas de las defensas ofrecidas.

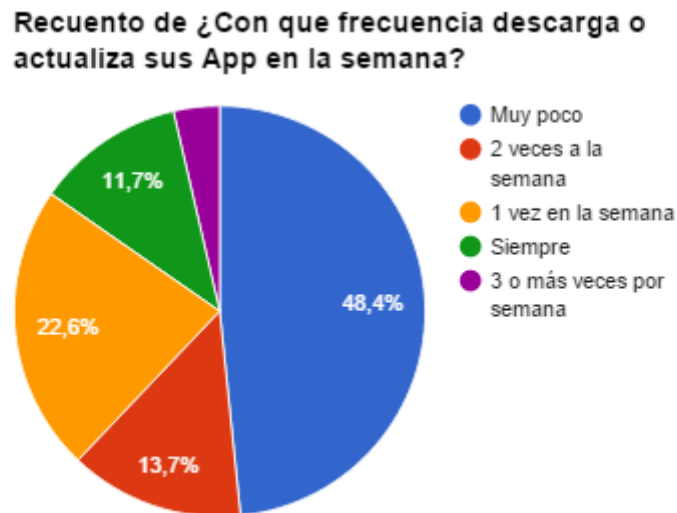
Muchas personas no comprenden la importancia de la seguridad que hay que tener con la información que se encuentra en nuestros equipos inteligentes piensan que andar con el equipo en el bolsillo está segura la información, hay muchas personas que espían el contenido que se almacena en los equipos inteligentes.

4.2 Análisis de la investigación de campo realizada a los alumnos de la UNICAES ciclo II 2015.

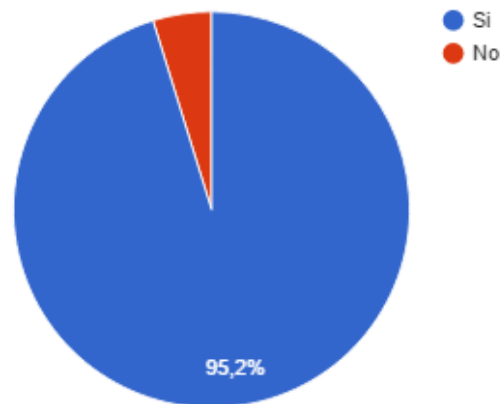
Mediante la serie de encuestas realizadas se pudo obtener mucha información la cual será muy importante y determinará que tanto los estudiantes de la Universidad Católica de El Salvador correspondiente al ciclo II del año 2015, saben administrar la información que tienen almacenada en sus Smartphone o sus Tablet se ha tratado de demostrar que son pocos los estudiantes que utilizan App para poder tener segura toda aquella información almacenada. Se tabulan las encuestas las cuales incluyen gráficos.

4.2.1 Análisis de la encuesta dirigida a los estudiantes

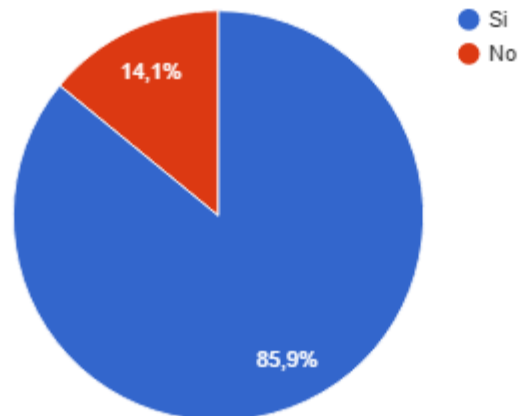
En el siguiente análisis se puede concluir:



Con referencia a con que tan frecuente se descargan y actualizan App los estudiantes encuestados, el 48.4% utilizan muy poco tiempo, el 22.6% solo 1 vez a la semana realiza esta función, el 13.7% 2 veces a la semana, el 3.6% se esmeran en descargar y actualizar en 3 o más veces a la semana solo 11.7% de los encuestados siempre están con sus App actualizadas y descargando información.

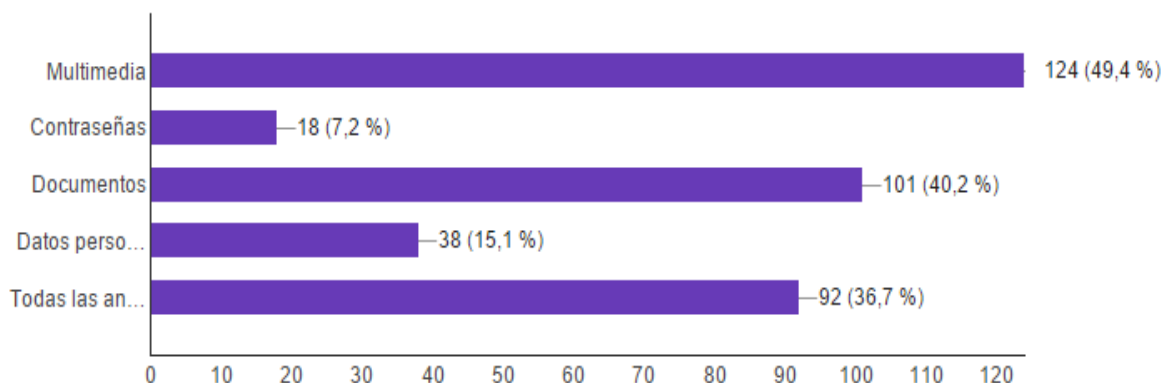
Recuento de ¿Posee un Smartphone?

95.2% de la población encuestada posee un Smartphone, esto da mucha ventaja para la realización de la investigación. Por otro lado un porcentaje menor de equivalente a 4.8% no poseen teléfonos inteligentes o ningún tipo de móvil.

Recuento de Conoce la tienda de App de su Smartphone

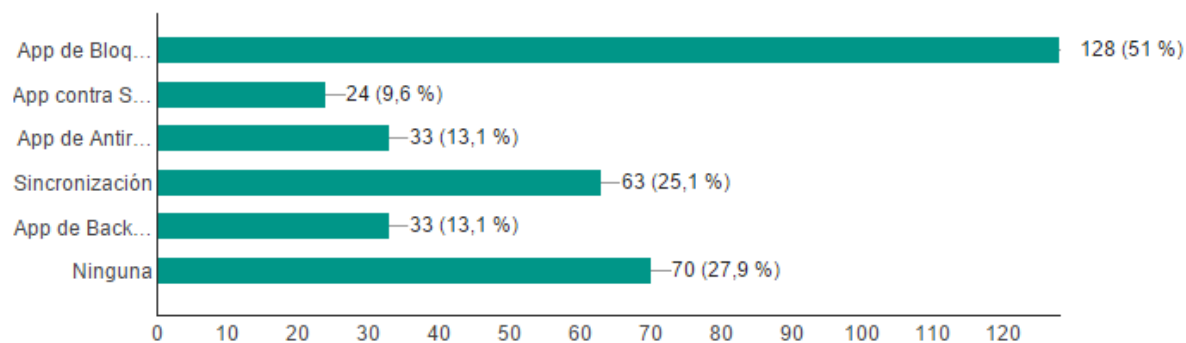
Con respecto al conocimiento de las tiendas de compra de App para cada uno de los sistemas operativos móviles el 85.9% de los estudiantes que poseen un Smartphone si lo conocen la tienda, el 14.1% no posee o no saben cuál es la tienda donde puedan descargar aplicaciones móviles por tal motivo se puede identificar que estos estudiantes son vulnerables al robo de información.

¿Cuál de estos tipos de Información se almacena en su equipo inteligente (Smartphone o Tablet)?



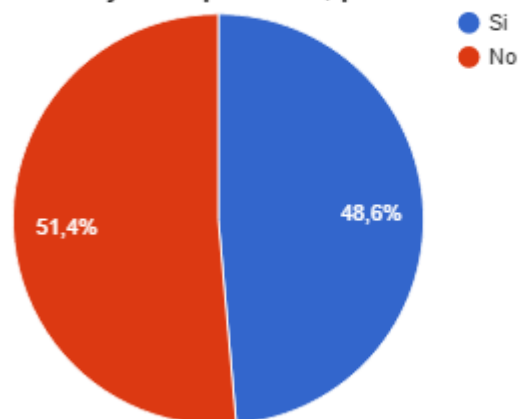
Un 49.4% de los encuestados poseen sus almacenados datos de multimedia (canciones, imágenes, videos), el 40.2% almacena documento de tarea, o algún otro tipo de documentos, 15.1% son datos personales como numero especiales, información relacionada a otras persona, solo 7.2% de los estudiantes almacenan contraseñas o algún tipo de password. Del total de los encuestado el 36.7% tienen de todo tipo de información.

¿De cuál de las siguientes formas de seguridad utiliza en su Smartphone o Tablet?



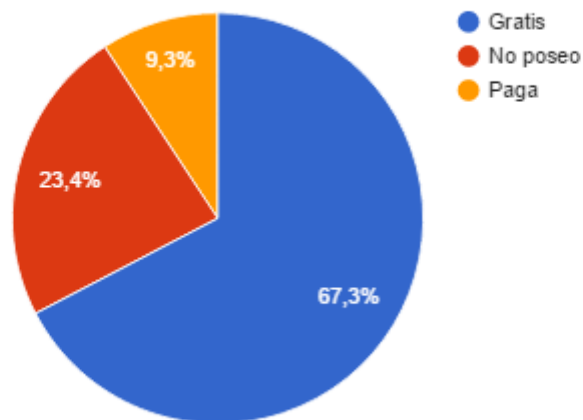
Del total de los encuestados preguntando qué tipo de seguridad es la que poseen instalados en sus equipos inteligentes el 51% indicó que poseen App de Bloqueo de acceso, un 9.6% tiene una App contra Spyware, el 13.1% poseen una App de Antirrobo, la Sincronización es utilizada por el 25.1%, Backup corresponde al 13.1%, y el 27.9% no poseen Ninguna App para resguardar la información.

Recuento. Ha sufrido de la pérdida de su información almacenada en su Smartphone o Tablet ya sea por robo, pérdida o destrucción...

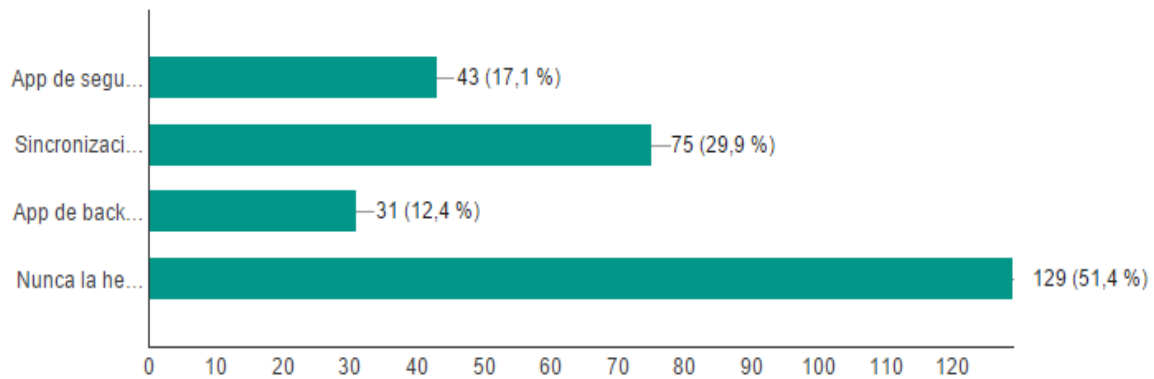


El 48.6% de los estudiantes encuestado ha sufrido la pérdida de información ya sea por robo, pérdida del equipo o alguna otra razón, la mayoría tiene la dicha de no sufrir este problema (51.4%). Del total de estudiantes que han perdido la información el 51.4% nunca la ha recuperado, el resto la ha recuperado mediante una App de seguridad el 17.1%, mediante sincronización de datos 29.9% y por back up 12.4%.

Recuento de Las App de seguridad que posee son:

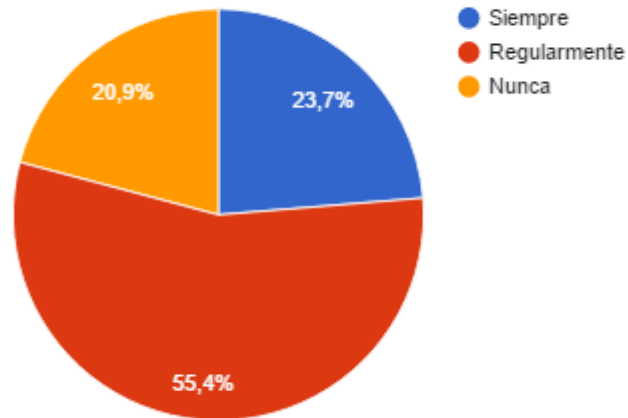


De los diferente tipos de adquisición de App el 9.3% utiliza las de Paga y el 67.3 % son App gratis, mientras el 23.4% no cuentan con app en sus equipos. Otro resultado que se obtuvo es que de todas las personas encuestadas al consultar que tan frecuente se conectan a redes WiFi públicas el resultado es que el 55.4% se conecta regularmente, el 23.7% siempre y el 20.9% nunca lo hacen.

Ha recuperado la Información perdida o robada mediante:

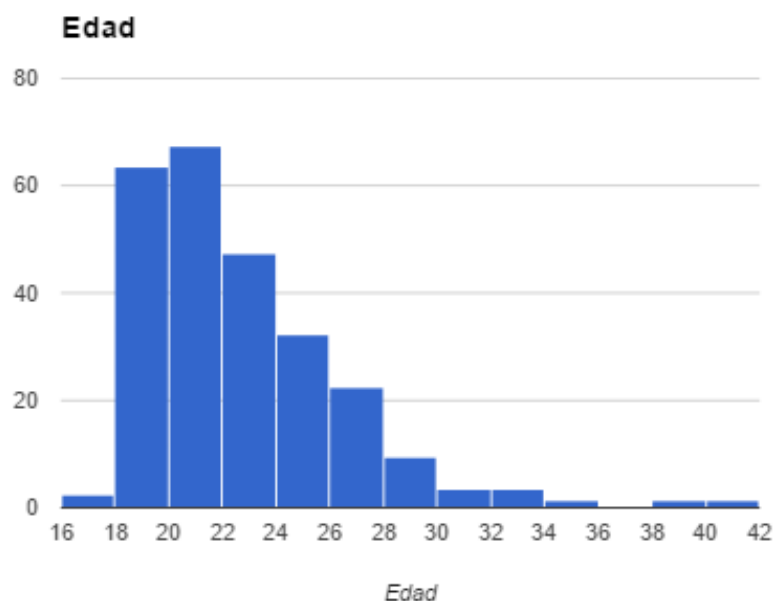
Cuando se pregunta a la población encuestada el 48.6% de las personas ha sufrido de robo o pérdida de su móvil, el de este porcentaje el 51.4% jamás vuelve a recuperar la información, por otro lado existen estudiantes que utilizan las App de seguridad con el 17.1%, el 29.9% usa la sincronización de datos, back up usado por el 12.4%.

Recuento de Al tener disponibilidad de una red Inalámbrica (WIFI) en un lugar público, ¿se conecta a dicha red?



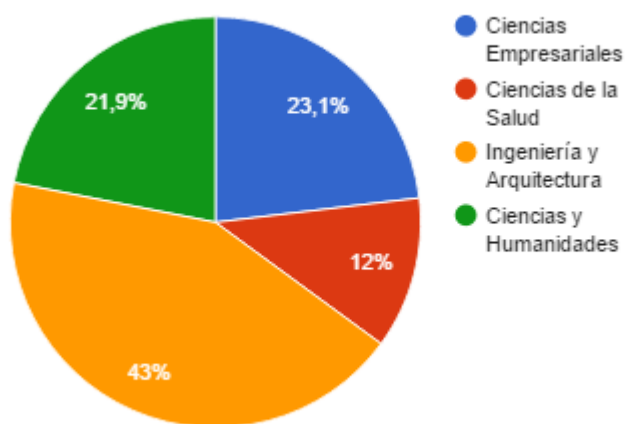
Por último se pregunta a cada estudiante con qué frecuencia se conectan a redes abiertas de inalámbricas (WIFI), ya que al conectarse a estas redes son muy vulnerables al robo de información sin saber qué es lo que está pasando del total encuestado el 55.4% se conecta regularmente, el 23.7% siempre se conectan sin pensar en lo que puede suceder, las personas más cuidadosas y nunca se conectan es el 20.9%.

Los estudiantes que se evaluaron se encuentra entre la edad de 16 años hasta los 42 años:



Se intentó abarcar las facultades que posee la institución las cuales se evalúan en el siguiente porcentaje:

Recuento de Seleccione la facultad a la cual pertenece



Con este análisis podemos concluir que hay muchas estudiantes que solo utilizan sus Smartphone como distracciones, juegos, o almacenamiento de datos, o para muchas otras funciones, sin embargo la seguridad que mantienen en estos equipos son mínimos son pocos los que se interesan en su seguridad móvil, además de la falta de conocimiento de muchos en cuanto al robo de información, perdidas de datos y muchos otros peligros expuestos cuando no se utilizan las App adecuadas para su seguridad

5. CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Se presenta las conclusiones y recomendaciones obtenidas durante la investigación, que servirán de referencia y que se deben tomar en cuenta si no queremos que nuestra información guardada en nuestros Smartphone o Tablet sea vulnerable y que cualquiera pueda tener acceso a ella.

Conclusiones:

La tecnología está avanzando día con día, ahora los móviles no solo sirven de aparatos de comunicación entre dos o más personas, ya no se llaman celulares ahora son Smartphone o equipos inteligente, muchos de estos equipos son usados como agendas telefónica, calendarización, almacenamiento de datos, reproductores de videos/música y hasta como mini computadoras capaz de crear todo tipo de documentos, muchas personas dejan a un lado tecnología reciente como los CD, las USB, y muy pronto las computadoras de escritorio, esto quiere decir que la información guardada en los Smartphone es de total importancia.

Es esta investigación se ha tratado de demostrar que la información almacenada en nuestro equipos inteligentes son vulnerables y están expuesta a cualquier persona ajena a nosotros, existen tantas formas de perder información tan simple con el solo hecho de conectarse a una red WIFI.

Los estudiantes de la Universidad Católica de El Salvador no dedican el tiempo suficiente para poder actualizar las app que poseen, así mismo el interés que toman en cuanto a la descarga de App de seguridad para resguardar información es mínima a comparación de App que solo utilizan como entretenimiento y personalización de móviles. Las App de Seguridad no solo cuidan la información almacenada en nuestros equipos inteligentes, hay muchas aplicaciones que nos ayudan en la pérdida del equipo para poder recuperar información.

Al hacer un buen uso de las diferentes App de seguridad que podemos encontrar en la tienda de cada uno de los sistemas operativos de nuestros Smartphone tendremos un equipo capaz de sustituir una computadora.

En cuanto a las hipótesis establecidas se concluye:

- El 48.2% de los encuestados demuestran muy poco interés y carecen de tiempo para proteger su información almacenada en sus Smartphone, la primera hipótesis se cumple ya que los estudiantes prefieren descargar o actualizar 1 vez a la semana las App

- De todas los estudiantes encuestados el 3.6% se enfocaron en descargar App de Seguridad, por tanto se verifico que la mayoría de estudiantes demuestran muy poco interés en mantener resguardada la información almacenada en el Smartphone.
- De todas las personas encuestadas se verifica que el 39.8% prefieren descargar App de entretenimiento en segundo lugar prefieren las actualizaciones de las Aplicaciones por tanto prefieren el entretenimiento antes que la seguridad.
- De todas las personas que han sufrido de robo de información que es el 48.6% de los encuestados han aprovechado las aplicaciones de seguridad para recuperar información. Como se ha demostrado en la investigación es posible recuperar información almacenada en nuestros Smartphone cuando se ha sufrido de robo, perdida o destrucción total de su equipo inteligente, lo único importante es utilizar adecuadamente las Aplicaciones requeridas el 51.4% son las personas que no pueden y nunca han logrado recuperar la información.
- Se plantearon varias opciones para poder recuperar la información algunos encuestados que si han podido recuperar esa información prefieren la sincronización de datos donde pueden almacenar y actualizar información importante estos son el 29.9%, en segundo lugar son las App de seguridad con él 17.1% las que les han ayudado, luego están las que usan Backup de información estas personas suman el 12.4%, en total el 59.4% de los encuestados han utilizado y aprovechado de la mejor manera y han recuperado información importante el resto de personas nunca han logrado utilizar las herramientas.

Recomendaciones:

Se recomienda a cada una de las personas que poseen una Smartphone descargar al menos un tipo de App de seguridad estar actualizándola si esta App es gratuita o realizar la compra de una buena App ya que es de suma importancia que nadie tenga acceso a la información almacenada

Adoptar un hábito para realizar copias de seguridad o Backup día con día en una computadora o en otro dispositivo confiable. Se recomienda evitar conectarse a redes públicas vía WIFI ya que por ser un acceso abierto puede encontrarse con agentes maliciosos que puede tener acceso a información almacenada, además de extraer nuestros documentos importantes.

Todo persona dueña de un Smartphone tiene que utilizar un patrón de bloqueo de acceso ya sea para acceder al equipo o alguna aplicación. Se recomienda descargar una aplicación de las tiendas de cada sistema operativo, y no de una página web externa. El descargarte un archivo de una web externa e instalarlo en tu dispositivo te puede abrir las puertas a la instalación conjunta de malware, sobre todo malware de publicidad excesivos.

Se recomienda que cuando accedemos al correo desde el teléfono móvil, debemos tener cuidado al hacer clic en enlaces y prestarle mucha atención a la página destino a la que nos lleve. Las estafas de phishing o suplantación de identidad no se limitan al correo electrónico, también un sms de texto o mensaje por whatsapp puede incitar a que hagas clic en un enlace "fiable" para solicitar información personal.

BIBLIOGRAFÍA

<http://elmundo.com.sv/salvadorenos-gastan-1-2-millones-al-dia-en-telefonía-movil/>

<http://www.hardwaremx.com/forum/topic/302366-kaspersky-lab-registro-de-nuevos-programas-maliciosos-baj%C3%B3-a-310000-por-d%C3%ADa-en-2015-a-la-par-que-cibercriminales-buscan-ahorrar-dinero/>

<http://www.quees.info/que-es-un-smartphone.html>

https://es.wikipedia.org/wiki/Sistema_operativo_m%C3%B3vil

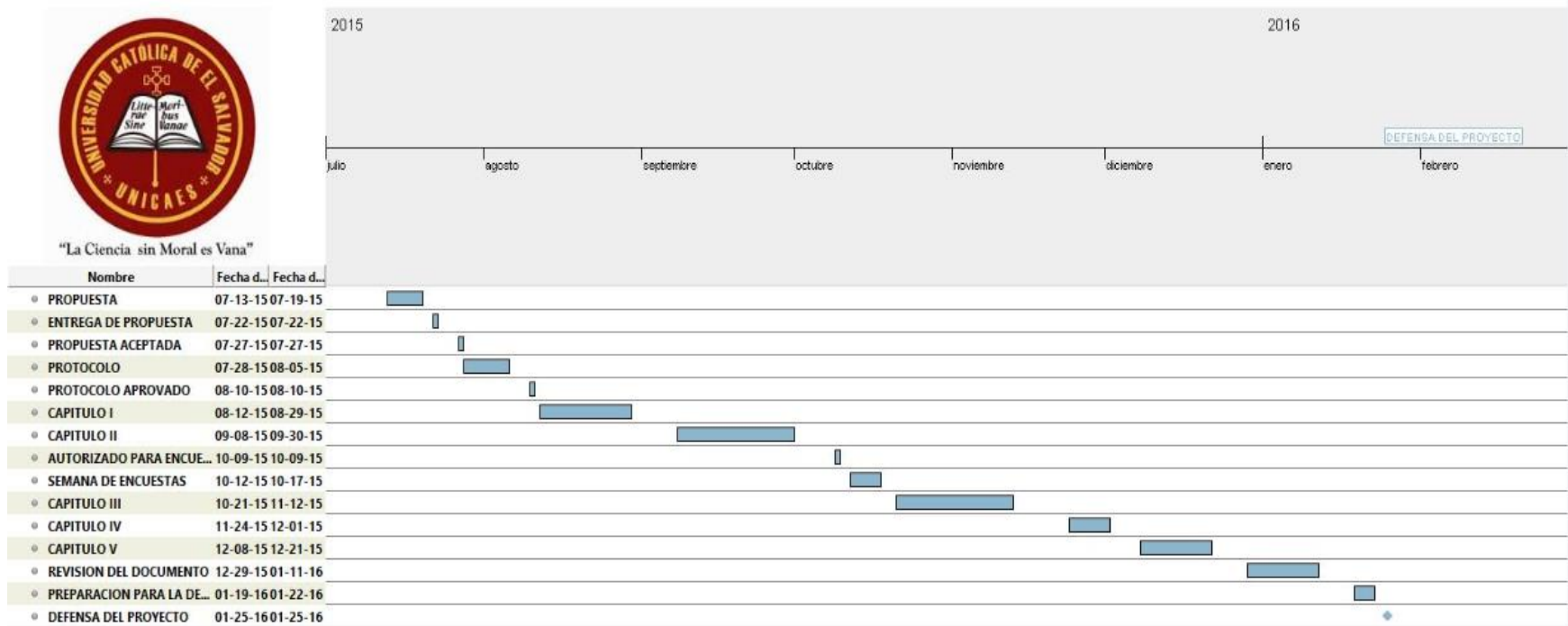
<https://www.yeeply.com/blog/beneficio-economico-de-las-apps/>

<http://www.lancetalent.com/blog/tipos-de-aplicaciones-moviles-ventajas-inconvenientes/>

https://es.wikipedia.org/wiki/Aplicaci%C3%B3n_m%C3%B3vil#Tiendas_de_aplicaciones:

<http://www.xatakamovil.com/aplicaciones/ovi-store-la-tienda-de-aplicaciones-de-nokia>

CRONOGRAMA DE LA INVESTIGACIÓN



"La Ciencia sin Moral es Vana"

ANEXOS

Encuesta dirigida a estudiantes de la Universidad Católica de El Salvador

UNIVERSIDAD CATÓLICA DE EL SALVADOR

Objetivo: Obtener información sobre el conocimiento y metodología que los estudiantes de la Universidad utilizan para la seguridad móvil



Edad *

Sexo *

- Femenino
- Masculino

Seleccione la facultad a la cual pertenece *

- Ingeniería y Arquitectura
- Ciencias y Humanidades
- Ciencias Empresariales
- Ciencias de la Salud

¿Posee un Smartphone? *

- Si
- No

¿Cuál es el Sistema Operativo de su Smartphone? *

- Android
- Microsoft Phone
- IOS
- BlackBerry

- Symbian
- Otros

¿Cuál es el tipo de plan de datos de su Smartphone?

- Pos-pago
- Pre-pago

Usted tiene su Smartphone pre-pago ¿con qué frecuencia compra paquetes de navegación? *

- Nunca
- Pocas veces
- Regularmente
- Siempre

Conoce la tienda de App de su Smartphone

- Si
- No

¿Con que frecuencia descarga o actualiza sus App en la semana?

- Muy poco
- 1 vez en la semana
- 2 veces a la semana
- 3 o más veces por semana
- Siempre

¿Cuál de los siguientes tipos de App descarga con más frecuencia? *

- Entretenimiento
- Seguridad
- Actualizaciones
- Personalización de su móvil
- Libros
- Otros

¿Cuál de estos tipos de Información se almacena en su equipo inteligente (Smartphone o Tablet)?*

- Multimedia
- Contraseñas
- Documentos
- Datos personales
- Todas las anteriores

¿De cuál de las siguientes formas de seguridad utiliza en su Smartphone o Tablet? *

- App de Bloqueo de acceso
- App contra Spyware
- App de Antirrobo
- Sincronización
- App de Backup
- Ninguna

Ha sufrido de la pérdida de su información almacenada en su Smartphone o Tablet ya sea por robo, pérdida o destrucción del equipo *

- Si
- No

Ha recuperado la Información perdida o robada mediante: *

- App de seguridad
- Sincronización de datos
- App de back up
- Nunca la he recuperado

Las App de seguridad que posee son:

- Paga
- Gratis
- No poseo

¿Por qué Utiliza las App de seguridad de paga?

- No le gusta la publicidad

- Mejor calidad
- Más confiable
- Mejores actualizaciones
- No aplica (no tengo instalado)

¿Por qué Utiliza las App de seguridad de gratis?

- No le gusta invertir
- Solo necesita un tiempo corto para usarlas
- No le toma importancia a su móvil
- No le interesa tener la mejor App
- No aplica (no tengo instalado)

Al tener disponibilidad de una red Inalámbrica (WIFI) en un lugar público, ¿se conecta a dicha red?

- Nunca
- Regularmente
- Siempre