



# UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

MAESTRÍA EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE LA  
INFORMACIÓN

## METODOLOGÍA PARA LA SELECCIÓN DE HERRAMIENTAS EFICIENTES Y PROTOCOLOS ADECUADOS PARA MEJORAR LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES.

Trabajo de titulación previo a la  
obtención del título de Magister en  
Gestión Estratégica de Tecnologías de  
la Información.

**Autora:**

Ing. Daysi Mireya Erreyes Pinzón  
C.I. 1103494736

**Director:**

PhD. Diego Arturo Ponce Vásquez  
C.I. 0101822609

CUENCA - ECUADOR

2017



## Resumen

En la actualidad existen herramientas para proteger la información contenida en los dispositivos móviles, muchos usuarios desconocen los riesgos que implica el no utilizar las medidas de protección adecuadas; por otra parte existen estándares internacionales que aportan con modelos completos para la gestión y mejora continua de los sistemas de gestión de seguridad de la información.

En esta investigación se revisa: la seguridad de la información, la seguridad en entornos móviles, revisión de los principales estándares relacionadas con la seguridad informática como: la norma ISO 27001, NIST 800-30, COBIT 5 y OWASP; mediante la adaptación del Método de Estudio de Similitud entre Modelos y Estándares (MSSS) se realizó un análisis de éstos estándares; finalmente se diseñó una metodología a la que se aplicó la respectiva fase de pruebas.

El objetivo de esta investigación fue diseñar una metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles, mismo que se ha cumplido con la creación de la metodología denominada: Metodología para Selección de Herramientas de Seguridad en Dispositivos Móviles (Ms-DisMov), la que permitirá a los usuarios y profesionales dedicados a la protección de la información, disponer de una guía práctica que les permita seleccionar herramientas validadas y puedan mejorar su nivel de protección de la información contenida en sus dispositivos móviles.

**Palabras clave:** Ciberseguridad, Seguridad Informática, Metodología seguridad, Seguridad móvil.



---

## Abstract

Currently there are tools to protect the information contained in mobile devices, many users are unaware of the risks involved in not using the appropriate protection measures; On the other hand there are international standards that provide complete models for the management and continuous improvement of information security management systems.

In this research, we review: information security, security in mobile environments, revision of the main standards related to computer security such as: ISO 27001, NIST 800-30, COBIT 5 and OWASP; By means of the adaptation of the Method of Study of Similarity between Models and Standards (MSSS) an analysis of these standards was made; Finally a methodology was designed to which the respective test phase was applied.

The objective of this research was to design a methodology for the selection of efficient tools and adequate protocols to improve the security of mobile devices, which has been fulfilled with the creation of the methodology called: Methodology for Selecting Security Tools in Mobile Devices (Ms-DisMov), which will allow users and professionals dedicated to the protection of information, have a practical guide that allows them to select validated tools and can improve their level of protection of the information contained in their mobile devices.

Keywords: Cybersecurity, Informatic Security, Security methodology, Mobile security.



---

## Índice de contenido

Resumen .....	2
Abstract.....	3
Cláusula de Reconocimiento del Derecho de la Universidad para publicar el documento.....	8
Cláusula de Propiedad Intelectual. ....	9
1. Introducción.....	10
2. Desarrollo .....	12
2.1. CAPITULO I: La seguridad informática.....	12
2.1.1. Concepto y principios de la seguridad informática.....	12
2.1.2. Amenazas .....	15
2.1.3. Vulnerabilidades .....	17
2.1.4. Ataques .....	19
2.1.5. Riesgo Tecnológico.....	20
2.1.6. Impactos.....	21
2.2. CAPITULO II: Seguridad en entornos móviles.....	22
2.2.1. Problemas de la seguridad móvil.....	22
2.2.2. Criterios de diseño de la seguridad móvil .....	27
2.2.2.1. Amenazas de la seguridad móvil .....	27
2.2.2.2. Vulnerabilidades en el diseño de teléfonos móviles.....	32
2.2.2.3. Ataques a dispositivos móviles .....	35
2.2.2.3.1. Ataques basados en la comunicación de datos.....	36
2.2.2.3.2. Ataques basados en vulnerabilidades en las aplicaciones de software .....	38
2.2.2.3.3. Ataques basados en vulnerabilidades de hardware.....	39
2.2.2.4. Argumento para mejorar el diseño de la seguridad móvil.....	39
2.3. CAPÍTULO III: Estándares de la seguridad informática .....	42
2.3.1. Norma: ISO 27001 .....	42
2.3.2. NIST: 800-30.....	50
2.3.3. COBIT 5 .....	54
2.3.4. OWASP Top Ten.....	60
2.4. CAPÍTULO IV: Análisis de los modelos y estándares .....	65
2.4.1. Establecer criterios para la selección adecuada de modelos y estándares para la seguridad de los dispositivos móviles.....	66
2.4.2. Selección de modelos y estándares .....	67
2.4.3. Definir aspectos a analizar en cada modelo o estándar seleccionado.....	68



2.4.4.	Elaboración de una matriz comparativa entre los modelos y estándares seleccionados.....	68
2.4.5.	Identificar similitudes entre los modelos y estándares seleccionados y los problemas de la seguridad móvil.....	71
2.4.6.	Presentar los resultados obtenidos .....	80
2.5.	Capítulo V: Diseño de la Metodología.....	88
2.5.1.	Problemática.....	88
2.5.2.	Solución del problema.....	89
2.5.3.	Metodología para seguridad en dispositivos móviles (Ms-DisMov).....	92
2.5.3.1.	Aspectos claves de la metodología .....	92
2.5.3.2.	Estructura.....	96
2.6.	CAPITULO VI: Validación de la Metodología .....	102
2.6.1.	Análisis de vulnerabilidades en dispositivos móviles.....	102
2.6.2.	Pruebas de la metodología.....	106
3.	Conclusiones y Recomendaciones .....	123
3.1.	Conclusiones.....	123
3.2.	Recomendaciones .....	126
4.	Referencias .....	129
5.	Anexos.....	132
5.1.	ANEXO A: HERRAMIENTAS.....	132
5.1.1.	SECCIÓN 1 – Incorrecto uso de la plataforma.....	132
5.1.2.	SECCIÓN 2 – Almacenamiento inseguro de datos.....	134
5.1.3.	SECCIÓN 3 – Comunicación insegura.....	137
5.1.4.	SECCIÓN 4 - Autenticación insegura - Autorización insegura.....	139
5.1.5.	SECCIÓN 5 – Criptografía insuficiente .....	141
5.2.	ANEXO B: PRUEBAS REALIZADAS.....	145
5.2.1.	SECCIÓN 1 – Incorrecto uso de la plataforma.....	145
5.2.2.	SECCIÓN 2 – Almacenamiento inseguro de datos.....	146
5.2.3.	SECCIÓN 3 – Comunicación insegura.....	154
5.2.4.	SECCIÓN 4 - Autenticación insegura - Autorización insegura.....	155
5.2.5.	SECCIÓN 5 – Criptografía insuficiente .....	156



---

## Índice de Tablas

Tabla 1: Riesgos Potenciales.....	20
Tabla 2: Metas Corporativas de COBIT 5.....	55
Tabla 3: Pasos de la Metodología (MSSS).....	66
Tabla 4 : Comparativa de estándares y proyectos profesionales de seguridad .....	69
Tabla 5: Dominios y Secciones.....	71
Tabla 6: Similitud ISO 27001 (Anexo A) y los problemas de la Seguridad Móvil .....	73
Tabla 7: Similitud NIST 800-30 y los problemas de la Seguridad Móvil .....	75
Tabla 8: Relación procesos COBIT 5 y metas de TI.....	77
Tabla 9: Similitud entre COBIT 5 y los problemas de la Seguridad Móvil .....	77
Tabla 10: Resumen modelos y estándares seleccionados.....	81
Tabla 11: Similitud entre los problemas de la seguridad móvil y los estándares seleccionados.....	83
Tabla 12: Acoplamiento de Controles ISO 27001 (Anexo A)-OWASP.....	84
Tabla 13: Controles para selección de herramientas .....	86
Tabla 14: Criterios para selección de herramientas .....	93
Tabla 15: Parámetros de valoración de criterios .....	95
Tabla 16: Parámetros de valoración de herramientas .....	95
Tabla 17: Vulnerabilidades identificadas .....	103
Tabla 18: Escenarios a evaluar .....	105
Tabla 19: Herramientas alineadas a los escenarios del OWASP .....	107
Tabla 20: Evaluación de criterios para selección de herramientas .....	108
Tabla 21: Fichas de resultados de pruebas .....	109
Tabla 22: Tabla de resultados .....	115
Tabla 23: Buenas prácticas .....	120



---

## Índice de Figuras

Figura 1: Relación de seguridad de la información .....	12
Figura 3: Servicios CIDAN .....	15
Figura 4: Relación entre Amenaza, Vulnerabilidad, Ataque e Impacto. ....	21
Figura 5: Modelo PDCA .....	44
Figura 6: Norma ISO 27001:2013 .....	45
Figura 7: Componentes de la Gestión de Riesgos.....	53
Figura 8: Análisis y Gestión de riesgos NIST 800-30.....	54
Figura 9: Ciclo de vida- Enfoque COBIT 5 .....	58
Figura 10: Modelo de Referencia de Procesos de COBIT 5 .....	59
Figura 11: Top ten Mobile .....	64
Figura 12: Modelos y estándares seleccionados.....	68
Figura 13 : Relación entre los problemas de Seguridad y Owasp Top Ten .....	78
Figura 14: Selección riesgos del Top ten. ....	79
Figura 15: Riesgos del Top ten (seleccionados) .....	79
Figura 16: Esquema de Resolución del Problema .....	91
Figura 17: Estructura de la Metodología.....	99



## Cláusula de Reconocimiento del Derecho de la Universidad para publicar el documento.



Universidad de Cuenca  
Cláusula de Licencia y Autorización para Publicación en el Repositorio Institucional

---

Daysi Mireya Erreyes Pinzón en calidad de autora y titular de los derechos morales y patrimoniales del trabajo de titulación **“Metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles”**, de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN reconozco a favor de la Universidad de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos.

Asimismo, autorizo a la Universidad de Cuenca para que realice la publicación de este trabajo de titulación en el Repositorio Institucional, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Cuenca, 28 de Julio de 2017

Daysi Mireya Erreyes Pinzón

C.I: 1103494736



## Cláusula de Propiedad Intelectual.



Universidad de Cuenca  
Cláusula de Propiedad Intelectual

---

Daysi Mireya Erreyes Pinzón, autora del trabajo de titulación **“Metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles”**, certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autora.

Cuenca, 28 de Julio de 2017

---

Daysi Mireya Erreyes Pinzón

C.I: 1103494736



## 1. Introducción

Los dispositivos móviles, proporcionan a los usuarios acceso a una variedad como el correo electrónico, Internet, WhatsApp, navegación GPS y muchas otras, al hacer uso de éstas frecuentemente almacenan: información confidencial, programación de reuniones, información de contacto, contraseñas y si revisamos las redes sociales mantienen una gran cantidad de información personal; desafortunadamente muchos usuarios desconocen las deficiencias de seguridad que pueden tener éste tipo de aplicaciones y generalmente no activan las opciones de seguridad instalada en sus dispositivos y asumen que navegar por Internet desde sus teléfonos es segura, sin considerar que los teléfonos móviles son cada vez más utilizados como objetivos de ataque gracias a la portabilidad y la similitud con las computadores personales.

Los cibercriminales analizan constantemente las vulnerabilidades de los dispositivos móviles usando viejas y nuevas técnicas de hackeo, mediante el cual pueden acceder de forma no autorizada empleando estrategias informáticas, para luego realizar ataques con consecuencias graves como: envío de la información contenida en el dispositivos a los atacantes, ejecución de comandos dañinos, propagación de virus en las PCs que se conectan, exposición de la información financiera contenida en el dispositivo como número de cuentas bancarias y tarjetas de crédito, exposición de nombres de usuario y contraseñas empleadas en el acceso de aplicaciones y servicios en línea y hasta divulgación de la información personal extraída del dispositivo; frente a este tipo de ataques, los usuarios deberían concientizarse y adoptar mecanismos de protección con la finalidad de mejorar la seguridad de sus dispositivos móviles.



---

Con la finalidad de dar un aporte en el campo de la seguridad informática, se ha desarrollado una metodología que permitirá a los usuarios mitigar de alguna manera los ataques a dispositivos móviles para ello se abordan seis capítulos que a continuación se describen.

En el capítulo uno, encontramos los aspectos teóricos relacionados con la seguridad de la información en general, sus principios, amenazas, ataques, vulnerabilidades, riesgo tecnológico; en el capítulo dos se presentan una revisión literaria de la seguridad en entornos móviles, sus principales amenazas, ataques y vulnerabilidades que se pueden presentar en el diseño de teléfonos móviles; en el capítulo tres se describe de forma detallada los principales estándares relacionadas con la seguridad informática como la norma ISO 27001, NIST 800-30, COBIT 5 y el proyecto profesional para dispositivos móviles OWASP Top Ten; luego en el capítulo cuatro se realizó un análisis de los modelos y estándares haciendo una adaptación del método de estudio de similitud entre modelos y estándares (MSSS); en el siguiente capítulo denominado diseño de la metodología se logró plasmar los estándares analizados en una metodología que permitirá a los usuarios y profesionales de dispositivos móviles disponer de una guía que les permite proteger la información contenida en sus dispositivos móviles; en el sexto capítulo se detallan las pruebas realizadas a la metodología propuesta; finalmente se presentan las respectivas conclusiones y recomendaciones de la presente tesis.

## 2. Desarrollo

### 2.1. CAPITULO I: La seguridad informática

#### 2.1.1. Concepto y principios de la seguridad informática

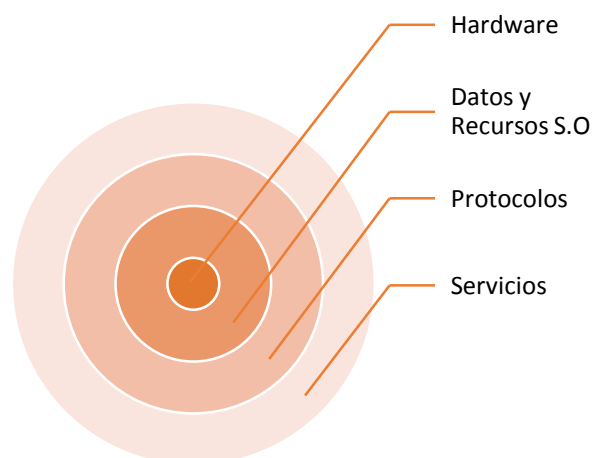
Se entiende como el proceso destinado al resguardo de la información de posibles pérdidas, divulgaciones inapropiadas y hasta modificaciones sin la debida autorización de su propietario.

Costas (2011), en su libro Seguridad Informática afirma lo siguiente:

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentran acreditadas y dentro de los límites de su autorización (p. 19).

En la figura 1 se muestra la protección en profundidad de la información:

*Figura 1: Relación de seguridad de la información*



*Fuente: Elaboración propia*



Se entiende que para lograr una protección en profundidad de la información, en primer lugar está el hardware que constituye la parte física con sus respectivas seguridades para la comunicación con el software; luego se encuentran los datos y los recursos de los sistemas operativos, mismos que incluyen configuraciones propias de seguridad; seguidamente encontramos los protocolos de comunicación que constituyen las reglas básicas para la transmisión de datos entre dispositivos (redes y host); a continuación tenemos los servicios y su protección para todo el abanico de aplicaciones que se puedan instalar sobre el hardware; por encima está el usuario; y, en un sentido más amplio podemos citar a la seguridad de la información, que está enfocada en el resguardo del activo más importante de la organización que es la información, para lo cual es necesario la implementación de estrategias necesarias para salvaguardar dicha información.

Todo componente informático sea hardware o software está expuesto a cualquier tipo de ataque, existen tres principios de protección que se han de ofrecer:

La **confidencialidad** para mantener protegidos los datos de usuarios no autorizados.

Según Costas (2011), a través de este principio un archivo es confidencial cuando puede ser visualizado solo por los usuarios autorizados.

La **integridad**, permite asegurar que la información no haya sido falseada.

Costas (2011) señala que la integridad permite identificar si un archivo ha sido o no manipulado por usuarios no autorizados, durante la transmisión de la información.



---

La **disponibilidad**, se entiende como la condición que la información debe tener para que sea accedida de forma permanente por los usuarios autorizados.

Según Costas (2011) la disponibilidad es la seguridad para que cualquier usuario autorizado pueda recuperar la información necesaria eficazmente.

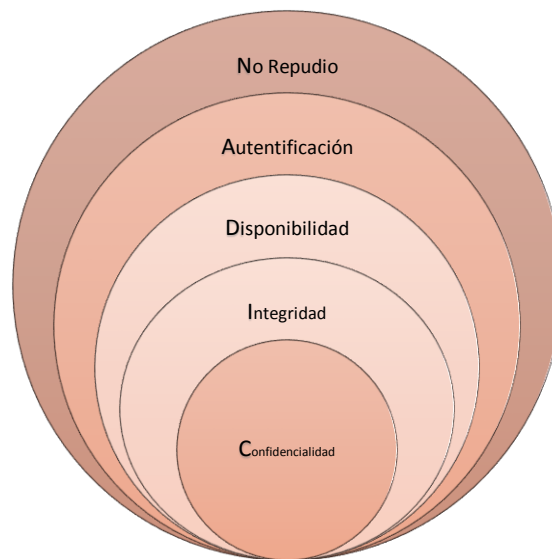
Además de éstos, tenemos la autenticación y no repudio para los sistemas de información.

Según Costas (2011), la **autenticación** es aquella situación por la que el usuario puede demostrar ser quien indica ser y luego de esta demostración se podrá considerar como autorizado, en los sistemas informáticos puede ser mediante el empleo de un usuario y una clave o contraseña.

El **no repudio**, proporciona la protección de un posible rechazo, de la participación tanto del emisor como del receptor en la comunicación, es decir que se pueda comprobar su participación en una determinada comunicación; la diferencia ante la autenticación es que el no repudio se ocasiona ante un tercero.

A éste grupo de principios de la protección se les conoce como CIDAN, considerando la inicial de cada una de ellas. En la figura 2 podemos visualizar la relación existente entre éstos cinco principios relacionados con la seguridad informática.

Figura 2: Servicios CIDAN



Fuente: Adaptación (Costas, 2011)

La figura de la parte superior nos indica la relación jerárquica existente entre los principios de la seguridad informática, por lo que no puede aplicar un principio si no tenemos presente el principio inmediato anterior, se observa además que el primer requisito es la confidencialidad.

### 2.1.2. Amenazas

Una amenaza se entiende como la situación de daño cuyo riesgo de producirse es significativo, debido a que puede deliberadamente o no, producir perjuicio contra la seguridad de la información.

Diariamente los seres humanos, estamos propensos a afrontar cualquier tipo de amenazas, sean provocadas o de manera accidental; el hardware y los sistemas no son la excepción, también pueden ser víctima de situaciones anómalas que interrumpen su normal funcionamiento.



---

López (2011) expresa que un daño en un sistema informático se entiende como el perjuicio que se presenta cuando éste deja de funcionar o falla, el mismo que debe ser cuantificado en términos de: coste económico ya sea por datos perdidos, tiempo de recuperación y el esfuerzo requerido para que nuevamente funcione el sistema; dicho daño puede ser provocado, o producirse de manera fortuita.

A continuación se presentan, los principales desafíos de la seguridad informática que pueden ser provocados por las personas, por amenazas lógicas, amenazas físicas y externas.

✓ *Personas*: el punto más débil relacionado con la seguridad hoy en día son las personas; es muy común reconocer que los principales gestores de ataques a nuestros sistemas informáticos son las mismas personas que realizan esta tarea ya sea de forma intencionada o inintencionada y que pueden causar desde daños leves hasta daños ilimitados.

Costas (2011) en su libro de Seguridad Informática, nos da a conocer que los tipos de personas que pueden convertirse en potenciales riesgos para nuestros sistemas informáticos están clasificados en dos grupos que son: atacantes pasivos, que únicamente espían los sistemas sin realizar cambios; y, los atacantes activos son lo que modifican y dañan los sistemas a su favor. Entre los principales tenemos: *personal, exempleados, curiosos, hackers, cracker, intrusos remunerados, etc.*

✓ *Amenazas lógicas*: en la actualidad contamos con cientos de herramientas para la seguridad que ayudan a proteger la información; sin embargo existen programas creados de forma intencionada para causar daños a los sistemas informáticos, comúnmente conocido como malware.



---

Según López (2011) entre las principales amenazas lógicas tenemos: *el software incorrecto, las herramientas para la seguridad, las puertas traseras, los canales cubiertos (canal forzado de comunicación, con fines ilícitos que atentan la seguridad de la información), virus, gusanos, caballos de troya, programas conejo o bacterias y las famosas bombas lógicas.*

- ✓ *Amenazas físicas:* estas también afectan gravemente a la seguridad de los equipos; así como también afectan al normal funcionamiento de los sistemas, entre los más conocidos tenemos: destrucción de sistemas, robos, sabotajes, además cortes, subida y bajada de la corriente eléctrica.
- ✓ *Amenazas Externas:* son generalmente provocadas por desastres naturales como por ejemplo un terremoto, fallas del sistema eléctrico, daños en la red de telecomunicaciones, que afectan enormemente a la integridad de la información; el aspecto político de un estado también constituye una amenaza por cuanto influye en los tres principios de la seguridad, constituyéndose en la amenaza con mayor grado de afectación para la disponibilidad de la información, por cuanto las políticas regulan, controlan, supervisan y en cierto modo condicionan el accionar en las organizaciones y por consiguiente el desarrollo de los sistemas de información.

### **2.1.3. Vulnerabilidades**

Actualmente en las organizaciones el denominador común son las vulnerabilidades.



---

Según López (2011), se entiende como vulnerabilidad a la o las deficiencias que se puedan encontrar en un sistema, misma que puede desembocar en un fallo del mismo.

Las vulnerabilidades pueden ser de todo tipo, se debe cuantificar qué vulnerabilidades implican un riesgo mayor que otras para crear planes adecuados de mitigación que reduzcan la posibilidad de que existan vulnerabilidades en los sistemas que se implementen. Existen vulnerabilidades en la fase de diseño, implementación y uso.

Entre las principales herramientas que nos indica López (2011) tenemos:

- **Listas bugtraq**, se debe revisar constantemente este tipo de listados especializados, ya que allí también se podrá encontrar las formas de proteger nuestros sistemas, de una determinada vulnerabilidad.

Es una de las listas más importantes hoy en día, para tener acceso es necesario subscribirse enviando un correo a [listserv@lists.securityfocus.com](mailto:listserv@lists.securityfocus.com), con el siguiente mensaje "subscribe bugtraq nombre"; existen otras listas como: Best of Security, Linux Security, Intrusion Detection Systems, etc.(Huerta, 2002).

- **Sistemas automáticos de análisis**, entre los que tenemos los *escáneres para búsqueda de vulnerabilidades, las redes trampa, la auditoría automática de código*,

Las principales vulnerabilidades se pueden presentar a nivel de: *Hardware* (equipos informáticos y telemáticos); y a nivel de *Software* (sistemas operativos,



configuraciones y puertos); Humano (ingeniería social y ambiente laboral); Negligencia (por no valorar el riesgo); y además por el desconocimiento.

#### **2.1.4. Ataques**

Ataque en ciberseguridad refiere al acto deliberado perpetrado por un hacker sobre la infraestructura informática y telemática o sobre la información que estos sistemas albergan.

Según López (2011), define al ataque como un acto deliberado que se produce cuando se intenta provocar un daño en un sistema específico; cualquier tipo de ataque constituye una amenaza a la seguridad informática, sin dejar a un lado los casos en los que el daño se produce de forma accidental por ejemplo los fallos en el hardware, cortes en el energía eléctrica, tormentas eléctricas, incendios y otros desastres naturales.

Los ataques son considerados como la forma mediante la cual un individuo, utiliza un sistema informático, para intentar controlar o desestabilizar y/o dañar a otro sistema informático.

Hay diversos tipos de ataques informáticos entre los más importantes tenemos: Ataques Pasivos que se producen por: ataque de intermediario (man in the middle); Ataques Activos, ocasionados por: eliminación, modificación, suplantación, Interceptación; Ataque combinado (hacker, cracker, cibercrimen), virus, worms, troyanos, spyware, malware, rootkis.



### 2.1.5. Riesgo Tecnológico

“Definiremos el riesgo (R) como el producto entre la magnitud de un daño (d) y la probabilidad de que éste tenga lugar (pd):  $R = d * pd$ ” (López, 2011, p. 258).

El riesgo tecnológico se origina debido al acelerado incremento de aplicaciones y herramientas tecnológicas, muchas de ellas no disponen de seguridades; por otra parte en muchas organizaciones aún no cuentan con una adecuada administración de las seguridades.

La revista Seguridad Cultura de Prevención para TI (Biom, Gerencia, Seguridad, Tecnol, & Electr, 2012), presenta al riesgo tecnológico de acuerdo a tres niveles que son: infraestructura TI (riesgos relacionados con el hardware o sea a nivel físico), lógico (riesgos relacionados con: información, software general, software aplicativo y sistemas informáticos) y factor humano (riesgos que se derivan del uso inadecuado de los factores físico y lógico).

A continuación en la tabla 1, se presentan los riesgos en relación con el impacto a los niveles mencionados:

Tabla 1: Riesgos Potenciales

RIESGO	Infraestructura TI	Lógico	Factor Humano
Acceso remoto a equipos	X		
Correos “anónimos” con contenido sensible o agresivo		X	
Correos basura enviados (Spamming)		X	
Violación de correo personal			X
Dstrucción de equipos	X		
Violación de claves de usuarios		X	
Intercepción y modificación de correos personales			X
Virus	X	X	
Acceso a información privada de empleados	X		X
Ingeniería social			X
Empleados no éticos			X
Fraudes informáticos			X
Aplicaciones tipo “bomba”	X	X	
Interrupción del servicio		X	X
Daño a soportes documentales			X



RIESGO	Infraestructura TI	Lógico	Factor Humano
Acceso anónimo en redes de datos	X		X
Robo o pérdida de portátiles	X		X
Acceso no autorizado a documentos impresos			X
Software ilícito		X	
Interrupción de comunicaciones			X
Alteración de información para beneficio de terceros			X
Brechas de seguridad en sistemas de redes		X	
Instalaciones por defecto		X	
Escalamiento de privilegios en sistemas operativos		X	
Puertos abiertos y vulnerables	X		
Hombre en el medio (Man in the middle)			X
Fragmentos de software (Exploits)		X	
Denegación de servicio		X	X
Actualización parches no instalados		X	
Falta de Backups		X	
Antivirus desactualizados		X	
Scaneo de puertos		X	

Fuente: Adaptación (Biom et al., 2012)- Riesgos Potenciales

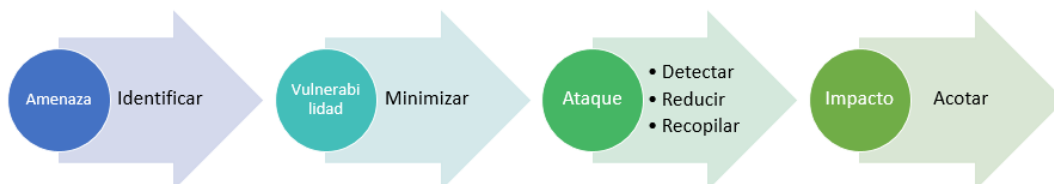
### 2.1.6. Impactos

Un impacto se produce por ataque a los equipos o sistemas informáticos, entre los principales tenemos:

- *Negocio*, que ocasiona principalmente pérdidas: económicas y de información, además credibilidad, reputación, competitividad.
- *Terceros*, ocasionado a proveedores y clientes, datos personales, acuerdos de servicio, daños y perjuicios, pérdida de oportunidades y desconfianza.

En el figura 3, se presenta la relación de los conceptos analizados:

Figura 3: Relación entre Amenaza, Vulnerabilidad, Ataque e Impacto.



Fuente: Elaboración propia



## 2.2. CAPITULO II: Seguridad en entornos móviles

### 2.2.1. Problemas de la seguridad móvil

Por los años 90 ya existían notables problemas de seguridad, pero las agencias de inteligencia europeas relajaron las medidas de seguridad con la red GSM más conocida como 2G, que apareció durante la guerra fría y que a pesar de la mejora en la seguridad tanto en red móvil 3G y 4G, provocó una brecha de seguridad que persiste hasta hoy en día, por lo que el tema de la protección de los dispositivos móviles constituye el principal elemento dentro de la organización, ya que mediante éstos se accede a información sensible y también a la Internet (Dwivedi, Clark, & Thiel, 2014).

Adams (2016), en su artículo denominado Possessing Mobile Devices, señala que la falta de control administrativo se vuelve cada vez más problemático para los proveedores de smartphone (fabricantes, proveedores, los integradores de sistemas, telecomunicaciones, etc.) al parecer quieren que los usuarios actualicen sus dispositivos con más frecuencia. Por otra parte existe un rápido desarrollo de nuevos modelos de iOS y Android y los proveedores nos están ofreciendo dispositivos antiguos con las actualizaciones y en otros casos dispositivos antiguos en los que las actualizaciones están implantándose muy poco.

Daniel Thomas y sus colegas recientemente mostraron que aunque Google parchea el sistema Android base, muchos fabricantes son muy lentos para alimentar dichos parches a través de los dispositivos de los usuarios: el 87% de las máquinas de Android en su estudio había conocido vulnerabilidades sin parches, (Adams, 2016).



---

Dwivedi , Clark y Thiel (2014) en su libro *Mobile Application Security*, nos dan a conocer un listado de problemas con los que se enfrentan diariamente los dispositivos móviles y las aplicaciones que se citan a continuación:

- ✓ **La seguridad física.-** siempre ha estado en riesgo, el principal caso se da cuando perdemos un teléfono móvil, esto económicamente quizá en algunos casos no represente un gran valor, pero éste en manos de un extraño representa una mina de oro, ya que tiene a disposición datos sensibles como correo electrónico e información de la organización para la cual trabaja; otro caso se da cuando se presta el teléfono a un tercero para que haga una llamada telefónica, el acceso temporal que tiene es suficiente para revisar información confidencial, descargar un malware, etc. situaciones que suceden también en el mundo de computadores de escritorio y portátiles, (Dwivedi et al., 2014).
- ✓ **Almacenamiento seguro de datos (en disco).-** tiene mucha relación con el anterior, debido a que ante una pérdida física del dispositivo, pc o portátil, el acceso a los datos almacenados no será un problema si no se encuentran protegidas, el intruso podrá acceder a documentación sensible, aplicaciones instaladas, archivos de contraseñas y tokens de autenticación, ante lo cual es importante promover en las empresas políticas que permitan la gestión adecuada de la computación móvil segura, (Dwivedi et al., 2014).
- ✓ **Autenticación fuerte.-** se refiere a claves de longitud mayor como las de la firma digital, fingerprint y se han de combinar con un secreto personal, para mejorar las exigencias de autenticación segura, más aún si el acceso es a datos sensibles como la propia cuenta bancaria y si se realiza desde nuestro dispositivo, (Dwivedi et al., 2014).



- ✓ **Apoyo a la seguridad de múltiples usuarios.-** los sistemas operativos tradicionales soportan varios usuarios, pero el inconveniente es que su arquitectura está diseñada para otorgar a cada usuario un entorno operativo diferentes con un usuario y contraseña independiente asegurando de alguna manera la información; mientras que en los dispositivos móviles aún no se puede trabajar como un usuario independiente, ya que no hay distinción entre las aplicaciones que utiliza, ni distinción de perfiles de usuario, ya que el dispositivo no lo soporta aún, (Dwivedi et al., 2014).
- ✓ **Navegación segura del medio ambiente.-** el mayor riesgo al que están expuestos los dispositivos móviles es el comportamiento que adopte el usuario al momento de navegar, en este punto surgen algunos aspectos técnicos como: no poder visualizar completamente la URL debido a la falta de espacio, convirtiéndose en presa fácil para cualquier phisher, por cuanto el usuario normal no puede determinar con facilidad que enlaces son seguros o no; así mismo un estafador puede fácilmente lograr su objetivo con usuarios móviles mediante el usos de las redes sociales, (Dwivedi et al., 2014).
- ✓ **Aseguramiento de los sistemas operativos.-** el desarrollo de sistemas operativos para móviles no es tarea fácil para los proveedores de software y aplicaciones; así mismo los fabricantes de dispositivos móviles deben considerar que la seguridad generalmente está relacionada con la pérdida de datos y con el tiempo de inactividad del sistema, (Dwivedi et al., 2014).
- ✓ **Aislamiento de aplicaciones.-** Un dispositivo móvil se utiliza para realizar desde una simple llamada telefónica, hasta el uso de aplicaciones para varias tareas como: entretenimiento, trabajo y social; mediante las cuales se requiere acceder a datos confidenciales contenidos en el dispositivo, por lo que es



---

necesario aislar adecuadamente las aplicaciones para garantizar la confidencialidad de la información almacenada; por otra parte el usuario debe realizar la configuración de los permisos necesarios a nivel del sistema operativo móvil, con el fin de lograr mayor protección en la información contenida, (Dwivedi et al., 2014).

- ✓ **Divulgación de información.-** considerando que para muchos usuarios la información contenida en el dispositivo es más valiosa que el propio dispositivo y que los dispositivos tienen una alta probabilidad de que se lo roben, se pierda o simplemente sea prestado a un tercero, se convierte en un conjunto potencial de problemas para las organizaciones de TI; generando varios escenarios en los que se requiere atención y deben ser tratados y mitigados de alguna manera, entre los que podemos citar: pérdida de datos almacenados en el dispositivo y acceso a través del dispositivo a redes corporativas mediante redes privadas virtuales (VPN), (Dwivedi et al., 2014).
- ✓ **Virus, gusanos, troyanos, spyware y malware.-** no solamente los dispositivos móviles, sino cualquier dispositivo que tenga acceso a internet puede ser abordado por cualquiera de éstas amenazas; la mayoría de desarrolladores tienen la suficiente experiencia en el desarrollo de software para escritorio, sin embargo para este nuevo entorno de dispositivos móviles deben ajustar su conocimiento para poder combatir con las amenazas actuales, (Dwivedi et al., 2014).
- ✓ **Difícil proceso de parcheo/actualización.-** esto no constituye un desafío técnico, ya que el parcheo se realiza normalmente a los programas y se lo hace con fines de corrección de errores y/o actualización; pero existe un inconveniente que es el poco tiempo que otorgan las grandes compañías de



- 
- telefonía móvil para la realización de las pruebas de parches, lo que se ha convertido en un verdadero obstáculo para los desarrolladores de software, (Dwivedi et al., 2014).
- ✓ **Uso estricto y ejecución de SSL.-** el uso adecuado del Secure Sockets Layer (SSL) resulta primordial para desarrollo de un entorno de trabajo seguro, (Dwivedi et al., 2014).
  - ✓ **Suplantación de identidad (Phishing).-** realmente constituye un gran problema a nivel de los dispositivos móviles, la principal razón es que los usuarios requieren hacer clic en los elementos de su teléfono para realizar sus actividades diarias y además que los navegadores ni siquiera muestran la URL completa para que el usuario sepa a donde lo llevan ciertos enlaces, (Dwivedi et al., 2014).
  - ✓ **Cross site request forgery (CSRF).-** se trata de un tipo de amenaza que afecta directamente a aplicaciones web, se basa en la actualización de información como dirección de correo electrónico y contraseña; este ataque se convierte en un gran problema para los sitios HTML móviles que son vulnerables, ya que los usuarios móviles no tienen más remedio que hacer clic en los enlaces desde páginas web o correos electrónicos para usar sus teléfonos con eficacia, (Dwivedi et al., 2014).
  - ✓ **Localización de privacidad / seguridad.-** la privacidad resulta bastante difícil de determinar, por cuanto cada usuario móvil requiere privacidad, pero sabemos que son los mismos usuarios quienes mediante el uso de aplicaciones de localización, GPS, o simplemente una página de Facebook ya están revelando y compartiendo su localización, lo que ha desembocado en un verdadero problema de privacidad, (Dwivedi et al., 2014).



- ✓ **Controladores de dispositivos inseguros.**- como es de conocimiento que en la capa de aplicación es donde se instalan las aplicaciones y los usuarios no deben tener acceso al sistema operativo del dispositivo; sin embargo, los controladores de dispositivos móviles tales como Bluetooth y controladores de vídeo, tiene acceso completo al sistema convirtiéndose en el talón de aquiles para los piratas informáticos, aunque existen muchos sistemas operativos para móviles que han construido esquemas de seguridad para mayor protección, existen ciertos controladores que tienen métodos que violan estos esquemas de protección, por lo que el dispositivo estará expuesto a los atacantes, (Dwivedi et al., 2014).
- ✓ **La autenticación de factores múltiples (MFA).**- sabemos que en cualquier momento un dispositivo móvil puede caer en manos de cualquier persona ya sea de forma accidental o prestado, frente a ello existen muchas aplicaciones web que tienen disponible una autenticación de múltiples factores invisible al usuario, a través de la creación de firmas del dispositivo asociadas al teléfono móvil del usuario que no son más que la combinación de cabecera HTTP más las propiedades de la conexión del dispositivo que son calculadas automáticamente cada vez que el usuario intenta navegar por la Internet, (Dwivedi et al., 2014).

## 2.2.2. Criterios de diseño de la seguridad móvil

### 2.2.2.1. Amenazas de la seguridad móvil

Según Quintana (2016), Kaspersky ha logrado detectar 291887 nuevas amenazas en los dispositivos móviles en el segundo trimestre de 2015, es decir 2,8 veces más que el número detectado en el primer trimestre de ese mismo año, éstas alteran el



funcionamiento del dispositivo y hasta son capaces de transferir y/o modificar los datos del usuario. Es por ello que las aplicaciones que se instalen en el dispositivo deben garantizar los principios de la seguridad informática principalmente la privacidad e integridad de la información; el usuario de smartphone deber ser precavido por cuanto algunas aplicaciones podrían ser ellos mismos el malware.

PCWorld (2013) publica en la sección de noticias del 13 de septiembre del 2013, la reaparición de un troyano Android denominado Obad.a que no es más que un malware que estafa mediante mensajes y su comportamiento se basa en enviar enlaces maliciosos a cualquier registro de la agenda de direcciones de la víctima.

Debido a la constante evolución de las redes, hoy en día tenemos a disposición varias opciones de entretenimiento como: videos en YouTube, diferentes aplicaciones de mensajería, varias redes sociales; pero sin embargo, la mayoría de usuarios no se preocupan por tener actualizado un antivirus y manejar información encriptada; por otra parte las empresas distribuidoras de software no se preocupan por proveer con mayor frecuencia las actualizaciones de los sistemas operativos; es decir aún no tomamos conciencia de los riesgos que conlleva la falta y uso de mecanismos para seguridad móvil.

Memon y Anwar (2016), en su artículo Tomorrow's Mobile Malware Threat, señalan que mientras todavía la comunidad de seguridad está comenzando a entender y detectar aplicaciones maliciosas individuales, una nueva amenaza está surgiendo, la "*Colusión de aplicaciones*"; en la que una operación se divide en partes más pequeñas y se distribuyen a través de múltiples aplicaciones; éstas aplicaciones se comunican o esperan una señal, para desempeñar su pequeña función que la hace



individualmente indetectable; cada app evita sospechas solicitando los permisos mínimos necesarios para ejecutar su función.

Un ejemplo de cuando dos apps pueden coludir, es el siguiente: si la primera app lee y transmite datos confidenciales, la segunda aplicación transmite datos hacia el mundo exterior; si se analizan individualmente, las apps serían consideradas como no maliciosas, debido a que no existe una ruta directa para la transmisión de datos sensibles, (Memon & Anwar, 2016).

Las principales amenazas en los dispositivos móviles son ocasionadas por los malware y spyware; a continuación se detallan las más relevantes:

*FAKEINST*: es una variante en la familia de malware Fakeinst que actúa como un instalador falso, se camufla para hacerse pasar por aplicaciones populares y cuando está activo es capaz de enviar mensajes a números de teléfono tarifados, incluso a servicios de pago por suscripción; utiliza la técnica de aleatorización para evitar la detección por los antivirus (Mikko, 2016).

*RUFRAUD*: conocido como caballo de troya, es común en dispositivos con sistema operativo Android, actúa realizando las siguientes acciones: enviando mensajes SMS a números de teléfono con tarifado adicional, ocultado los fondos de escritorio del computador, juegos y aplicaciones de escritorio, sin el permiso del usuario luego de que éste abre la aplicación; se descubrió en Europa y Rusia (Symantec, 2016).

*TAPLOGGER*: se trata de un troyano que captura los datos de la clave empleada para bloquear la pantalla del teléfono y los datos de los contactos que el usuario digita en la pantalla táctil al hacer las llamadas telefónicas; este troyano requiere permiso



de la red y no del movimiento realizado con el dispositivo, para enviar hacia un atacante externo los datos capturados (Ling et al., 2016).

*CLEANEDOUT*: este troyano fue descubierto por Kaspersky y se distribuía por google play, se caracteriza porque permite a un atacante tomar el control del dispositivo de forma remota; además cuando el dispositivo se conecta a un computador con sistema operativo Windows, se ejecuta el instalador del malware, a través de esta aplicación el atacante podía obtener el número telefónico del usuario, su ubicación, el contenido de sus mensajes, etc. (Lookout, 2016).

*ILEGACY/LEGACY NATIVE*: se trata de un tipo de malware de la familia de Gamex que oculta en las versiones de aplicaciones legítimas que requieren acceso al root en el teléfono; la funcionalidad Gamex se divide en tres componentes que cooperan para infectar el dispositivo, primero obtiene los privilegios de super usuarios, segundo se comunican con su huésped o servidor remoto y tercero inicia con una instalación silenciosa de aplicaciones en el dispositivo; este tipo de malware otorga el control remoto del dispositivo al atacante. (ASENCIOS & PONTIFICIA, 2013)

*TOUHLOGGER*: este tipo de malware es de tipo sensorial, en el que el atacante es capaz de receptar los movimientos realizados por el usuario que manipula el dispositivo táctil a través de los sensores, obteniendo información sensible, además puede realizar capturas de pantalla (ASENCIOS & PONTIFICIA, 2013)

*ANDROID.WALKIN WAT*: constituye una modificación al troyano que pertenece a la aplicación Walk and Text de Android, permite el control del dispositivo a un servidor remoto, éste podrá robar información personal del teléfono; con la información



obtenida el troyano envía mensajes antipiratería a los contactos existentes en directorio del teléfono. (ASENCIOS & PONTIFICIA, 2013).

En el 2015 en el artículo Transactions on Dependable and Secure Computing de la IEEE, Lei Cen y sus colegas propusieron un modelo altamente preciso para detectar malware en aplicaciones Android, los autores observaron que los mercados distribuían aplicaciones que facilitan la descompilación y análisis; además, observaron que las plataformas móviles proporcionan APIs semánticamente ricas; lo que les permitió desarrollar un modelo de aprendizaje discriminativo probabilístico, basado en la regresión logística regularizada, que detecta malware por usar el código y la información descompilados de las aplicaciones acerca de los permisos necesarios, (Bertino, 2016).

Ruggiero y Foote (2011), nos dan a conocer algunas medidas de protección que podemos adoptar frente a éstas amenazas como las que se listan a continuación:

- ✓ Al elegir un teléfono móvil, tenga en cuenta sus características de seguridad.
- ✓ Configurar el dispositivo para que sea más seguro.
- ✓ Configurar cuentas de Internet para uso de conexiones seguras.
- ✓ No seguir enlaces en los mensajes de correo electrónico o de texto sospechosos.
- ✓ Limite la exposición de su número de teléfono móvil.
- ✓ Considere cuidadosamente la información que desea almacenar en el dispositivo.
- ✓ Sea selectivo al seleccionar e instalar aplicaciones.



- 
- ✓ Mantener el control físico del dispositivo, especialmente en lugares públicos o semi-públicos.
  - ✓ Deshabilitar las interfaces que no están actualmente en uso, tales como Bluetooth, infrarrojos o Wi- Fi gratuita.
  - ✓ Evitar unirse a redes Wi-Fi y desconocidos utilizando puntos de acceso público Wi-Fi.
  - ✓ Eliminar toda la información almacenada en un dispositivo antes de descartarlo.
  - ✓ Tenga cuidado al utilizar aplicaciones de redes sociales.

#### **2.2.2.2. Vulnerabilidades en el diseño de teléfonos móviles.**

Como usuarios corporativos o personales de dispositivos móviles, tenemos mucho que ver con la generación de vulnerabilidades al instalar aplicaciones de dudosa procedencia por el hecho de que estas aplicaciones representan soluciones sencillas e inmediatas a las tareas que se requieren en determinados momentos y lo único que nos importa es que se nos facilite realizar la tarea.

Según lo señalado por ESET, “Los cibercriminales están comenzando a enfocarse cada vez más en explotar agujeros de seguridad en sistemas operativos para móviles como Android.” (ESET, 2014).

Las vulnerabilidades existen no solo a nivel de aplicaciones, sino también a nivel del diseño de los algoritmos de cifrado de los teléfonos móviles. Jøsang, Miralabé, & Dalot ( 2015), nos da a conocer que para el cifrado del enlace de radio de segunda generación (2G) se utilizó el algoritmo A5, tanto para A5/1 y A5/2. Inicialmente se concibió así: para los países europeos se debía utilizar el A5/1 porque supuestamente



era más fuerte (realmente es vulnerable) y fuera de Europa debían utilizar el algoritmo más débil A5/2, con una longitud de clave de 56 bits para los dos; al principio éstos diseños fueron secretos, hasta que en 1994 se filtraron.

Según Jøsang, Miralabé y Dallot ( 2015), en relación a la seguridad en 3G UMTS señalan que en esta generación se emplean algoritmos( $f \#$ ) / funciones( $F \#$ ), desde la  $f_1$  a  $f_5$  dentro del dominio del Módulo de Identificación del Abonado (HE/USIM); cada función se implementa con un algoritmo / función específica; con lo que se obtiene una red móvil global menos vulnerable a ataques criptográficos, por cuanto un ataque normalmente afectaría solamente a un pequeño conjunto de operadores de redes móviles.

Según Jøsang, Miralabé y Dallot (2015), señalan que para la tecnología Evolución a Largo Plazo Cuarta Generación (LTE 4G), el diseño de LTE consta de técnicas criptográficas fuertes; así mismo se ha incorporado en la arquitectura mecanismos para la autenticación segura entre pares de elementos de la red LTE; en lo que respecta a la protección criptográfica se ha desarrollado varias capas de protección para 4G, que incluye una jerarquía de claves multinivel, se introdujo además el uso de múltiples funciones de derivación de claves y se requiere un número grande de claves criptográficas; por lo que ésta arquitectura de seguridad requiere mayores exigencias en la gestión de operaciones de seguridad por el Operador de Red Móvil (MNO).

Flynn y Klieber (2016), en su artículo Smartphone Security publicado en la revista Computing Edge, nos dan a conocer que solo el 0.7 por ciento teléfonos Android utilizan la última versión del sistema operativo, existiendo un gran número de



dispositivos con versiones antiguas, muchos de ellos no actualizan porque no reciben actualizaciones, otros las reciben rara vez, lo que se ha convertido en un gran problema, ya que éstos en cualquier momento pueden ser atacados por la vulnerabilidad existente en su plataforma, llegando a un número aproximado de 950 millones de teléfonos que siguen siendo vulnerables.

En android, muchos de las aplicaciones son puramente escritas en Lenguaje Java, lo cual limita el punto de ataque a: las aplicaciones que usan código nativo, vulnerabilidades en la máquina virtual de Java, el entorno de ejecución de Java y las vulnerabilidades en el sistema operativo subyacente (Flynn & Klieber, 2016).

Carver, Sritapan y Corbett (2016), nos hablan de establecer y mantener la confianza en un dispositivo móvil mediante Roots de confianza móvil (RoT) como un chip especializado incluido en el hardware (módulo de confianza de la plataforma) para computadores de escritorio y portátiles; pero para los dispositivos móviles por ser recursos más delicados haría falta un mecanismo más especializado que permita proporcionar RoT al hardware, por lo que la única solución sería proporcionar RoT al software, esto lamentablemente es difícil debido a la sofisticación de las amenazas actuales y por la facilidad con la que la información de un móvil puede ser extraída y modificada.

Por otra parte, las especificaciones de seguridad como Trusted Computing Móvil del Grupo Trusted Module, no apoyan el mecanismo de desarrollar RoT en el software, ni tampoco la dirección dinámica asignada para la verificación del dispositivo y su comportamiento, mientras las aplicaciones de software se estén ejecutando (Carver et al., 2016).



---

BlueRISC está desarrollando MobileRoT, totalmente basado en software, se trata de un módulo dinámico de confianza móvil, bajo el soporte de la tecnología DHS S&T Cyber Security División (CSD), que mide y verifica un dispositivo estático y el estado en tiempo de ejecución (por ejemplo, cargador de arranque, sistema operativo, aplicaciones y memoria en tiempo de ejecución); para mejorar la confianza y la seguridad global del dispositivo, puede ser utilizada para detectar cambios de sistema malicioso o actividad y garantizar que el acceso a la información crítica y software sólo se puede realizar en un estado de confianza y con ello apuntalar el desarrollo de la seguridad móvil, (Carver et al., 2016).

### **2.2.2.3. Ataques a dispositivos móviles**

Dado que ningún sistema de cómputo está completamente inmune al ataque y que la protección de la privacidad debe hacerse y podría variar considerablemente dependiendo del sistema; también enfrentamos los ciberataques modernos que proceden de varios hosts, implican múltiples sesiones y apuntan a varios objetivos simultáneamente. Tales ataques multipunto desafían los enfoques tradicionales de seguridad, como sistemas independientes o la detección de intrusiones de malware, (Hurlburt, 2016).

Bishop (2004), en su libro nos dá a conocer los principales objetivos de los atacantes como: datos, identidad, disponibilidad, profesionales, ladrones, hackers de sombrero negro (su objetivo es el de atacar concretamente la disponibilidad del dispositivo y según Olson (2013) el objetivo es desarrollar virus y causar daño al dispositivo), los hackers de sombrero gris (Según Lemos (2002), se centran en



exponer las vulnerabilidades del dispositivo, sin la intención de dañar el dispositivo o robar información del dispositivo).

### **2.2.2.3.1. Ataques basados en la comunicación de datos**

#### **a) Ataques mediante SMS y MMS**

Existen modelos de teléfonos móviles que presentan inconvenientes al momento de gestionar el Servicio de Mensajes Simples (SMS) binarios, como los que se cita a continuación:

- ✓ Puede suceder que mediante el envío de un bloque de datos inadecuadamente, el teléfono se reinicie, lo que conduce finalmente a ser víctima de un ataque de denegación de servicio, Siemens (2010).
- ✓ Otro ataque sucede cuando un usuario emplea el Servicio de Mensajes Multimedia (MMS), con un archivo adjunto infectado con un virus a otros dispositivos móviles. Luego de ser receptados de los MMS, el usuario puede optar por abrir el archivo adjunto, si este es abierto el teléfono se infecta y el virus envía un MMS con un archivo adjunto infectado a todos los contactos de la libreta de direcciones del dispositivo.

Según Töyssy, Sampo y Helenius (2006), un ejemplo es el virus Commwarrior, que se menciona en su artículo publicado en el año 2016, mismo que hace uso de la libreta de direcciones para enviar mensajes MMS con un archivo infectado adjunto a los destinatarios.

#### **b) Ataques mediante redes de comunicación inalámbrica**

Los ataques mediante redes de comunicación pueden ser: basados en las redes del Sistema Global para las Comunicaciones Móviles (GSM), basados en Wi-Fi y Bluetooth



El algoritmo empleado para el cifrado de red GSM se basa en la familia de algoritmos A5; originalmente existían dos versiones del algoritmo. A5/1 (relativamente fuerte) y el A5/2 (débil, para facilitar el criptoanálisis y espionaje), luego de que algoritmo se publicó, se demostró que A5/2 podía ser roto así lo manifiesta en su artículo Gendrullis Timo (2008).

Según el European Telecommunications Standards Institute (2011), existen otros algoritmos incorporados a la norma GSM, como el A5/3(KASUMI) y A5/4(UEA1).

A través de las comunicaciones Wi-Fi, un atacante puede tratar de obtener información sensible como nombres de usuario y contraseñas, generalmente los teléfonos móviles son los más vulnerables a este tipo de ataque debido a que el único mecanismo de comunicación a la Internet es mediante Wi-Fi, que emplean claves débiles denominadas Privacidad Equivalente a Cableado (WEP) cortas y siempre es el mismo para todos los usuarios conectados.

Según Gittleson Kim (2014), muchos de los teléfonos inteligentes para Redes de Área Local (LAN) inalámbricas generalmente ya están conectados, con lo que se evita que el usuario tenga que volver a identificarse con cada conexión. Pero esto constituye una ventaja para un atacante ya que podría crear un doble punto de acceso Wi-Fi con los mismos parámetros y características que la red real.

Mulliner (2006), en su tesis nos da a conocer que los ataques basados en Bluetooth, presentan numerosos problemas en los diferentes teléfonos, ya que resulta bastante fácil explotar las vulnerabilidades; como es de nuestro conocimiento que si un servicio no ha sido debidamente registrado no requiere de procesos de



autenticación y los sistemas que presentan ciertas vulnerabilidades tienen puertos virtuales que son empleados por los atacantes para manipular el teléfono; por lo que cualquier atacante no necesita más que conectarse al puerto vulnerable y tendrá acceso suficiente para controlar el dispositivo.

Cabir, emplea como medio de propagación la conexión Bluetooth, el gusano escanea los teléfonos cercanos con Bluetooth en modo de detección y se envía automáticamente al dispositivo de destino. El usuario debe aceptar el archivo entrante e instalar el programa; luego éste infecta el dispositivo, Töyssy, Sampo; Helenius (2006).

#### **2.2.2.3.2. Ataques basados en vulnerabilidades en las aplicaciones de software**

Este tipo de ataque se basa en fallos del sistema operativo o aplicaciones instaladas en el teléfono; los más importante son:

✓ *Ataque al Sistema Operativo:*

Según Becher (2009) nos da a conocer que en la mayoría de los sistemas operativos es posible romper sus mecanismos de seguridad implementados en éstos; a pesar de que en los teléfonos inteligentes los archivos de instalación del sistema operativo se almacenan en la memoria ROM y difícilmente pueden ser modificados por el malware, existe la posibilidad de que pueda ser atacado.

✓ *Navegador Web:* los navegadores móviles, sirven tanto para la navegación web pura, con widgets y plugins, en algunos casos se emplea navegadores móviles nativos, es decir la forma de navegación es muy similar a la de un navegador web tradicional.



Otros ataques relacionados con la web son: Phishing y sitios web maliciosos; debido a que éstos dispositivos aún no disponen de un fuerte software antivirus Becher (2009).

#### **2.2.2.3.3. Ataques basados en vulnerabilidades de hardware**

Entre las principales tenemos: formas de ondas electromagnéticas y jugo Jacking.

Kasmi Chaouki (2015), nos da a conocer que en el 2015, varios investigadores de la agencia del gobierno francés ANSSI lograron demostrar la forma de activar la interfaz de voz de algunos smartphones remotamente mediante "formas de onda electromagnéticas específicas", así mismo el conocido exploit (fragmento de software para aprovechar las vulnerabilidades de seguridad de sistemas de información), que es capaz de inyectar comandos a través de la interfaz de audio, mientras el teléfono inteligente está conectado a las tomas de salida de audio del dispositivo.

Otra forma de ataque es mediante el conocido jugo de Jacking, que no es más que un método basado en el uso con doble propósito de la entrada USB, ya que la toma de corriente de los dispositivos móviles funcionan también como puerto de transferencia de datos, esto lo expone a ser víctima de ataque de malware, ya sea mediante la utilización de los quioscos de carga maliciosos creados en lugares públicos, o escondidos en los adaptadores de carga normal, IICS (2012).

#### **2.2.2.4. Argumento para mejorar el diseño de la seguridad móvil**

La propiedad no es un concepto absoluto que otorga todos los derechos posibles a un elemento; sin embargo los smartphones cuyo hardware como: micrófonos, cámaras, acelerómetros, GPS, software y datos tales como listas de contactos, fotos,



mensajes de redes sociales, correo electrónico, comunicaciones y consumo de medios, que son tan útiles pero también tan riesgosos en términos de privacidad y seguridad, porque no son de propiedad de sus usuarios, sino la compañía telefónica, del fabricante de hardware, del integrador de sistemas, que constituyen los propietarios prácticos de los dispositivos, (Adams, 2016).

Hurlburt (2016) recalca el resultado de la investigación realizada en el año 2014 por Cyber Security Intelligence Index, en la que se señala que "más 95 por ciento de todos los incidentes investigados [Seguridad] se reconoce un 'error humano' como un factor contribuyente; los errores humanos más comunes son mala configuración del sistema, mala gestión de parches, el uso de nombres de usuario y contraseñas predeterminados o contraseñas fáciles de adivinar, la pérdida de ordenadores portátiles o dispositivos móviles y la divulgación de la información a través del uso de una dirección de correo electrónico incorrecta. Los errores humanos más frecuentes son: hacer doble clic en un archivo adjunto infectado o una URL insegura".

El aspecto político, económico y tecnológico ha influido en la seguridad de la información desde la década de los 80, por lo que hoy nos toca convivir con las vulnerabilidades en la seguridad de las redes y teléfonos móviles, cuya consecuencia está en el hecho de que en cualquier momento nuestra comunicación puede ser interceptada.

Frente a un entorno inseguro en el que observamos un sinnúmero de vulnerabilidades en todas las generaciones de los celulares hasta la actualidad, millones de amenazas que se han creado para dañar, espiar y robar información confidencial, diferentes tipos y formas de ataques, falta de propiedad de la información y muchos errores humanos



a los que diariamente están expuestos los dispositivos móviles, se requiere mejorar la privacidad y la protección de los datos; para ello afortunadamente existe un argumento denominado end-to-end.

Saltzer, Reed y Clark (1991), nos dan a conocer en su artículo “End-To-End Arguments in System Design”, aspectos claves para la protección de extremo a extremo en el diseño de sistemas como:

1. Si el sistema de transmisión de datos realiza el cifrado y descifrado, debe ser de confianza para administrar de forma segura las claves de cifrado necesarias.
2. Los datos estarán en claro y, por lo tanto son vulnerables, cuando pasa al nodo destino y se desplaza a la aplicación destino.
3. La autenticidad del mensaje deber ser verificada mediante la aplicación, si la aplicación realiza cifrado de extremo a extremo, obtiene la verificación de la autenticación requerida.

Por lo tanto, para satisfacer los requisitos de seguridad de las aplicaciones, no hay necesidad de que el subsistema de comunicación proporcione cifrado automático en todo el tráfico, sino que la aplicación se encargue de la autenticación de extremo a extremo; si se desea proteger que la información transmitida por un usuario o programa no sea expuesta deliberadamente en la red, lo podemos hacer mediante la configuración adecuada de los Firewall, (Saltzer et al., 1991).



---

## 2.3. CAPÍTULO III: Estándares de la seguridad informática

### 2.3.1. Norma: ISO 27001

La Organización Internacional para la Estandarización (ISO) 27000, presenta un enfoque global relacionado con las normas de la serie 27000, en las que se define el alcance y propósito de la publicación de éstas normas, así como el fundamento de la importancia de un Sistema de Gestión de Seguridad de la Información (SGSI) para la organización; se analiza también los lineamientos requeridos para la definición, seguimiento y mejora continua de un SGSI. Los rangos generados por la ISO son: 27000 - 27019, 27030 - 27044 y con 27799.

Según Online Browsing Platform OBP (2013), en su documentación publicada la sobre la ISO señala que esta norma se creó con la finalidad de facilitar la gestión de los SGSI y constituye una decisión estratégica para la organización y su implementación está directamente ligada a los objetivos de la organización, requerimientos de seguridad, procesos organizativos, tamaño y estructura; considerando además que todo SGSI permite la consecución de los principios implícitos en la seguridad informática, mediante una adecuada aplicación de la gestión de riesgos.

La norma se emplea básicamente en la evaluación de la capacidad de la organización en cuanto al cumplimiento de los requisitos de seguridad de la información de las organizaciones.

ISO/IEC 27001: 2013 presenta los elementos necesarios para lograr el establecimiento, implementación, mantenimiento y mejoramiento continuo de los SGSI en el marco de la organización. Esta norma contempla además los requisitos



para la gestión y evaluación de los riesgos que se encuentran implícitos en la seguridad de información y su respectiva adaptación a los requerimientos de la organización independientemente del tipo, tamaño o naturaleza.

La norma se publicó en octubre de 2005 y revisada en septiembre de 2013. Se la reconoce como la principal norma de la serie y dispone de los elementos fundamentales de los SGSI; se originó de la BS 7799-1:2002, misma que fue anulada. En el Anexo A de la norma, se enumeran de manera concisa los siguientes objetivos: proteger la confidencialidad, integridad y la disponibilidad de la información en las empresas, a través de la evaluación de riesgos y mitigación del riesgo (ISO/IEC 27001, 2012).

Para el año 2012 existen alrededor de 19.577 empresas certificadas con esta norma, lo que les permite fomentar su actividad y que sus procesos estén más seguros, debido a que disponen de sistemas de protección de la información, incrementando notablemente su imagen y seguridad de la que finalmente se verá reflejada en la confianza antes sus clientes (EOI, 2016).

**Alcance.-** La ISO/IEC 27001, engloba a empresas comerciales, gubernamentales y Ong's, para lo cual se describen los requisitos para poner en marcha el enfoque del proceso de éste estándar, considerando los riesgos comerciales generales de las organizaciones; así mismo se describe el establecimiento de controles específicos para la seguridad de la información, orientados a las necesidades de las organizaciones (ISO/IEC 27001, 2005).

**Objetivos.-** Los objetivos de la norma están orientados a:

- ✓ Definir Políticas de Seguridad

- ✓ Permitir la Administración de la Seguridad
- ✓ Realizar la adecuada Administración de Activos
- ✓ Asegurar el Recurso Humano
- ✓ Asegurar el Cumplimiento de Políticas y Normatividad Legal.

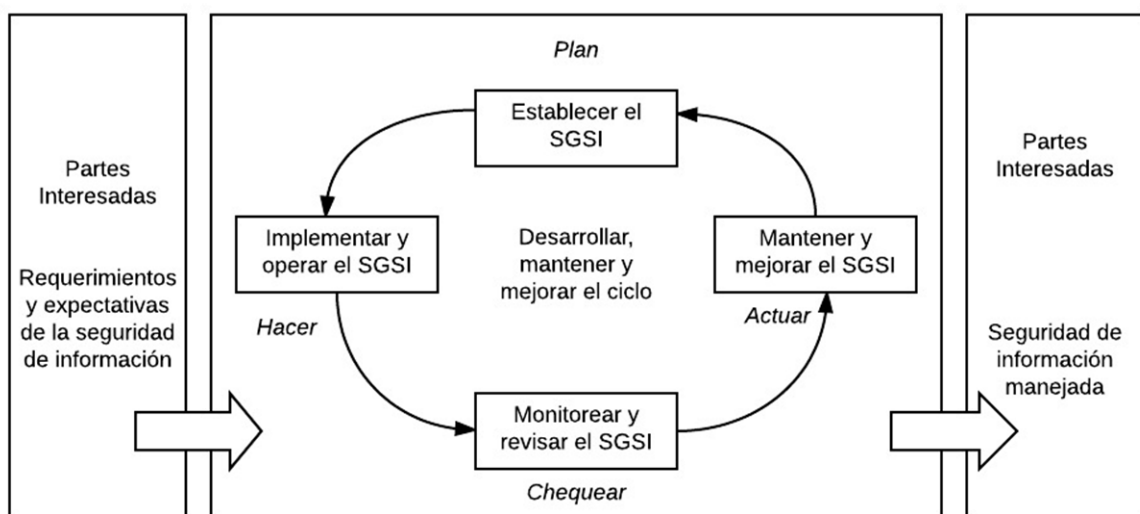
### Enfoque.-

Según la ISO/IEC 27001 (2005), el enfoque del proceso descrito en el documento relacionado con la gestión de seguridades, señala que las empresas requieren establecer, implementar, operar, monitorear, mantener y mejorar el SGSI, con la finalidad de ejecutar sus actividades eficientemente.

La ISO/IEC 27001, adopta un modelo de proceso basado en Planear-Hacer-Chequear-Actuar, conocido como PDCA (Plan-Do-Check-Act).

En la figura 4, tomada de ISO/IEC 27001 (2005), se muestra el enfoque del estándar.

Figura 4: Modelo PDCA



Fuente:(ISO/IEC 27001, 2005)

1. *Planear* → *establecer el SGSI:*

Se centra en identificar posibles causas, clarificar objetivos, comparar mejores prácticas etc.

2. *Hacer* → *implementar y operar el SGSI:*

Implementar la solución.

3. *Chequear* → *monitorear y revisar el SGSI:*

Validar lo que hemos implementado.

4. *Actuar* → *mantener y mejorar el SGSI:*

Corregir si fuera necesario y estandarizar la solución o mejora que se ha logrado.

### Estructura.-

Según ISO/IEC (2012), la norma en su estructura está conformada por 10 cláusulas, que se muestran en la figura 5:

Figura 5: Norma ISO 27001:2013



Fuente: Adaptación estructura ISO 27001:2013 (ISO/IEC 27001, 2012)



---

*Introducción.*- se refiere al orden de presentación de los requerimientos, dicho orden no determina la importancia ni tampoco el orden en que serán implementados.

*El alcance.*- determina que los requerimientos establecidos en la norma son genéricos y se pueden aplicar, independientemente del tipo, tamaño o naturaleza de la organización.

*Referencias normativas.*- se señalan las referencias necesarias para la aplicación de la norma como: ISO / IEC 27000, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Visión general y vocabulario, (OBP, 2013).

*Términos y definiciones.*- se aplican los términos y definiciones dados en ISO / IEC 27000.

*Contexto de la organización.*- en esta sección es importante que se identifiquen los aspectos internos y externos que afectan a los resultados del sistema de gestión; así mismo identificar las partes interesadas y requisitos que tiene que ver con la seguridad de la información, (GUZMÁN, 2015).

*Liderazgo.*- el liderazgo de los directivos con la organización es un aspecto primordial para que el SGSI se vincule con los procesos y se alinie con los objetivos estratégicos de la organización, (GUZMÁN, 2015).

*Planificación.*- se estructura de dos elementos, el primer elemento se relaciona con los aspectos internos y externos, además con los requerimientos de las partes interesadas, resultado de esto se tiene la identificación de riesgos y oportunidades para que el SGSI mejore; mientras que en el segundo elemento se aclara que la



organización será la encargada de definir los objetivos relacionados con la seguridad de la información y en concordancia con las políticas de seguridad, así como su respectiva difusión, (GUZMÁN, 2015).

*Apoyo/Soporte.*- el apoyo se enmarca en elementos claves para el buen desarrollo del SGSI como la gestión adecuada de: recursos, competencia, concientización y la respectiva documentación de la información, (GUZMÁN, 2015).

*Operación.*- nos es más que la ejecución de lo planificado, considerando que cada proceso realizado deberá ser documentado, de tal manera que se generen las evidencias adecuadas, (GUZMÁN, 2015).

*Evaluación del desempeño.*- como en todo proceso es necesario medir el desempeño de los SGSI, para ello es necesario considerar los siguientes aspectos: monitoreo, medición, análisis y evaluación; auditorías internas y revisión por la dirección, (GUZMÁN, 2015)

*Mejora.*- para que la mejora continua sea efectiva se requiere considerar los siguientes aspectos: no conformidad y acción correctiva y la mejora continua, (GUZMÁN, 2015).

En la versión 2013, el Anexo A se lo conoce ahora como “objetivos de control de referencia y controles”, se establece que los objetivos de control y los controles derivan directamente de ISO/IEC 27002:2013, este Anexo es utilizado en el contexto de la Cláusula 6.1.3 y durante la revisión de ISO/IEC 27002 el número de controles ha sido reducido de 133 controles a 114 controles, el número de cláusulas mayores ha sido expandido de 11 a 14, así mismo los objetivos disminuyeron a 35 de los 39 que constaban en la versión 2015, (ISO/IEC 27001, 2012).



En el anexo A de la norma ISO 27001, se encuentran todas las especificaciones relacionadas con la seguridad de la información, en él se encuentran una lista de 14 categorías de control (del 5 al 18) para lograr una gestión adecuada de la seguridad de la información en las organizaciones; el propósito de las secciones del mencionado anexo, se resume en la página web de la Advisera Expert Solutions Ltd. A continuación se detalla:

- ✓ **5 Políticas de seguridad de la información:** encontramos controles para saber cómo las políticas serán escritas y revisadas, (Kosutic, 2017).
- ✓ **6 Organización de la seguridad de la información:** los controles para la asignación de responsabilidades, además los controles relacionados con los dispositivos móviles y el teletrabajo, (Kosutic, 2017).
- ✓ **7 Seguridad de los recursos humanos:** “controles antes, durante y después de emplear”, (Kosutic, 2017).
- ✓ **8 Gestión de recursos:** aquí se encuentran los controles para el inventario de recursos y su uso aceptable; así mismo la clasificación de la información y la gestión de los medios de almacenamiento, (Kosutic, 2017).
- ✓ **9 Control de acceso:** “controles para las políticas de control de acceso, gestión de acceso de los usuarios, control de acceso para el sistema y las aplicaciones y responsabilidades del usuario”, (Kosutic, 2017).
- ✓ **10 Criptografía:** “controles relacionados con la gestión de encriptación y claves”, (Kosutic, 2017).
- ✓ **11 Seguridad física y ambiental:** “controles que definen áreas seguras, controles de entrada, protección contra amenazas, seguridad de equipos, descarte seguro, políticas de escritorio y pantalla despejadas, etc.”,(Kosutic, 2017).



- ✓ **12 Seguridad operacional:** “muchos de los controles relacionados con la gestión de la producción en TI: gestión de cambios, gestión de capacidad, malware, respaldo, bitácoras, espejos, instalación, vulnerabilidades, etc.”,(Kosutic, 2017).
- ✓ **13 Seguridad de las comunicaciones:** “controles relacionados con la seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, etc.”, (Kosutic, 2017).
- ✓ **14 Adquisición, desarrollo y mantenimiento de sistemas:** “controles que definen los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte”, (Kosutic, 2017).
- ✓ **15 Relaciones con los proveedores:** “controles acerca de qué incluir en los contratos y cómo hacer el seguimiento a los proveedores”, (Kosutic, 2017).
- ✓ **16 Gestión de Incidentes en las seguridad de la información:** “controles para reportar los eventos y debilidades, definir responsabilidades, procedimientos de respuesta y recolección de evidencias”, (Kosutic, 2017).
- ✓ **17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio:** “controles que requieren la planificación de la continuidad del negocio, procedimientos, verificación y revisión y redundancia de TI”, (Kosutic, 2017).
- ✓ **18 Cumplimiento:** “controles que requieren la identificación de las leyes y regulaciones aplicables, protección de la propiedad intelectual, protección de datos personales y revisiones de la seguridad de la información”, (Kosutic, 2017).



### 2.3.2. NIST: 800-30

El National Institute of Standards and Technology (Instituto Nacional de Estándares de Tecnología), apareció en el año 1901, por primera vez como una agencia federal dedicada a la Administración de Tecnología del Departamento de Comercio en los Estados Unidos.

La NIST SP 800-30, se encarga de la gestión de riesgos, orientada a procesos mediante un adecuado análisis y gestión del riesgo, proporcionando una evaluación cuantitativa y cualitativa, así como métodos semicualitativos que permiten administrar eficazmente el riesgo para la seguridad de la información.

#### **Alcance.-**

Según NIST (2012), señala que la NIST SP 800-30 está orientada especialmente a los profesionales vinculados con la gestión de riesgos en las organizaciones como: jefes de los organismos, directores generales, jefe de operaciones, ejecutivo de riesgo; los individuos encargados de la vigilancia de la seguridad de la información, su gestión y responsabilidades operativas (por ejemplo, los directores de información, oficiales de alto rango, los administradores y propietarios de sistemas de información, los proveedores de control comunes etc).

#### **Objetivos.-** Entre los principales objetivos de la norma tenemos:

- Asegurar que los sistemas de información almacenen, procesen y transmitan información.
- Gestionar los riesgos.
- Optimizar la gestión de riesgos en base a los resultados del análisis de riesgos.



- Velar por alcanzar la misión de la organización.
- Ser una función esencial de la administración en la organización.

### **Principios.-**

- Proveer una base para el desarrollo de la gestión del riesgo.
- Proveer información acerca de controles de seguridad en función de la rentabilidad del negocio.

### **Enfoque.-**

Según NIST (2012), el enfoque de la norma está conformada por 4 componentes requeridos para la gestión de riesgos que son:

El primer componente, se ocupa de cómo las *organizaciones tienen la intención de evaluar, responder y monitorear los riesgos*, de tal manera que les permita a los directivos tomar decisiones explícitas; el propósito es producir una estrategia base para el proceso de gestión de riesgos, estableciendo adecuadamente los límites para la toma de decisiones estratégicas en base al control de riesgos y acorde con las necesidades de la organización, (NIST, 2012).

El segundo componente, se encarga de analizar el cómo las organizaciones *van a evaluar el riesgo en el contexto del marco de riesgo de la organización*; el objetivo principal de éste componente es buscar: las amenazas; las vulnerabilidades internas y externas; el daño que pueden ocurrir frente a los riesgos potenciales para la explotación de vulnerabilidades; y la probabilidad de ocurrencia del daño, (NIST, 2012).



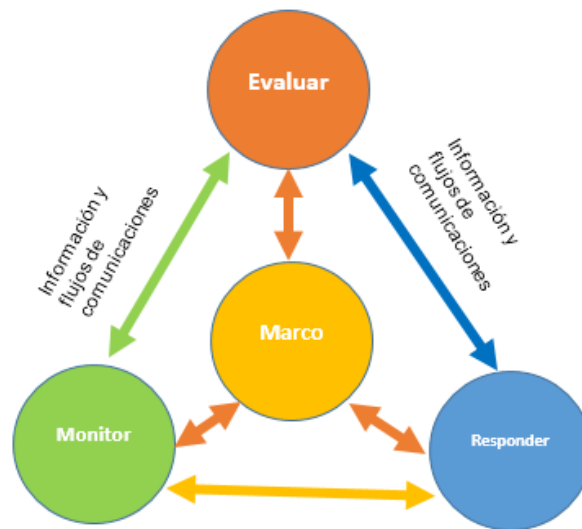
---

El tercer componente, encargado de encontrar cómo las organizaciones *responden a arriesgar una vez que el riesgo se determina considerando los resultados de la evaluación de riesgos*; tiene por objetivo proporcionar una respuesta coherente al riesgo para ello se necesita: el desarrollo de cursos alternativos de acción para responder a los riesgos; la evaluación de los cursos de acción alternativos; la determinación de las formas de actuación coherente con la tolerancia al riesgo de la organización; y la implementación de respuestas a los riesgos sobre la base de los cursos seleccionados de acción, (NIST, 2012).

El cuarto componente, se ocupa de analizar cómo las organizaciones *monitorean el riesgo*; el propósito del componente de monitoreo de riesgos comprende: establecer la efectividad de las respuestas al riesgo en curso; identificar los cambios de riesgo que afectan a los sistemas de información de la organización y los entornos en los que operan los sistemas; y verificar que las respuestas al riesgo previsto se implementen y que los requisitos de seguridad de la información se deriven de la misión de organización, la legislación federal, directivas, reglamentos, políticas, normas y directrices, (NIST, 2012).

En la figura 6 se presenta la relación de los cuatro componentes:

Figura 6: Componentes de la Gestión de Riesgos

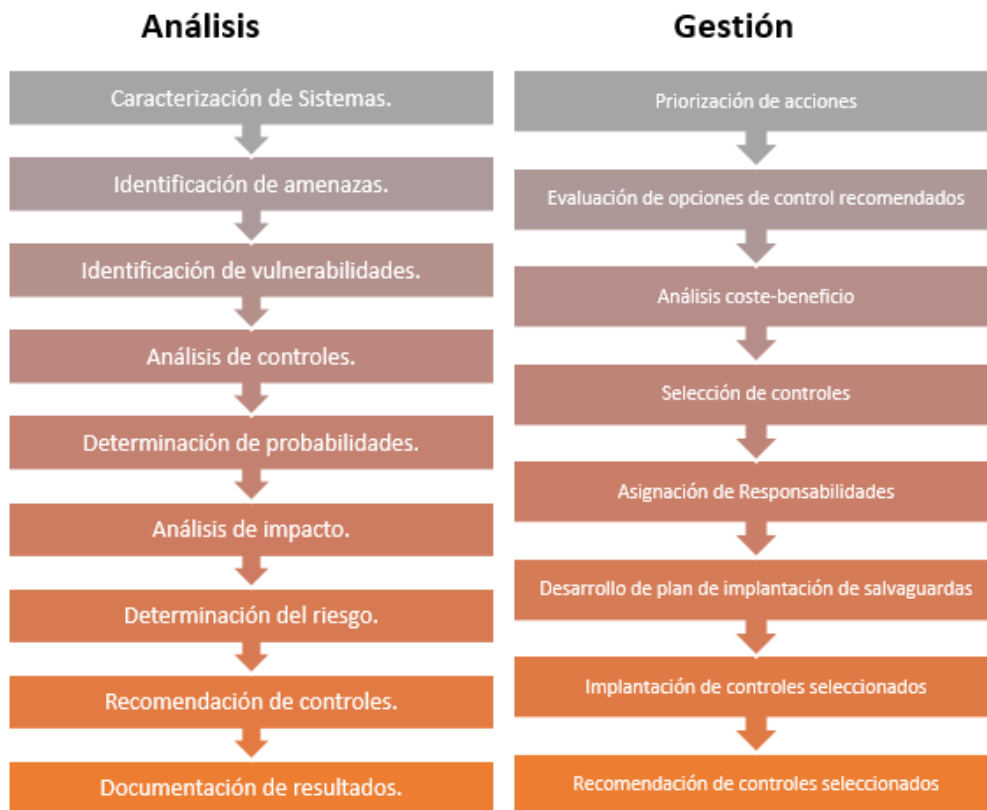


Fuente: Adaptación componentes gestión de riesgos (NIST, 2012)

### Estructura.-

Según Marcos, Bedón, Utrilla y Ortega (2012), la norma en su estructura está conformada por 9 subprocesos para el análisis del riesgo y 7 subprocesos para la gestión de riesgos. La estructura del análisis y gestión de riesgos según la Norma NIST 800-30, se muestra en la figura 7:

Figura 7: Análisis y Gestión de riesgos NIST 800-30



Fuente: Adaptación análisis y gestión de riesgos (Marcos et al., 2012)

### 2.3.3. COBIT 5

COBIT 5, permite que las empresas alcancen los objetivos planteados en lo relacionado con la administración y gobierno de Tecnologías de la Información (TI) mediante la presentación de un marco de trabajo integral; es decir apoya a las organizaciones para el mejoramiento de la Infraestructura Tecnológica tanto en la gestión del riesgo como en la optimización de recursos.

COBIT 5 ha sido construida luego de más de quince años de aplicación e implementación en diferentes organizaciones y personal de empresas relacionadas con las TI, gestión de riesgos y seguridad.



**Alcance.-** “COBIT 5, permite una administración total de las TI en la organización, en la que se considera principalmente a las unidades estratégicas, objetivos estratégicos y departamentos responsables de la Infraestructura Tecnológica, así como también involucra stakeholders, personal interno y externo, relacionadas con las TI” (Riesgos & Villafuerte, 2014)

### Objetivos.-

Según ISACA (2012), se señala que en COBIT 5 se establecen 17 objetivos que se encuentran descritos en la tabla 2, en la que se identifica a relacione primarias con la letras P y las secundarias con la letra S.

Tabla 2: Metas Corporativas de COBIT 5

Dimensión del CMI	Meta Corporativa	Relación con los Objetivos de Gobierno		
		Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos
Financiera	1. Valor para las partes interesadas de las Inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		S
	9. Toma estratégica de Decisiones basada en Información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	12. Optimización de los costes de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	S	P	P
	17. Cultura de innovación de producto y negocio	P		

Fuente: Metas Corporativas de COBIT 5 (ISACA, 2012)

### Principios.-

Según ISACA (2012), claramente se establecen 5 ejes claves en los que se basa COBIT 5 para el gobierno y la gestión de las Tecnologías de la Información en las empresas, lo que se citan a continuación:



✓ *Satisfacer las necesidades de las partes interesadas*

Sabemos que en toda organización se presta mayor atención a los stakeholders, por lo tanto ésta debe preocuparse por interpretar y extraer sus necesidades con la finalidad de generar valor mediante la obtención de beneficios, optimizando los riesgos y recursos.

✓ *Cubrir la empresa de extremo a extremo*

Se logra considerando el gobierno y la gestión de las tecnologías de la información en la organización; para ello se debe incluir el gobierno de TI (procesos y funciones) dentro del gobierno de la empresa. Se refiere a cubrir la empresa de forma completa, de esta manera COBIT 5 dirige el gobierno y la gestión tratando de dar la mayor cobertura posible mediante componentes clave como son: los enablers (catalizadores) de gobierno que permiten que todos los procesos funcionen, el alcance de gobierno y los roles que intervienen en el gobierno empresarial.

✓ *Aplicar un marco de referencia único integrado*

Para cumplir con este principio COBIT 5 se alinea a estándares, normas y marcos más relevantes usados por las organizaciones, apegado a los lineamientos establecidos inicialmente por ISACA, manteniendo una arquitectura simple y una cobertura completa en la organización, además COBIT 5 usa un lenguaje no técnico entendible para cualquier usuario final.

✓ *Hacer posible un enfoque holístico*

Consiste en un enfoque que ayuda a manejar la complejidad de los procesos en la organización a través de un proceso sistémico que se basa en un conjunto de



enablers o catalizadores que no son más que factores que en forma individual o colectiva permiten que algo funcione, para ello se han identificado 7 enablers que son guiados por las cascadas de metas (transformar las necesidades de los stakeholders en metas específicas dentro la organización) y cada uno tiene sus propias características y se encuentran descritos en 7 categorías.

Cada uno de los enablers tienen una dimensión, que les permiten afrontar sus situaciones en la organización entres éstos están: stakeholders, buenas prácticas, ciclo de vida, metas.

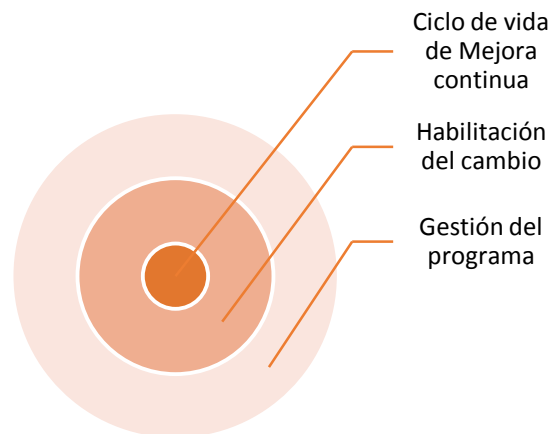
✓ *Separar el Gobierno de la Gestión*

Existe una diferencia entre gobierno y gestión planteada por COBIT 5, en la que cada una abarca diferentes actividades y requiere una estructura organizativa diferente; el gobierno garantiza que se evalúen las necesidades y disposiciones de los stakeholders, para determinar que se alcancen las metas corporativas acordadas, estableciendo la dirección a través de la priorización y toma de decisiones, midiendo además el rendimiento y cumplimiento respecto a la dirección y metas acordadas, bajo el liderazgo del presidente del directorio de la organización; mientras que la gestión lo que hace es ejecutar el círculo virtuoso (planificar, construir, ejecutar y superar).

**Enfoque.-**

Según ISACA (2012), el enfoque se basa en el ciclo de vida que permite a la organización de forma práctica y simple usar COBIT, permitiendo dar una solución práctica a los inconvenientes que se pueden presentar en la implementación. Los elementos del ciclo de vida se presentan en la figura 8:

Figura 8: Ciclo de vida- Enfoque COBIT 5

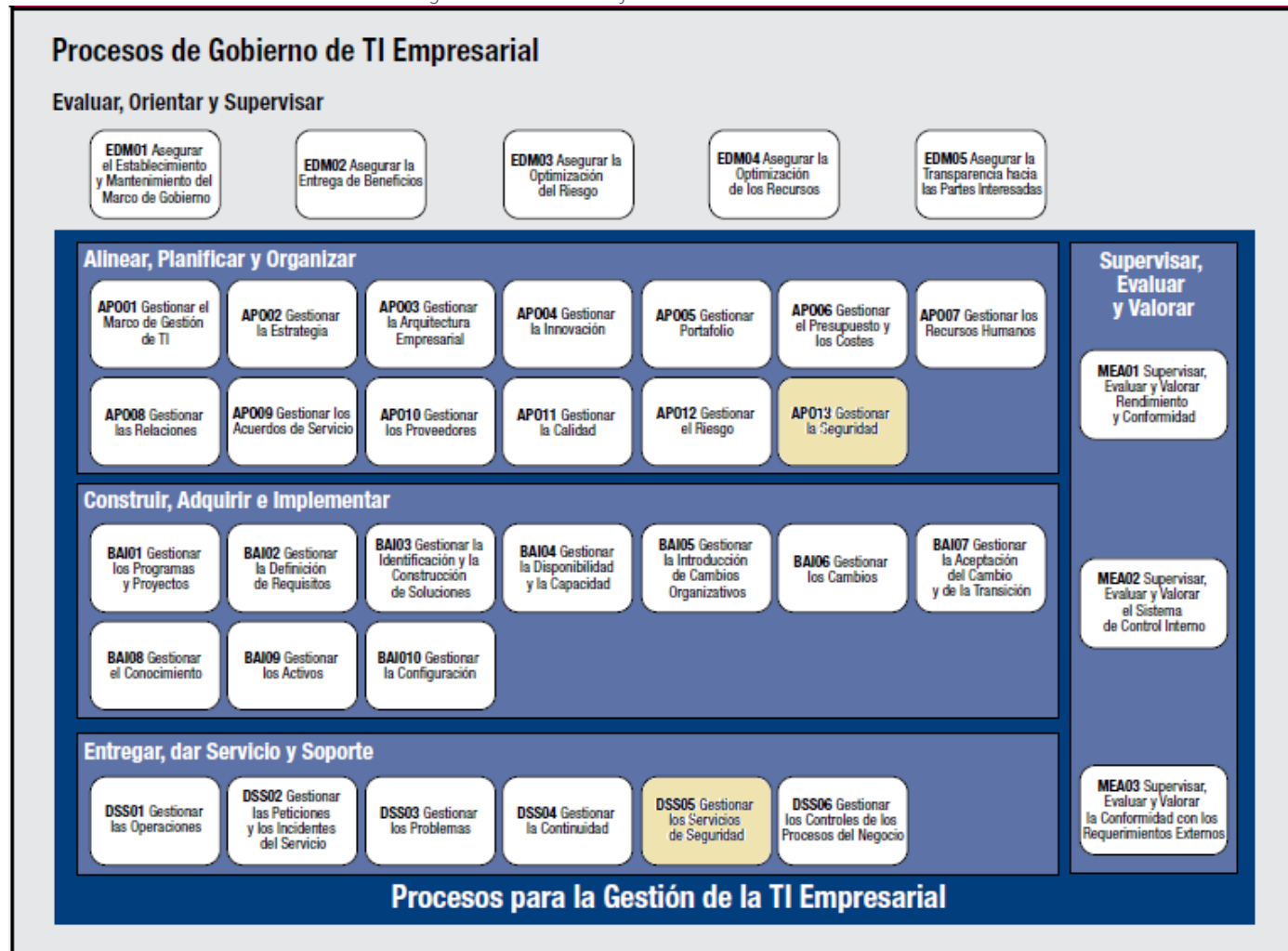


Fuente: Adaptación ciclo de vida (ISACA, 2012)

**Estructura.-** COBIT 5 es el sucesor del modelo de procesos de COBIT 4.1, además integra los modelos de procesos de Risk IT y Val IT. En la figura 9 se presentan los 37 procesos de gobierno y gestión, (ISACA, 2012).



Figura 9: Modelo de Referencia de Procesos de COBIT 5



Fuente: (ISACA, 2012)



#### 2.3.4. OWASP Top Ten

El Proyecto de Seguridad Open Web Application Security Project (OWASP) Móvil es un recurso de Seguridad, creado con la finalidad de ofrecer a los programadores de aplicaciones informáticas y miembros de equipos de seguridad de TI, los recursos que se requieran para la implementación y mantenimiento de aplicaciones móviles seguras (OWASP, 2016).

El OWASP Top 10 para entornos web fue lanzado por primera vez en 2003, se hicieron actualizaciones menores en 2004 y 2007, la versión de 2010 y 2013 fueron renovadas con la finalidad de dar prioridad al riesgo, la versión de OWASP Top 10 2017 será lanzada en julio o agosto de 2017.

La versión El OWASP Top 10 para entornos móviles inició en el 2012 y fue actualizada en el 2013 y 2014; con la finalidad de analizar y volver a categorizar los riesgos en el año 2015 se efectuó una encuesta, con ello lanzaron el Top Ten 2016 móvil.

**Alcance.-** El OWASP Top 10 de móviles pretende ser una herramienta que permita tener una perspectiva clara de los 10 problemas que más aquejan a los móviles hoy en día, permitiendo establecer escenarios de riesgos de manera clara.

El Top10 tiene como objetivo fundamental adiestrar a: diseñadores, programadores, arquitectos de software, gerentes y en general a las organizaciones; en lo que tiene que ver con las consecuencias de las vulnerabilidades de seguridad más frecuentes y proveer de técnicas básicas de protección en aplicaciones web (OWASP, 2016).



**Objetivos.-** El OWASP, tiene por objetivo categorizar los riesgos de la seguridad móvil y definir los controles de desarrollo para minimizar su impacto o la probabilidad de explotación, con mayor atención en la capa de aplicación de las plataformas móviles. Así mismo se centra no sólo en las aplicaciones móviles desplegadas para los dispositivos móviles del usuario, sino también en la infraestructura del servidor, con el que las aplicaciones móviles se comunican; en otras palabras OWASP Móvil está interesada en la integración entre la aplicación móvil, servicios de autenticación remotas y las características concretas de la plataforma en la nube (OWASP, 2016).

### **Principios.-**

Según OWASP (2016) se señala que esta organización es sin fines de lucro, su fin es el de lograr en el futuro que el proyecto tenga el éxito deseado y para el cual fue creado, es por ello que la mayor parte de los integrantes son voluntarios, incluso la junta directiva de proyectos, así mismo los miembros de comités y proyectos; líderes de capítulos, etc. Todos ellos apoyan la investigación innovadora relacionada con la seguridad.

### **Estructura.-**

En el sitio oficial de OWASP (2016), se encuentran publicados los siguientes riesgos:

- ✓ *M1 - Incorrecto uso de plataforma:* se refiere al mal uso de alguna función de la plataforma o falta de uso de controles en la seguridad de la plataforma, los ejemplos más comunes serían: mala asignación de permisos sobre la plataforma, el mal uso de TouchID, el llavero (almacén



---

para guardar datos confidenciales como usuarios, contraseñas del dispositivo), o algún otro control de seguridad que es parte del sistema operativo móvil.

- ✓ *M2 - Almacenamiento inseguro de datos:* se relaciona con el hecho de que los datos se almacenen sin el respectivo control de seguridad y además a la fuga de datos no deseados o datos sensibles causada por empleados descontentos.
- ✓ *M3 - Comunicación insegura:* esto tiene que ver con los protocolos de enlace, SSL versiones incorrectas, la negociación débil, la comunicación sin cifrar de los activos sensibles, entre otras.
- ✓ *M4 - Autenticación insegura:* en esta categoría se presenta las nociones relacionadas con la autenticación del usuario final o mala gestión de sesiones.
- ✓ *M5 - Criptografía insuficiente:* este escenario se refiere al código, ya que se aplica la criptografía a un activo de información sensible. Sin embargo, la criptografía es insuficiente en alguna manera.
- ✓ *M6 - Autorización insegura:* permite detectar cualquier fallo en la autorización por ejemplo, las decisiones de autorización en el lado del cliente, navegación forzada, etc.
- ✓ *M7 - Calidad código de cliente:* en esta categoría tiene que ver con desbordamientos de búfer, vulnerabilidades de cadena de formato (cuando se acepta sin validar las entradas del usuario) y varios otros errores a nivel de código, donde la solución es volver a escribir algo de código que se ejecuta en el dispositivo móvil.



- ✓ *M8 - Manipulación de código:* Esta categoría tiene que ver con parchear el código, la modificación de los recursos locales y la modificación de la memoria dinámica. Una vez que la aplicación se envía al dispositivo móvil, los recursos de código y datos residen en este país. Un atacante o bien puede modificar directamente el código, cambiar el contenido de la memoria dinámica, cambiar o reemplazar las API del sistema que utiliza la aplicación, o modificar los datos y recursos de la aplicación. Esto puede proporcionar al atacante un método directo de subvertir el uso previsto del software para beneficio personal o monetario.
- ✓ *M9 - Ingeniería inversa:* Esta categoría incluye el análisis del binario del núcleo final para determinar su código fuente, bibliotecas, algoritmos y otros activos. Software como IDA Pro (Proveedor: Hex-Rays), Hopper (macOS), otool (BeSprout Technology) y otras herramientas de inspección binarios darán la visión atacante en el funcionamiento interno de la aplicación. Esto puede ser usado para explotar otras vulnerabilidades nacientes en la aplicación, así como información reveladora acerca de los servidores back end, constantes criptográficos y sistemas de cifrado y la propiedad intelectual.
- ✓ *M10 - Funcionalidad extraña:* A menudo, los desarrolladores incluyen funcionalidad de puerta trasera oculta u otros controles de seguridad internos de desarrollo que no están destinadas a ser liberadas en un entorno de producción. Por ejemplo, un desarrollador puede incluir accidentalmente una contraseña como un comentario en una aplicación híbrida. Otro ejemplo incluye la desactivación de la autenticación de 2

factores durante la prueba que asegura que el usuario pueda acceder a su cuenta, a pesar que la contraseña se conocida por alguien más.

En la figura 10, se resume los escenarios de los riesgos del Top 10 2013.

Figura 10: Top ten Mobile



Fuente: Adaptación Top ten (OWASP, 2016).



## 2.4. CAPÍTULO IV: Análisis de los modelos y estándares

Para realizar el análisis de los estándares y normas que soportarán la metodología a desarrollar, ha sido necesario adaptar el *Método de Estudio de Similitud entre Modelos y Estándares (MSSS)*, (Gasca, 2010).

El citado método ha sido propuesto por un grupo de investigadores de la Universidad Politécnica de Madrid, mismo que ha sido validado en diferentes ámbitos de estudio. Calvo-Manzano J, Cuevas G , Muñoz M (2008).

A continuación se señala los pasos del método:

1. Seleccionar estándares y modelos
2. Elegir modelo de referencia.
3. Seleccionar los procesos a analizar.
4. Establecer el nivel de detalle del análisis.
5. Definir una plantilla de comparación.
6. Identificar similitudes.
7. Recoger resultados.

Éstos pasos se muestran de manera general en la tabla 3, para lo cual ha sido necesario realizar un ajuste, con la finalidad adaptar al estudio comparativo de modelos, estándares y proyectos de profesionales como OWASP.



Tabla 3: Pasos de la Metodología (MSSS)

Pasos (Original)	Pasos (Ajustado)	Justificación
1. Seleccionar estándares y modelos	1. Establecer criterios para la selección adecuada de modelos y estándares para la seguridad de los dispositivos móviles.	Es necesario definir claramente criterios que permitan buscar modelos y estándares que se enmarquen en la seguridad de los dispositivos móviles.
2. Elegir modelo de referencia.	2. Selección de modelos y estándares	En este paso se podrá establecer los modelos y estándares a ser investigados.
3. Seleccionar los procesos a analizar.	3. Definir aspectos a analizar en cada modelo o estándar seleccionado.	Para que el análisis comparativo final sea fácil de realizar se debe definir los aspectos a considerar en el estudio de los modelos y estándares relacionados con la seguridad de los dispositivos móviles.
4. Establecer el nivel de detalle del análisis.	4. Elaboración de una matriz comparativa entre los modelos y estándares seleccionados	Se ha unido los dos pasos en vista de que una vez realizado el paso 3 ya se puede elaborar el cuadro comparativo correspondiente.
5. Definir una plantilla de comparación.		
6. Identificar similitudes.	5. Identificar similitudes entre los modelos y estándares seleccionados y los problemas de la seguridad móvil.	Las similitudes se deben realizar en este caso entre los modelos y estándares y los principales problemas a considerar en la seguridad de la información en general.
7. Recoger resultados.	6. Presentar los resultados obtenidos	Con los pasos realizados anteriormente ya se podrá presentar los resultados encontrados.

Fuente: Adaptación a seguridad de los dispositivos móviles

#### 2.4.1. Establecer criterios para la selección adecuada de modelos y estándares para la seguridad de los dispositivos móviles

En esta paso se ha determinado tres criterios a tomar en cuenta para el estudio comparativo de modelos y estándares de la seguridad de los dispositivos móviles:



1. Los modelos y estándares deberán estar orientados a la seguridad en un sentido amplio o directamente con la seguridad de información en dispositivos móviles.
2. De todos los modelos y estándares disponibles, se procederá a seleccionar aquellos que tengan mayor relación con la seguridad de información en dispositivos móviles.
3. Selección de aquellos en los que la información esté disponible.

#### **2.4.2. Selección de modelos y estándares**

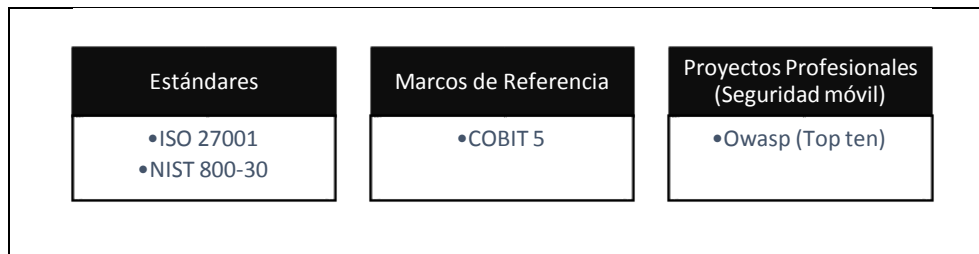
Conforme los criterios mencionados en el paso 1, se seleccionó los siguientes modelos y estándares.

1. *Norma ISO/27001 (Estándar)*
2. *NIST: 800-30 (Estándar)*
3. *COBIT 5 (Marco de referencia)*
4. *\*OWASP (Proyecto Profesional)*

*\* Por la estrecha relación que tiene el Proyecto de Seguridad Open Web Application Security Project, más conocido como OWASP, que corresponde al Top ten para dispositivos móviles, se lo considerará para el estudio respectivo de la presente investigación.*

En la figura 11, se muestran los modelos y estándares seleccionados:

Figura 11: Modelos y estándares seleccionados



Fuente: Elaboración propia.

### 2.4.3. Definir aspectos a analizar en cada modelo o estándar seleccionado

Se han definido los siguientes criterios, tanto para los modelos y estándares como para el proyecto profesional Owasp.

- Alcance.*
- Objetivos.*
- Principios.*
- Enfoque.*
- Estructura.*

### 2.4.4. Elaboración de una matriz comparativa entre los modelos y estándares seleccionados.

De acuerdo a los criterios señalados en el paso anterior, en la investigación se seleccionaron los siguientes modelos, estándares y proyecto profesional. En la tabla 4 se presenta el resumen de las normas/estándares y proyecto profesional analizados.



Tabla 4 : Comparativa de estándares y proyectos profesionales de seguridad

Norma /Proyecto Profesional	Alcance	Objetivos	Principios	Enfoque	Estructura
ISO 27001 (Norma)	Empresas comerciales, gubernamentales, Ong's.	<ul style="list-style-type: none"> <li>✓ Definir políticas de seguridad</li> <li>✓ Permitir la administración de la seguridad</li> <li>✓ Realizar la adecuada Administración de activos</li> <li>✓ Asegurar el recurso humano</li> <li>✓ Asegurar el cumplimiento de políticas y normatividad legal.</li> </ul>		<b>PDCA</b> Planear-Hacer-Chequear-Actuar	<i>Introducción</i> <i>Alcance</i> <i>Términos y definiciones</i> <i>Contexto de la Organización</i> <i>Liderazgo</i> <i>Planificación</i> <i>Apoyo/Soporte</i> <i>Operación</i> <i>Evaluación del desempeño</i> <i>Mejora.</i> <i>Anexo A (Controles)</i>
NIST 800-30 (Norma)	Profesionales vinculados con la gestión de riesgos.	<ul style="list-style-type: none"> <li>✓ Asegurar que los sistemas de información almacenen, procesen y transmitan información.</li> <li>✓ Gestionar los riesgos.</li> <li>✓ Optimizar la gestión de riesgos en base a los resultados del análisis de riesgos.</li> <li>✓ Velar por alcanzar la misión de la organización.</li> <li>✓ Ser una función esencial de la administración en la organización.</li> </ul>	<ul style="list-style-type: none"> <li>✓ Proveer una base para el desarrollo de la gestión del riesgo.</li> <li>✓ Proveer información acerca de controles de seguridad en función de la rentabilidad del negocio.</li> </ul>	<b>Primer componente:</b> Cómo las organizaciones tienen la intención de evaluar, responder y monitorear los riesgos <b>Segundo componente:</b> Cómo las organizaciones van a evaluar el riesgo en el contexto del marco de riesgo de la organización. <b>Tercer componente:</b> Cómo las organizaciones responden a arriesgar una vez que el riesgo se determina considerando los resultados de la evaluación de riesgos. <b>Cuarto componente:</b> Cómo las organizaciones monitorean el riesgo	<b>Análisis de riesgos:</b> <i>Caracterización de sistemas</i> <i>Identificación de amenazas</i> <i>Identificación de vulnerabilidades</i> <i>Análisis de controles</i> <i>Determinación de probabilidades</i> <i>Análisis de impacto</i> <i>Determinación del riesgo</i> <i>Recomendación de resultados</i> <b>Gestión de riesgos:</b> <i>Priorización de acciones.</i> <i>Evaluación de opciones de control recomendados.</i> <i>Análisis coste-beneficio.</i> <i>Selección de controles.</i> <i>Asignación de responsabilidades.</i> <i>Desarrollo de plan de implantación de salvaguardas.</i>



Norma /Proyecto Profesional	Alcance	Objetivos	Principios	Enfoque	Estructura
					<i>Implantación de controles seleccionados.</i>
COBIT 5 (Marco de Referencia integrado)	Permite una administración total de las TI en la organización, en la que se considera principalmente a las unidades estratégicas, objetivos estratégicos y departamentos responsables de la Infraestructura Tecnológica, así como también involucra stakeholders, personal interno y externo, relacionadas con las TI	En COBIT 5 se establecen 17 objetivos relacionados la dimensión del CMI, metas corporativas y objetivos de Gobierno (ISACA, 2012)	Según ISACA (2012), se proponen los siguientes principios: <ul style="list-style-type: none"> <li>✓ Satisfacer las Necesidades de las Partes Interesadas</li> <li>✓ Cubrir la Empresa Extremo a Extremo</li> <li>✓ Aplicar un Marco de Referencia único integrado</li> <li>✓ Hacer Posible un Enfoque Holístico</li> <li>✓ Separar el Gobierno de la Gestión.</li> </ul>	Según ISACA (2012), a través del ciclo de vida que comprende: <ul style="list-style-type: none"> <li>✓ Ciclo de vida de Mejora continua.</li> <li>✓ Habilitación del cambio</li> <li>✓ Gestión del programa</li> </ul>	Según ISACA (2012), los procesos de gobierno de TI empresarial son: <ul style="list-style-type: none"> <li>✓ Alinear, Planificar y Organizar (AP)</li> <li>✓ Construir, Adquirir e Implementar (BAI)</li> <li>✓ Entregar, dar Servicio y Soporte (DSS)</li> </ul>
OWASP Top ten (Proyecto profesional)	Establecer escenarios de riesgos de manera clara, sobre los 10 principales problemas que aquejan a los móviles.	<ul style="list-style-type: none"> <li>✓ Clasificar los riesgos de la seguridad móvil.</li> <li>✓ Proporcionar los controles de desarrollo para reducir su impacto o la probabilidad de explotación.</li> </ul>	Sin fines de lucro. Lograr en el futuro que el proyecto tenga éxito. Apoyo a la investigación innovadora relacionada con la seguridad.	El principal enfoque está en la capa de aplicación de las plataformas móviles.  Infraestructura del servidor con el que las aplicaciones móviles se comunican.	<b>Top ten</b> <i>Incorrecto uso de plataforma</i> <i>Almacenamiento inseguro de datos</i> <i>Comunicación insegura</i> <i>Autenticación insegura</i> <i>Criptografía insuficiente</i> <i>Autorización insegura</i> <i>Calidad código de cliente</i> <i>Manipulación de código</i> <i>Ingeniería inversa</i> <i>Funcionalidad extraña</i>

Fuente: Elaboración propia.



## 2.4.5. Identificar similitudes entre los modelos y estándares seleccionados y los problemas de la seguridad móvil

### 1. Similitud entre la ISO 27001 y los problemas de la seguridad móvil

Sabemos que la información constituye un activo vital para lograr un buen posicionamiento de la organización y asegurar dicho activo será el principal objetivo de toda organización (ISO -International Organization for Standardization, 2011).

Según la página oficial de la ISO 27001 (2012), encontramos los dominios y controles de la norma ISO 27001:2013, que se detallan en la tabla 5:

Tabla 5: Dominios y Secciones

Nro.	Dominios	Secciones
5	Políticas de seguridad de la información.	5.1 Directrices de la Dirección en seguridad de la información.
6	Organización de la seguridad de la información	6.1 Organización interna. 6.2 Dispositivos para movilidad y teletrabajo.
7	Seguridad de los recursos humanos	7.1 Antes de la contratación. 7.2 Durante la contratación. 7.3 Cese o cambio de puesto de trabajo.
8	Gestión de recursos	8.1 Responsabilidad sobre los activos. 8.2 Clasificación de la información. 8.3 Manejo de los soportes de almacenamiento.
9	Control de acceso	9.1 Requisitos de negocio para el control de accesos. 9.2 Gestión de acceso de usuario. 9.3 Responsabilidades del usuario. 9.4 Control de acceso a sistemas y aplicaciones.
10	Criptografía	10.1 Controles criptográficos.
11	Seguridad física y ambiental	11.1 Áreas seguras. 11.2 Seguridad de los equipos.
12	Seguridad operacional	12.1 Responsabilidades y procedimientos de operación. 12.2 Protección contra código malicioso. 12.3 Copias de seguridad. 12.4 Registro de actividad y supervisión. 12.5 Control del software en explotación. 12.6 Gestión de la vulnerabilidad técnica.



		12.7 Consideraciones de las auditorías de los sistemas de información.
13	Seguridad de las telecomunicaciones	13.1 Gestión de la seguridad en las redes. 13.2 Intercambio de información con partes externas.
14	Adquisición, desarrollo y mantenimiento de sistemas	14.1 Requisitos de seguridad de los sistemas de información. 14.2 Seguridad en los procesos de desarrollo y soporte. 14.3 Datos de prueba.
15	Relaciones con los proveedores	15.1 Seguridad de la información en las relaciones con suministradores. 15.2 Gestión de la prestación del servicio por suministradores.
16	Gestión de incidentes en la seguridad de la información	16.1 Gestión de incidentes de seguridad de la información y mejoras.
17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	17.1 Continuidad de la seguridad de la información. 17.2 Redundancias.
18	Cumplimiento	18.1 Cumplimiento de los requisitos legales y contractuales. 18.2 Revisiones de la seguridad de la información.

*Elaboración propia.*

En la tabla 6, se observa las similitudes entre los problemas de la seguridad móvil y los dominios y controles del Anexo A de la norma ISO 27001.



Tabla 6: Similitud ISO 27001 (Anexo A) y los problemas de la Seguridad Móvil

<b>Problemas de la Seguridad Móvil</b> (Dwivedi et al., 2014)	<b>Dominios</b> (Kosutic, 2017)	<b>ISO 27001: Anexo A de la norma</b> <b>Controles</b> (ISO/IEC 27001, 2012)
La seguridad física	11 Seguridad física y ambiental	11.1.4 Protección contra las amenazas externas y ambientales.
Almacenamiento seguro de datos (en el disco)	8 Gestión de recursos	8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito.
Autenticación fuerte	9 Control de acceso  10 Criptografía	9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.3.1 Uso de información confidencial para la autenticación. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.  10.1.1 Política de uso de los controles criptográficos.
Apoyo a la seguridad de múltiples usuarios	9 Control de acceso  6 Organización de la seguridad de la información	9.1.1 Política de control de acceso. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.4.1 Restricción del acceso a la información.  6.1.1 Asignación de responsabilidades para la seguridad de la información. 6.1.2 Segregación de tareas.
Navegación segura del medio ambiente	11 Seguridad física y ambiental	11.1.4 Protección contra las amenazas externas y ambientales.
Aseguramiento de los sistemas operativos	9 Control de acceso  8 Gestión de recursos	9.4.2 Procedimientos seguros de inicio de sesión. 9.4.4 Uso de herramientas de administración de sistemas.  8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes.
Aislamiento de aplicaciones	9 Control de acceso	9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario. 9.4.5 Control de acceso al código fuente de los programas.



<b>Problemas de la Seguridad Móvil</b> (Dwivedi et al., 2014)	<b>Dominios</b> (Kosutic, 2017)	<b>ISO 27001: Anexo A de la norma</b> <b>Controles</b> (ISO/IEC 27001, 2012)
	14 Adquisición, desarrollo y mantenimiento de sistemas	14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software.
Divulgación de información	9 Control de acceso  12 Seguridad operacional	9.4.1 Restricción del acceso a la información.  12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6.2 Restricciones en la instalación de software.
Virus, gusanos, troyanos, spyware y malware	12 Seguridad operacional	12.2.1 Controles contra el código malicioso.
Difícil proceso de parcheo/actualización	12 Seguridad operacional  14 Adquisición, desarrollo y mantenimiento de sistemas	12.6.2 Restricciones en la instalación de software.  14.2.1 Política de desarrollo seguro de software 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.3.1 Protección de los datos utilizados en pruebas.
Uso estricto y ejecución de SSL	13 Seguridad de las telecomunicaciones  18. Cumplimiento.	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.  18.1.5 Regulación de los controles criptográficos.
Suplantación de identidad (Phishing)	12 Seguridad operacional	12.2.1 Controles contra el código malicioso.
Cross Site Request Forgery (CSRF)	12 Seguridad operacional	12.4.2 Protección de los registros de información.
Localización de privacidad / seguridad	18 Cumplimiento	18.1.4 Protección de datos y privacidad de la información personal. 18.1.5 Regulación de los controles criptográficos.
Controladores de dispositivos inseguros	6 Organización de la seguridad de la información	6.2.1 Política de uso de dispositivos para movilidad.
La autenticación de factores múltiples (MFA)	9 Control de acceso	9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.3.1 Uso de información confidencial para la autenticación.

Fuente: Elaboración propia



Se concluye que de los 14 dominios se relacionan 9 y de los 114 controles que se encuentran en el Anexo A de la norma ISO 27001, 39 que tienen relación con los problemas de la seguridad móvil.

## 2. Similitud entre la NIST 800-30 y los problemas de la seguridad móvil

Para analizar la similitud, se ha considerado que la norma en su estructura está conformada por 9 subprocesos para el análisis del riesgo y 7 subprocesos para la gestión del riesgo.

En la tabla 7, se podrá observar la similitud encontrada entre los subprocesos del análisis de riesgos, en la que existen dos subprocesos que no se relacionan con los problemas de la seguridad móvil que son: Análisis de impacto y Documentación de resultados.

Tabla 7: Similitud NIST 800-30 y los problemas de la Seguridad Móvil

Problemas de la Seguridad Móvil (Dwivedi et al., 2014)	NIST 800-30 (NIST, 2012)
La seguridad física	
Almacenamiento seguro de datos (en el disco)	Caracterización de sistemas
Autenticación fuerte	
Apoyo a la seguridad de múltiples usuarios	Identificación de vulnerabilidades
Navegación segura del medio ambiente	
Aseguramiento de los sistemas operativos	Caracterización de sistemas
Aislamiento de aplicaciones	
Divulgación de información	
Virus, gusanos, troyanos, spyware y malware	Identificación de amenazas, Determinación de probabilidades, Determinación del riesgo.
Difícil proceso de parcheo/actualización	
Uso estricto y ejecución de SSL	
Suplantación de identidad (Phishing)	Identificación de amenazas,
Cross-Site Request Forgery (CSRF)	Determinación de probabilidades
Localización de privacidad / seguridad	Identificación de vulnerabilidades
Controladores de dispositivos inseguros	Identificación de vulnerabilidades, Análisis de controles, Determinación del riesgo, Recomendación de controles
La autenticación de factores múltiples (MFA)	

Fuente: Elaboración propia.



Los 7 subprocesos definidos para la gestión de riesgos, no tiene similitud con los problemas de la seguridad móvil.

### 3. Similitud entre COBIT 5 y los problemas de la seguridad móvil

Según ISACA (2012), señala que el modelo de referencia COBIT 5, divide los procesos en dos grandes dominios como son: gobierno y gestión.

- **Gobierno:** compuesta por 5 procesos **EDM: Evaluación, Orientación y Supervisión**, ISACA (2012).
- **Gestión:** compuesta por 4 ámbitos, vinculadas a los elementos de **PBRM** que corresponde a: planificar (**Plan**), construir (**Build**), ejecutar (**Run**) y supervisar (**Monitor**); logrando cubrir los procesos de TI de extremo a extremo en la organización, (ISACA, 2012).

Según ISACA (2012), estos ámbitos son una evolución de la estructura de procesos y dominios de COBIT 4.1. los nombres se especifican según el área y función al que pertenece y se nominan mediante verbos de la siguiente manera:

- ✓ Alinear, Planificar y Organizar (Align, Plan and Organise, **APO**)
- ✓ Construir, Adquirir e Implementar (Build, Acquire and Implement, **BAI**)
- ✓ Entregar, dar Servicio y Soporte (Deliver, Service and Support, **DSS**)
- ✓ Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, **MEA**)



La similitud entre la estructura de COBIT 5 y los problemas de la seguridad móvil se observa en la tabla 8, en la que se ha considerado únicamente los procesos que se vinculan con las metas relacionadas con las TI.

Tabla 8: Relación procesos COBIT 5 y metas de TI

Procesos de COBIT 5	Meta relacionada con las TI.	
	Uso adecuado de aplicaciones, información y soluciones tecnológicas.(ISACA, 2012)	Seguridad de la información, infraestructura de procesamiento y aplicaciones.(ISACA, 2012)
<b>APO13</b> Gestionar la Seguridad.	S	P
<b>DSS05</b> Gestionar los Servicios de Seguridad	S	P

\*S significa relación secundaria y P primaria

Fuente: Extracto de (ISACA, 2012)

En la tabla 9 se presenta el mapeo correspondiente entre los problemas de la seguridad móvil y los dos procesos de COBIT vinculados con las metas relacionadas a las TI.

Tabla 9: Similitud entre COBIT 5 y los problemas de la Seguridad Móvil

Problemas de la Seguridad Móvil (Dwivedi et al., 2014)	COBIT 5 (Meta relacionada con las TI) (ISACA, 2012)
La seguridad física	
Almacenamiento seguro de datos (en el disco)	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Autenticación fuerte	
Apoyo a la seguridad de múltiples usuarios	Seguridad de la información, infraestructura de procesamiento y aplicaciones
Navegación segura del medio ambiente	
Aseguramiento de los sistemas operativos	Seguridad de la información, infraestructura de procesamiento y aplicaciones
Aislamiento de aplicaciones	
Divulgación de información	
Virus, gusanos, troyanos, spyware y malware	
Difícil proceso de parcheo/actualización	
Uso estricto y ejecución de SSL	
Suplantación de identidad (Phishing)	
Cross-Site Request Forgery (CSRF)	
Localización de privacidad / seguridad	Seguridad de la información, infraestructura de procesamiento y aplicaciones
Controladores de dispositivos inseguros	Seguridad de la información, infraestructura de procesamiento y aplicaciones
La autenticación de factores múltiples (MFA)	

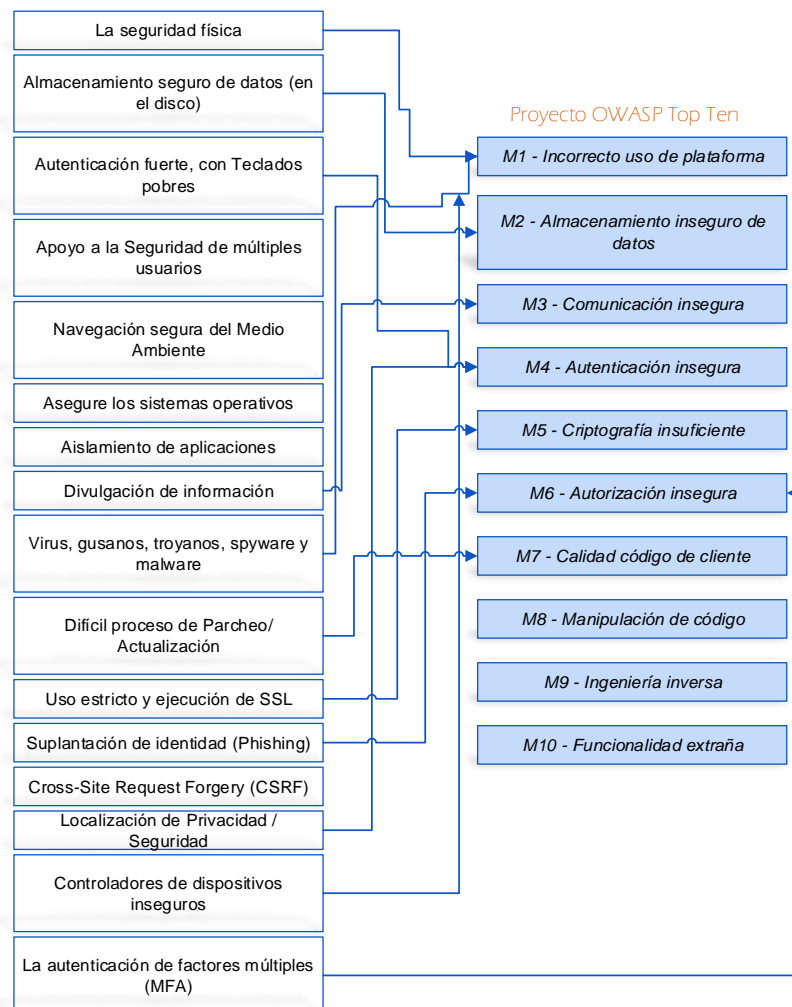
Fuente: Elaboración propia

## 4. Similitud entre el Proyecto Owasp y los problemas de la seguridad móvil

Para encontrar la similitud existente entre el Owasp y los problemas de la seguridad en dispositivos móviles se ha realizado la figura 12:

Figura 12 : Relación entre los problemas de Seguridad y Owasp Top Ten

Elementos de la Seguridad Móvil



Fuente: Elaboración propia

Luego del análisis realizado se representa gráficamente los riesgos del Top ten que tienen relación con los problemas de seguridad en dispositivos móviles

(ver figura 13), se aclara que del M7 al M10, no se los considerará debido a que tiene una mayor relación con el desarrollo de aplicaciones móviles.

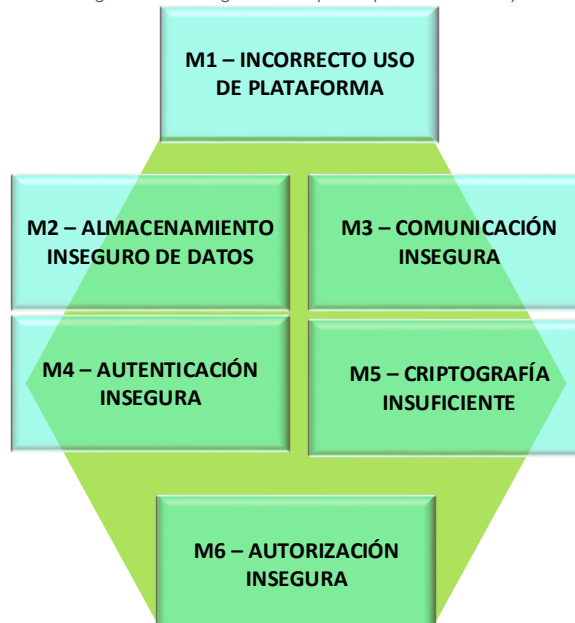
Figura 13: Selección riesgos del Top ten.



Fuente: Elaboración propia

Del análisis realizado entre los riesgos del Top ten y los problemas de seguridad en dispositivos móviles, se obtuvo como resultado 6 riesgos (ver figura 14), mismos que se tomarán en cuenta en el desarrollo de la metodología propuesta en la presente investigación, por tener mayor relación con la seguridad en los dispositivos móviles.

Figura 14: Riesgos del Top ten (seleccionados)



Fuente: Elaboración propia



---

#### **2.4.6. Presentar los resultados obtenidos**

Para la presentación de los resultados se ha realizado lo siguiente:

- Se ha realizado la revisión literaria de varios modelos y estándares, entre los que se ha considerado a los siguientes: ISO 27001, NIST 80-30, COBIT 5 y además al OWASP Top ten por ser un Proyecto profesional relacionado estrechamente con la seguridad móvil.

A continuación en la tabla 10 se resume el análisis realizado, presentando principalmente una evaluación de las particularidades y carencias en relación con la seguridad en dispositivos móviles de cada uno de los modelos, estándares y proyecto profesional analizados.



Tabla 10: Resumen modelos y estándares seleccionados

Norma /Proyecto Profesional	Objetivos	Enfoque	Relación con la seguridad en dispositivos móviles
ISO 27001 (Norma)	<ul style="list-style-type: none"> <li>✓ Definir Políticas de Seguridad</li> <li>✓ Permitir la Administración de la Seguridad</li> <li>✓ Realizar la adecuada Administración de Activos</li> <li>✓ Asegurar el Recurso Humano</li> <li>✓ Asegurar el Cumplimiento de Políticas y Normatividad Legal.</li> </ul>	<p><b>PDCA</b> Planear-Hacer-Chequear-Actuar</p>	<p><i>Define las políticas y el conocimiento general relacionado con la seguridad de la información.</i></p> <p><i>Constituye un estándar completo y de gran utilidad para la gestión de la seguridad de TI, aplicable a cualquier tipo de organización.</i></p> <p><i>Carece de un enfoque específico para los la seguridad en dispositivos móviles, en el que se especifique los procesos necesarios para mejorar la seguridad de ese entorno.</i></p>
NIST 800-30 (Norma)	<ul style="list-style-type: none"> <li>✓ Asegurar que los sistemas de información almacenen, procesen y transmitan información.</li> <li>✓ Gestionar los riesgos.</li> <li>✓ Optimizar la gestión de riesgos en base a los resultados del análisis de riesgos.</li> <li>✓ Velar por alcanzar la misión de la organización.</li> <li>✓ Ser una función esencial de la administración en la organización.</li> </ul>	<p><b>Primer componente:</b> Cómo las organizaciones tienen la intención de evaluar, responder y monitorear los riesgos</p> <p><b>Segundo componente:</b> Cómo las organizaciones van a evaluar el riesgo en el contexto del marco de riesgo de la organización.</p> <p><b>Tercer componente:</b> Cómo las organizaciones responden a arriesgar una vez que el riesgo se determina considerando los resultados de la evaluación de riesgos.</p> <p><b>Cuarto componente:</b> Cómo las organizaciones monitorean el riesgo</p>	<p><i>Esta norma contiene un conjunto completo de componentes y procesos para el análisis y gestión de riesgos, como un proceso clave para el éxito de las organizaciones.</i></p> <p><i>Esta norma carece de componentes relacionados con la seguridad de la información en dispositivos móviles.</i></p>



Norma /Proyecto Profesional	Objetivos	Enfoque	Relación con la seguridad en dispositivos móviles
COBIT 5 (Marco de Referencia integrado)	<ul style="list-style-type: none"> <li>✓ En COBIT 5 se establecen 17 objetivos relacionados la dimensión del CMI, metas corporativas y objetivos de Gobierno.</li> </ul>	<p>A través del ciclo de vida que comprende:</p> <ul style="list-style-type: none"> <li>✓ Ciclo de vida de Mejora continua.</li> <li>✓ Habilitación del cambio</li> <li>✓ Gestión del programa</li> </ul>	<p><i>Este marco de referencia integrado orientado al Gobierno y la Gestión de las TI de la Empresa</i></p> <p><i>Constituye un marco completo y general de gran utilidad para la gestión de la seguridad de TI, aplicable a cualquier tipo de organización.</i></p> <p><i>Existen 2 procesos que son: APO13 Gestionar la Seguridad y DSS05 Gestionar los Servicios de Seguridad, relacionados con la seguridad en general, es importante mencionar que carece de un enfoque específico para los la seguridad en dispositivos móviles,</i></p>
OWASP Top ten (Proyecto profesional)	<ul style="list-style-type: none"> <li>✓ Clasificar los riesgos de la seguridad móvil.</li> <li>✓ Proporcional los controles de desarrollo para reducir su impacto o la probabilidad de explotación.</li> </ul>	<p>El principal enfoque está en la capa de aplicación de las plataformas móviles.</p> <p>Infraestructura del servidor con el que las aplicaciones móviles se comunican.</p>	<p><i>Este proyecto define claramente los escenarios de riesgos relacionado con la seguridad de la información en dispositivos móviles.</i></p> <p><i>Constituye un referente importante y de gran utilidad para la gestión de la seguridad de TI, aplicable a cualquier tipo de organización.</i></p> <p><i>El enfoque es centrado en la seguridad en dispositivos móviles, en el que se especifica los elementos necesarios para mejorar la seguridad móvil.</i></p>

Fuente: Elaboración propia.



- En la tabla 11 se muestran los resultados de la comparación que permitirán determinar la similitud entre los problemas de la seguridad móvil para determinar y los estándares, modelos y proyecto profesional.

Tabla 11: Similitud entre los problemas de la seguridad móvil y los estándares seleccionados

Problemas de la Seguridad Móvil	ISO 27001	NIST 800-30	COBIT 5	OWASP
La seguridad física	√			√
Almacenamiento seguro de datos (en el disco)	√	√	√	√
Autenticación fuerte	√			√
Apoyo a la seguridad de múltiples usuarios	√	√	√	√
Navegación segura del medio ambiente	√			
Aseguramiento de los sistemas operativos	√	√	√	
Aislamiento de aplicaciones	√			
Divulgación de información	√			√
Virus, gusanos, troyanos, spyware y malware	√	√		√
Difícil proceso de parcheo/actualización	√			√
Uso estricto y ejecución de SSL	√			√
Suplantación de identidad (Phishing)	√	√		√
Cross-Site Request Forgery (CSRF)	√	√		√
Localización de privacidad / seguridad	√	√	√	√
Controladores de dispositivos inseguros	√	√	√	√
La autenticación de factores múltiples (MFA)	√			√

Fuente: Elaboración propia.

- En la tabla 12, se muestra el acoplamiento entre los controles de la norma ISO 27001 con los escenarios del proyecto profesional OWASP.



Tabla 12: Acoplamiento de Controles ISO 27001 (Anexo A)-OWASP

<b>ISO 27001: Anexo A de la norma</b>		<b>OWASP(OWASP, 2016)</b>
<b>Dominios (Kosutic, 2017)</b>	<b>Controles(ISO/IEC 27001, 2012)</b>	
6 Organización de la seguridad de la información	6.1.1 Asignación de responsabilidades para la seguridad de la información. 6.1.2 Segregación de tareas. 6.2.1 Políticas de uso de dispositivos para movilidad	M2 – Almacenamiento Inseguro de datos
8 Gestión de recursos	8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito.	M2 – Almacenamiento Inseguro de datos
9 Control de acceso	9.1.1 Política de control de acceso. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso 9.3.1 Uso de información confidencial para la autenticación. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario. 9.4.4 Uso de herramientas de administración de sistemas. 9.4.5 Control de acceso al código fuente de los programas.	M4 - Autenticación insegura M6 – Autorización Insegura
10 Criptografía	10.1.1 Política de uso de los controles criptográficos.	M5 - Criptografía insuficiente
11 Seguridad física y ambiental	11.1.4 Protección contra las amenazas externas y ambientales	M1 – Incorrecto uso de plataforma
12 Seguridad operacional	12.2.1 Controles contra el código malicioso. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.6.2 Restricciones en la instalación de software.	M1 – Incorrecto uso de plataforma



ISO 27001: Anexo A de la norma		OWASP(OWASP, 2016)
Dominios (Kosutic, 2017)	Controles(ISO/IEC 27001, 2012)	
13 Seguridad de las telecomunicaciones	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	M3 - Comunicación insegura
14 Adquisición, desarrollo y mantenimiento de sistemas	14.2.1 Política de desarrollo seguro de software 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.3.1 Protección de los datos utilizados en pruebas.	M1 – Incorrecto uso de plataforma
18 Cumplimiento	18.1.4 Protección de datos y privacidad de la información personal. 18.1.5 Regulación de los controles criptográficos.	M5 - Criptografía insuficiente

Fuente: Elaboración propia.

- En la tabla 13, se ha planteado controles para cada escenario de OWASP en vista que la tabla del acoplamiento entre los controles de la norma ISO 27001 con los escenarios del proyecto profesional OWASP no existen controles orientados específicamente a la validación de herramientas de seguridad en dispositivos móviles.



Tabla 13: Controles para selección de herramientas

<b>OWASP(OWAS P, 2016)</b>		<b>Controles para selección de herramientas</b>	
<b>M1 – INCORRECTO USO DE LA PLATAFORMA</b>	<b>M.1.1.</b> Permite agregar opciones de seguridad para el dispositivo <b>M.1.2.</b> Permite gestionar un bloqueo automático para proteger la aplicación de accesos no autorizados <b>M.1.3.</b> Permite ocultar datos sensibles en caso de intentos de acceso al dispositivo		
<b>M2 – ALMACENAMIENTO INSEGURO DE DATOS</b>	<b>M.2.1.</b> Encriptar información (mensajes personales mediante contraseña) <b>M.2.2.</b> Almacenar información mediante contraseña <b>M.2.3.</b> Permite almacenamiento seguro de usuarios y contraseñas de diferentes plataformas <b>M.2.4.</b> Permite bloqueo de acceso a la Información mediante bloqueo (patrón de desbloqueo o pin) <b>M.2.5.</b> Permite acceso mediante interfaz web y aplicación móvil <b>M.2.6.</b> Permite edición conjunta de archivos <b>M.2.7.</b> Permite compartición de Archivos multimedia, de texto, carpetas, etc <b>M.2.8.</b> Permite almacenamiento de información de otras librerías instaladas en el equipo <b>M.2.9.</b> Permite acceso a la información sin conexión <b>M.2.10.</b> Permite visualización de archivos sin necesidad de descarga <b>M.2.11.</b> Mostrar versiones anteriores en los archivos y visualización de cambios realizados por otros usuarios. <b>M.2.12.</b> Permite una capacidad de almacenamiento de 10GB <b>M.2.13.</b> Permite configuración de PIN de acceso a la aplicación <b>M.2.14.</b> Permite compartición de información contenida en el repositorio de otros usuarios mediante la generación de un enlace con o sin cifrado <b>M.2.15.</b> Permite compartición de enlaces mediante mensajería instalada en nuestro equipo		
<b>M3 – COMUNICACIÓN INSEGURO</b>	<b>M.3.1.</b> Permite comunicación segura a redes privadas		
<b>M4 - AUTENTICACIÓN INSEGURO - M6 - AUTORIZACIÓN INSEGURO</b>	<b>M.4.1.</b> Permite control de acceso a usuarios. Privacidad en el manejo de aplicaciones. Control de seguridad en cada una de ellas <b>M.4.2.</b> Permite protección de seguimiento, conexiones, navegación y aplicaciones		
<b>M5 – CRIPTOGRAFÍA INSUFICIENTE</b>	<b>M.5.1.</b> Realizar la encriptación de un sistema local de archivos disponible en nuestro dispositivo. <b>M.5.2.</b> Controlar la organización de la información mediante contenedores <b>M.5.3.</b> Ocultar información sensible dentro de los archivos de configuración del sistema a fin de que no sean visibles en caso de robo. <b>M.5.4.</b> Permite generación de contraseñas seguras, mediante en ingreso de caracteres (letras, números) previstos por el usuario. <b>M.5.5.</b> Permite técnicas de Estenografía (ocultar información en imágenes) <b>M.5.6.</b> Permite encriptación de documentos de texto, archivos multimedia (imagen y video) entre otros mediante contraseñas asignadas <b>M.5.7.</b> Permite almacenamiento de contraseñas en lugares seguros y con encriptación mediante contraseña <b>M.5.8.</b> Permite la creación de una clave maestra (principal) para acceder a los directorios que contiene la información segura <b>M.5.9.</b> Permite la organización de la información almacenada mediante la creación y el uso de paneles <b>M.5.10.</b> Encriptar mensajes para envío de información sensible <b>M.5.11.</b> Generar contraseñas seguras.		

Fuente: Elaboración propia.



Se concluye que el modelo de referencia, base para el desarrollo de la metodología propuesta, producto del análisis realizado, es la norma ISO 27001; por ser una norma de seguridad de la información estándar, que se enfoca en el ciclo de mejora continua, que permitirá identificar controles dentro de los escenarios del OWASP que mitiguen los problemas de la seguridad móvil.



## 2.5. Capítulo V: Diseño de la Metodología

### 2.5.1. Problemática

El creciente número de usuarios de dispositivos móviles se ha incrementado considerablemente en los últimos años y con ello el desconocimiento en relación a la información que están exponiendo desde sus dispositivos al descargar y utilizar aplicaciones móviles, pudiendo cada una de éstas constituir un riesgo para su información y es precisamente allí en donde surge la necesidad de escalar posiciones en cuanto a la curva de aprendizaje con respecto a la seguridad de información en dispositivos móviles.

Entre los principales problemas de seguridad que podemos encontrar, están: virus, robo o pérdida del dispositivo móvil, extracción de datos privados del usuario, riesgos tecnológicos y rastreo.

Indudablemente las conexiones inalámbricas y las apps pueden convertirse en el principal puente para la fuga de Información sin que el usuario se dé cuenta, además existen usuarios poco precavidos que al momento de instalar aplicaciones, no tienen cuidado de proporcionar datos relacionados con su identificación; son motivos más que suficientes por los que debemos idear métodos eficientes y herramientas seguras que permitan detectar a tiempo la presencia de malware y spyware que finalmente comprometerían la privacidad de la información personal, contenida en los dispositivos móviles.

En base a lo investigado en el capítulo “Seguridad en entornos móviles”, en el que se encuentra detallado las principales vulnerabilidades, amenazas, ataques y la descripción del argumento para mejorar el diseño de seguridad móvil; así



como lo analizado en el capítulo “Estándares de la seguridad informática” y lo acotado en el estudio y análisis de modelos, estándares y proyectos profesionales, realizado en el capítulo “Análisis de modelos y Estándares”. Se llega a la conclusión que actualmente no existe una metodología definida para garantizar la seguridad de la información en dispositivos móviles, que además permita analizar varias herramientas con base en escenarios y realizar la selección de éstas bajo criterios acertados.

El objetivo principal de la definición de una metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles es generar una metodología que facilite el refinamiento de la misma en todos los escenarios de despliegue de aplicativos móviles y así comparar herramientas y soluciones para finalmente permitir seleccionar las herramientas candidatas para cada una de las fases propuestas en la metodología y realizar el lanzamiento de soluciones (software, hardware, protocolos, etc.) en cada escenario definido en el Mobile Top 10 2016 de OWASP y así se garantizará la eficiencia en el ciclo de implementación.

### **2.5.2. Solución del problema**

Para la solución del problema se toma como referencia la revisión bibliográfica que se realizó en el capítulo “Análisis de los modelos y estándares”. El resultado de dicha revisión bibliográfica está basada en la selección de la norma ISO 27001, la misma que es el estándar internacional para seguridad de información, resaltando la selección de la norma por sus características (flexibilidad y adaptabilidad a cualquier ámbito y entorno en donde se requiera implementar



seguridad de la información). De la normativa ISO 27001 se ha tomado como referencia una gran parte de su estructura y se la ha orientado a la seguridad de información en dispositivos móviles, de manera transversal, la metodología se ha apoyado en los escenarios de riesgos propuestos en el Mobile Top 10 2016 de OWASP, los mismos que han sido seleccionados y orientados a todos los tipos de usuarios de dispositivos móviles.

Para el proceso de solución del problema se toma las actividades expuestas en la Norma ISO 9001 que comprende en identificar las entradas, definir el proceso y obtener la salida esperada, es decir el proceso conocido como entradas, procesos y salidas.

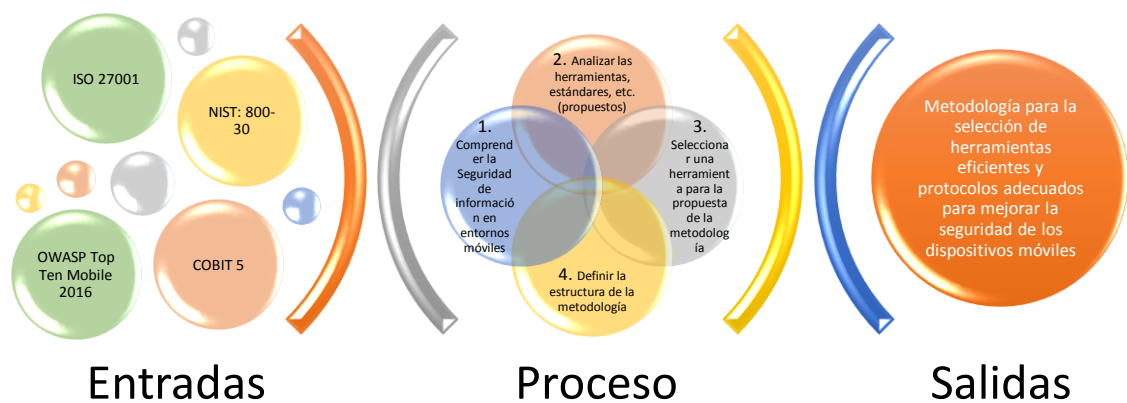
La solución del trabajo de investigación está basada en las actividades mencionadas anteriormente que son las siguientes:

- **Entradas:** en cuanto a las entradas para el proceso de solución se considera las siguientes:
  - Marco teórico de seguridad de la información y entornos móviles.
  - Identificación de herramientas y estándares.
    - Norma ISO 27001
    - NIST: 800-30
    - COBIT 5
    - OWASP Top Ten Mobile 2016
- **Proceso:** para la definición de una metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles, para ello se tiene las siguientes actividades:

- Comprender la seguridad de la información en entornos móviles (dispositivos móviles)
  - Analizar las herramientas, estándares, etc. (propuestos)
  - Seleccionar una herramienta para la propuesta de la metodología.
  - Definir la estructura de la metodología.
- **Salidas:** metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles.

En la figura 15 se puede apreciar el proceso de solución para la definición de una metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles.

Figura 15: Esquema de Resolución del Problema



Fuente: Elaboración propia



### **2.5.3. Metodología para seguridad en dispositivos móviles (Ms-DisMov)**

La metodología para la selección de herramientas eficientes para mejorar la seguridad de los dispositivos móviles, se la denominará: Ms-DisMov, que proviene de sus siglas abreviadas - **M**etodología para selección de herramientas de **S**eguridad en **D**ispositivos **M**óviles -; está basada en la Norma ISO 27001 y el OWASP Top Ten Mobile 2016, que se adapta a las características de los entornos móviles.

La selección de la Norma ISO 27001 se justifica ya que ésta es el estándar internacional para sistemas de gestión de seguridad, la misma que ha adoptado un modelo de proceso basado en PDCA, además de la selección del Top Ten Mobile 2016 de OWASP, ya que este nos permite tener una perspectiva clara en lo referente a problemas de seguridad y ha realizado una clasificación en escenarios (niveles), el Top Ten propone 10 escenarios de riesgos que se debe mitigar para agregar mayor seguridad en un ambiente móvil.

#### **2.5.3.1. Aspectos claves de la metodología**

Aspectos clave a considerar para el uso de la metodología Ms-DisMov:

a) *El alcance de la metodología Ms-DisMov, en cuanto a la Norma ISO 27001:*

- Proceso basado en PDCA, para el establecimiento, implementación y mejoramiento continuo en entornos móviles.
- Gestión de Requisitos para la definición en entornos móviles.



b) *El alcance de la metodología Ms-DisMov, en cuanto a escenarios de Top*

*Ten Mobile 2016 de OWASP:*

- Con respecto a usuario final
  - Uso de los seis primeros escenarios del Top Ten (que corresponden a soluciones móviles)
  - Unificación del escenario 4 y 6 que corresponden a autenticación y autorización insegura.
- Fuera de alcance
  - Son los escenarios que están orientados al desarrollo de aplicaciones móviles, los mismos que son:
    - M7 - Calidad del Código de Cliente
    - M8 – Manipulación de Código
    - M9 - Ingeniería Inversa
    - M10 - Funcionalidad Extraña

c) *Criterios para selección de herramientas:*

En la tabla 14, se muestran los criterios a considerar, para realizar una correcta selección de las herramientas de seguridad:

*Tabla 14: Criterios para selección de herramientas*

<b>Criterio</b>	<b>Descripción</b>	<b>Escala cualitativa</b>
1. Confidencialidad	C.1 Que la información sea accedida por el usuario que tenga el rol.	Cumple a satisfacción: Si C1 y C2
	C.2 Que la información sea accedida por el usuario que tenga permisos necesarios para acceder a dicha información.	Cumple parcialmente: Si C1 o C2 No cumple: inexistencia de C1 y C2
2. Integridad	C.3 Que la información no haya podido ser modificada por un tercero que no posea el rol.	Cumple a satisfacción: Si C3 y C4 Cumple parcialmente: Si C3 o C4
	C.4 Que la información no haya podido ser modificada por un tercero que no posea los permisos necesarios para hacerlo.	No cumple: inexistencia de C3 y C4



Criterio		Descripción	Escala cualitativa
3. Disponibilidad	C.5	Que la información esté disponible cuando el usuario la requiera utilizar.	Cumple a satisfacción: Si C5 y C6
	C.6	Que no se tenga contratiempos o esperas al momento de obtener la información.	Cumple parcialmente: Si C5 o C6 No cumple: inexistencia de C5 y C6
4. Funcionalidad y facilidad de uso	C.7	Capacidad del sistema de ofrecer cambio de password.	Cumple a satisfacción: Si C7 y C8
	C.8	Uniformidad en nomenclatura de etiquetado de botones.	Cumple parcialmente: Si C7 o C8 No cumple: inexistencia de C7 y C8
5. Estabilidad	C.9	Capacidad de procesar la información y cumplir los objetivos de desarrollo del sistema sin tener fallos.	Cumple a satisfacción: Si C9 y C10
	C.10	Capacidad de procesar información teniendo la menor cantidad de fallos posibles para cumplir el proceso para el que fue diseñado.	Cumple parcialmente: Si C9 o C10 No cumple: inexistencia de C9 y C10
6. Compatibilidad	C.11	Si la herramienta puede ejecutarse en todas las versiones de Android.	Cumple a satisfacción: Si C11 y C12
	C.12	Solo la herramienta puede ejecutarse en determinada versión de Android.	Cumple parcialmente: Si C11 o C12 No cumple: inexistencia de C11 y C12
7. Interoperabilidad	C.13	Capacidad que pueda tener la herramienta para comunicarse con otras herramientas.	Cumple a satisfacción: Si C13 y C14
	C.14	Capacidad que pueda tener la herramienta para enviar/recibir información en un formato que sea común en el entorno en el que se ejecuta.	Cumple parcialmente: Si C13 o C14 No cumple: inexistencia de C13 y C14
8. Soporte y Garantía	C.15	Capacidad que la empresa que ofrece la herramienta tenga para responder inquietudes, o resolver problemas referentes al producto que está ofreciendo.	Cumple a satisfacción: Si C15 y C16
	C.16	Forma en que la empresa que ofrece el software tenga para ayudar en la reparación de posibles fallos.	Cumple parcialmente: Si C15 o C16 No cumple: inexistencia de C15 y C16
9. Actualización	C.17	Capacidad de respuesta de la empresa desarrolladora para cubrir fallos del programa que han sido identificados de manera general.	Cumple a satisfacción: Si C17 y C18
	C.18	Capacidad de respuesta de la empresa desarrolladora para añadir nuevas funcionalidades o características del programa.	Cumple parcialmente: Si C17 o C18 No cumple: inexistencia de C17 y C18
10. Costo Inicial y futuro	C.19	Si el costo directo de la herramienta viene dada por el licenciamiento temporal o de por vida.	Cumple a satisfacción: Si C19 y C20
	C.20	Si el costo indirecto de la herramienta viene dada por la funcionalidad adicional.	Cumple parcialmente: Si C19 o C20 No cumple: inexistencia de C19 y C20



criterio	Descripción	Escala cualitativa	
11. Algoritmos criptográficos	C.21	Si para las opciones de encriptación de datos utiliza alguno de éstos algoritmos: AES (Rijndael) de hasta 256 bits, RC6 de hasta 256 bits, Serpent 256 bits, Blowfish 448 bits, Twofish 256 bits, GOST 256 bits, Threefish plus de 1024 bits, SHACAL-2 de 512 bits, SHA de 512 bits, RIPEMD de 160 bits, Algoritmos hash Whirlpool.	Cumple a satisfacción: Si C21 y C22 Cumple parcialmente: Si C23 No cumple: inexistencia de C21, C22 y C23
	C.22	Posee un generador de claves con cifrado.	
	C.23	Existencia de políticas de administración controlada para seguridad móvil.	

d) *Parámetros para valoración de criterios:*

Para la valoración de los criterios, se considera la tabla 15, en la que se establecen los parámetros de valoración, a tomar en cuenta frente a los criterios explicados en el punto c).

Tabla 15: Parámetros de valoración de criterios

Indicador	Valoración Numérica	Explicación
Cumple a satisfacción	3	Que el concepto se cumple en su totalidad en el aplicativo evaluado
Cumple parcialmente	2	Que el concepto se cumple parcialmente en el aplicativo evaluado
No cumple	1	Que el concepto no se cumple en el aplicativo evaluado
No Aplica	0	Que el aplicativo carece de dicho concepto o el escenario no se puede aplicar en el aplicativo

e) *Parámetros para valoración de herramientas:*

Para definir si una herramienta es factible de ser seleccionada como herramienta para la seguridad móvil, se considerará los valores de la tabla 16.

Tabla 16: Parámetros de valoración de herramientas

Indicador	Valoración Controles
Herramienta eficiente	90% - 100%
Medianamente eficiente	70% - 89%
Parcialmente eficiente	40% - 69%
No alcanza los requerimientos de eficiencia	<=40%



### 2.5.3.2. Estructura.

La estructura de Ms-DisMov, está compuesta por la Norma ISO 27001 y el Top Ten Mobile 2016 de OWASP, de los cuales se utiliza estos componentes de la siguiente manera:

- a) El núcleo de la metodología, es la Norma ISO 27001, se ha tomado el modelo de proceso basado en PDCA.
- b) El modelo de proceso que se ejecutará en toda la metodología propone los siguientes pasos:
  - a. Planear y establecer la Ms-DisMov
  - b. Hacer, implementar y operar la Ms-DisMov
  - c. Chequear, monitorear y revisar la Ms-DisMov
  - d. Actuar, mantener y mejorar la Ms-DisMov
- c) Los escenarios de la metodología son 6:

#### M1 – Incorrecto uso de plataforma

Ciclo PDCA	
<b>Planear</b>	Búsqueda de herramientas para asegurar las plataformas móviles
<b>Hacer</b>	Implementación de herramientas. <i>(La metodología está abierta a la evaluación de N herramientas)</i>
<b>Verificar</b>	V1.- Para la selección de las herramientas, considerar los puntos c) y d) del apartado 'Aspectos clave de la metodología'.  V2.- Evaluación de cada una de las herramientas, mediante pruebas sobre entornos móviles Los controles a evaluar son: <ul style="list-style-type: none"><li>✓ M.1.1. Permite agregar opciones de seguridad para el dispositivo</li><li>✓ M.1.2. Permite gestionar un bloqueo automático para proteger la aplicación de accesos no autorizados</li><li>✓ M.1.3. Permite ocultar datos sensibles en caso de intentos de acceso al dispositivo</li></ul>
<b>Actuar</b>	Repetición del ciclo para validar brechas de seguridad en los aplicativos seleccionados.



## M2 – Almacenamiento Inseguro de datos

<b>Ciclo PDCA</b>	
<b>Planear</b>	Búsqueda de herramientas para asegurar el almacenamiento de datos en plataformas móviles
<b>Hacer</b>	Implementación de herramientas. (La metodología está abierta a la evaluación de N herramientas)
<b>Verificar</b>	V1.- Para la selección de herramientas para almacenamiento (nativo y en línea), considerar los puntos c) y d) del apartado 'Aspectos clave de la metodología'.  V2.- Evaluación de cada una de las herramientas: Los controles a evaluar son: ✓ M.2.1. <i>Encriptar información (mensajes personales mediante contraseña)</i> ✓ M.2.2. <i>Almacenar información mediante contraseña</i> ✓ M.2.3. <i>Permite almacenamiento seguro de usuarios y contraseñas de diferentes plataformas</i> ✓ M.2.4. <i>Permite bloqueo de acceso a la Información mediante bloqueo (patrón de desbloqueo o pin)</i> ✓ M.2.5. <i>Permite acceso mediante interfaz web y aplicación móvil</i> ✓ M.2.6. <i>Permite edición conjunta de archivos</i> ✓ M.2.7. <i>Permite compartición de Archivos multimedia, de texto, carpetas, etc</i> ✓ M.2.8. <i>Permite almacenamiento de información de otras librerías instaladas en el equipo</i> ✓ M.2.9. <i>Permite acceso a la información sin conexión</i> ✓ M.2.10. <i>Permite visualización de archivos sin necesidad de descarga</i> ✓ M.2.11. <i>Mostrar versiones anteriores en los archivos y visualización de cambios realizados por otros usuarios.</i> ✓ M.2.12. <i>Permite una capacidad de almacenamiento de 10GB</i> ✓ M.2.13. <i>Permite configuración de PIN de acceso a la aplicación</i> ✓ M.2.14. <i>Permite compartición de información contenida en el repositorio de otros usuarios mediante la generación de un enlace con o sin cifrado</i> ✓ M.2.15. <i>Permite compartición de enlaces mediante mensajería instalada en nuestro equipo</i>
<b>Actuar</b>	Repetición del ciclo para validar brechas de seguridad en los aplicativos seleccionados.

## M3 - Comunicación insegura

<b>Ciclo PDCA</b>	
<b>Planear</b>	Búsqueda de herramientas y protocolos para mejorar la comunicación en dispositivos móviles
<b>Hacer</b>	Implementación de herramientas. (La metodología está abierta a la evaluación de N herramientas)
<b>Verificar</b>	V1.- Para la selección de herramientas considerar los puntos c) y d) del apartado 'Aspectos clave de la metodología'.  V2.- Evaluación de cada una de las herramientas Los controles a evaluar son: ✓ M.3.1. <i>Permite comunicación segura a redes privadas</i>
<b>Actuar</b>	Repetición del ciclo para validar brechas de seguridad en los aplicativos seleccionados.



### M4 - Autenticación insegura M6 – Autorización Insegura

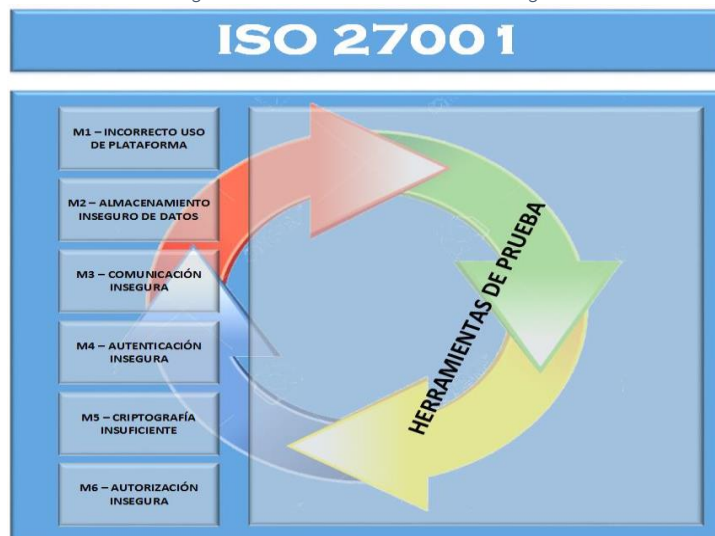
Ciclo PDCA	
<b>Planear</b>	Búsqueda de soluciones móviles para asegurar la autenticación y autorización de acceso a usuarios.
<b>Hacer</b>	Implementación de herramientas. <i>(La metodología está abierta a la evaluación de N herramientas)</i>
<b>Verificar</b>	V1.- Para la selección de las herramientas, considerar los puntos c) y d) del apartado 'Aspectos clave de la metodología'.  V2.- Realizar la evaluación de las herramientas Los controles a evaluar son: <ul style="list-style-type: none"><li>✓ M.4.1. Permite control de acceso a usuarios. Privacidad en el manejo de aplicaciones. Control de seguridad en cada una de ellas</li><li>✓ M.4.2. Permite protección de seguimiento, conexiones, navegación y aplicaciones</li></ul>
<b>Actuar</b>	Repetición del ciclo para validar brechas de seguridad en los aplicativos seleccionados.

### M5 - Criptografía insuficiente

Ciclo PDCA	
<b>Planear</b>	Búsqueda de herramientas que permitan encriptar información en dispositivos móviles
<b>Hacer</b>	Implementación de herramientas. <i>(La metodología está abierta a la evaluación de N herramientas)</i>
<b>Verificar</b>	V1.- Para la selección de las herramientas, considerar los puntos c) y d) del apartado 'Aspectos clave de la metodología'.  V2.- Evaluación de cada una de las herramientas, mediante pruebas sobre entornos móviles Controles a evaluar son: <ul style="list-style-type: none"><li>✓ M.5.1. Realizar la encriptación de un sistema local de archivos disponible en nuestro dispositivo.</li><li>✓ M.5.2. Controlar la organización de la información mediante contenedores</li><li>✓ M.5.3. Ocultar información sensible dentro de los archivos de configuración del sistema a fin de que no sean visibles en caso de robo.</li><li>✓ M.5.4. Permite generación de contraseñas seguras, mediante el ingreso de caracteres (letras, números) previstos por el usuario.</li><li>✓ M.5.5. Permite técnicas de Estenografía (ocultar información en imágenes)</li><li>✓ M.5.6. Permite encriptación de documentos de texto, archivos multimedia (imagen y video) entre otros mediante contraseñas asignadas</li><li>✓ M.5.7. Permite almacenamiento de contraseñas en lugares seguros y con encriptación mediante contraseña</li><li>✓ M.5.8. Permite la creación de una clave maestra (principal) para acceder a los directorios que contiene la información segura</li><li>✓ M.5.9. Permite la organización de la información almacenada mediante la creación y el uso de paneles</li><li>✓ M.5.10. Encriptar mensajes para envío de información sensible</li><li>✓ M.5.11. Generar contraseñas seguras.</li></ul>
<b>Actuar</b>	Repetición del ciclo para validar brechas de seguridad en los aplicativos seleccionados.

La figura 16 resume la estructura de la metodología Ms-DisMov propuesta.

Figura 16: Estructura de la Metodología



Fuente: Elaboración propia

d) Los pasos de la metodología son los siguientes:

**Paso 1:** Realice la fase “Planear”, por cada uno de los escenarios de la metodología, como resultado obtendrá una matriz con las posibles herramientas a evaluar.

**Paso 2:** Ejecute la fase “Hacer”, con cada una de las herramientas a evaluar.

**Paso 3:** Realice la tarea V1 de la fase “Verificar”, como resultado obtendrá una matriz con la siguientes especificaciones:

- Las columnas corresponden a: los 11 criterios para selección de herramientas; agregue una columna denominada “Valoración promedio”.
- Las filas serán los nombres de las herramientas que desee evaluar.
- Coloque en cada celda la evaluación que se hará en base a los “Parámetros de valoración de criterios”, con respecto a la herramienta que está evaluando.



- Calcule el valor promedio y coloque en la celda de “Valoración promedio”.

**Paso 4:** De la matriz anterior, realice un listado de herramientas con las que obtuvieron mayor puntuación por escenario.

**Paso 5:** Evalúe los controles descritos en la tarea V2 de la fase “**Verificar**” con las herramientas del listado obtenido en el paso 4. Los resultados deberán ser registrarlos en una matriz que contenga las siguientes especificaciones:

- Encabezado: Nombre de la herramienta y Escenarios a validar
- Columnas: 1) Controles, 2) Resultados, 3) Validado/no Validado, 4) Observaciones.
- Totalice los valores obtenidos en la columna “Validado /no Validado”, por cada herramienta validada.
- Calcule el porcentaje mediante la relación (nro. de controles validados / nro. total de controles propuestos por escenario \*100).

**Paso 6:** Diseñe una Matriz de resultados, con las siguientes especificaciones:

- Las columnas corresponden a: 1) Herramienta, 2) Valoración controles, 3) Estado.
- Las filas corresponden a las herramientas validadas.
- Traslade el valor del porcentaje obtenido a la columna “Validado/no Validado” de la matriz obtenida en el paso 5 a la herramienta correspondiente.
- Defina el estado para la herramienta, colocando bajo la columna “Estado”, en base a los “Parámetros de valoración de herramientas”.



**Paso 7:** Ejecute la fase “**Actuar**”. El ciclo termina cuando no tenga más herramientas que validar o encuentre una herramienta segura.

**Paso 8:** Presente los resultados por cada escenario de la metodología conforme la estructura planteada del ciclo PDCA. (opcional)



## **2.6. CAPITULO VI: Validación de la Metodología**

### **2.6.1. Análisis de vulnerabilidades en dispositivos móviles**

Para realizar el proceso de validación de vulnerabilidades en dispositivos móviles se tomó como base las recomendaciones que se lanzan en un proyecto de OWASP (Open Web Application Security Project) que es una organización sin fines de lucro, que mantiene proyectos de código abierto encaminados en proporcionar a las instituciones formas seguras para desarrollar, comprar y mantener aplicaciones confiables en sus sistemas.

Con este fin OWASP se ha planteado proyectos que buscan proporcionar a desarrolladores y grupos de seguridad informática controles sobre los principales riesgos de seguridad en los diferentes ámbitos y como muestra de su trabajo se tiene proyectos tan emblemáticos en el área de seguridad de la información tales como el OWASP TOP 10 que se refiere a los 10 más grandes riesgos de seguridad en aplicativos web, OWASP ZAP que se refiere a una herramienta tipo proxy que incluye muchos complementos que facilitan realizar pruebas de penetración en aplicativos web, OWASP TOP 10 Móvil cuyo objetivo primordial es clasificar los riesgos de seguridad móvil y proporcionar controles de desarrollo para reducir su impacto o probabilidad de explotación, planteándonos un escenario de 10 vulnerabilidades encontradas a nivel mundial en la tecnología móvil, las cuales servirán como alcance para la presente investigación.



Tabla 17: Vulnerabilidades identificadas

Vulnerabilidad	Descripción	Criticidad	Facilidad de explotación
M1 – Incorrecto uso de plataforma	Esta categoría cubre el mal uso de una función de la plataforma o la falta de uso de los controles de seguridad de la plataforma. Podría incluir la mala asignación de permisos sobre la plataforma, el mal uso de TouchID, el llavero de contraseñas, o algún otro control de seguridad que es parte del sistema operativo móvil. Hay varias maneras de que las aplicaciones móviles pueden experimentar este riesgo.	Alto	Fácil
M2 – Almacenamiento Inseguro de datos	Este escenario cubre el almacenamiento de datos inseguros y la fuga de datos no deseados, planteando la posibilidad de que cualquier aplicativo puede convertirse en un potencial vector de ataque.	Alta	Medio
M3 - Comunicación insegura	Este escenario cubre la comunicación con protocolos de enlace inseguros, versiones incorrectas SSL, negociación débil, la comunicación sin cifrar de los activos sensibles, etc.	Alta	Fácil
M4 - Autenticación insegura	Esta categoría captura nociones de la autenticación del usuario final o de la mala gestión de sesiones. Esto puede incluir: <ul style="list-style-type: none"><li>• El no poder identificar al usuario en absoluto cuando deberían estar obligados</li><li>• No se mantiene la identidad del usuario cuando se requiere</li><li>• Las deficiencias en la gestión de sesiones</li></ul>	Alta	Media
M5 - Criptografía insuficiente	Este escenario se refiere al código fuente de los aplicativos, se aplica la criptografía a un activo de información sensible. Sin embargo, la criptografía es insuficiente de alguna manera. Se debe tener en cuenta que cualquier tema relacionado con TLS o SSL va en el escenario M3. Además, si la aplicación no hace uso de la criptografía en absoluto cuando debe, pertenece probablemente al escenario M2. Esta categoría es para los escenarios en los que se intentó la implementación de criptografía, pero no se ha realizado correctamente.	Alta	Media
M6 - Autorización insegura	Esta es una categoría para capturar cualquier fallo en la autorización (por ejemplo, las decisiones de autorización en el lado del cliente, navegación forzada, etc.). Es distinto de los problemas de autenticación (por ejemplo, el registro del dispositivo, la identificación del usuario, etc.).  Si la aplicación no autentica a los usuarios en absoluto en una situación en la que debería (por ejemplo, la concesión de acceso anónimo a algún recurso o servicio)	Alta	Alta



	cuando se autentica y se requiere el acceso autorizado), entonces eso es un error de autenticación no un error de autorización.		
M7 - Calidad Código de cliente	Este escenario se define por "Las decisiones de seguridad a través de entradas no confiables ", una de nuestras categorías de menor difusión. Este sería el cajón de sastre de los problemas de implementación a nivel de código en el cliente móvil. Siendo distinto de errores de codificación del lado del servidor. En este tipo de problemas se puede capturar cosas como desbordamientos de búfer, vulnerabilidades de cadena de formato y varios otros errores a nivel de código, donde la solución es volver a escribir algo de código que se ejecuta en el dispositivo móvil.	Alta	Alta
M8 - Manipulación de Código	Esta categoría abarca la alteración de binarios, la modificación de los recursos locales, métodos como el swizzling y la modificación de la memoria dinámica.  Una vez que la aplicación se envía al dispositivo móvil, los recursos de código y datos residen en este dispositivo. Un atacante o bien puede modificar directamente el código, cambiar el contenido de la memoria dinámica, cambiar o reemplazar las API del sistema que utiliza la aplicación, o modificar los datos y recursos de la aplicación. Esto puede proporcionar al atacante un método directo de subvertir el uso previsto del software para beneficio personal o monetario.	Alta	Alta
M9 - Ingeniería inversa	Esta categoría incluye el análisis del binario del núcleo final para determinar su código fuente, bibliotecas, algoritmos y otros activos. Software como IDA Pro, Hopper, otool y otras herramientas de inspección binarios dará la visión atacante en el funcionamiento interno de la aplicación. Esto puede ser usado para explotar otras vulnerabilidades nacientes en la aplicación, así como información reveladora acerca de los servidores back end, constantes criptográficos y sistemas de cifrado y la propiedad intelectual.	Alta	Alta
M10 - funcionalidad extraña	A menudo, los desarrolladores incluyen funcionalidad de puerta trasera oculta u otros controles de seguridad internos de desarrollo que no están destinados a ser liberados en un entorno de producción. Por ejemplo, un desarrollador puede incluir accidentalmente una contraseña como un comentario en una aplicación híbrida. Otro ejemplo incluye la desactivación de la autenticación de 2 factores durante la prueba.	Alta	Alta

Fuente: Elaboración propia.



De los 10 escenarios de vulnerabilidades planteados en el OWASP top 10 móvil 2016, para efecto de este proyecto se procederá a analizar 5 escenarios, planteados en el alcance inicial, los cuales serán puestos a evaluación y se deberá proponer herramientas que nos permitan minimizar los riesgos inherentes a los entornos móviles planteados. Los escenarios a evaluar se muestran en la tabla 18:

Tabla 18: Escenarios a evaluar

Vulnerabilidad	Alcance Planteado
M1 – Incorrecto uso de plataforma	SI
M2 – Almacenamiento Inseguro de datos	SI
M3 - Comunicación insegura	SI
M4 - Autenticación insegura	SI
M5 - Criptografía insuficiente	SI
M6 - Autorización insegura	SI
M7 - Calidad Código de cliente	NO
M8 - Manipulación de Código	NO
M9 - Ingeniería inversa	NO
M10 - funcionalidad extraña	NO

Fuente: Elaboración propia.



## 2.6.2. Pruebas de la metodología

En función de los escenarios determinados en el apartado de vulnerabilidades y de la metodología propuesta se procede a realizar *Pruebas de Concepto*, que consiste en la ejecución de la metodología paso a paso, con la finalidad de verificar que los conceptos definidos en los ciclos PDCA de los seis escenarios del OWASP propuestos, son susceptibles de ser ejecutados paso a paso hasta llegar a la selección de una herramienta relacionadas con la seguridad de la información en dispositivos móviles y poder determinar las mejores prácticas de uso de las herramientas evaluadas frente a cada escenario del OWASP.

Siguiendo el modelo de proceso planteado por la metodología se definió tres procesos:

### a. Planeación

En la planeación se consideró el paso 1 de la metodología:

- ✓ Planear y establecer de la Ms-DisMov,

En esta fase se sugiere la búsqueda de herramientas para asegurar las plataformas móviles, etc. El resultado de esta búsqueda se observa en la tabla 19.



Tabla 19: Herramientas alineadas a los escenarios del OWASP

OWASP	HERRAMIENTAS
<b>M1 – INCORRECTO USO DE LA PLATAFORMA</b>	<i>mSecure</i> <i>Secure Settings</i> <i>AirCover Security Suite</i>
<b>M2 – ALMACENAMIENTO INSEGURO DE DATOS</b>	<i>WiSeID</i> <i>Box</i> <i>MEGA</i>
<b>M3 – COMUNICACIÓN INSEGURO</b>	<i>TLS/SSL Tunnel</i> <i>JuicesSSH</i> <i>AnyConnect</i>
<b>M4 - AUTENTICACIÓN INSEGURO - M6 - AUTORIZACIÓN INSEGURO</b>	<i>Área TEE</i> <i>Swivel Secure</i> <i>Mobile Secure</i>
<b>M5 – CRIPTOGRAFÍA INSUFICIENTE</b>	<i>Secret Space Encryptor for Android</i> <i>Encrypted Data Storage EDS Lite</i> <i>EDS</i>

Fuente: Elaboración propia.

## b. Ejecución y evaluación

Para la ejecución de la metodología se ha considerado, el escenario general de pruebas, definido para estas pruebas fue un dispositivo tipo Tablet de marca Samsung con sistema operativo Android en su versión 4.4, con la configuración de fábrica, en el que se instalaron las herramientas de prueba.

Para la evaluación se consideró los pasos del 2 al 5 de la metodología:

- ✓ Hacer, implementar y operar la Ms-DisMov

En el proceso de 'Hacer', se procedió a instalar las herramientas seleccionadas, luego se realizaron los pasos descritos en el 'Verificar' de cada escenario en que se encuentran dos tareas: la selección y la evaluación,

Para la selección se consideró los puntos c) y d) del apartado 'Aspectos clave de la metodología, el resultado se muestra en la tabla 20.

Tabla 20: Evaluación de criterios para selección de herramientas

Herramienta a evaluarse	Confidencialidad	Integridad	Disponibilidad	Funcionalidad y Facilidad de Uso	Estabilidad	Compatibilidad	Interoperabilidad	Soporte y Garantía	Actualización	Costo inicial y futuro	Algoritmos criptográficos	Valoración Promedio
mSecure	2	2	2	1	2	2	2	1	2	1	2	1,7
<b>Secure Settings</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>3</b>	<b>2</b>	<b>2,0</b>
AirCover Secure Suite	2	2	2	1	2	1	2	2	2	1	1	1,6
<b>WiSeiD</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1,9</b>
<b>Box</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1,9</b>
<b>MEGA</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1,9</b>
<b>TLS/SSL Tunel</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>3</b>	<b>2,0</b>
JuicesSSH	2	2	2	1	2	2	2	2	2	1	3	1,9
AnyConnect	2	2	2	1	2	2	1	2	1	1	2	1,6
Área TEE	2	2	2	1	2	2	2	2	2	1	1	1,7
Swivel Secure	2	2	2	1	2	2	2	1	2	1	1	1,6
<b>Mobile Secure</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>3</b>	<b>2,0</b>
<b>Secret Space Encrypt</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>3</b>	<b>2,0</b>
<b>Encrypted Data Storage Lite</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>1</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>2</b>	<b>3</b>	<b>2,0</b>
EDS with SANs	2	2	2	1	2	2	1	2	2	1	1	1,6

Fuente: Elaboración propia.

De la tabla anterior se define que las herramientas factibles de ser evaluadas son 8:

- ✓ M1: Secure Settings
- ✓ M2: WiSeiD, Box y Mega
- ✓ M3: TLS/SSL Tunel
- ✓ M4 y M6: Mobile Secure
- ✓ M5: Secret Space Encrypt y Encrypted Data Storage Lite

Con el listado de herramientas evaluadas, se procedió a la ejecución del ciclo PDCA implementado en cada escenario del OWASP, la evaluación de cada herramienta se registró en los siguientes escenarios:



Tabla 21: Fichas de resultados de pruebas

<b>Herramienta:</b> Secure Setting					
<b>Escenario:</b> M1 – Incorrecto uso de plataforma					
<b>Referencia:</b> Anexo B, SECCIÓN 1					
Controles	Resultados	Validado/no Validado			Observaciones
		WISel D	BOX	Mega	
M.1.1. Permite agregar opciones de seguridad para el dispositivo	Esta herramienta permite controlar configuraciones de seguridad específicas del dispositivo móvil. (activar o desactivar funcionalidades, controlar acciones a realizar de las herramientas instaladas en el dispositivo.	1			
M.1.2. Permite gestionar un bloqueo automático para proteger la aplicación de accesos no autorizados	Permite gestionar la cantidad de intentos de acceso al dispositivo.	1			
M.1.3. Permite ocultar datos sensibles en caso de intentos de acceso al dispositivo	Para garantizar la seguridad de la información almacenada en el dispositivo mediante configuraciones con esta herramienta permite ocultar información en caso de intentos fallidos continuos en la aplicación.	0			Para controlar este y otro tipo de funcionalidades específicas es necesario incluir algunas aplicaciones complementarias a esta.
Total		2			
%		67%			

<b>Herramienta:</b> WISelD, BOX, Mega					
<b>Escenario:</b> M2 – Almacenamiento Inseguro de datos					
<b>Referencia:</b> Anexo B, SECCIÓN 2					
Controles	Resultados	Validado/no Validado			Observaciones
		WISel D	BOX	Mega	
M.2.1. Encriptar información (mensajes personales mediante contraseña)	Se puede encriptar todo tipo de información. Es necesario no desinstalar la aplicación para poder acceder nuevamente a los datos.	1	0	0	En caso de desencriptar un archivo se genera una copia de la información contenida y se sigue manteniendo el archivo encriptado.
M.2.2. Almacenar información mediante contraseña	La información aquí creada se maneja mediante contraseñas establecidas por el usuario.	1	0	0	Es recomendable el uso de contraseñas



					fáciles de recordar por el usuario.
<i>M.2.3. Permite almacenamiento seguro de usuarios y contraseñas de diferentes plataformas</i>	La información puede ser, usuario y contraseñas de redes sociales y aplicaciones de mensajería. Números de tarjetas de crédito, fecha de vencimiento y códigos de seguridad. Datos de aerolíneas o compañías de su preferencia. Claves bancarias, etc.	1	0	0	
<i>M.2.4. Permite bloqueo de acceso a la Información mediante bloqueo (patrón de desbloqueo o pin)</i>	Para acceder a la información almacenada en esta herramienta, es importante asignar una contraseña de acceso, en este caso las opciones a configurar son: Patrón de deslizamiento y pin de seguridad.	1	0	0	
<i>M.2.5. Permite acceso mediante interfaz web y aplicación móvil</i>	Se puede visualizar correctamente y en el mismo orden los archivos en las dos interfaces	0	1	0	* Permite realizar vistas previas de los archivos sin descargarlos
<i>M.2.6. Permite edición conjunta de archivos</i>	Se puede visualizar los usuarios que se encuentran conectados para la edición del archivo sin embargo no se visualizan en tiempo real las modificaciones realizadas.	0	1	0	Para evitar la pérdida de información es necesario que no se utilice la modificación conjunta.
<i>M.2.7. Permite compartición de Archivos multimedia, de texto, carpetas, etc.</i>	Las seguridades que maneja la aplicación para compartir enlaces o URL son: Acceso: Permite acceder al archivo a cualquier persona a la que le haya sido enviado el enlace. Finalizar enlace: Deshabilita el enlace después de una fecha concreta. Permitir descarga: Permite que otras personas descarguen el archivo. Contraseña: Establecer una contraseña para el enlace (letras, números, caracteres). * Se puede compartir el enlace mediante herramientas de mensajería instaladas en el dispositivo.	1	1	0	* Para mayor seguridad es importante establecer una contraseña antes de compartir un archivo. * Utilizar solamente aplicaciones seguras para poder compartir un enlace.
<i>M.2.8. Permite almacenamiento de información de otras librerías instaladas en el equipo</i>	Se puede unificar la información en esta aplicación para proteger y mantener organizada la información que se encuentra en el dispositivo.	0	1	0	



M.2.9. Permite acceso a la información sin conexión	Se puede visualizar una vista previa del archivo seleccionado sin conexión.	0	1	0	Es importante no marcar para visualizar archivos sin conexión a archivos con información sensible.
M.2.10. Permite visualización de archivos sin necesidad de descarga	Cuando el archivo se encuentra sin conexión no se pueden tener una vista previa del archivo seleccionado.	1	1	1	
M.2.11. Mostrar versiones anteriores en los archivos y visualización de cambios realizados por otros usuarios.	Permite visualizar modificaciones realizadas con anterioridad en un archivo tanto del dueño del documento, así como de las personas a las que les fue compartido el archivo.	1	1	0	Se puede visualizar fecha y hora exacta de modificaciones
M.2.12. Permite una capacidad de almacenamiento de 10GB	Es posible almacenar cualquier tipo de información	1	1	0	En caso de sobrepasar el espacio en esta aplicación, se puede adquirir una licencia premium.
M.2.13. Permite configuración de PIN de acceso a la aplicación		0	0	1	
M.2.14. Permite compartición de información contenida en el repositorio de otros usuarios mediante la generación de un enlace con o sin cifrado	Link sin clave de cifrado: Cualquier persona que tenga acceso a este link puede obtener la información compartida. Clave de cifrado: genera una contraseña segura para poder acceder a la información. Link con clave de cifrado: genera el link de descarga incluido el código para la visualización.	0	1	1	Es recomendable generar el enlace en dos partes: primero el enlace para acceso y luego clave de cifrado para poder acceder al archivo.
M.2.15. Permite compartición de enlaces mediante mensajería instalada en nuestro equipo	Se comparte los enlaces mediante los servicios de mensajería instaladas en el dispositivo.	0	0	1	Sería necesario compartir estos enlaces solamente mediante mensajería segura.
<b>Total</b>		<b>8</b>	<b>9</b>	<b>4</b>	
%		53%	60%	27%	



<b>Herramienta:</b> TLS/ SSL Tunnel			
<b>Escenario:</b> M3 - Comunicación insegura			
<b>Referencia:</b> Anexo B, SECCIÓN 3			
Controles	Resultados	Validado/no Validado	Observaciones
<i>M.3.1. Permite comunicación segura a redes privadas</i>	Permite interconectar dispositivos por medio de protocolos de comunicación remota segura. Esta aplicación crea y abre un túnel y conecta una aplicación con otra a través de un puerto determinado.	1	Este aplicativo crea túneles TLS para comunicación segura
Total		1	
%		100%	

<b>Herramienta:</b> Mobile Secure			
<b>Escenario:</b> M4 - Autenticación insegura -M6 – Autorización Insegura			
<b>Referencia:</b> Anexo B, SECCIÓN 4			
Controles	Resultados	Validado/no Validado	Observaciones
<i>M.4.1. Permite control de acceso a usuario. Privacidad en el manejo de aplicaciones. Control de seguridad en cada una de ellas</i>	Permite controlar el acceso no autorizado a usuarios. Garantiza el correcto funcionamiento en seguridad de cada una de las aplicaciones instaladas en el dispositivo evitando posibles ingresos mal intencionados.	1	
<i>M.4.2. Permite protección de seguimiento, conexiones, navegación y aplicaciones.</i>	Protección de la información en las diferentes acciones que el usuario realice en el dispositivo. Esta es una herramienta gratuita y complementaria que garantiza la seguridad del usuario.	1	Complemento gratuito de la aplicación F-Secure Freedom
Total		2	
%		100%	



<b>Herramienta:</b> Encrypted Data Storage Lite, SSE - Secret Space Encrypt				
<b>Escenario:</b> M5 - Criptografía insuficiente				
<b>Referencia:</b> Anexo B, SECCIÓN 5				
Controles	Resultados	Validado/no Validado		Observaciones
		Encrypted Data Storage Lite	SSE - Secret Space Encrypt	
M.5.1. Realizar la encriptación de un sistema local de archivos disponible en nuestro dispositivo.	Permite la encriptación de documentos que se encuentran almacenados en el dispositivo, además permite encriptar archivos del sistema que sea considerado información sensible por parte del usuario.	1	0	En caso de que la herramienta sea desinstalada del equipo, no se podrá acceder a la información que fue encriptada.
M.5.2. Controlar la organización de la información mediante contenedores	Contenedores son carpetas generales que se crean para almacenar uno o varios archivos a la vez. Un contenedor puede estar almacenado en la memoria interna del dispositivo o en una memoria externa.	0	0	
M.5.3. Ocultar información sensible dentro de los archivos de configuración del sistema a fin de que no sean visibles en caso de robo.	Se puede almacenar la información en la memoria del dispositivo o en una tarjeta interna.	1	0	En caso de almacenamiento o externo es necesario controlar el acceso a esta tarjeta.
M.5.4. Permitir generación de contraseñas seguras, mediante el ingreso de caracteres (letras, números) previstos por el usuario.	El sistema no controla la cantidad de caracteres que se ingresan.	1	0	No se valida si la contraseña es segura o no.
M.5.5. Permitir técnicas de Estenografía (ocultar información en imágenes)	Esta herramienta permite ocultar información dentro de una imagen, se puede asignar o no una contraseña.	0	1	En caso de intentar acceder a la información oculta en una imagen es



				necesario tener instalado en el dispositivo esta herramienta.
<i>M.5.6. Permite encriptación de documentos de texto, archivos multimedia (imagen y video) entre otros mediante contraseñas asignadas.</i>	Permite encriptar uno o varios documentos a la vez mediante contraseñas establecidas.	0	1	Se recomienda utilizar una contraseña fácil de recordar, en caso de olvido no se podrá acceder a estos datos.
<i>M.5.7. Permite almacenamiento de contraseñas en lugares seguros y con encriptación mediante contraseña</i>	Se puede almacenar contraseñas de diferentes servicios que el usuario maneje, protegidas por una clave maestra.	0	1	
<i>M.5.8. Permite la creación de una clave maestra (principal) para acceder a los directorios que contiene la información segura</i>	La creación de esta clave se realiza al iniciar el uso de la aplicación. Se permite el ingreso de letras, números y caracteres especiales.	0	1	
<i>M.5.9. Permite la organización de la información almacenada mediante la creación y el uso de paneles</i>	Mediante los paneles se puede categorizar la información que vamos a almacenar por ejemplo podemos crear paneles para almacenar claves de redes sociales, tarjetas de crédito, claves de acceso a sistemas, entre otros.	0	1	
<i>M.5.10. Encriptar mensajes para envío de información sensible</i>	Es posible encriptar mensajes con contenido personal o privado y enviar a un destinatario. Para esto se puede utilizar mensajería instantánea instalada en el dispositivo. Además se puede establecer una contraseña para poder acceder al mensaje.	0	1	Para que otro usuario pueda visualizar el mensaje recibido en caso de que el mensaje tenga contraseña de acceso éste debe tener instalado el programa en su dispositivo.



M5.11. Generar contraseñas seguras	Esta herramienta permite al usuario crear contraseñas seguras a fin de que los datos del usuario se encuentren totalmente protegidos. Estas contraseñas pueden ser utilizadas en esta aplicación u otros servicios utilizados.	0	1	Es recomendable utilizar frases fáciles de recordar a fin de evitar el olvido de la contraseña generada.
Total		<b>4</b>	<b>7</b>	
%		36%	64%	

Fuente: Elaboración propia.

### c. Conclusión

En esta fase se consideró el paso 6 y paso 7 de la metodología Ms-DisMov.

- ✓ Chequear, monitorear y revisar la Ms-DisMov
- ✓ Actuar, mantener y mejorar la Ms-DisMov

Para la validación final de las herramientas se ha realizado la tabla 22, tabla que muestra los resultados:

Tabla 22: Tabla de resultados

Herramienta	Valoración Controles	Estado
<b>Secure Settings</b>	67%	Parcialmente eficiente
<b>WiSeID</b>	53%	Parcialmente eficiente
<b>Box</b>	60%	Parcialmente eficiente
<b>MEGA</b>	29%	No alcanza los requerimientos de eficiencia
<b>TLS/SSL Tunel</b>	100%	Herramienta eficiente
<b>Mobile Secure</b>	100%	Herramienta eficiente
<b>Secret Space Encrypt</b>	36%	No alcanza los requerimientos de eficiencia
<b>Encrypted Data Storage Lite</b>	64%	Parcialmente eficiente

Fuente: Elaboración propia.

Se concluye que de las 8 herramientas seleccionadas: 2 son eficientes (TLS/SSL Tunel y Mobile Secure) y corresponden al escenario M3, M4-M6; 4 son parcialmente eficientes (Secure Settings, WiSeID, Box Encrypted Data Storage



Lite) y corresponden a los escenarios M1, M2 y M5; 2 herramientas que no alcanzan los requerimientos de eficiencia (MEGA y Secret Space Encryt) y corresponden al escenario M2 y M5.

A continuación se presentan el resumen de la validación de la metodología por cada escenario de OWASP.

a) M1 – Incorrecto uso de plataforma

<b>Ciclo PDCA</b>	
<b>Planear</b>	Búsqueda de herramientas para asegurar las plataformas móviles  <i>*Existen varias herramientas de seguridad que han sido investigadas, se detallan en el Anexo "A", SECCIÓN 1; y el resumen de éstas se observa en la tabla 19.</i>
<b>Hacer</b>	Implementación de herramientas. (La metodología está abierta a la evaluación de N herramientas)  <i>*Dentro de la fase HACER que corresponde a la implementación de herramientas en el presente caso de estudio se utilizaron algunas herramientas clasificadas por cada escenario del Top Ten de Owasp, las mismas que como referencia para la validación de la metodología se las detallaron en el Anexo "B", SECCIÓN 1.</i>
<b>Verificar</b>	V1.- Para la selección de las herramientas, considerar los puntos c) y d) del apartado 'Aspectos clave de la metodología'.  <i>* Para la selección de las herramientas ejemplo se realizó un cuadro comparativo ver tabla 20.</i>  V2.- Evaluación de cada una de las herramientas, mediante pruebas sobre entornos móviles Los controles a evaluar son: ✓ M.1.1. Permite agregar opciones de seguridad para el dispositivo ✓ M.1.2. Permite gestionar un bloqueo automático para proteger la aplicación de accesos no autorizados ✓ M.1.3. Permite ocultar datos sensibles en caso de intentos de acceso al dispositivo  <i>* Para la evaluación de las herramientas ejemplo se realizó un cuadro comparativo ver tabla 21. * Los resultados para determinar si es una herramienta eficiente están en la tabla 22.</i>
<b>Actuar</b>	Repetición del ciclo para validar brechas de seguridad en los aplicativos seleccionados.

b) M2 – Almacenamiento Inseguro de datos

<b>Planear</b>	<p>Búsqueda de herramientas para asegurar el almacenamiento de datos en plataformas móviles</p> <p><i>*Existen varias herramientas de seguridad que han sido investigadas, se detallan en el Anexo "A", SECCIÓN 2; y el resumen de éstas se observa en la tabla 19.</i></p>
<b>Hacer</b>	<p>Implementación de herramientas. (La metodología está abierta a la evaluación de N herramientas)</p> <p><i>* Dentro de la fase HACER que corresponde a la implementación de herramientas en el presente caso de estudio se utilizaron algunas herramientas clasificadas por cada escenario del Top Ten de Owasp, las mismas que como referencia para la validación de la metodología se las detallaron en el Anexo "B", SECCIÓN 2.</i></p>
<b>Verificar</b>	<p>V1.- Para la selección de herramientas para almacenamiento (nativo y en línea), considerar los puntos c) y d) del apartado 'Aspectos clave de la metodología'.</p> <p><i>* Para la selección de las herramientas ejemplo se realizó un cuadro comparativo ver tabla 20.</i></p> <p>V2.- Evaluación de cada una de las herramientas: Los controles a evaluar son:</p> <ul style="list-style-type: none"> <li>✓ M.2.1. Encriptar información (mensajes personales mediante contraseña)</li> <li>✓ M.2.2. Almacenar información mediante contraseña</li> <li>✓ M.2.3. Permite almacenamiento seguro de usuarios y contraseñas de diferentes plataformas</li> <li>✓ M.2.4. Permite bloqueo de acceso a la Información mediante bloqueo (patrón de desbloqueo o pin)</li> <li>✓ M.2.5. Permite acceso mediante interfaz web y aplicación móvil</li> <li>✓ M.2.6. Permite edición conjunta de archivos</li> <li>✓ M.2.7. Permite compartición de Archivos multimedia, de texto, carpetas, etc</li> <li>✓ M.2.8. Permite almacenamiento de información de otras librerías instaladas en el equipo</li> <li>✓ M.2.9. Permite acceso a la información sin conexión</li> <li>✓ M.2.10. Permite visualización de archivos sin necesidad de descarga</li> <li>✓ M.2.11. Mostrar versiones anteriores en los archivos y visualización de cambios realizados por otros usuarios.</li> <li>✓ M.2.12. Permite una capacidad de almacenamiento de 10GB</li> <li>✓ M.2.13. Permite configuración de PIN de acceso a la aplicación</li> <li>✓ M.2.14 Permite compartición de información contenida en el repositorio de otros usuarios mediante la generación de un enlace con o sin cifrado</li> <li>✓ M.2.15. Permite compartición de enlaces mediante mensajería instalada en nuestro equipo</li> </ul> <p><i>* Para la evaluación de las herramientas ejemplo se realizó un cuadro comparativo ver tabla 21.</i></p> <p><i>* Los resultados para determinar si es una herramienta eficiente están en la tabla 22.</i></p>
<b>Actuar</b>	<p>Repetición del ciclo para validar brechas de seguridad en los aplicativos seleccionados.</p>



c) M3 - Comunicación insegura

<b>Planear</b>	Búsqueda de herramientas y protocolos para mejorar la comunicación en dispositivos móviles  <i>*Existen varias herramientas de seguridad que han sido investigadas, se detallan en el Anexo "A", SECCIÓN 3; y el resumen de éstas se observa en la tabla 19.</i>
<b>Hacer</b>	Implementación de herramientas. (La metodología está abierta a la evaluación de N herramientas)  <i>*Dentro de la fase HACER que corresponde a la implementación de herramientas en el presente caso de estudio se utilizaron algunas herramientas clasificadas por cada escenario del Top Ten de Owasp, las mismas que como referencia para la validación de la metodología se las detallaron en el Anexo "B", SECCIÓN 3.</i>
<b>Verificar</b>	V1.- Para la selección de herramientas considerar los puntos c) y d) del apartado 'Aspectos clave de la metodología'.  <i>* Para la selección de las herramientas ejemplo se realizó un cuadro comparativo ver tabla 20.</i>  V2.- Evaluación de cada una de las herramientas Los controles a evaluar son: M.3.1. Permite comunicación segura a redes privadas  <i>* Para la evaluación de las herramientas ejemplo se realizó un cuadro comparativo ver tabla 21.</i> <i>* Los resultados para determinar si es una herramienta eficiente están en la tabla 22.</i>
<b>Actuar</b>	Repetición del ciclo para validar brechas de seguridad en los aplicativos seleccionados. Despliegue de soluciones y repetición del ciclo de implementación.

d) M4 - Autenticación insegura M6 – Autorización Insegura

<b>Planear</b>	Búsqueda de soluciones móviles para asegurar la autenticación y autorización de acceso a usuarios.  <i>*Existen varias herramientas de seguridad que han sido investigadas, se detallan en el Anexo "A", SECCIÓN 4; y el resumen de éstas se observa en la tabla 19.</i>
<b>Hacer</b>	Implementación de herramientas. (La metodología está abierta a la evaluación de N herramientas)  <i>*Dentro de la fase HACER que corresponde a la implementación de herramientas en el presente caso de estudio se utilizaron algunas herramientas clasificadas por cada escenario del Top Ten de</i>



		<i>Owasp, las mismas que como referencia para la validación de la metodología se las detallaron en el Anexo "B", SECCIÓN 4.</i>
<b>Verificar</b>	<p>V1.- Para la selección de las herramientas, considerar los puntos c) y d) del apartado 'Aspectos clave de la metodología'.</p> <p><i>* Para la selección de las herramientas ejemplo se realizó un cuadro comparativo ver tabla 20.</i></p> <p>V2.- Realizar la evaluación de las herramientas Los controles a evaluar son:</p> <ul style="list-style-type: none"> <li>✓ <i>M.4.1. Permite control de acceso a usuarios. Privacidad en el manejo de aplicaciones. Control de seguridad en cada una de ellas</i></li> <li>✓ <i>M.4.2. Permite protección de seguimiento, conexiones, navegación y aplicaciones</i></li> </ul> <p><i>* Para la evaluación de las herramientas ejemplo se realizó un cuadro comparativo ver tabla 21.</i></p> <p><i>* Los resultados para determinar si es una herramienta eficiente están en la tabla 22.</i></p>	
<b>Actuar</b>	<p>Seleccionar el mecanismo más seguro para la autenticación de usuarios. Refinar el ciclo, re-evaluar la implementación y ejecutar los cambios propuestos.</p>	

e) M5 - Criptografía insuficiente

Ciclo PDCA	
<b>Planear</b>	<p>Búsqueda de herramientas que permitan encriptar información en dispositivos móviles.</p> <p><i>*Existen varias herramientas de seguridad que han sido investigadas, se detallan en el Anexo "A", SECCIÓN 5; y el resumen de éstas se observa en la tabla 19.</i></p>
<b>Hacer</b>	<p>Implementación de herramientas. (La metodología está abierta a la evaluación de N herramientas)</p> <p><i>*Dentro de la fase HACER que corresponde a la implementación de herramientas en el presente caso de estudio se utilizaron algunas herramientas clasificadas por cada escenario del Top Ten de Owasp, las mismas que como referencia para la validación de la metodología se las detallaron en el Anexo "B", SECCIÓN 5.</i></p>
<b>Verificar</b>	<p>V1.- Para la selección de las herramientas, considerar los puntos c) y d) del apartado 'Aspectos clave de la metodología'.</p> <p><i>* Para la selección de las herramientas ejemplo se realizó un cuadro comparativo ver tabla 20.</i></p> <p>V2.- Evaluación de cada una de las herramientas, mediante pruebas sobre entornos móviles Controles a evaluar son:</p> <ul style="list-style-type: none"> <li>✓ <i>M.5.1. Realizar la encriptación de un sistema local de archivos disponible en nuestro dispositivo.</i></li> <li>✓ <i>M.5.2. Controlar la organización de la información mediante contenedores</i></li> </ul>



	<ul style="list-style-type: none"> <li>✓ M5.3. Ocultar información sensible dentro de los archivos de configuración del sistema a fin de que no sean visibles en caso de robo.</li> <li>✓ M.5.4. Permite generación de contraseñas seguras, mediante en ingreso de caracteres (letras, números) previstos por el usuario.</li> <li>✓ M.5.5. Permite técnicas de Estenografía (ocultar información en imágenes)</li> <li>✓ M.5.6. Permite encriptación de documentos de texto, archivos multimedia (imagen y video) entre otros mediante contraseñas asignadas</li> <li>✓ M.5.7. Permite almacenamiento de contraseñas en lugares seguros y con encriptación mediante contraseña</li> <li>✓ M.5.8. Permite la creación de una clave maestra (principal) para acceder a los directorios que contiene la información segura</li> <li>✓ M.5.9. Permite la organización de la información almacenada mediante la creación y el uso de paneles</li> <li>✓ M.5.10. Encriptar mensajes para envío de información sensible</li> <li>✓ M.5.11. Generar contraseñas seguras.</li> </ul> <p style="text-align: center;">* Para la evaluación de las herramientas ejemplo se realizó un cuadro comparativo ver tabla 21. * Los resultados para determinar si es una herramienta eficiente están en la tabla 22.</p>
<b>Actuar</b>	<p>Selección de los mejores mecanismos para encriptar información en dispositivos móviles. Ejecución de niveles de personalización de herramientas, repetición del ciclo.</p>

Finalmente se plantean buenas prácticas (ver tabla 23), para cada uno de los escenarios de vulnerabilidades establecidos y que puedan ser seguidos por los usuarios.

Tabla 23: Buenas prácticas

<b>OWASP</b>	<b>BUENAS PRÁCTICAS</b>
<p><b>M1</b> – Incorrecto uso de la plataforma</p>	<ul style="list-style-type: none"> <li>✓ En este escenario se cubre el mal uso de una función de plataforma o falta de uso de los controles de seguridad de la plataforma, para estos casos los usuarios deberían incluir controles que les permitan:</li> <li>✓ Establecer una opción de seguridad para el acceso al dispositivo, podría ser un código pin, contraseña, patrón, desbloqueo facial, huella dactilar, considerando que cada uno de estas opciones tiene sus fortalezas y debilidades.</li> <li>✓ Configurar un número de intentos fallidos antes de bloquear por un tiempo o totalmente el dispositivo por completo, en un escenario de olvido o pérdida del dispositivo.</li> <li>✓ Determinar permisos específicos a las aplicaciones que instalamos en el dispositivo, tomando en cuenta consideraciones generales como: si es un aplicativo de linterna no me tendría que pedir acceso a mis contactos o a la cámara.</li> <li>✓ Estas buenas prácticas pueden ser llevadas a cabo con la ayuda de la herramienta seleccionada en la presente investigación.</li> </ul>
<p><b>M2</b> – Almacenamiento inseguro de datos</p>	<ul style="list-style-type: none"> <li>✓ Para este escenario debemos considerar los problemas referentes a como se está almacenando la información nuestra en el celular, recordando que se genera gran cantidad en todas las aplicaciones que usamos y mucha de esta información puede ser considerada confidencial de cada persona y se podría estar exponiendo sin que lo sepamos, para ello debemos considerar las siguientes recomendaciones:</li> </ul>



	<ul style="list-style-type: none"> <li>✓ Almacenar la información sensible encriptada, es decir deberíamos clasificar la información que manejamos en nuestro dispositivo móvil y con la más crítica proceder a encriptarla, para que no sea de fácil acceso por terceros.</li> <li>✓ Se debería establecer un acceso por contraseña para la información sensible, adicionando de esta manera un control para evitar que esta información sea accedida por error cuando prestamos o perdimos nuestro dispositivo móvil.</li> <li>✓ Establecer contenedores seguros de información a través del uso de una herramienta adicional, como recomienda la metodología, la cual permita dar acceso a información confidencial como usuarios y contraseñas.</li> </ul>
<p><b>M3 –</b> Comunicación insegura</p>	<ul style="list-style-type: none"> <li>✓ Para este escenario se plantea los problemas de seguridad derivados del uso de protocolos inseguros para la comunicación entre el dispositivo móvil y los servidores de servicios que usan las diferentes aplicaciones instaladas y que usamos, permitiendo a terceros acceder a nuestra información haciendo interceptación de datos en el medio de comunicación, que al ser el espectro es muy fácil de interceptar, para este tipo de escenarios se debe considerar:</li> <li>✓ Utilizar aplicaciones que creen un túnel de datos TLS/SSL, el cual permita tener acceso a dispositivos e información en forma remota de manera segura, al impedir que terceros al interceptar el tráfico puedan identificar la información y conexiones existentes en el túnel, ya que estas viajan cifradas.</li> <li>✓ No se debe utilizar conexiones abiertas de comunicación como wifi de aeropuertos o lugares públicos de manera directa, ya que toda la información que viaja en esa conexión podría ser interceptada y vulnerada nuestra confidencialidad, integridad, para esto se debe hacer uso de las mismas a través de aplicaciones que creen túneles de comunicación cifrados.</li> <li>✓ Se debe actualizar los métodos y protocolos de comunicación y cifrado de nuestras conexiones, en especial aquellos en los que información delicada se vaya a transmitir por medio del dispositivo móvil.</li> </ul>
<p><b>M4</b> - Autenticación insegura - <b>M6</b> - Autorización insegura</p>	<ul style="list-style-type: none"> <li>✓ Dentro del escenario de autenticación insegura se establece vulnerabilidades que al explotarse pueden permitir a un tercero, sea software o un individuo el poder hacerse pasar por un usuario válido del sistema o de las aplicaciones y acceder a nuestra información, para este tipo de casos se debe considerar las siguientes observaciones:</li> <li>✓ Verificar los permisos de las aplicaciones del dispositivo, estableciendo si se usa una sesión para identificar en todo momento quien está accediendo a que información, permitiéndonos rastrear un acceso no autorizado.</li> <li>✓ Implementar controles de acceso específicos para cada aplicación que gestione información sensible en el dispositivo.</li> <li>✓ El establecer un control de acceso, que limite el uso del dispositivo a personas no autorizadas, pidiendo ingresar una contraseña, patrón de desbloqueo, o huella dactilar y de no poder ingresar esta información, se proceda a un bloqueo total del dispositivo.</li> </ul>
<p><b>M5</b> - Criptografía insuficiente</p>	<ul style="list-style-type: none"> <li>✓ El escenario de criptografía insuficiente plantea vulnerabilidades que podrían ser imperceptibles para un usuario tradicional, ya que se refiere a problemas con la criptografía, en sus métodos o aplicación y que por ende no permite que nuestra información este almacenada de manera segura, al contrario de lo que pensaríamos a usar un aplicativo para encriptación de la información sensible, para estos casos se puede recomendar las siguientes acciones:</li> <li>✓ Utilizar herramientas de encriptación actualizadas y legales, las cuales permitan poder resguardar nuestra información importante de manera segura.</li> </ul>



	<ul style="list-style-type: none"><li>✓ Cada archivo que se considere información sensible del usuario debe estar en un contenedor seguro encriptado.</li><li>✓ No olvidar las claves de encriptación de los diferentes archivos que se guarden en el dispositivo, ya que la mayoría de herramientas no cuentan con procesos de recuperación de las mismas.</li><li>✓ Se puede verificar no tener aplicaciones maliciosas en nuestro dispositivo móvil, las cuales pudieran estar tratando de acceder a nuestra información encriptada.</li><li>✓ Siguiendo estos consejos se podrá mantener un nivel de seguridad aceptable en nuestro dispositivo móvil, pero como la tecnología avanza a diario es importante estarnos informando y capacitando a cada momento en los temas de seguridad de la información.</li></ul>
--	--



### 3. Conclusiones y Recomendaciones

#### 3.1. Conclusiones

- ✓ Actualmente no existe una metodología, que sirva de guía para la selección de herramientas, para dispositivos móviles en cuanto a seguridad de información que fusione la norma ISO 27001 con los escenarios de riesgos del Top Ten de OWASP, es por eso que en el presente proyecto se plantea la definición de Ms-DisMov, que permitirá suplir la falencia expuesta.
- ✓ La metodología Ms-DisMov, diseñada para la selección de herramientas para seguridad de información en dispositivos móviles, se basa en la ISO 27001 referente de seguridad a nivel mundial y en el OWASP Top Ten Mobile 2016, dándonos una perspectiva más amplia de la seguridad de la información y un alcance planteado a nivel de dispositivos móviles.
- ✓ La metodología Ms-DisMov está basada en el ciclo PDCA adaptado a la Norma ISO 27001 que es un estándar internacional de seguridad, para el establecimiento, implementación y mejoramiento continuo de SGSI en entornos móviles y que se ejecutará en cada uno de los escenarios del Top Ten Mobile 2016 de OWASP.
- ✓ Al implementar la metodología planteada en el presente trabajo se fusiona la ISO 27001 (Gestión de seguridad de la información) y el OWASP Top Ten Mobile 2016 (10 Riesgos de Seguridad en dispositivos móviles) lo cual permitió hacer un análisis general de la



---

seguridad de la información y cruzarla con los riesgos identificados en móviles a nivel mundial por el trabajo de OWASP, permitiendo armonizar las dos tendencias en una base sólida para armar la metodología aquí propuesta.

- ✓ Los escenarios de vulnerabilidades planteados para su evaluación se pueden explotar en un entorno móvil con sistema operativo Android sin la necesidad de requerir un conocimiento alto de programación o tecnología en general, esto debido al alto índice de penetración que posee este tipo de tecnologías y al elevado número de herramientas automatizadas de explotación de vulnerabilidades que se encuentran en internet hoy en día.
- ✓ Se requiere el uso de herramientas o configuraciones adicionales en los dispositivos móviles para evitar la explotación de las vulnerabilidades detectadas en este tipo de entornos, algunas herramientas se analizaron en el presente trabajo siendo de libre acceso a través del Google play algunas teniendo un costo y sin costo de licenciamiento y se presenta su correspondiente configuración para evitar ser víctimas de los riesgos descritos.
- ✓ La metodología de acuerdo a su estructura se adapta para trabajar con cualquier herramienta que se alinee con los escenarios del OWASP Top Ten Mobile 2016.



- 
- ✓ Se establece que el uso de herramientas adicionales puede ayudar a evitar la explotación de vulnerabilidades presentes en los entornos Android.
  - ✓ Al ser Android un entorno cambiante, podría cambiar el resultado obtenido en estas pruebas en función de la versión instalada en cada dispositivo.
  - ✓ Algunas herramientas presentan una interfaz muy intuitiva y de fácil uso, como WiseID, facilitando el proceso de adopción de las mismas al diario uso, mientras que otras herramientas se dificulta su utilización ya que intervienen conceptos técnicos que no son de conocimiento general de todo tipo de usuarios tal es el caso de Secure Settings.
  - ✓ Al ser los dispositivos móviles de uso cotidiano y parte de nuestro diario vivir, somos más propensos a ser víctimas de robo de nuestra información y que esto ocurra sin darnos cuenta, debido a que en él se encuentran muchas aplicaciones, conexiones de red y datos que podrían estar abiertas incluso cuando nosotros no estuviéramos usando el dispositivo.



### 3.2. Recomendaciones

- ✓ Como usuarios de sistemas informáticos debemos estar conscientes de que las medidas de seguridad comprenden un conjunto de elementos que no puede dejarse de lado ninguno de ellos como son hardware, software, comunicaciones, así como controles organizativos y legales de la organización.
- ✓ Como profesionales de la Informática es importante conocer por lo menos elementos básicos a cerca de la seguridad de la información, para tener una idea de qué tan seguro es el dispositivo móvil que usamos a diario.
- ✓ Es necesario que las herramientas que se someterán a una evaluación mediante la metodología planteada, tengan características que pueden cumplir o suplir los escenarios seleccionados del OWASP Top Ten Mobile 2016.
- ✓ Se recomienda el uso de herramientas libres y pago principalmente las segundas ya que de éstas se puede explotar todas sus características.
- ✓ Establecer una actualización de las vulnerabilidades definidas en los dispositivos móviles con una periodicidad mínima de 12 meses, que es el tiempo promedio para que se actualice el hardware un dispositivo y también el software base.



- ✓ Verificar que en función de los cambios producto de la personalización del sistema operativo base Android, algunas vulnerabilidades han sido cubiertas por parches de actualización de cada fabricante del dispositivo.
- ✓ Ampliar la investigación en otros proyectos que permitan evaluar condiciones como la programación del software que usan los dispositivos móviles y de los cuales se desprenden algunas vulnerabilidades que han quedado fuera del alcance del presente trabajo.
- ✓ Desarrollar aplicaciones que permitan al usuario final de una manera más sencilla auto configurar los controles necesarios para evitar la explotación de las vulnerabilidades descritas.
- ✓ Se recomienda ir actualizando los resultados de las pruebas efectuadas conforme se tenga una nueva versión de los aplicativos y del sistema operativo base.
- ✓ Establecer mecanismos de unificación de resultados en las pruebas que se ejecuten en dispositivos móviles con sistema operativo Android y que contengan una capa de personalización tipo touchwiz, miui, sense.
- ✓ Existe mucha información en diferentes sitios y foros de internet acerca de los peligros en dispositivos móviles, por citar algunos <http://www.hackplayers.com>,  
<https://www.osi.es/es/actualidad/blog>, <https://www.adslzone.net/forum>



---

111.html, pero al ser de corte geek/técnico estos sitios no brindan una información clara y en un lenguaje natural para que pueda ser fácilmente accedido y comprendido por cualquier tipo de usuario.

- ✓ Crear campañas de concientización en los usuarios finales para que conozcan sobre las vulnerabilidades que sufren los dispositivos móviles y como pueden protegerse de ellas.



#### 4. Referencias

- Adams, A. A. (2016). Possessing Mobile Devices. *Journal in Computing Edge*, 2(February), 17–23.
- ASENCIOS, R. C., & PONTIFICIA. (2013). DOCUMENTO DE INVESTIGACION Y CLASIFICACION DE ATAQUES DE SEGURIDAD A LA PLATAFORMA ANDROID 4.1 SEGÚN PRINCIPIOS DE SEGURIDAD DE LA INFORMACION.
- Becher, M. (2009). Security of Smartphones at the Dawn of their Ubiquitousness. article.
- Bertino, E. (2016). Securing Mobile Applications. *Journal in Computing Edge*, 2(March), 4.
- Biom, D., Gerencia, P., Seguridad, I., TecnoI, R., & Electr, V. (2012). Leyes de protección de datos personales en el mundo y la protección de datos biométricos Parte 2. *Seguridad Cultura de Prevención Para TI.*, 14(1), 4–9.
- Bishop M. (2004). *Introduction to Computer Security* (Addison We). book.
- BOX. (2016). Sus archivos en cualquier dispositivo, desde cualquier lugar. misc.
- Calvo-Manzano, J., Cuevas, G., Muñoz, M., & San Feliu, T. (2008). Process similarity study: Case study on project planning practices based on CMMI-DEV v1. 2. *Proc. EuroSPI*. article.
- Carver, K., Sritapan, V., & Corbett, C. (2016). Establishing and Maintaining Trust in a Mobile Device. *Journal in Computing Edge*, 2(February), 14–16.
- CISCO. (2016). Release Notes for Cisco AnyConnect Secure Mobility Client, Release 4.3. misc.
- Costas, S. J. (2011). *Seguridad Informática* (Ediciones). Bogotá.
- Dwivedi, H., Clark, C., & Thiel, D. (2014). *Mobile Application Security*. *Computer* (Vol. 47). book. <https://doi.org/10.1109/MC.2014.156>
- EOI. (2016). ESCUELA DE ORGANIZACIÓN INDUSTRIAL.
- ESET. (2014). Enjoy Safere Technology. misc. Retrieved from [www.eset.es](http://www.eset.es)
- Flynn, L., & Klieber, W. (2016). Smartphone Security. *Journal in Computing Edge*, 2(February), 8–12.
- Gasca, G. (2010). Estudio de Similitud del Proceso de Gestión de Riesgos en Proyectos de Outsourcing de Software: Utilización de un Método. *Revista Ingenierías Universidad de Medellín*, 9, 119–129.
- Gendrullis Timo. (2008). A real-world attack breaking A5/1 within hours, 266–282. article. Retrieved from [http://link.springer.com/chapter/10.1007/978-3-540-85053-3\\_17](http://link.springer.com/chapter/10.1007/978-3-540-85053-3_17)
- Giesecke & Devrient GmbH. (2016). TSM de TEE: Protección de datos e integridad de dispositivos más inteligentes en la era de las aplicaciones para móviles.
- Gittleson, K. (2014). Data-stealing Snoopy drone unveiled at Black Hat. article. Retrieved from <http://www.bbc.com/news/technology-26762198>
- GUZMÁN, J. W. A. Z. Y. S. E. L. (2015). ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL Facultad de Ingeniería en Electricidad y Computación “ ANÁLISIS DE LA IMPLEMENTACIÓN DEL GOBIERNO Previa a la obtención del título : INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES Presentado por : Jonathan Wladimir. Retrieved from <http://www.dspace.espol.edu.ec/xmlui/bitstream/handle/123456789/30146/D-84662.pdf?sequence=1&isAllowed=y>
- Huerta, A. V. (2002). SEGURIDAD EN UNIX Y REDES. Retrieved from <https://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node372.html>
- Hurlburt, G. (2016). “Good Enough” Security: The Best We’ll Ever Have. *Journal in Computing Edge*, 2(November), 10–13.
- IICS. (2012). Cyber Security. misc. Retrieved from



- <https://iicybersecurity.wordpress.com/2013/12/03/>  
Institute, E. T. S. (2011). "3GPP Confidentiality and Integrity Algorithms & UEA1 UIA1." misc. Retrieved from <http://www.etsi.org/index.php/services/security-algorithms/3gpp-algorithms>
- IntangibleObjects. (2016). Secure Settings is a Locale/Tasker. misc.
- ISACA. (2012). *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*.
- ISO/IEC 27001. (2005). Estandar Internacional ISO / IEC 27001, 2005, 41. article. Retrieved from <https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf>
- ISO/IEC 27001. (2012). ISO 27000. misc. Retrieved from <http://www.iso27000.es/iso27000.html>
- ISO -International Organization for Standardization. (2011). Familias de las Normas ISO 27000, 19. article.
- Jøsang, A., Miralabé, L., & Dallot, L. (2015). Vulnerability by Design in Mobile Network Security \*, 14(4). article.
- Kasmi C, L. E. J. (2015). IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones. misc. Retrieved from <http://ieeexplore.ieee.org/document/7194754?reload=true&arnumber=7194754>
- Kosutic, D. (2017). Academy27001. Retrieved from <https://advisera.com/27001academy/es/knowledgebase/resumen-del-anexo-a-de-la-norma-iso-270012013/>
- Lemos, R. (2002). "New laws make hacking a black-and-white choice." misc. Retrieved from <https://www.cnet.com/topics/tech-industry/>
- Ling, Z., Luo, J., Chen, Q., Yue, Q., Yang, M., Yu, W., & Fu, X. (2016). Secure fingertip mouse for mobile devices. *Proceedings - IEEE INFOCOM, 2016-July*. article. <https://doi.org/10.1109/INFOCOM.2016.7524368>
- Lookout. (2016). Lookout. misc. Retrieved from <https://blog.lookout.com/blog/2013/02/07/security-alert-cleanedout/>
- López, M. J. L. (2011). *Criptografía y Seguridad de Computadores*. Jaen.
- Marcos, M., Bedón, S., Utrilla, J. T., & Ortega, J. R. (2012). Un Proceso Práctico de Análisis de Riesgos de Activos de Información Estándar Australiano.
- Memon, A. M., & Anwar, A. (2016). Tomorrow's Mobile Malware Threat. *Journal in Computing Edge*, 2(March), 31–35.
- Mikko. (2016). F-Secure. misc. Retrieved from [https://www.f-secure.com/v-descs/trojan\[\\_\]android\[\\_\]fakeinst.shtml](https://www.f-secure.com/v-descs/trojan[_]android[_]fakeinst.shtml)
- mSeven Software LLC. (2016). mSecure: Complete protection on any device. misc.
- Mulliner, C. (2006). Security of Smart Phones. *Department of Computer Science, Master's T*(June). article.
- NIST. (2012). Guide for conducting risk assessments, (September), 95. article. <https://doi.org/10.6028/NIST.SP.800-30r1>
- OBP. (2013). Online Browsing Platform. article. Retrieved from <https://www.iso.org/obp/ui/{#}iso:std:iso-iec:27001:ed-2:v1:en>
- Olson, P. (2013). "Your smartphone is hackers' next big target." misc. Retrieved from <http://edition.cnn.com/2013/08/26/opinion/olson-mobile-hackers/index.html>
- OWASP. (2016). Mobile Top 10 2016-Top 10. misc. Retrieved from [https://www.owasp.org/index.php/Mobile\\_Top\\_10\\_2016-Top\\_10](https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10)
- Paranoia Works. (2016). Secret Space Encryptor for Android. misc.
- PCWorld. (2013). PCWorld España.
- Quintana, A. D. D. (2016). Relationship between computer viruses (malware) and attacks vulnerable countries using computer security with Principal Component Analysis (PCA), 1–11.
- Riesgos, D. E., & Villafuerte, J. R. (2014). DISEÑO DE UN SISTEMA DE GESTIÓN



---

DE SEGURIDAD DE INFORMACIÓN PARA UNA CENTRAL PRIVADA DE  
INFORMACIÓN DE RIESGOS, 1–57.

- Rouse, M. (2016). Storage Encryption. misc.
- Ruggiero, P., & Foote, J. (2011). Cyber Threats to Mobile Phones, 1–6.
- Saltzer, J. H., Reed, D. P., Clark, D. D., & Science, C. (1991). END-TO-END ARGUMENTS IN SYSTEM DESIGN, 509–512.
- Secure, S. (2016). AuthControl, Intelligent authentication made easy. misc.
- Siemens. (2010). “Series M Siemens SMS DoS Vulnerability.” article. Retrieved from <http://www.securityfocus.com/bid/7004/>
- Small-Apps. (2016). Small-Apps: TLS/SSL Tunnel Communication. misc.
- Softland. (2016). AirCover Security1.5.1. misc.
- Sonelli Ltd. (2016). JuiceSSH - Free SSH client for Android. misc.
- Sovworks. (2016). EDS Program feautres. misc.
- Swivel Secure Ltd. (2013). Autenticación basada en aplicación móvil.
- Symantec. (2016). Symantec. misc. Retrieved from <https://www.symantec.com/security{ }response/writeup.jsp?docid=2011-121306-2304-99>
- Töyssy, Sampo; Helenius, M. (2006). “About malicious software in smartphones.” *Journal in Computer Virology. Springer Paris*, 2, 109–119. article.
- WISeKey SA. (2016). Securing mobile communications and storage for individuals and businesses. misc.



## 5. Anexos

### 5.1. ANEXO A: HERRAMIENTAS

#### 5.1.1. SECCIÓN 1 – Incorrecto uso de la plataforma

**Nombre:** mSecure

**Descripción:**

Protección completa para dispositivos móviles, protección de contraseñas almacenadas en memoria o en archivos de autenticación en contra de vulnerabilidades o ataques que puedan poner en riesgo la información del dispositivo.

Garantiza la seguridad de todas las operaciones realizadas en dispositivos móviles, puesto que asegura el almacenamiento, administración y publicación de información sensible (como contraseñas y datos personales, números de cuenta, etc.), el método utilizado es la codificación por métodos externos (blowfish de 256 bits) para proteger esta información (mSeven Software LLC, 2016).

**Características:**

- Bloqueo automático para proteger la aplicación de intrusos
- Generador de contraseñas de acceso
- Sincronización en la nube (arquitectura orientada a servicios en la nube)
- Copias de seguridad para respaldo de información sensible
- Autodestrucción opcional en casos de hackeo o intento de hackeo
- Opciones que permite ocultar datos sensibles en caso de intentos de acceso al dispositivo
- Bloqueo remoto de los datos en la nube (autodestrucción en casos extremos)
- Navegador de Internet ultra seguro para asegurar transacciones en Internet
- Facilidad de configuración y uso

**Costo:** \$9,99

**Nombre:** Secure Settings

**Descripción:**

Plugin que permite agregar opciones de seguridad para Android desde la versión 2.2 y superiores, gestionando el sistema de una forma más apropiada y garantizando la seguridad en todas las transacciones tanto internas como externas, que se puedan realizar en los aplicativos (IntangibleObjects, 2016).

**Características:**

- Corrige errores y asegura intentos fallidos de autenticación



- Creación de accesos rápidos a Google Now
- Gestión eficiente de llamadas salientes
- Generación de códigos secretos
- Aseguramiento de la seguridad de un dispositivo Android (desde la versión 2.2 y superiores) cuando está en modo Avión
- Agregar seguridad a la transmisión y emparejamiento Bluetooth
- Habilitar y deshabilitar el modo Keyguard
- Agregar seguridad para el uso de la cámara del dispositivo
- Habilitar opciones de administración en modalidad root
- Gestión segura de acciones administrativas en el dispositivo
- Gestión personalizable de todos los sensores y dispositivos del terminal Android
- Habilitar y deshabilitar opciones de ABD
- Gestión segura de permisos para acceso al dispositivo

**Costo:** Gratuita (con publicidad)

**Nombre:** AirCover Security Suite

**Descripción:**

Aplicación que ofrece un conjunto de servicios para proteger los datos personales de un usuario, gestión de notificaciones y alertas en caso de incursiones no deseadas, además de ofrecer protección contra pérdidas, copias de seguridad y bloqueos remotos, además de una completa sincronización de datos en la nube, protección de llamadas entrantes y salientes (bloqueo de llamadas y mensajes de texto), monitoreo de aplicaciones potencialmente peligrosas, etc. (Softland, 2016).

**Características:**

- **Seguridad móvil:**
  - **Check – up** que por medio de un clic permite proteger el sistema en contra de virus, malware, spyware y cualquier tipo de amenaza como troyanos y gusanos
  - **Antivirus:** El aplicativo está dotado de un potente escáner removedor de virus para Android que además tiene protección en tiempo real
  - **Protección web:** Escudo protector en contra de páginas Phishing, fraudulentas o sitios con malware, además de protección para el navegador para la realización de operaciones financieras
- **Seguridad familiar:**
  - Creación de perfiles que le permiten al usuario enviar alertas mediante correo electrónico y avisos mediante ventanas emergentes, en caso de eventualidades, el mensaje envía la ubicación del dispositivo mediante un correo electrónico
- **Copias de seguridad en la nube:**



- Permite realizar copias de seguridad en la nube de todos los datos del dispositivo
- Almacenamiento personalizado de contactos y contenido del dispositivo
- **Localizador antirrobo:**
  - Localización por medio de un portal web del dispositivo a través del GPS de la unidad
  - Respaldo de contactos, mensajes y datos sensibles
  - Emisión de sonidos de alarma para identificar el dispositivo
  - Alerta de intrusión para protección de información personal (fotos, mensajes, contactos, llamadas, etc.)
  - Borrado remoto de toda la información del teléfono en casos extremos
  - Monitoreo de la tarjeta sim que envía un correo electrónico con la información de una nueva tarjeta SIM en caso de reemplazo de la tarjeta del propietario del teléfono
- **Optimización de sistema y batería**
  - Gestionar tareas del sistema
  - Gestión de memoria RAM
  - Cerrar aplicaciones en segundo plano
  - Eliminar archivos temporales
  - Reportes de carga, descarga y temperatura de la batería

**Costo:** Aplicativo gratuito (servicios en la nube hasta 2 GB gratuito, y de pago \$24,99 al año)

### 5.1.2. SECCIÓN 2 – Almacenamiento inseguro de datos

**Nombre:** WISeID

**Descripción:** permite a los usuarios almacenar información en un formato cifrado que utiliza un estándar de bitencripción de 256 de forma local en los dispositivos móviles (WISeKey SA, 2016).

**Características:**

- El almacenamiento local evitar un alto porcentaje de violación de datos
- WISeID no almacena información en servidores propios, ya que estos pueden ser comprometidos por ataques a los sistemas de la herramienta.
- Para que un hacker pueda comprometer la información almacenada localmente, este tendría vulnerar al dispositivo móvil y luego a la aplicación.
- La aplicación está protegida por una contraseña maestra que el usuario creará para acceder a los archivos almacenados
- Dentro de las características de las contraseñas, la herramienta brinda la opción de patrones de reconocimiento facial



- La aplicación además permite a los usuarios proteger documentos con contraseñas individuales, los que son de contraseñas compartidas, es decir se puede enviar documentos o fotos o cualquier otro archivo cifrado y que requiera una clave de descifrado.

**Costo:** Gratuita

**Nombre:** Box

**Descripción:** es una herramienta independiente con una oferta buena de servicios en la nube que permite compartir los contenidos almacenados y trabajar de forma conjunta.

Box también cuenta con opciones multiplataforma que hacen que sea fácil acceder al servicio desde prácticamente cualquier equipo conectado. En concreto, los usuarios con Mac Windows, Android, iOS, Windows Phone o BlackBerry pueden hacer uso de esta plataforma (BOX, 2016).

**Características de manera General (BOX, 2016):**

- **Trabajo disponible**
  - Permite compartir de manera segura archivos de gran tamaño con un simple enlace o URL, además controla el acceso a estos archivos con niveles de seguridad en contraseñas establecidos.
  - Facilita el trabajo en conjunto por lo tanto también permite obtener la última versión de los archivos, además de guardar las versiones anteriores.
  - Permite realizar vistas previas de los archivos sin descargarlos
- **Mantiene Informados a todos los miembros del equipo**
  - Al centralizar los archivos permite al equipo tener un solo lugar para compartir, editar, analizar y aprobar archivos. Además, cuando se realizan ediciones, las notificaciones en tiempo real lo mantienen informado.
  - Permite trabajar a un conjunto de usuarios sobre un mismo documento al mismo tiempo.
  - Facilita realizar una gestión de proyectos (establecer fechas, asignar tareas, etc.)
- **Simplifique los procesos gracias a la automatización**
  - Posee un proceso definido principalmente para aprobación de ingreso de nuevos miembros en el equipo y aprobación de documentos.
  - Permite detectar actividades sospechosas de usuario desconocidos.
- **Movilidad:**
  - Permite llevar los archivos a cualquier lugar.
  - Ver y compartir archivos, en línea o sin conexión.
  - Compartir archivos de manera segura con su equipo, clientes o agencias externas en cualquier dispositivo con la aplicación de Box para dispositivos móviles.
  - Permite realizar búsquedas rápidas en los documentos.

- **Seguridad**

- Permite gestionar de manera simple las políticas de accesos y uso compartido dentro y fuera de la empresa.
- Asegura la confidencialidad e integridad de sus archivos con el cifrado para contenido en tránsito y en reposo, con la opción de claves de cifrado gestionadas por el cliente.
- Utiliza varios centros de datos con recursos energéticos y sistemas de respaldo confiables para ofrecer un 99,9 % de acuerdos de nivel de servicio (SLA) y redundancia.
- Box también respalda a los clientes globales con ISO 27001, ISO27018, SOC 1 (SSAE 16), PCI DSS, FedRamp y el almacenamiento de datos en la región en Europa y Asia.

**Costo y Capacidades (BOX, 2016):**

- **Planes Personales**

- **Gratis**
  - Almacenamiento de 10 GB
  - Límite de carga de archivos 250 MB (por archivo)
- **Personal Pro**
  - \$11.50 mensual
  - Almacenamiento de 100 GB
  - Límite de carga de archivos 5 GB (por archivo)

- **Planes Business**

- **Starter**
  - \$6.00 por usuario/mensual
  - Requiere un mínimo de 3 usuarios y un máximo de 10 usuarios
  - 100 GB de almacenamiento seguro
  - Límite de carga de archivos de 2 GB
  - Acceso móvil
  - Sincronización del escritorio
  - Control de versiones de los archivos
  - Cifrado SSL y en reposo
  - Autenticación de dos factores
  - Gestión del usuario
  - Soporte estándar para la empresa
  - Acceso a la API de Box: 25 000 acciones mensuales
- **Business**
  - \$17.00 por usuario/mensual
  - Incluye todas las funciones de Starter, más:
  - Requiere un mínimo de 3 usuarios
  - Almacenamiento ilimitado
  - Límite de carga de archivos de 5 GB
  - Integración con inicio de sesión único (SSO)
  - Creación de informes de seguridad y de usuario avanzado
  - Marcas personalizadas



- Controles de seguridad móvil
- Integraciones con proveedores de EMM
- Prevención de la pérdida de datos (DLP)
- Acceso a la API de Box: 50 000 acciones mensuales

**Nombre:** MEGA

**Descripción:** es un servicio seguro de almacenamiento en la nube, que permite que los datos sean cifrados y descifrados solamente por los dispositivos de los propietarios y no por el equipo que conforma MEGA.

**Características:**

- Encriptado Punto a punto
  - Consiste en darle el control del encriptado a los usuarios, es decir: “tú tienes control sobre el encriptado, tú tienes las claves y tú decides a quién dar o denegar acceso a tus archivos, sin necesitar instalaciones de software peligroso”
- Acceso Global
  - Los datos están disponibles en cualquier momento, desde cualquier dispositivo.
  - Proporciona almacenamiento fiable en la nube con un nivel de privacidad adecuado y siempre activo.
- Colaboración segura
  - Permite compartir contenido con los contactos y permite ver las actualizaciones en tiempo real.

**Costo y Capacidades:**

- Suscripción PRO LITE: \$5,50 al mes o \$55,22 al año
  - 200 GB de espacio de almacenamiento
  - 1 TB de ancho de banda al mes.
- Suscripción PRO I: \$11,03 al mes o \$110,45 al año
  - 500 GB de espacio de almacenamiento
  - 2 TB de ancho de banda al mes.
- Suscripción PRO II: \$22,08 al mes o 220,91 € al año
  - 2 TB de espacio de almacenamiento
  - 4 TB de ancho de banda al mes.
- Suscripción PRO III: \$33,12 al mes o \$331,38 al año
  - 4 TB de espacio de almacenamiento
  - 8 TB de ancho de banda al mes.

### 5.1.3. SECCIÓN 3 – Comunicación insegura

**Nombre:** TLS/SSL Tunnel

**Descripción:**

Aplicativo que permite mejorar la seguridad de las conexiones TLS entre terminales Android, asegurando así las comunicaciones entre aplicaciones. Esta



aplicación crea y abre un túnel y conecta una aplicación con otra a través de un puerto determinado. Se puede utilizar certificados CAcert y soporta servicios TLS remotos

A través del túnel se puede comunicar múltiples aplicaciones entre dispositivos (se requiere conexión a Internet para la verificación de los certificados digitales TLS/SSL) (Small-Apps, 2016).

#### **Características:**

- Gestión de certificados por medio de llaves públicas y privadas
- Gestión de aplicativos de comunicación
- No requiere permiso Root en las terminales Android
- Importación de certificados desde el aplicativo
- Gestión de certificados personalizados mediante almacenes de certificados
- Gestión remota de certificados personalizados
- Opciones de encriptación de datos mediante "Force AES"
- Uso de protocolos SSLVPN para gestión de túneles
- Gestión automática de reconexiones

**Costo:** Freeware (con publicidad)

**Herramienta:** JuicesSSH

#### **Descripción:**

Terminal para Android que permite interconectar dispositivos por medio de protocolos de comunicación remota incluyendo SSH, Shell local, Mosh y Telnet (Sonelli Ltd., 2016).

#### **Características:**

- Cliente/Terminal SSH
- Uso de métodos abreviados para acceso al aplicativo
- Mensajes de teclado para encontrar características personalizadas
- Soporte para dispositivos externos
- Gestos para IRSSI, Weechat, Tmux
- Uso de plugins externos
- Soporte para comunicación por SSH, Telnet, Mosh, Shell local
- Soporte para almacenamiento de configuraciones y sesiones
- Soporte IPv6
- Soporte para claves públicas y privadas
- Soporte para claves privadas OpenSSH (ECDSA, RSA, DSA)
- Generador de claves RSA (con cifrado)
- Copias de seguridad cifradas AES-256
- Bloqueos de seguridad para proteger dispositivos y aplicación
- Sincronización en la nube



**Costo:** Gratuito y versión de pago con características adicionales

**Herramienta:** AnyConnect

**Descripción:**

AnyConnect provee conexiones seguras entre dispositivos con encriptación fácil de desplegar a través de redes (seguras o inseguras), la conectividad se asegura mediante acceso seguro y personalizado para cada terminal, aplicativo y usuario.

Con el uso de esta aplicación el usuario se garantizará que todos los datos que procese en las comunicaciones entre correos electrónicos, sesiones de acceso remoto a escritorio y entre aplicaciones por el uso de acceso corporativo y aplicaciones de conectividad para negocios, la seguridad está provista por protocolos propios de negociación segura (CISCO, 2016).

**Características:**

- Adaptaciones automáticas para túneles VPN por medio de métodos basados en restricciones de red usando TLS y DTLS
- Optimización de red DTLS
- IPsec e IKEv2 disponibles en la plataforma
- Capacidad de disposición y uso de redes roaming para garantizar la duración de una sesión de conexión cuando se pierden las direcciones IP o cuando existen cambios en las mismas
- Amplio rango de opciones de autenticación
- Despliegue de certificados de seguridad confiables integrando SCEP e importación vía URI
- Políticas de acceso locales configurables, además de actualización remota de pasarelas de seguridad
- Acceso a recursos IPv4 e IPv6
- Políticas de administración controlada de túneles
- Adaptación regional de idioma y configuraciones de seguridad de acuerdo a la localización del dispositivo

**Costo:** Aplicativo gratuito, pago por servicios empresariales

#### 5.1.4. SECCIÓN 4 - Autenticación insegura - Autorización insegura

**Nombre:** Área TEE

**Descripción:**

Sus siglas en inglés TTE (Trusted Execution Environment) es conocido como un entorno de ejecución confiable que ha desarrollado una tecnología en donde su principal objetivo es brindar un estándar de alta seguridad para la ejecución de aplicaciones de dispositivos móviles (Giesecke & Devrient GmbH, 2016).



A el TEE también se lo considera como un área del procesador de los dispositivos móviles que permite que la información importante y sensible de los usuarios de dispositivos móviles puedan procesarla, almacenarla y protegerla en entornos seguros y aislados, en donde se pueda tener el control total de las aplicaciones que solicitan accesos a dicha información.

### **Características:**

- TEE situado en seguridad de un terminal distingue los siguientes entornos para gestionar aplicaciones con niveles de seguridad los mismo que son:
  - Rich OS
    - Sistema operativo de alto nivel en donde se ejecutan las aplicaciones de los distintos sistema operativos de dispositivos móviles (Android, iOS o Windows Phone).
    - Entorno dedicado principalmente a la descarga y ejecución de aplicaciones.
  - TEE:
    - La función principal de TEE es brindar un entorno seguro aislado para la ejecución de aplicaciones previamente autorizadas, basado en una seguridad de cifrado end-to-end.
    - TEE posee la capacidad de permitir ejecutar aplicaciones con interfaz de usuario amigable, pero con un rendimiento alto en cuando a procesamiento y memoria.
  - Secure Element (SE)
    - Considerado el entorno más seguro de los que ofrece TEE para la gestión de aplicaciones. Es considerado de está manera ya que el nivel de seguridad que brinda no solamente es a nivel de software sino también se considera el hardware.
    - Una característica esencial es que los SE pueden ser movidos de un terminal a otro incluyendo toda la información almacenada de manera segura.
    - La principal desventaja que tiene SE es que no es para nada agradable en cuanto a experiencia de usuario.

**Costo:** Gratuito

**Nombre:** Swivel Secure

### **Descripción:**

Es una plataforma de autenticación que ofrece una solución móvil orientada a usuarios finales es decir personas que utilicen dispositivos móviles, la cual permite entregar cadenas de seguridad que son otorgadas directamente desde sus propios servidores (Secure, 2016).

### **Características:**

- Entrega cadenas de seguridad directamente desde el servidor Swivel.



- Permite almacenar hasta 99 cadenas de seguridad y sin costes por SMS
- Permite a los usuarios trabajar en áreas con cobertura de telefonía móvil limitada o nula durante lapsos de tiempos extendidos.
- Las cadenas de seguridad se actualizan al momento que el dispositivo vuelva a tener cobertura.
- La configuración de la aplicación es automática para los clientes móviles basada en los siguientes aspectos (Swivel Secure Ltd, 2013):
  - **Código de una sola vez**
    - En esta característica se configuran para la extracción manual OTC utilizando el protocolo de extracción única PINsafe propia de Swivel o a través de la introducción del PIN del dispositivo. El código recibido se lo introduce una única vez en el inicio de sesión.
  - **PINsafe**
    - Está basado en el uso de PIN registrados con cadenas de seguridad aleatorias de 10 dígitos.
    - La combinación de los dígitos del PIN permitirán resolver códigos de acceso OTC únicos, esto traducido a una autenticación fuerte y segura.

**Costo:** Gratuito

### 5.1.5. SECCIÓN 5 – Criptografía insuficiente

**Herramienta:** Secret Space Encryptor for Android

**Descripción:**

Herramienta que permite proteger información sensible e importante de un dispositivo, ya sean mensajes de texto, contraseñas, archivos y otro tipo de información que pueda ser considerada importante para un usuario, utiliza métodos de encriptación de datos de manera rápida, eficiente y segura, además posee otro tipo de herramientas que garantizan que exista el mejor uso y se asegure la información del usuario, se trata de una herramienta todo en uno que integra múltiples servicios para hacer que la información de los usuarios sea únicamente accesible para el propietario de la información (Paranoia Works, 2016).

**Características:**

- **Almacén de contraseñas:** Manejo y administración de contraseñas, PINS y notas que aseguran en sitios secretos y protegidos por contraseñas maestras todas las credenciales de acceso del usuario, además de tener una opción de importación y exportación de archivos encriptados que contienen llaves únicas de acceso a las contraseñas del usuario (documentos en xml con métodos de encriptación ultra – segura)



- **Encriptación de texto:** Mensajes clave, notas de texto y archivos sensibles que contengan texto para lectores, serán encriptados por S.S.E, puesto que está dotado de una base de datos interna que permite por medio de métodos de copiado/pegado para utilizar dichas notas de texto en las demás aplicaciones, toda esta información se encriptará con una contraseña segura que garantice que cada email, nota de texto, mensaje de texto, mensajes de redes sociales, etc. Estén asegurados por un número indefinido de contraseñas de acceso
- **Encriptación de archivos:** Con S.S.E se puede encriptar fotos, archivos de respaldo, vídeos, e inclusive carpetas mediante contraseñas o mecanismos seguros que faciliten el acceso únicamente a la sesión y al propietario de los mismos, sin importar si un atacante “roba” los archivos puesto que necesitará las credenciales de acceso para poder acceder al contenido de los mismos
- **Algoritmos de encriptación:** Absolutamente todo lo que sucede en S.S.E está encriptado con algoritmos de tipo AES (Rijndael) de hasta 256 bits, RC6 de hasta 256 bits, Serpent 256 bits, Blowfish 448 bits, Twofish 256 bits, GOST 256 bits y los algoritmos únicos de Threefish plus de 1024 bits y SHACAL-2 de 512 bits para la versión Pro
- **Esteganografía:** Uso de técnicas de esteganografía para ocultar contenido sensible dentro de otro tipos de información, uso de algoritmos F5 para aplicación de combinaciones para “camuflar” cualquier tipo de elementos en imágenes JPGE
- **Herramientas y utilitarios:** Uso de herramientas para la generación de contraseñas, limpieza de clipboard, algoritmos de comprobación de rendimiento.

**Costo:** Versión gratuita con publicidad y versión PRO por servicios desde \$32

**Herramienta:** Encrypted Data Storage EDS Lite

**Detalles:**

Conjunto de herramientas que facilitan el almacenamiento de contenido en contenedores seguro, el método de encriptación de almacén es un mecanismo que facilita la encriptación de todo el contenido que ha sido guardado en carpetas seguras, todas las carpetas y archivos almacenados en estos contenedores encriptados están protegidos por métodos de encriptación seguros para evitar accesos indebidos a la información (Rouse, 2016).

**Características:**

- Encriptación TrueCrypt ® para soportar la mayor cantidad de elementos de software disponibles (asegura cualquier tipo de archivo)
- Soporte para métodos de encriptación AES, Serpent, Twofish
- Soporte para algoritmos SHA de 512 bits, RIPEMD de 160 bits y algoritmos hash Whirlpool
- Encriptado y desencriptado de cualquier tipo de archivo
- Contenedores de archivos remotos TrueCrypt ®



- Se puede realizar cualquier tipo de acciones con los archivos contenidos en los almacenes seguros
- Se puede compartir archivos encriptados con familiares, amigos, etc. Esta opción es particularmente útil para fotos, videos y todo tipo de contenido multimedia
- Es una solución basada en técnicas OpenSource
- Encriptación segura para dispositivos extraíbles (Memorias SD)

**Costo:** Freeware

**Herramienta:** EDS

**Detalles:**

Herramienta para ocultar y proteger archivos dentro de carpetas encriptadas y contenedores asegurados por mecanismos de encriptación ultra seguros.

Este programa puede operar en dos modos, en el uno, el usuario puede crear un contenedor EDs y agregar todos los archivos que desea asegurar, ocultar o proteger, dentro del mismo o se puede “crear carpetas remotas” por medio de sistemas de aseguramiento de repositorios en la red llamados SANs (Storage Area Networks) [Áreas de Almacenamiento de Red] (Sovworks, 2016).

**Características:**

- Soporte para los siguiente métodos de encriptación
  - VeraCrypt ®
  - TrueCrypt ®
  - LUKS
  - EncFs
  - CyberSafe ®
  - SAN
- Integración con repositorios externos (Dropbox o Google Drive) Por medio de EncFs
- Cinco criterios de seguridad cipher
- Combinaciones cipher soportadas, es decir, un contenedor puede ser encriptado por múltiples mecanismos cipher para asegurar encriptación personalizada
- Encriptación y desencriptación de cualquier tipo de archivo
- Soporte para archivos de contraseñas
- Montaje y desmontaje de contenedores seguros con cualquier gestor de archivos o programas de galería de imágenes o contenido multimedia
- Opciones para compartir carpetas con otros usuarios
- Montaje de carpetas compartidas en diferentes plataformas (Android, iOS, Windows, Linux, etc.) a través de redes wifi o en la nube
- Operaciones estándar entre archivos dentro de los contenedores
- Se puede abrir y previsualizar archivos multimedia en la plataforma



- Uso de varios métodos de acceso a contenedores (patrón de bloqueo, contraseña, PIN, etc)
- Sincronización de contenedores seguros en la nube (mediante aplicativos o páginas web)
- Se puede crear accesos directos en las terminales móviles
- Soporte para uso de Tarjetas de memoria externa
- Conexiones de red a través de wifi o internet
- Verificador de licencias a través de servicios de Google

**Costo:** \$5.60 aplicación, suscripción anual por servicios en la nube

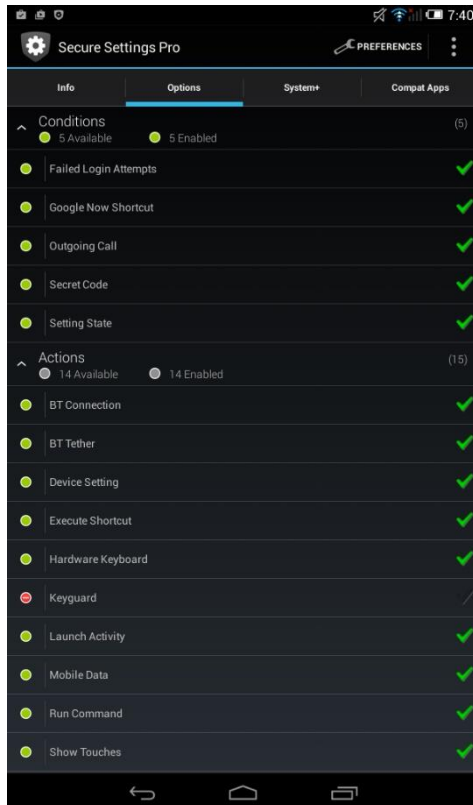


## 5.2. ANEXO B: PRUEBAS REALIZADAS

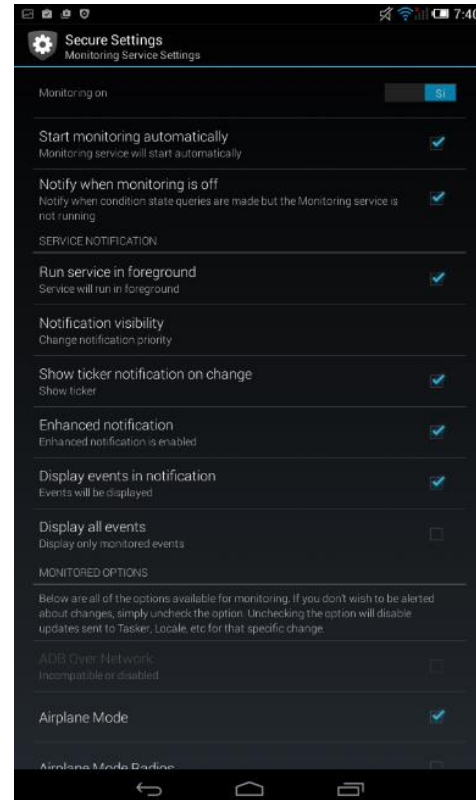
### 5.2.1. SECCIÓN 1 – Incorrecto uso de la plataforma

#### 1. Secure Settings

##### 1.1 Opciones de seguridad configurables en esta herramienta.



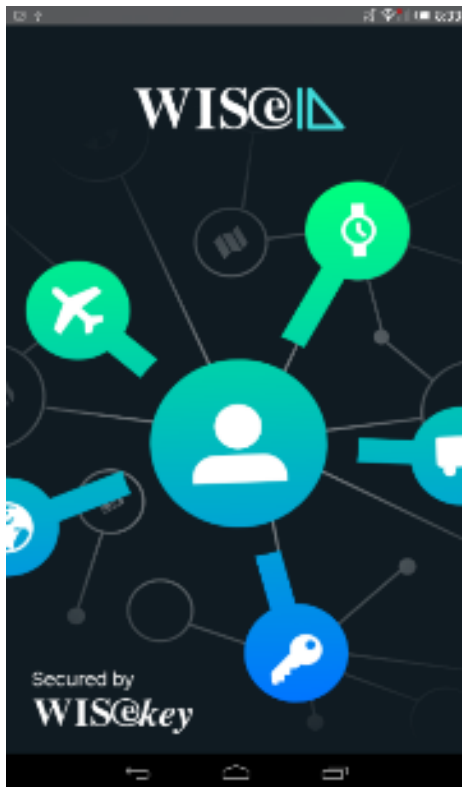
##### 1.2 Monitoreo de configuraciones programadas.



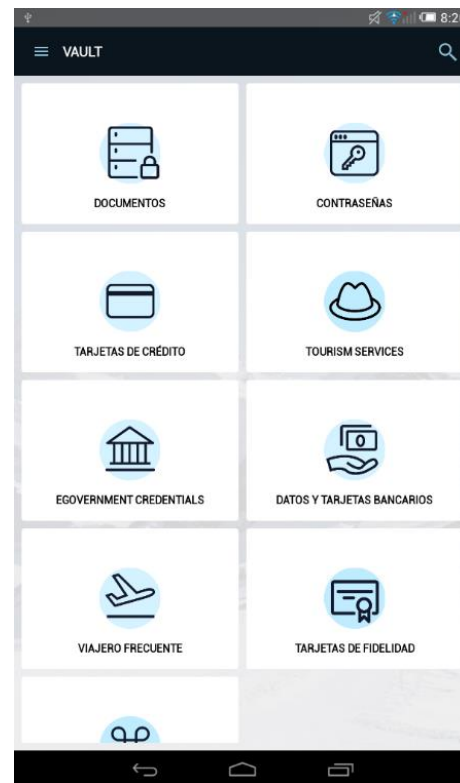
## 5.2.2. SECCIÓN 2 – Almacenamiento inseguro de datos

### 2. WiseID

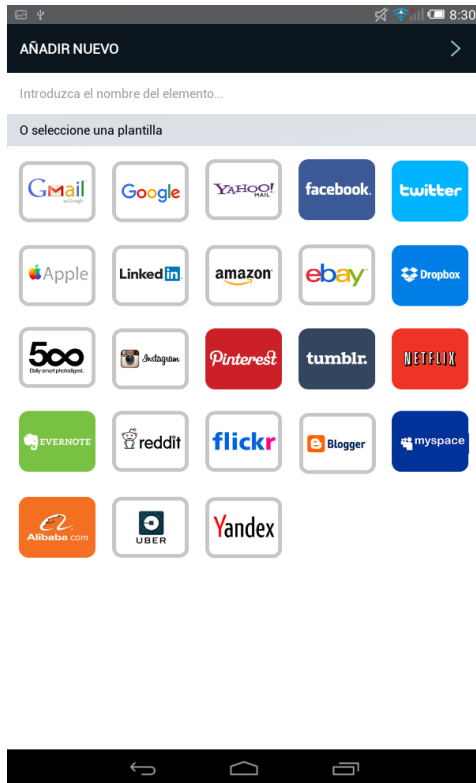
#### 2.1 Interfaz principal de la aplicación



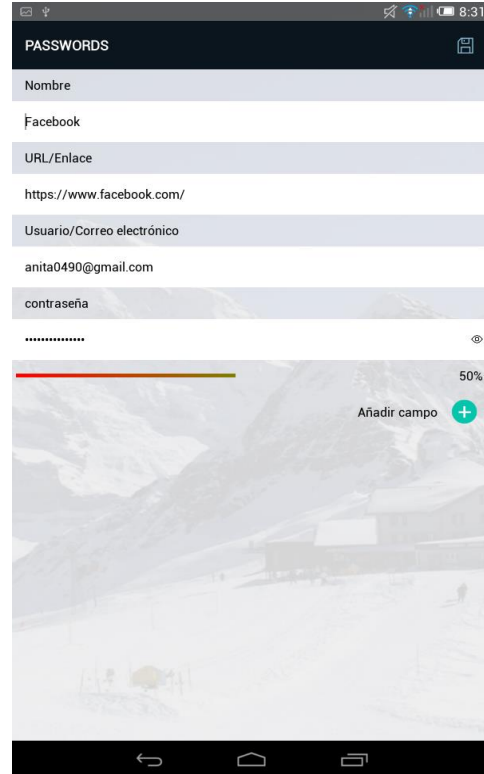
#### 2.2 Categorías para almacenamiento de información sensible



### 2.3 Categoría Contraseñas – Crear nueva contraseña

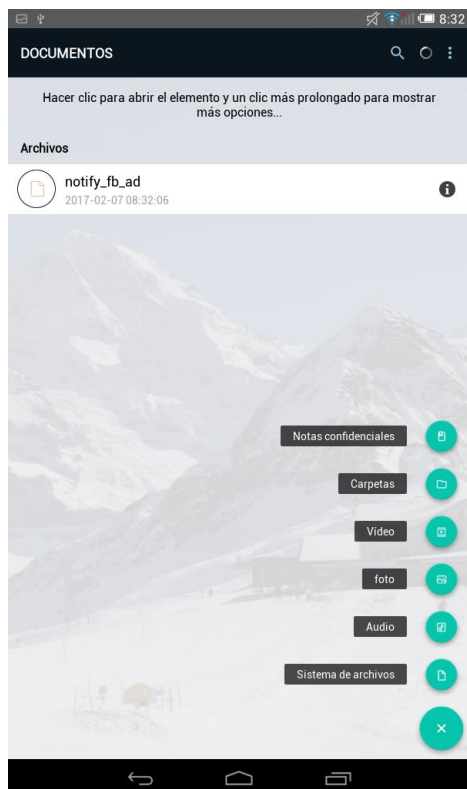


### 2.4 Creación de una nueva contraseña -

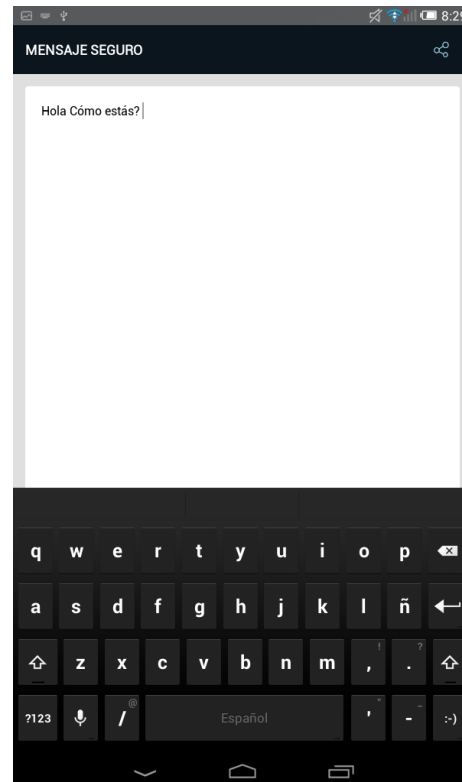


Facebook

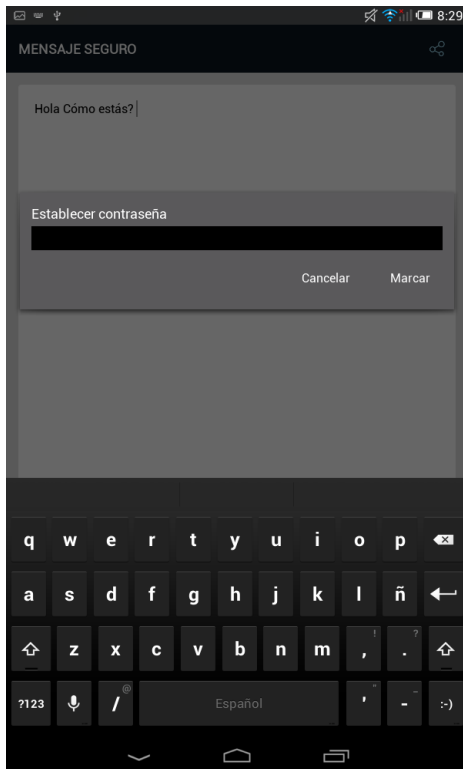
### 2.5 Configuraciones de seguridad en Documentos.



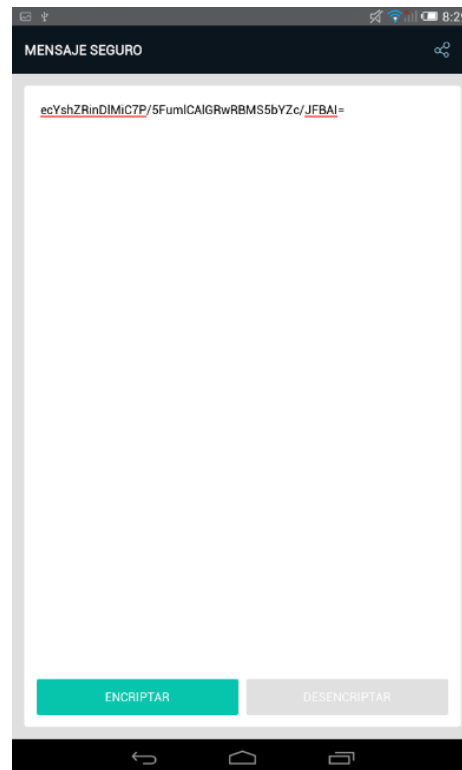
### 2.6 Encriptación de mensajes personales



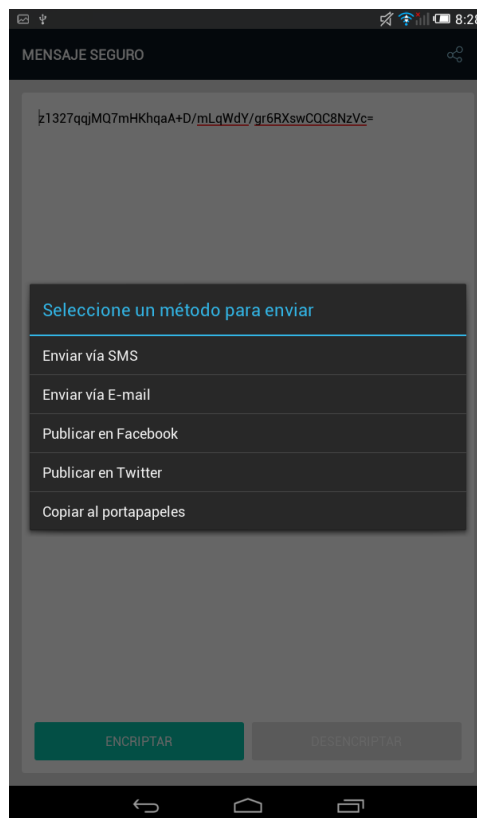
## 2.7 Encriptación seguro (mediante contraseña) de mensajes



## 2.8 Mensaje encriptado

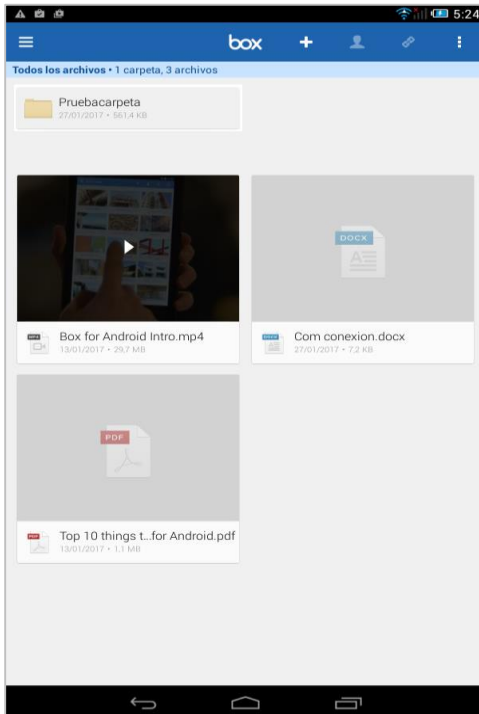


## 2.9 Opciones de envío para mensajes encriptados

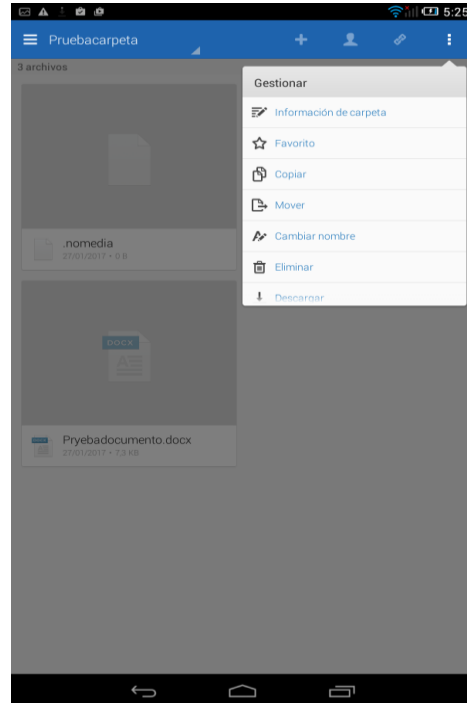


### 3. Box

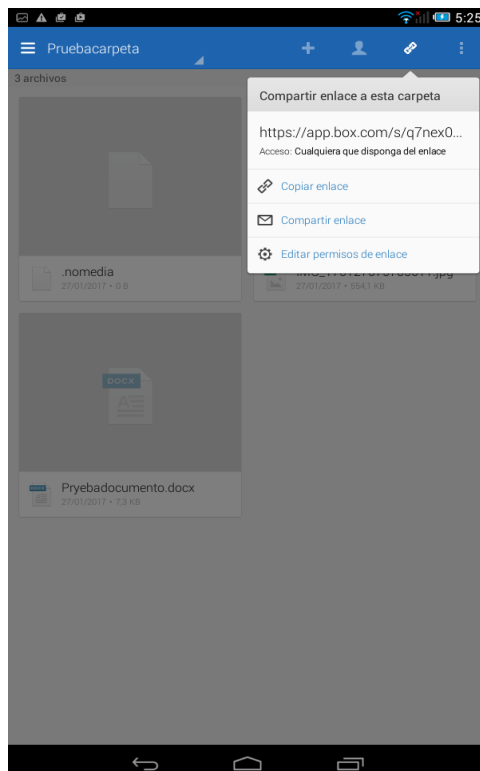
#### 3.1 Vista Principal de la aplicación



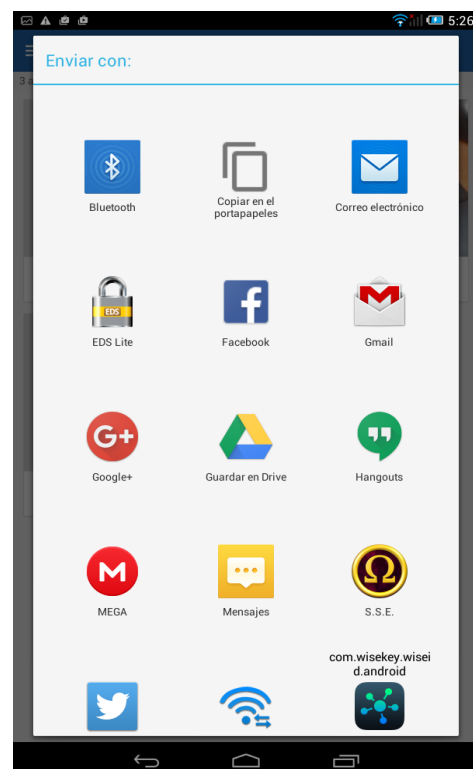
#### 3.2 Opciones disponibles en la app



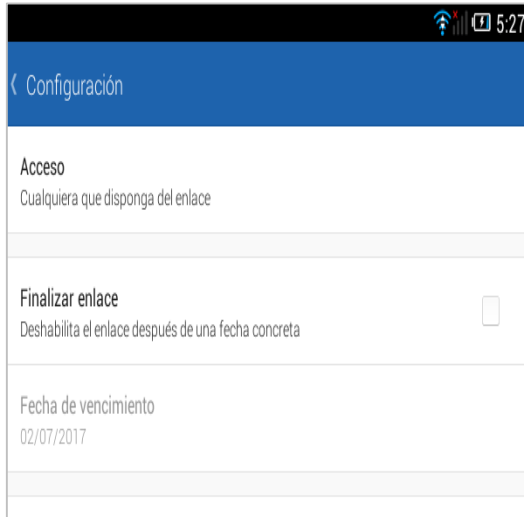
#### 3.3 Compartición de enlaces



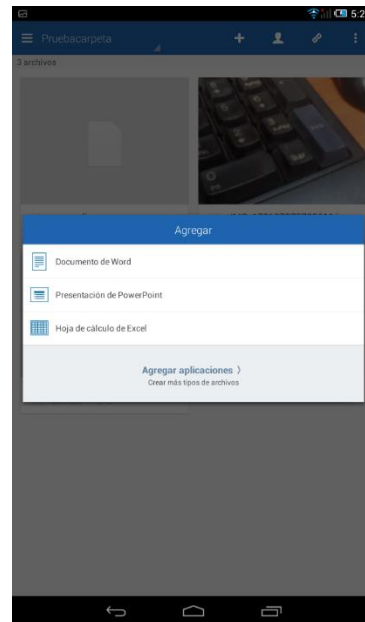
#### 3.4 Aplicaciones con las que se pueden compartir los enlaces



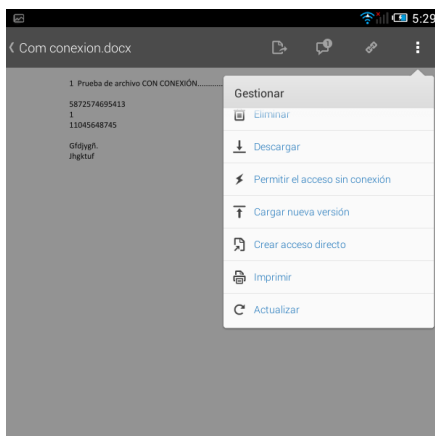
### 3.5 Configuraciones de seguridad para la generación de enlaces



### 3.6 Creación de Documentos dentro de la aplicación



### 3.7 Opciones de configuración – Marcar como “Sin conexión” un archivo

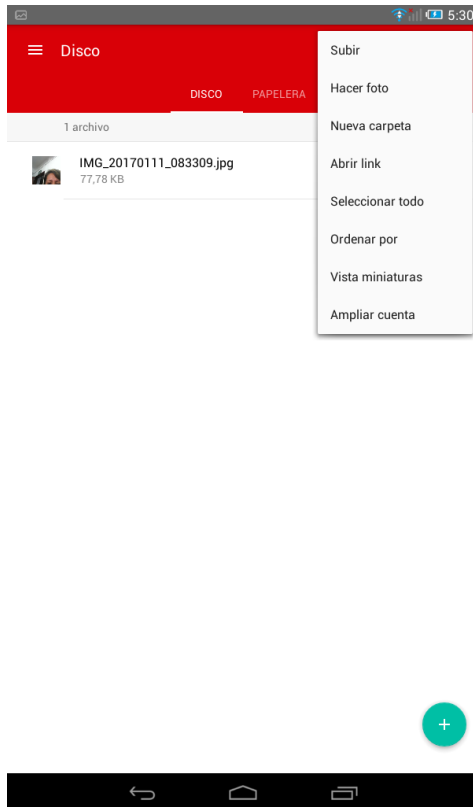


### 3.8 Vista previa de un archivo marcado “Sin Conexión”

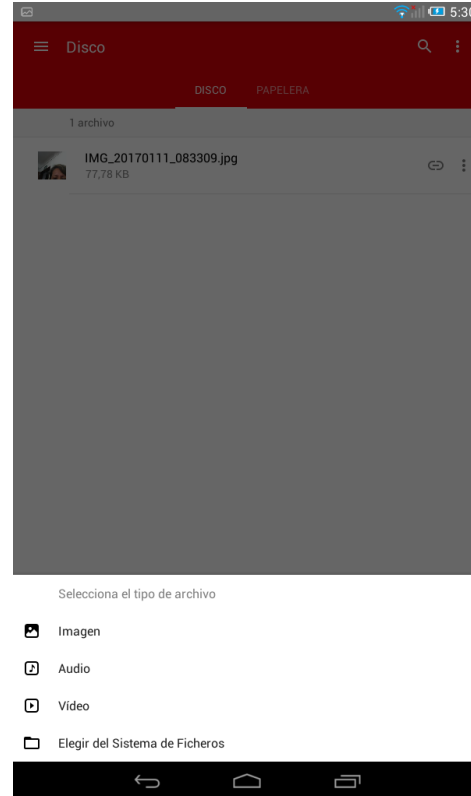


## 4. Mega

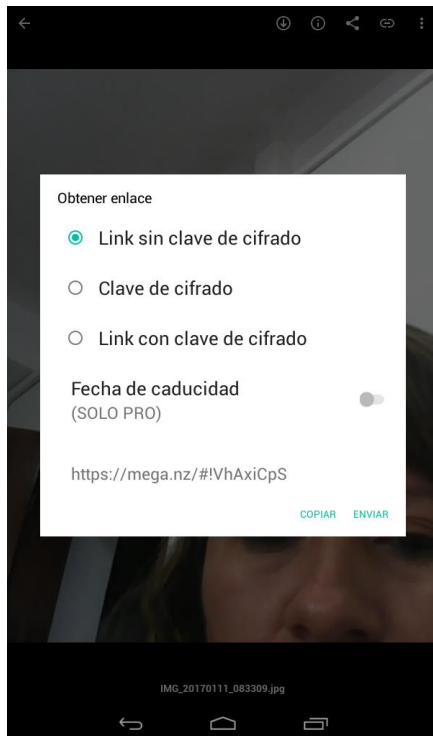
### 4.1 Vista Principal de la aplicación.



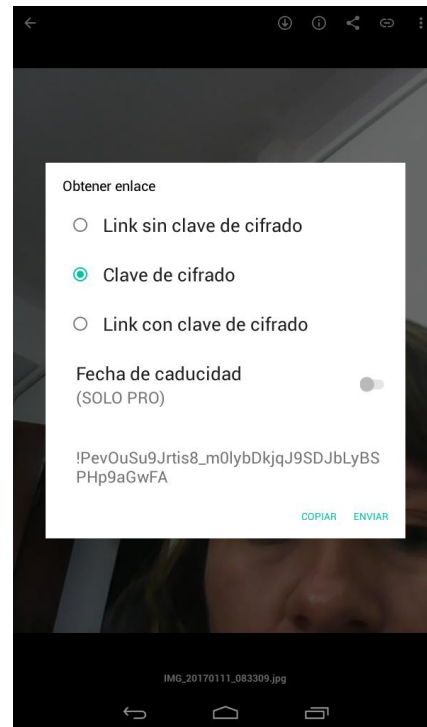
### 4.2 Tipos de archivos que se puede almacenar en la aplicación.



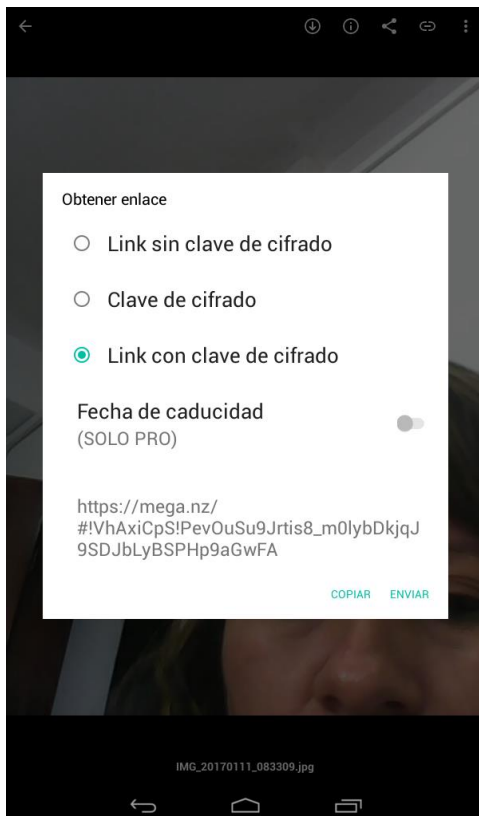
#### 4.3 Generación de enlace sin clave de cifrado



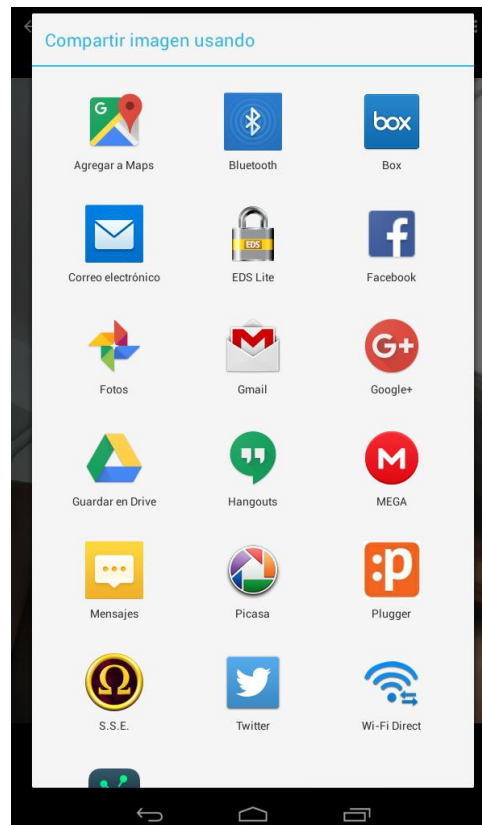
#### 4.4 Generación de enlace con clave de cifrado



#### 4.5 Generación de enlace con la clave de cifrado incluida.



#### 4.6 Aplicaciones del dispositivo con las que se puede compartir el enlace.

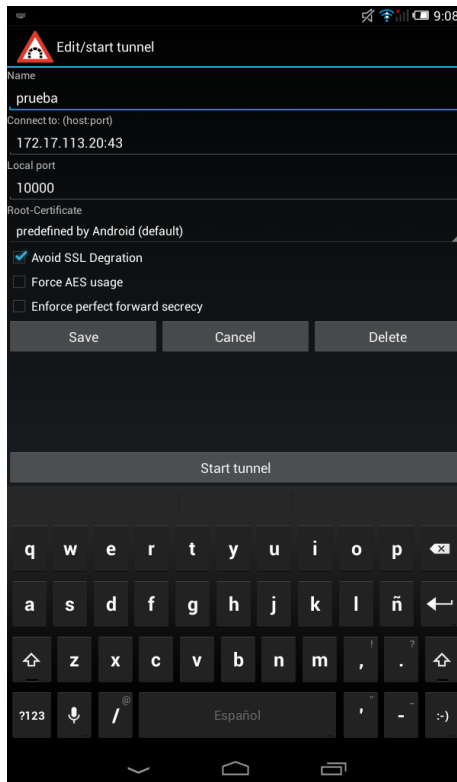




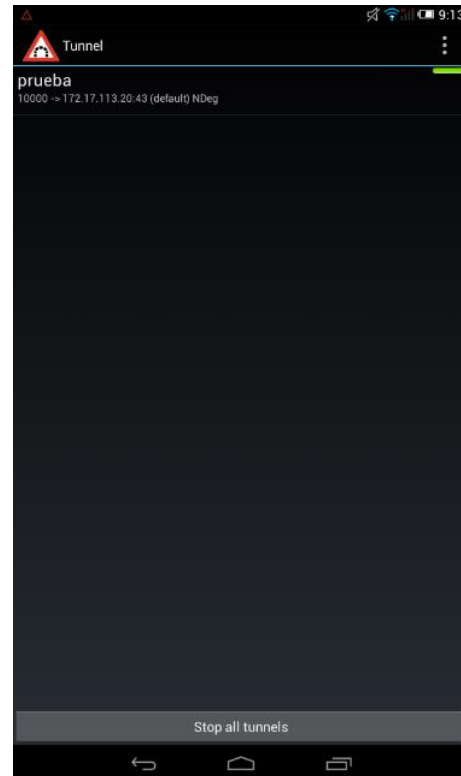
### 5.2.3. SECCIÓN 3 – Comunicación insegura

#### 5. TLS/SSL Tunnel

##### 5.1 Creación de una nueva conexión



##### 5.2 Conexión Segura Activada

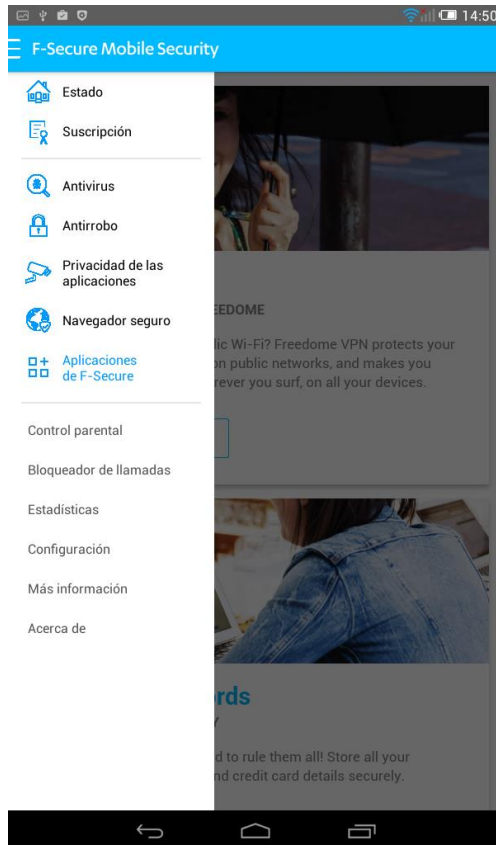




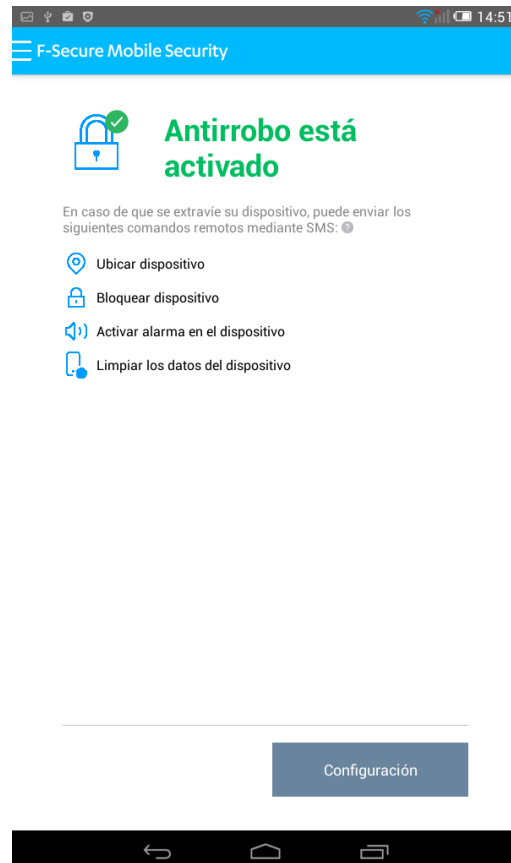
## 5.2.4. SECCIÓN 4 - Autenticación insegura - Autorización insegura

### 6. Secure Mobile

#### 6.1 Configuraciones principales de la herramienta



#### 6.1 Configuraciones de seguridad y privacidad – Acceso seguro



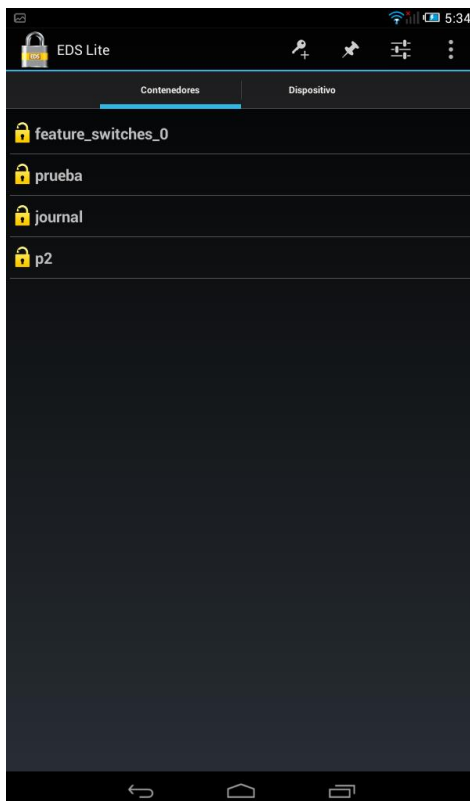
### 6.3 F-Secure Freedome



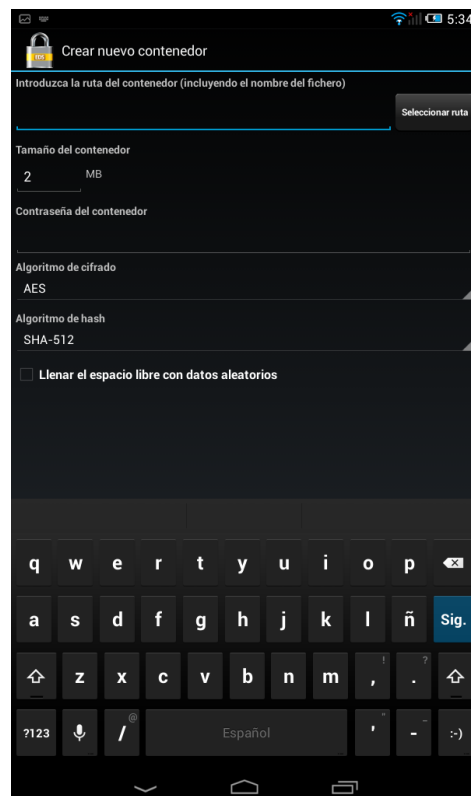
## 5.2.5. SECCIÓN 5 – Criptografía insuficiente

### 7. Encrypted Data Storage Lite

#### 7.1 Vista principal de la aplicación – Contenedores de información



#### 7.2 Creación de un contenedor nuevo

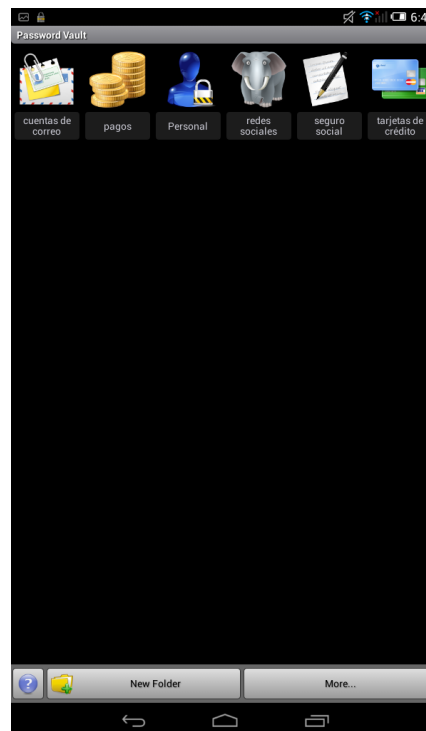


## 8. SSE Universal - Secret Space Encrypt

### 8.1 Vista principal de la aplicación

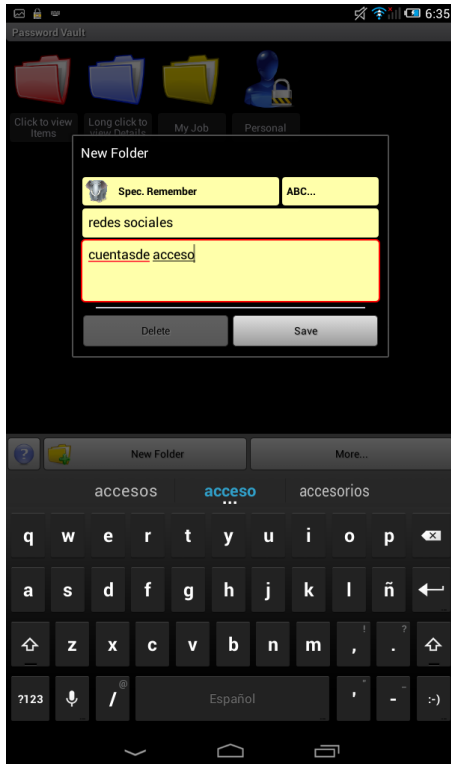


### 8.2 Carpetas contenedoras de información

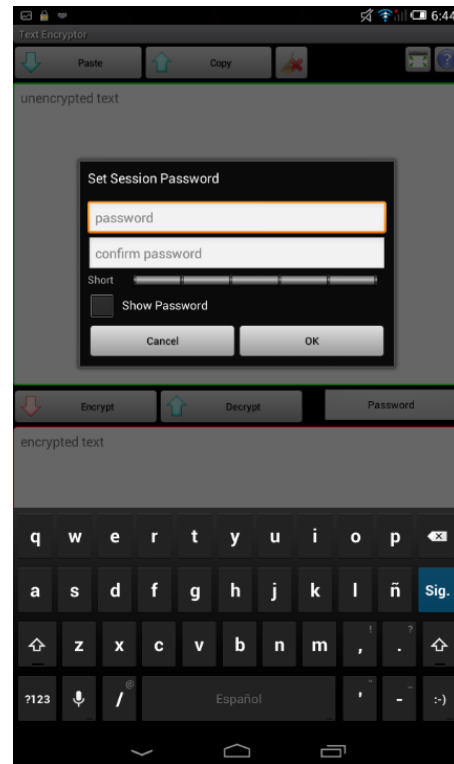




### 8.3 Creación de contenedores de acuerdo a la necesidad.



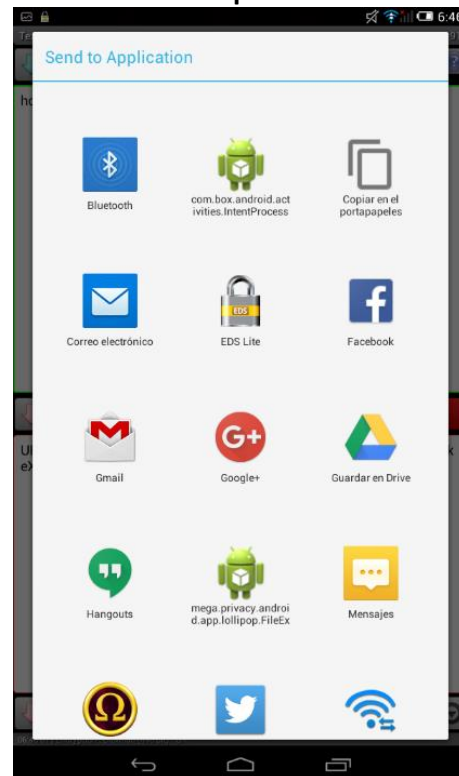
### 8.4 Asignación de usuario y contraseña para encriptación de mensajes



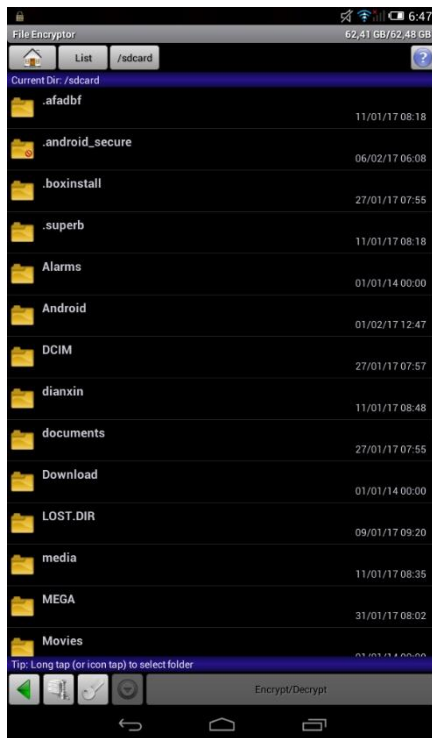
### 8.5. Encriptación de mensajes



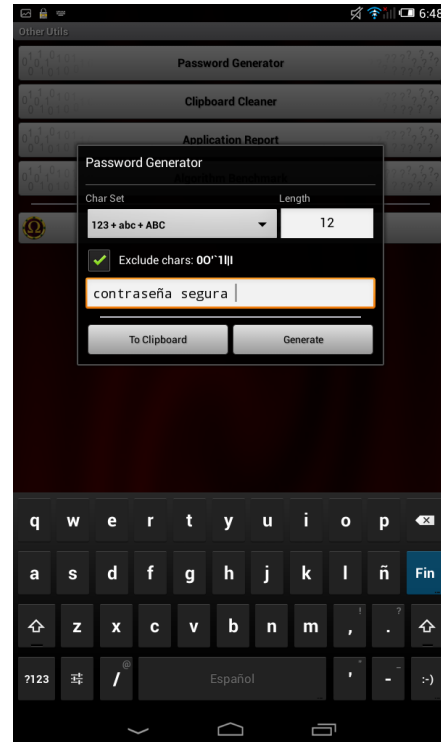
### 8.6 Herramientas para enviar mensajes encriptados



### 8.7 Encriptación de Sistema de Archivos



### 8.8 Generación de contraseñas seguras – Ingreso de caracteres



### 8.9 Generación de contraseñas seguras – Obtención de contraseña

