Metodología de validación de herramientas para la seguridad en dispositivos móviles

***Daysi Erreyes Pinzón*[1], *Diego Ponce Vásquez*[2]**

[1] Estudiante de Posgrado de Ingeniería, Universidad de Cuenca, Av. 12 de Abril y Agustín Cueva, Cuenca, Ecuador, 01.01.168.

[2] Departamento de Ciencias de la Computación, Universidad de Cuenca, Av. 12 de Abril y Agustín Cueva, Cuenca, Ecuador, 01.01.168.

Autores para correspondencia: daymire@gmail.com, diego.ponce@ucuenca.edu.ec

Fecha de recepción: 30 de julio de 2017 - Fecha de aceptación: 15 de agosto de 2017

RESUMEN

Los usuarios de dispositivos de telefonía móvil celular requieren información actualizada en tiempo real y aplicaciones para satisfacer distintas necesidades. Sin embargo, estas aplicaciones pueden ser vulnerables, están sujetas a amenazas, por lo que requieren medidas de protección para mitigar potenciales ataques. Este artículo presenta el diseño de una metodología para la validación de herramientas de seguridad dirigida a usuarios de dispositivos móviles. Para su desarrollo, se realizó una revisión teórica de la seguridad de la información en entornos móviles, un análisis mediante el modelo Estudio de Similitud entre Modelos y Estándares (MSSS) de los principales estándares relacionadas con la seguridad informática como la norma ISO 27001, NIST 800-30, COBIT 5 y recomendaciones de OWASP Mobile Security Proyect. Como resultado se generó una metodología sencilla denominada Ms-DisMov, diseñada mediante la fusión del ciclo PDCA de la ISO 27001 con los escenarios del OWASP top ten mobile 2016, metodología que permitió armonizar las dos tendencias en una base sólida que por su estructura se adapta para trabajar con cualquier herramienta que se alinee con los escenarios del OWASP, y de esa forma permite al usuario proteger la información contenida en sus dispositivos móviles.

Palabras clave: CC, ciberseguridad, metodología seguridad, seguridad informática, seguridad móvil.

ABSTRACT

Users of mobile phone devices require updated information in real time. Many users are unaware of existing vulnerabilities, threats, and protective measures to mitigate potential attacks. This article presents the design of a methodology for the validation of security tools aimed at users of mobile devices; for development. A theoretical review of information security in mobile environments was carried out, an analysis consisting of a Similarity Study between Models and Standards (MSSS) of the main standards related to computer security such as ISO 27001, NIST 800-30, COBIT 5 and OWASP recommendations Mobile Security Project. As a result, a simple methodology called Ms-DisMov was designed by merging the PDCA cycle of ISO 27001 with the scenarios of OWASP top ten mobile 2016, which allowed to harmonize the two trends on a solid basis that according to its structure adapts to work with any tool that is aligned with OWASP scenarios, allowing the user to protect the information contained in their mobile devices.

Keywords: CC, cyber security, IT security, methodology security, mobile security.

1. INTRODUCCIÓN

En la actualidad, los dispositivos móviles proporcionan a los usuarios acceso a un gran número de aplicaciones. Pero el uso de estas herramientas tiene un precio: diariamente almacenan información confidencial de esos usuarios, información que se vuelve vulnerable. Desafortunadamente, un porcentaje significativo de las personas desconocen los problemas, amenazas, vulnerabilidades y deficiencias en el diseño de algoritmos criptográficos que pueden poseer este tipo de aplicaciones y la forma en que esos problemas podrían afectar a los datos almacenados. Ciertamente, las aplicaciones de los móviles se han convertido en un objetivo de ataque para los cibercriminales, debido a su portabilidad y a la información de la que disponen.

De acuerdo con Dwivedi, Clark, & Thiel (2014), los problemas usuales con los que se enfrentan los dispositivos móviles y las aplicaciones son: falta de seguridad física, almacenamiento poco seguro de datos (en disco), riesgos de que se divulgue información confidencial o personal, virus, gusanos, troyanos, spyware y malware, entre otros. Según ESET (2014), los cibercriminales están comenzando a enfocarse cada vez más en explotar agujeros de seguridad en sistemas operativos para móviles como Android. Klieber, Flynn, Bhosale, Jia, & Bauer (2014) explican que existe un 0.7% de teléfonos Android con versiones antiguas, con muchas de las aplicaciones puramente escritas en Lenguaje Java. Memon & Anwar (2016) advirtieron sobre amenazas como la colusión de aplicaciones. Por todo esto, la seguridad en los teléfonos celulares se ha convirtido en un gran problema, ya que en cualquier momento pueden ser atacados debido a las vulnerabilidades existentes en la plataforma. He ahí la importancia de pensar en mecanismos de seguridad. Este texto busca justamente brindar algunas alternativas a ese problema.

Cabe anotar que ningún sistema de cómputo está completamente inmune al ataque. Todos deben la proteger la privacidad, si bien la forma varía considerablemente dependiendo del sistema que debe protegerse (Hurlburt, 2016). Algunas empresas, por ejemplo, recurren al diseño de 4G LTE que emplea técnicas criptográficas fuertes. Otras han incorporado en la arquitectura mecanismos para la autenticación segura entre pares de elementos de la red LTE (Jøsang, Miralabé, & Dallot, 2015). Lei Cen y sus colegas, lo explica Bertino (2016) propusieron un modelo altamente preciso para detectar Malware en aplicaciones Android.

Este artículo presenta el diseño de una metodología para la validación de herramientas que permitan proveer seguridad a la información contenida en dispositivos móviles. Se analizan estándares que se realizaron mediante la adaptación del método Estudio de Similitud entre Modelos y Estándares (MSSS), entre los problemas de la seguridad móvil y la norma ISO 27001 (ISO/IEC 27001, 2012), la norma NIST 800-30 (Task & Transformation, 2012), COBIT 5 (ISACA, 2012) y el proyecto profesional para dispositivos móviles OWASP Top Ten (OWASP, 2016). Se incluye, asimismo, la definición de aspectos claves para el diseño y la estructura y los pasos necesarios para su ejecución. Finalmente se exponen las conclusiones a las que se ha llegado luego de la investigación realizada.

2. MATERIALES Y MÉTODOS

Para el análisis de los estándares y normas que soportarán la metodología que se empleará en la propuesta, se realizó la adaptación del Método de Estudio de Similitud entre Modelos y Estándares (MSSS), método propuesto por un grupo de investigadores de la Universidad Politécnica de Madrid, validado en diferentes ámbitos de estudio (Gasca, 2010). Los pasos del citado método son: seleccionar estándares y modelos, elegir de entre ellos un modelo de referencia, seleccionar los procesos que deben analizarse, establecer el nivel de detalle del análisis, definir una plantilla de comparación, identificar similitudes, recoger resultados (Calvo-Manzano, Cuevas, Muñoz, & San Feliu, 2008).

Para los fines de esta propuesta fue necesario el método original del estudio comparativo de modelos, estándares y proyectos de profesionales como OWASP, de tal forma que permita seleccionar modelos y estándares para la seguridad de los dispositivos móviles. Los pasos seguidos fueron: (1) establecer criterios para la selección adecuada de modelos y estándares para la seguridad de los

dispositivos móviles, (2) seleccionar modelos y estándares, (3) definir aspectos que deben analizarse en cada modelo o estándar seleccionado, (4) elaborar una matriz comparativa entre los modelos y estándares seleccionados, (5) identificar similitudes entre los modelos y estándares seleccionados y los elementos de la seguridad móvil, y (6) presentar los resultados obtenidos.

La revisión literaria de varios modelos y estándares, primer momento de la metodología, ha considerado a los siguientes: ISO 27001, NIST 80-30, COBIT 5 y OWASP. Se evaluó las particularidades y carencias de cada uno en relación con la seguridad en dispositivos móviles. Según nuestro análisis, *ISO 27001 (Norma)*, define las políticas y entrega la información general relacionada con la seguridad de la información, constituye un estándar completo y de gran utilidad para la gestión de la seguridad de TI, se aplica a cualquier tipo de organización. Sin embargo, carece de un enfoque específico para la seguridad en dispositivos móviles, donde se especifiquen los procesos necesarios para mejorar la seguridad de ese entorno.

En cuanto a *NIST 800-30 (Norma)*, se aprecia que la 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; pero que carece de componentes relacionados con la seguridad de la información en dispositivos móviles. *COBIT 5 (Marco de referencia)*, por su lado, destaca por su marco de referencia integrado orientado al Gobierno y la Gestión de las TI de la empresa, constituye un marco completo y general de gran utilidad para la gestión de la seguridad de TI, aplicable a cualquier tipo de organización. Dispone de dos procesos relacionados con la seguridad en general, son: APO13 Gestionar la Seguridad y DSS05 Gestionar los Servicios de Seguridad. Pero al igual que los anteriores, carece de un enfoque específico para la seguridad en dispositivos móviles. En cuanto al *OWASP Top ten* (*Proyecto profesional*), analizamos que define claramente los escenarios de riesgos relacionados con la seguridad de la información en dispositivos móviles, por lo que constituye un referente importante y de gran utilidad para la gestión de la seguridad de TI, aplicable a cualquier tipo de organización. El enfoque se centra en la seguridad en dispositivos móviles, y especifica los elementos necesarios para mejorar la seguridad móvil.

La Tabla 1 muestra, en resumen, la similitud entre los problemas de la seguridad móvil y los estándares seleccionados con mayor detalle.

Tabla 1. Similitud entre los problemas de la seguridad móvil y los estándares seleccionados.

Problemas de la seguridad móvil (Dwivedi *et al*., 2014)	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	√	√	√	√
Autenticación de factores múltiples (MFA)	√			√

Ha sido necesario realizar un acoplamiento entre los controles que se encuentran en el Anexo A de la norma ISO 27001 y los escenarios del proyecto profesional OWAP. Como resultado apreciamos que entre los controles de la norma ISO 27001 y los escenarios del OWASP no existen controles orientados específicamente para validar herramientas de seguridad en dispositivos móviles, por lo que

es necesario plantear controles que sí faculten evaluar las herramientas. El análisis concluye que el modelo de referencia más pertinente para el desarrollo de la metodología propuesta para este trabajo es la norma ISO 27001, por ser una norma de seguridad de la información estándar que se enfoca en el ciclo de mejora continua y porque, a través de los controles planteados dentro de los escenarios de OWASP, ayudará a validar herramientas de seguridad que mitiguen los problemas de la seguridad móvil.

3. RESULTADOS

3.1. Diseño de la metodología

Para el diseño de la metodología se tomó como referencia las actividades expuestas en la Norma ISO 9001 que comprende tres pasos: identificar las entradas, definir el proceso y obtener la salida esperada, es decir, el proceso conocido como entradas, procesos y salidas, (Management, 2008). En la Figura 1 se puede apreciar el proceso de solución para el diseño de una metodología para la validación de herramientas eficientes para mejorar la seguridad de los dispositivos móviles.

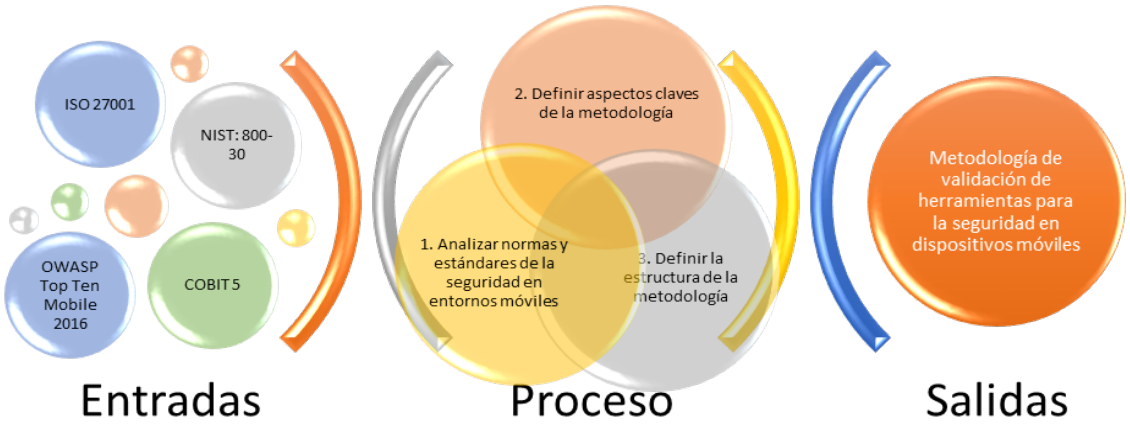

Figura 1. Esquema de resolución del problema.

3.2. Aspectos claves para el diseño de la metodología

La metodología de validación de herramientas para la seguridad en dispositivos móviles se denominará Ms-DisMov, que proviene de sus siglas abreviadas - **M**etodología de validación de herramientas para la **S**eguridad en **Dis**positivos **Móv**iles. A continuación se presentan algunos aspectos claves necesarios para su diseño. El alcance de la metodología Ms-DisMov, en cuanto a *la Norma ISO 2700*1, consiste en un proceso basado en PDCA, para el establecimiento, implementación y mejoramiento continuo en entornos móviles. El alcance en cuanto a *escenarios de Top Ten Mobile 2016 de OWASP*, con respecto a usuario final, emplea los seis primeros escenarios del Top Ten (que corresponden a soluciones móviles), unifica los escenarios 4 y 6 que corresponden a autenticación y autorización insegura y deja fuera de alcance de la metodología los escenarios que están orientados al desarrollo de aplicaciones móviles: M7 - Calidad del código de cliente, M8 - Manipulación de código, M9 - Ingeniería inversa, M10 - Funcionalidad extraña.

Para realizar una correcta selección de las herramientas debemos considerar los parámetros y la escala cualitativa que se presentan en la Tabla 2.

Tabla 2. Criterios para selección de herramientas.

Criterio		Parámetros	Escala cualitativa
1. Confidencialidad	C.1	Que la información sea accedida por el usuario que cumpla el rol.	Cumple a satisfacción: Sí C1 y C2 Cumple parcialmente: Sí C1 o C2 No cumple: inexistencia de C1 y C2
	C.2	Que la información sea accedida por el usuario que disponga de permisos necesarios para acceder a dicha información.	
2. Integridad	C.3	Que la información no haya podido ser modificada por un tercero que no posea el rol.	Cumple a satisfacción: Sí C3 y C4 Cumple parcialmente: Sí C3 o C4 No cumple: inexistencia de C3 y C4
	C.4	Que la información no haya podido ser modificada por un tercero que no disponga de los permisos necesarios para hacerlo.	
3. Disponibilidad	C.5	Que la información esté disponible cuando el usuario la requiera utilizar.	Cumple a satisfacción: Sí C5 y C6 Cumple parcialmente: Sí C5 o C6 No cumple: inexistencia de C5 y C6
	C.6	Que no se presenten contratiempos o esperas en el momento de obtener la información.	
4. Funcionalidad y facilidad de uso	C.7	Capacidad del sistema de ofrecer cambio de password.	Cumple a satisfacción: Sí C7 y C8 Cumple parcialmente: Sí C7 o C8 No cumple: inexistencia de C7 y C8
	C.8	Uniformidad en nomenclatura de etiquetado de botones.	
5. Estabilidad	C.9	Capacidad de procesar la información y cumplir los objetivos de desarrollo del sistema sin fallos.	Cumple a satisfacción: Sí C9 y C10 Cumple parcialmente: Sí C9 o C10 No cumple: inexistencia de C9 y C10
	C.10	Capacidad de procesar información con la menor cantidad de fallos posibles para cumplir el proceso para el que fue diseñado.	
6. Compatibilidad	C.11	Si la herramienta puede ejecutarse en todas las versiones de Android.	Cumple a satisfacción: Sí C11 y C12 Cumple parcialmente: Sí C11 o C12 No cumple: inexistencia de C11 y C12
	C.12	Solo la herramienta puede ejecutarse en determinada versión de Android.	
7. Interoperabilidad	C.13	Capacidad de la herramienta para comunicarse con otras herramientas.	Cumple a satisfacción: Sí C13 y C14 Cumple parcialmente: Sí C13 o C14 No cumple: inexistencia de C13 y C14
	C.14	Capacidad de la herramienta para enviar/recibir información en un formato que sea común en el entorno en el que se ejecuta.	
8. Soporte y garantía	C.15	Capacidad de la empresa que ofrece la herramienta para responder inquietudes o resolver problemas referentes al producto que está ofreciendo.	Cumple a satisfacción: Sí C15 y C16 Cumple parcialmente: Sí C15 o C16 No cumple: inexistencia de C15 y C16
	C.16	Forma en que la empresa que ofrece el software ayuda en la reparación de posibles fallos.	
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: Sí C17 y C18 Cumple parcialmente: Sí C17 o C18 No cumple: inexistencia de C17 y C18
	C.18	Capacidad de respuesta de la empresa desarrolladora para añadir nuevas funcionalidades o características del programa.	

Criterio		Parámetros	Escala cualitativa
10. Costo inicial y futuro	C.19	Si el costo directo de la herramienta viene dado por el licenciamiento temporal o de por vida.	Cumple a satisfacción: Sí C19 y C20 Cumple parcialmente: Sí C19 o C20 No cumple: inexistencia de C19 y C20
	C.20	Si el costo indirecto de la herramienta viene dado por la funcionalidad adicional.	
11. Algoritmos criptográficos	C.21	Si para las opciones de encriptación de datos utiliza alguno de estos 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: Sí C21 Cumple parcialmente: Sí C22 o 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.	

Las métricas correspondientes para valorar los criterios se presentan en la Tabla 3.

Tabla 3. Métricas de valoración de criterios.

Indicador	Valoración numérica	Explicación
Cumple a satisfacción	3	Que el concepto se cumpla en su totalidad en el aplicativo evaluado.
Cumple parcialmente	2	Que el concepto se cumpla parcialmente en el aplicativo evaluado.
No cumple	1	Que el concepto no se cumpla en el aplicativo evaluado.
No aplica	0	Que el aplicativo carezca de dicho concepto o el escenario no se pueda aplicar.

Para validar las herramientas se deben considerar los controles definidos por cada escenario de OWASP, como se aprecia en la Tabla 4.

Tabla 4. Controles para la validación.

OWASP	Controles
M1 - Incorrecto uso de la plataforma	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.
M2 - Almacenamiento inseguro de datos	M.2.1. Encriptar información (mensajes personales mediante contraseña). M.2.2. Almacenar información mediante contraseña. M.2.3. Permite almacenamiento seguro de usuarios y contraseñas de diferentes plataformas. M.2.4. Permite bloqueo de acceso a la información mediante bloqueo (patrón de desbloqueo o pin). M.2.5. Permite el acceso mediante interfaz web y aplicación móvil. M.2.6. Permite la edición conjunta de archivos. M.2.7. Permite compartir archivos multimedia, de texto, carpetas, etc. M.2.8. Permite almacenar información de otras librerías instaladas en el equipo. M.2.9. Permite acceder a la información sin conexión. M.2.10. Permite visualizar archivos sin necesidad de descarga. M.2.11. Muestra versiones anteriores en los archivos y visualiza cambios realizados por otros usuarios. M.2.12. Permite una capacidad de almacenamiento de 10GB. M.2.13. Permite configurar el PIN de acceso a la aplicación. M.2.14 Permite compartir información contenida en el repositorio de otros usuarios

	mediante la generación de un enlace con o sin cifrado. M.2.15. Permite compartir enlaces mediante mensajería instalada en nuestro equipo.
M3 - Comunicación insegura	M.3.1. Permite comunicación segura a redes privadas.
M4 - Autenticación insegura - M6 - Autorización insegura	M.4.1. Permite control de acceso a usuarios, privacidad en el manejo de aplicaciones. Control de seguridad en cada una de ellas. M.4.2. Permite protección de seguimiento, conexiones, navegación y aplicaciones.
M5 - Criptografía insuficiente	M.5.1. Realiza la encriptación de un sistema local de archivos disponible en nuestro dispositivo. M.5.2. Controla la organización de la información mediante contenedores. M.5.3. Oculta información sensible dentro de los archivos de configuración del sistema a fin de que no sean visibles en caso de robo. M.5.4. Permite generar contraseñas seguras, mediante el ingreso de caracteres (letras, números) previstos por el usuario. M.5.5. Permite técnicas de estenografía (ocultar información en imágenes). M.5.6. Permite encriptar documentos de texto, archivos multimedia (imagen y video) entre otros mediante contraseñas asignadas. M.5.7. Permite almacenar contraseñas en lugares seguros y con encriptación mediante contraseña. M.5.8. Permite crear una clave maestra (principal) para acceder a los directorios que contienen la información segura. M.5.9. Permite organizar la información almacenada mediante la creación y el uso de paneles. M.5.10. Encripta mensajes para el envío de información sensible. M.5.11. Genera contraseñas seguras.

Para definir si una herramienta es factible de ser seleccionada como herramienta para la seguridad móvil, se considerarán los valores de la Tabla 5.

Tabla 5. Métricas para la validación de herramientas

Indicador	Rango valoración de controles
Herramienta eficiente	90% - 100%
Medianamente eficiente	70% - 89%
Parcialmente eficiente	40% - 69%
No alcanza los requerimientos de eficiencia	<40%

3.3. Estructura de la metodología

La estructura de la metodología MS-DisMov está compuesta por la Norma ISO 27001 y el top ten mobile 2016 de OWASP, de los cuales se utilizan estos componentes de la siguiente manera:

a) El proceso PDCA se muestra en la Tabla 6. Se podrá aplicar en cualquiera de los cinco escenarios de la metodología.

Tabla 6. El proceso PDCA

Ciclo PDCA	
Planear	Búsqueda de herramientas para asegurar las plataformas móviles.
Hacer	Implementación de herramientas Realice la instalación de la herramienta en su dispositivo. (La metodología está abierta a la evaluación de N herramientas)
Verificar	T1.- *Selección de las herramientas*, para esta tarea diseñamos una matriz que llamaremos (MAT_T1), con las siguientes especificaciones: Las columnas corresponden a los 11 criterios para seleccionar herramientas. Agregamos una columna más denominada “Valoración promedio”. Las filas serán los nombres de las herramientas que se deseen evaluar. Para la evaluación se procede de este modo: se selecciona el primer criterio, se analizan los

	parámetros y la escala cualitativa de la tabla *"Criterios para selección de herramientas"*, luego se verifica la escala cualitativa en la tabla de *"Métricas para valoración de criterios"*, se asigna la valoración numérica correspondiente en la celda de evaluación. Este proceso se repite con los criterios disponibles, luego se calcula el valor promedio por cada herramienta y se coloca en la celda de "Valoración promedio". T2.- *Evaluación de cada una de las herramientas*, para ello se considera los controles por cada escenario y se diseña una matriz (MAT_T2) con las siguientes especificaciones: La primera columna se etiqueta con el nombre: "Criterios" y bajo esta columna se colocan los controles de la tabla "Controles para la validación", según el escenario a evaluar. Las columnas siguientes serán el nombre de cada herramienta que se requiere evaluar. Coloque en cada celda de la matriz los valores (0 = no validado y 1 = validado) por cada control evaluado y bajo la columna de la herramienta que se requiere evaluar. Totalice los valores de validación obtenidos por cada columna (herramienta evaluada) según corresponda. Calcule el porcentaje en relación (nro. de controles validados / total de controles del escenario evaluado *100), por cada herramienta evaluada. ** La matriz MAT_T1, se crea una sola vez, si es la segunda vez que se ejecuta el ciclo, agregue una fila al final de la matriz por cada herramienta a evaluar.* **La matriz MAT_T2, se crea una sola vez, si es la segunda vez que se ejecuta el ciclo, agregue una columna a la derecha de la matriz por cada herramienta a evaluar.*
Actuar	Diseñe una matriz que se denominará (MAT_Resul), con las siguientes especificaciones: Las columnas corresponden a: (1) nombre de la herramienta, (2) valoración de controles, (3) estado. Las filas corresponden a las herramientas conforme se van evaluando. Traslade el valor del porcentaje obtenido en la columna de validación de cada herramienta evaluada de la matriz MAT_T2 a la columna "valoración de controles" de la MAT_Resul. Para definir el "Estado", considere la tabla de *"Métricas para validación de herramientas"*.

b) Los pasos de la metodología son los siguientes:

Paso 1: Seleccionar el escenario en el que desea validar las herramientas.
Paso 2: Realizar la tarea propuesta en la fase "Planear" del ciclo PDCA; como resultado se obtendrán las posibles herramientas a validar.
Paso 3: Ejecutar la tarea señalada en la fase de "Hacer" del ciclo PDCA de la metodología, conforme se tengan herramientas disponibles.
Paso 4: Realizar la tarea "T1" de la fase "Verificar"; como resultado se obtendrá la Matriz (MAT_T1).
Paso 5: Evaluar los controles descritos en la tarea "T2" de la fase "Verificar" con las herramientas evaluadas en el paso 4, si su valoración promedio es >= 1.5, como resultado se obtendrá la Matriz (MAT_T2).
Paso 6: Ejecutar la fase "Actuar" del ciclo PDCA, como resultado obtendrá la Matriz (MAT_Resul).
Paso 7: Repetir el ciclo para validar más herramientas de seguridad. El ciclo termina cuando no tenga más herramientas o cuando el usuario lo desee.

4. DISCUSIÓN

La constante evolución de las redes ha permitido una variedad de opciones de entretenimiento como videos en YouTube, diferentes aplicaciones de mensajería, varias redes sociales. Sin embargo, y este es el problema que busca solucionar esta investigación, la mayoría de usuarios no se preocupa por tener actualizado un antivirus y manejar información encriptada, problema al que se suma el hecho de que las empresas distribuidoras de software no se interesan por proveer con mayor frecuencia las actualizaciones de los sistemas operativos, es decir, los usuarios aún no tienen conciencia de los riesgos que conlleva la falta y el no uso de mecanismos para seguridad móvil.

Entre las principales amenazas de seguridad informática que podemos encontrar están: virus, gusanos, caballos de troya, bombas lógicas, robo y sabotajes (Lucena, 2011). Además, existen vulnerabilidades en los dispositivos móviles en su diseño lo que da lugar a que piratas informáticos y hackers se aprovechen de la situación, muchas veces logran comprometer ciertos procesos para usurpar datos e información confidencial. La tecnología móvil no está exenta de estos inconvenientes técnicos, pese a su tamaño y facilidad de uso, también requiere de hardware y software que puede presentar ciertos fallos conocidos como vulnerabilidades.

Con base en el análisis de estándares realizado, se ha considerado la norma ISO 27001, que es el estándar internacional para seguridad de información, por sus características de flexibilidad y adaptabilidad a cualquier ámbito y entorno en donde se requiera implementar seguridad de la información (ISO/IEC 27001, 2012). De esta norma se ha adoptado el proceso basado en PDCA y de manera transversal la metodología se ha apoyado en seis de los diez escenarios de riesgos propuestos en el mobile top 10 2016 de OWASP. Para la definición de escenarios de la Ms-DisMov se unieron los escenarios 4 y 6, con lo que se disponen de 5 escenarios en los que se han propuesto controles de validación que permitirán definir si una herramienta es eficiente o no. La Figura 2 resume la estructura de la metodología Ms-DisMov propuesta.

Figura 2. Estructura de la metodología MS-DisMov.

En función de los elementos clave y pasos definidos en la estructura de la metodología Ms-DisMov, se procedió con las respectivas pruebas y se pudo verificar las tareas descritas en los ciclos PDCA, hasta seleccionar una herramienta relacionada con la seguridad de la información en dispositivos móviles; finalmente se determinó que de las quince herramientas validadas para el escenario M1: Incorrecto uso de la Plataforma, la herramienta Secure Settings (Google-Play, 2015a) resultó parcialmente eficiente; para el escenario M2: almacenamiento inseguro de datos, las herramientas WiSeID (Google-Play, 2017c) y Box(Google-Play, 2017a) resultaron parcialmente eficientes; para el escenario M3: comunicación insegura, la herramienta TLS/SSL Túnel (Google-Play, 2015b) es eficiente; para el escenario M4: autenticación insegura - M6:Autorización insegura, la

herramienta Mobile Secure (Google-Play, 2017b) es eficiente; para el escenario M5: criptografía insuficiente, la herramienta Encrypted Data Storage Lite (Google-Play, 2014) resultó parcialmente eficiente; mayores detalles de las pruebas realizadas podrá encontrar en Erreyes (2017).

5. CONCLUSIONES

El presente análisis de normas y estándares disponibles en la industria de la seguridad informática, ha permitido la fusión de la ISO 27001 con el OWASP top ten mobile 2016, basado principalmente en el ciclo PDCA, que es el ciclo de mejora continua en donde se ha definido un comportamiento mediante controles de validación por cada escenario del OWASP, logrando de esta manera que la metodología desarrollada se oriente a ambientes móviles.

La estructura de la metodología propuesta permite su fácil adaptación para trabajar con cualquier herramienta que se alinee con los escenarios del OWASP top ten mobile 2016. Se establece, además, que el uso de herramientas adicionales puede ayudar a evitar la explotación de vulnerabilidades presentes en los entornos Android, considerando que algunas herramientas presentan una interfaz muy intuitiva y de fácil uso y facilitan el proceso de su adopción al uso diario, mientras que otras herramientas son difíciles de utilizar ya que se requieren conceptos técnicos que no son de conocimiento general de todo tipo de usuarios.

Como el Android es un entorno cambiante, podría cambiar también el resultado obtenido luego de la ejecución de los pasos propuestos en la metodología para validar las herramientas en función de la versión instalada en cada dispositivo. Por tanto, es necesario tanto un análisis previo de la herramienta que debe ser validada como que el usuario conozca el uso de las herramientas o configuraciones adicionales y las realice en sus dispositivos móviles, de ese modo evita la explotación de las vulnerabilidades detectadas en este tipo de entornos.

Para desarrollos futuros se propone ampliar la metodología para los cuatro escenarios de OWASP que estén orientados al desarrollo de aplicaciones móviles (M7 - Calidad del código, de Cliente, M8 - Manipulación de código, M9 - Ingeniería inversa y M10 - Funcionalidad extraña).

REFERENCIAS

Bertino, E. (2016). Securing Mobile Applications. *Journal in Computing Edge*, *2*(3), 4-6.

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. In: Proc. EuroSPI, pp. 11-23.

Dwivedi, H., Clark, C., Thiel, D. (2010). *Mobile application security*. New York, US: McGraw-Hill, Inc., 432 p.

Erreyes, D. (2017). *Metodología para la selección de herramientas eficientes y protocolos adecuados para mejorar la seguridad de los dispositivos móviles.* Tesis de Posgrado, 159 pp, Universidad de Cuenca, Cuenca, Ecuador. Disponible en http://dspace.ucuenca.edu.ec/handle/123456789/27971

ESET. (2014). *Enjoy Safere Technology*. Disponible en www.eset.es.

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.

Hurlburt, G. (2016). Good Enough Security: The Best We'll Ever Have. *Journal in Computing Edge*, *2*(11), 10-13.

ISACA. (2012). *Un marco de negocio para el gobierno y la gestión de las TI de la empresa*. Disponible en https://articulosit.files.wordpress.com/2013/07/cobit5-framework-spanish.pdf

ISO/IEC 27001. (2012). *ISO 27000*. Disponible en http://www.iso27000.es/iso27000.html

Jøsang, A., Miralabé, L., Dallot, L. (2015). Vulnerability by design in mobile network security. *The Journal of Information Warfare*, *14*(4), 3-5.

Klieber, W., Flynn, L., Bhosale, A., Jia, L., Bauer, L. (2014). *Android taint flow analysis for app sets*. SOAP'14 Proceedings of the 3rd ACM SIGPLAN International Workshop on the State of the Arty in Java Program Analysis. pp. 1-6.

Lucena, J. (2011). *Criptografía y seguridad de computadores*. Version 4-0.8.1. Universidad de Jaen, 307 pp. Disponible en https://ldc.usb.ve/~figueira/cursos/Seguridad/Material/ManuelLucena/cripto.pdf

Management, T. (2008). Traducción oficial Official translation Traduction officielle ISO. Disponible en http://www.umc.edu.ve/pdf/calidad/normasISO/ISO_9001(ES)_CERT_2008_final.pdf

Memon, A. M., Anwar, A. (2016). Colluding Apps: Tomorrow's mobile malware threat. *Journal in Computing Edge*, *2*(3), 31-35.

OWASP. (2016). *Mobile top 10 2016-Top 10*. Disponible en https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

Task, J., Transformation, F. (2012). *Guide for conducting risk assessments*, Disponible en http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Google play

Google-Play, 2014. EDS Lite. Descargado de https://play.google.com/store/apps/details?id=com.sovworks.edslite el 14 de marzo de 2017.

Google-Play, 2015. Secure Settings. Descargado de https://play.google.com/store/apps/details?id=com.intangibleobject.securesettings.plugin el 7 de febrero de 2017.

Google-Play, 2015. Tunnel, TLS/SSL. Descargado de https://play.google.com/store/apps/details?id=eu.smallapps.tunnel&hl=es el 23 de febrero de 2017.

Google-Play. (2017a). Box. Descargado de https://play.google.com/store/apps/details?id=com.box.android el 10 de febrero de 2017.

Google-Play. (2017b). Mobile Secure. Descargado de https://play.google.com/store/apps/details?id=com.fsecure.ms.dc&hl=es el 10 de marzo de 2017.

Google-Play. (2017c). WISeID. Descargado de https://play.google.com/store/apps/details?id=com.wisekey.wiseid.android el 8 de febrero de 2017.