Tipo de artículo: Artículo original

Metodología para evaluar el nivel de seguridad de las aplicaciones móviles sobre plataforma Android en ETECSA

Methodology to evaluate the security level of mobile applications on Android platform in ETECSA

Odalys Sardiñas Hernández[1*], https://orcid.org/0000-0001-5480-5451
Raquel Hernández Borrego[2], https://orcid.org/0000-0001-5663-7324
Henry Raúl González Brito[3], https://orcid.org/0000-0002-3226-9210

[1] Dpto de Organización y Control de la Seguridad de las TIC. Empresa de Telecomunicaciones de Cuba S. A. odalys.hernandez@etecsa.cu
[2] Dpto Docente. Universidad Militar de Ciencias Jurídicas Comandante Arides Estévez Sánchez. rtome660@gmail.com.cu
[3] Centro de Telemática, Facultad 2, Universidad de las Ciencias Informáticas. henryraul@uci.cu

*** Autor para correspondencia: odalys.hernandez@etecsa.cu**

Resumen

La investigación surge por la necesidad de tener en los procesos de trabajo de ETECSA procedimientos orientados a las pruebas de seguridad de las aplicaciones móviles, fundamentalmente desarrolladas o adquiridas sobre plataforma Android. La presente investigación propone una metodología para evaluar el nivel de seguridad de las aplicaciones móviles sobre plataforma Android en ETECSA, que incluye las mejores prácticas y estándares a nivel internacional en correspondencia con las características de la Empresa. La misma se sometió a un proceso de validación mediante el método de las evaluaciones de los expertos y la realización de un experimento. Los resultados alcanzados demuestran que es factible detecta las vulnerabilidades y contribuye a evaluar el nivel de seguridad de las aplicaciones móviles sobre plataforma Android desarrolladas o adquiridas por la Empresa.

Palabras clave: vulnerabilidades de seguridad; pruebas de seguridad; aplicaciones móviles; Android.

Abstract

The research arises from the need to have procedures in ETECSA's work processes oriented to security testing of mobile applications, mainly developed or acquired on the Android platform. This research proposes a methodology to evaluate the security level of mobile applications on the Android platform in ETECSA, which includes the best practices and international standards in correspondence with the characteristics of the Company. It underwent a validation process using the method of expert evaluations and the performance of an experiment. The results achieved show that it is feasible, detects vulnerabilities and contributes to evaluating the level of security of mobile applications on the Android platform developed or acquired by the company.

Keywords: *security vulnerabilities; security tests; mobile applications; Android.*

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

Recibido: 18/09/2020
Aceptado: 21/11/2020

Introducción

El número de usuarios de dispositivos móviles ha aumentado significativamente en los últimos años, y las aplicaciones móviles se han convertido en herramientas integrales para la vida diaria (ALI and KAUR 2021; JADHAV *et al.* 2015; STATISTA 2021). En el mundo de los dispositivos móviles existen diversas plataformas como iOS y Android, aunque este último se destaca por estar instalado en un mayor número de dispositivos, lo que representa un 74,3%, con respecto a otros sistemas operativos (STATCOUNTER_GLOBALSTATS 2020). Puede afirmarse que las características de apertura y flexibilidad de esta plataforma, lo ha convertido en el líder del mercado de la telefonía móvil (CHEN, S. *et al.* 2020; DASHEVSKYI *et al.* 2020; LEE and PARK 2020; SURESH *et al.* 2019).

Las operaciones realizadas a través de las aplicaciones desarrolladas para Android y el aumento del almacenamiento de la información personal, han convertido a los dispositivos móviles en uno de los principales blancos de ataques de los cibercriminales (PAL *et al.* 2020; VACHON 2020; WANG *et al.* 2020; WEICHBROTH and ŁYSIK 2020). Las aplicaciones móviles, a pesar de su utilidad, pueden presentar serios riesgos de seguridad para una organización y sus usuarios, debido a las vulnerabilidades que pueden existir dentro de su software (HUANG *et al.* 2019; QAMAR *et al.* 2019; SAUDI *et al.* 2019). Varios autores opinan que la seguridad se ha convertido en una preocupación central para los dispositivos móviles (CHEN, GONG *et al.* 2019; WEICHBROTH and ŁYSIK 2020). Las vulnerabilidades de las aplicaciones móviles y los defectos de seguridad representan una preocupación constante ante la explotación de vulnerabilidades por los adversarios (HAMMOOD *et al.* 2020; JIGO 2020; QIAN *et al.* 2018).

En Cuba, en los últimos años se ha masificado el uso de las tecnologías de la información y las comunicaciones, así como en el acceso a Internet. Paralelamente, en la actualidad en el país se desarrollan aplicaciones, principalmente para móviles con plataforma Android, que elevan el bienestar de la población y acelera el desarrollo económico y social de la nación. A tenor de este crecimiento, la Empresa de Telecomunicaciones de Cuba S.A. (ETECSA) viene desarrollando diversas aplicaciones para plataforma Android, tanto para usos empresariales como para la población, que facilitan la informatización de la sociedad cubana. A medida que avanza el desarrollo de aplicaciones móviles Android y más equipos conectados a internet en Cuba, surgen nuevos ataques y más vías de accesos para los adversarios. En este sentido, se ha identificado que el incremento constante de los servicios y de los usuarios conectados a Internet en Cuba, va unido por un conocimiento limitado de su población en general acerca de la seguridad informática. Por otra parte, en ETECSA se requiere un proceder robusto que permita garantizar, de una forma organizada, el nivel de seguridad de las aplicaciones móviles que se desarrollan o se adquieren por la Empresa.

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

Ante esta situación, se propuso diseñar una metodología para evaluar el nivel de seguridad de las aplicaciones móviles sobre plataforma Android en ETECSA.

Escoger y llevar a cabo una metodología permite trabajar de forma organizada y cubrir la totalidad de las pruebas que se deben realizar, obteniendo así un resultado más completo y correcto. La literatura consultada plantea que existen diversos estándares y mejores prácticas, que constituyen modelos de referencia internacional, los cuales proporcionan diversas opciones, requisitos o pautas a seguir en cuestión de seguridad de aplicaciones móviles (ABUSALIM *et al.* 2021; BERGADANO *et al.* 2020; KHOKHLOV and REZNIK 2018; PALMA *et al.* 2020). Constituyen referentes teóricos de la presente investigación, diversos aspectos de los estándares y mejores prácticas, tales como la Guía de pruebas de OWASP (MUELLER *et al.* 2019; PAN 2019), las actividades que propone NIST para realizar una prueba de verificación de la seguridad de una aplicación móvil (HOWELL *et al.* 2020; OGATA *et al.* 2018) y el procedimiento de cálculo de riesgo de OWASP para obtener la lista de los principales riesgos de seguridad móviles (ACHARYA *et al.* 2015; SINGH THAKUR and CARTER 2016).

Materiales y métodos

En el estudio se estableció el siguiente problema de investigación: ¿Cómo contribuir a evaluar en ETECSA el nivel de seguridad de las aplicaciones móviles desarrolladas para plataforma Android? Para dar respuesta al problema descrito y lograr los objetivos de la investigación se elaboró la siguiente hipótesis: Una metodología que incluya las mejores prácticas y estándares a nivel internacional en correspondencia con las características de ETECSA, contribuirá a evaluar el nivel de la seguridad de las aplicaciones móviles sobre plataforma Android. Para la investigación se aplicaron los siguientes métodos y técnicas:

- **Métodos Teóricos**: se utilizó el método analítico-sintético para analizar los referentes teóricos y las mejores prácticas a nivel mundial del objeto de estudio y campo de acción y el método histórico-lógico para determinar los antecedentes y la evolución de las pruebas de seguridad a las aplicaciones móviles sobre plataformas android.
- **Métodos Empíricos:** se utilizó la entrevista para constatar el problema científico, específicamente la existencia en ETECSA de procesos de trabajo que permitan garantizar el nivel de seguridad de las aplicaciones móviles sobre plataforma android y obtener las características o peculiaridades de la empresa. el análisis de documentos, para determinar en la reglamentación de la entidad las brechas prácticas que existen

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

en este sentido. el experimento y la consulta a los expertos para validar la propuesta de metodología para evaluar el nivel de la seguridad de las aplicaciones móviles sobre plataforma Android.

Para el diseño del método de expertos, se seleccionaron 13 expertos en seguridad informática y seis especialistas de ETECSA. Se escogieron muestras intencionales a partir de la experiencia práctica de los sujetos con el objeto de la investigación. Además, fueron seleccionados al azar 10 especialistas de seguridad informática de las distintas unidades organizativas de la Empresa. La metodología se aplicó en seis de las aplicaciones que se le solicitaron pruebas de seguridad en el período comprendido entre marzo y octubre de 2020, lo cual representa el 100 % de las solicitudes realizadas.

Resultados y discusión

En la presente investigación se define como metodología para evaluar el nivel de seguridad de las aplicaciones móviles sobre plataforma Android en ETECSA, al conjunto de técnicas de trabajo y actividades que ejecutan los especialistas para realizar los procedimientos que permiten preparar el entorno de trabajo, recepcionar la solicitud de aval de seguridad y realizar su auditoría de forma organizada, estructurada y estandarizada, a fin de identificar las vulnerabilidades, los riesgos y el impacto asociado a ellas.

La Metodología propuesta está compuesta por dos etapas, tres subprocesos y 13 actividades, las que se relacionan en la figura 1. La primera etapa, tiene como objetivo definir las principales herramientas y entornos de pruebas que se deben emplear. Los entornos de prueba pueden ser los emuladores o los dispositivos móviles. Los emuladores permiten recrear cualquier dispositivo y versión de Android, facilitan la interacción con la aplicación de la misma manera que un dispositivo móvil y proporcionan diferentes funciones para realizar las pruebas de seguridad, sin embargo, presentan algunas desventajas cuando se trata de aplicaciones que trabajan con una red de datos específica y la ejecución de la aplicación es lenta. Es por ello que se propone realizar las pruebas de seguridad utilizando un dispositivo móvil físico siempre que sea posible. Los emuladores que propone esta metodología son los que utiliza el Mobile Security Framework (MobSF) y Android Studio (BERGADANO *et al.* 2020; IBRAR *et al.* 2017; WHITE 2020).

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

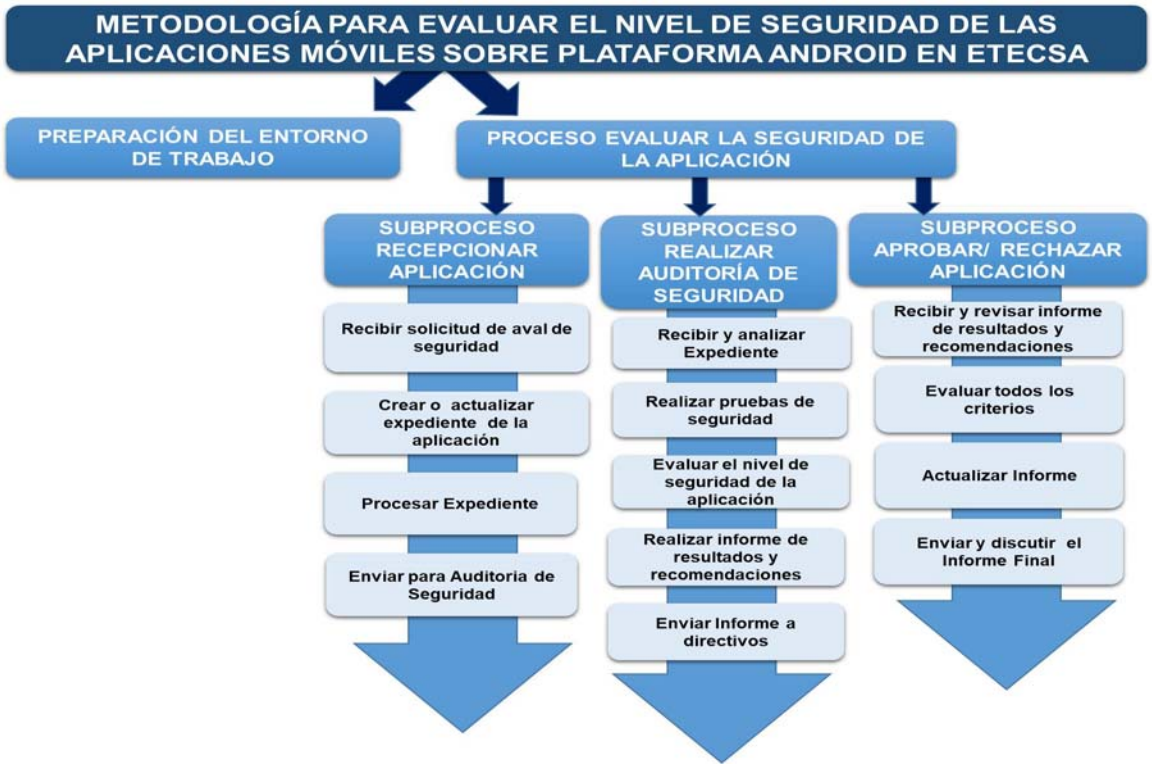

Figura 1. Metodología para evaluar el nivel de seguridad de las aplicaciones móviles sobre plataforma Android en ETECSA.

Para evaluar la comunicación en la red de las aplicaciones móviles con los servidores, se emplean las herramientas OWASP ZAP, Burp Suite y Wireshark, las herramientas Dex2jar, apktools, MobSF y Java Descompiler-GUI para examinar el código APK (Android Application Package), las herramientas Drozer y adb se utilizan para el análisis dinámico de los diferentes componentes que conforman las apk y PidCat para revisar los registros de la aplicación en tiempo real (MALIK *et al.* 2017; PALACIOS *et al.* 2019; RAHALKAR 2021). En la segunda etapa se realiza los subprocesos de recepción, auditoría y aprobación o rechazo de la aplicación mediante el flujo de trabajo representado en la figura 2:

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

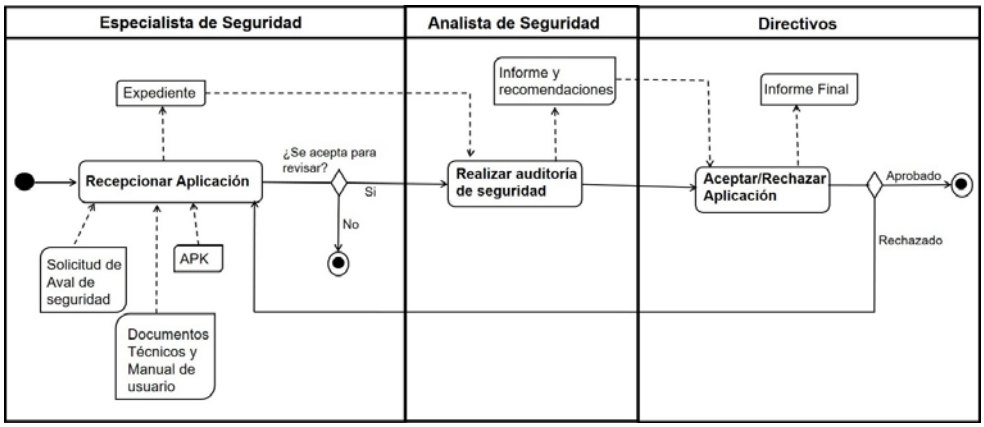

Figura 2. Fase Subproceso Evaluar la seguridad de la aplicación móvil sobre plataformas Android. Elaboración propia.

En el subproceso Recepcionar Aplicación se define la documentación a entregar por los desarrolladores y/o responsables de la aplicación a evaluar, así como los pasos a realizar por el especialista de seguridad a cargo de la recepción, como se representa en la figura 3:

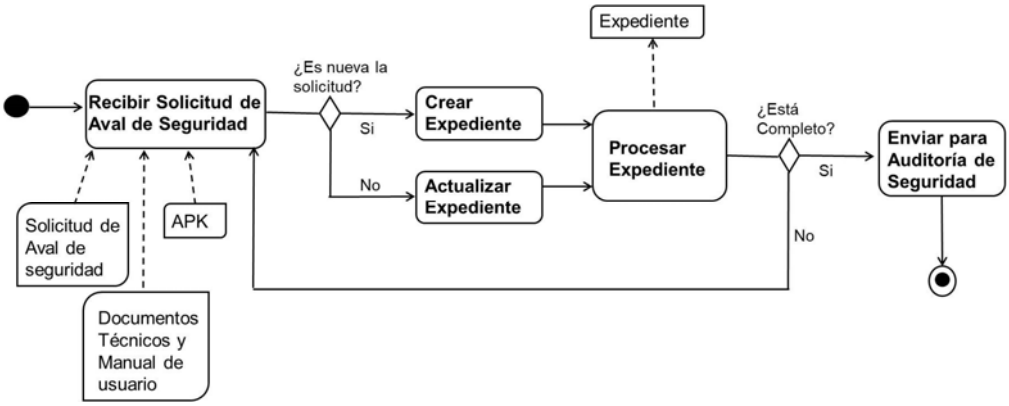

Figura 3. **S**ubproceso Recepcionar aplicación. Elaboración propia.

El subproceso Realizar Auditoría de Seguridad tiene cuatro actividades principales. En las dos primeras actividades se describen las pruebas de seguridad, estructuradas en seis grupos: Recopilación de información, Fuga de información confidencial, Comunicación, Validación de datos, Calidad del código y Manipulación e Ingeniaría Inversa. En este subproceso, como tercera actividad, se calcula el nivel de seguridad de la aplicación a partir de las vulnerabilidades encontradas (figura 4) y se realiza el informe con los resultados obtenidos en la auditoría de seguridad. Para ello se aplica la lista de chequeo de la tabla 1.

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

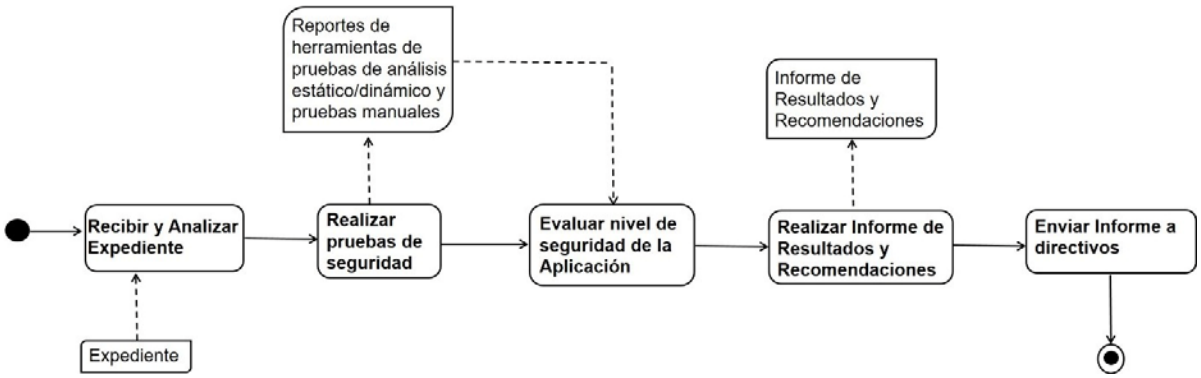

Figura 4. Subproceso Realizar Auditoría de Seguridad. Elaboración propia.

Tabla 1. Pruebas de Seguridad que se deben de realizar en las actividades. Elaboración propia.

Actividad	**Grupo de Pruebas**	**Objetivo**	**Pruebas de Seguridad**	**Herramientas**
Recibir y analizar expediente	Recopilación de información	Recopilar información sobre la aplicación a evaluar.	Detectar posibles vulnerabilidades públicas en las bibliotecas de terceros.	Documentación entregada, MobFS, motores de búsquedas, apktools, d2j-dex2jar, Dev2jar, JD-GUI
			Obtener la configuración de la aplicación.	
Realizar pruebas de seguridad	Fuga de información confidencial	Identificar si la aplicación expone información confidencial y útil para un atacante.	Prueba de manejo de errores y divulgación de Información confidencial a través de la Interfaz de usuarios.	Pruebas manuales, Dev2jar, JD-GUI, MobSF, Drozer, adb, PidCat, Burp Suite, Wireshark
			Determinar si la memoria caché del teclado está deshabilitada.	
			Prueba de almacenamiento local para datos confidenciales.	
			Pruebas de registros (logs) para datos confidenciales.	
			Prueba de exposición de funcionalidades sensibles y datos almacenados	
			Determinar si los datos confidenciales se envían a terceros.	
	Comunicación	Verificar que la información transmitida	Prueba de verificación de protocolos seguros de comunicación.	Burp Suite, Wireshark, OWASP ZAP

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

		no pueda ser manipulada.	Pruebas de verificación de identidad de punto final, de almacenes de certificados personalizados y fijación de certificados	
	Validación de datos	Asegurar que los datos recibidos procedan de fuentes confiables. Se valida la entrada de los datos a la aplicación.	Prueba de inyección de fragmentos.	MobSF, JD-GUI, Drozer
			Prueba de ejecución de JavaScript en WebViews.	
			Prueba de controladores de protocolo WebView y objetos Java	
	Calidad del código	Identificar si se siguieron buenas prácticas de desarrollo.	Asegurarse de que la aplicación esté firmada correctamente.	MobSF, JD-GUI
			Pruebas de ofuscación.	
	Manipulación e Ingeniería Inversa	Determinar si la aplicación que se está revisando posee mecanismos que dificulten los procesos de manipulación e ingeniería inversa.	Prueba de comprobaciones de integridad de archivos.	apktools, Ejecución de diferentes herramientas de Análisis Dinámico, Dispositivo Ruteado, Emulador de Android Studio o de MobSF
			Pruebas de las comprobaciones de integridad del tiempo de ejecución.	
			Prueba de detección de root	
			Prueba de detección de emulador	
			Prueba de detección anti-depuración	

Las pruebas propuestas pueden realizarse de conjunto con otras más específicas si existen requisitos especiales de la aplicación móvil. A continuación, se procede a realizar la evaluación del nivel de seguridad de la aplicación analizada. Para ello se deberá identificar el riesgo de las vulnerabilidades encontradas con los siguientes indicadores:

- **Probabilidad de Ocurrencia:** Se calcula según la calificación utilizado por OWASP (SINGH THAKUR and CARTER 2016).
- **Impacto del negocio: S**e identificaron nueve indicadores de impacto al negocio, se calificará cada indicador de 0 a 3 en correspondencia con la importancia de la aplicación y en qué condiciones será empleada. Los indicadores son:
    a. El robo de identidad
    b. Daño a la reputación de la Empresa
    c. Interrupción de servicios
    d. Violación de la privacidad de un cliente
    e. Robo de información confidencial

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

f. Acceso no autorizado a datos
g. Robo de propiedad intelectual
h. Degradación en el rendimiento de la aplicación móvil
i. Pérdidas de ingreso debido a la piratería

El riesgo de la vulnerabilidad obtenido es el resultado de la interceptación de los valores alcanzados en los indicadores probabilidad de ocurrencia de la vulnerabilidad e impacto al negocio según se muestra en la tabla 2:

Tabla 2. Cálculo del riesgo de la vulnerabilidad. Elaboración propia.

	Impacto		
Probabilidad de Ocurrencia	Bajo	Moderado	Alto
Bajo	Bajo	Bajo	Moderado
Moderado	Bajo	Moderado	Alto
Alto	Moderado	Alto	Crítico

Posteriormente, se establece la calificación general de la aplicación y por tanto su nivel de seguridad. Esta calificación se calcula según la cantidad de vulnerabilidades críticas, altas, medias y bajas encontradas (tabla 3):

Tabla 3. Escala de calificación del nivel de seguridad de las aplicaciones revisadas. Elaboración propia.

Escala	**Valor obtenido en el análisis de riesgo**	**Nivel de seguridad**
Al menos una vulnerabilidad Crítica	Crítico	Muy bajo
Vulnerabilidades Altas >2		
Vulnerabilidades Medias >8		
Vulnerabilidades Bajas >26		
Vulnerabilidades Altas<3	Alto	Bajo
2<Vulnerabilidades Medias<9		
8<Vulnerabilidades Bajas<27		
Vulnerabilidades Medias <3	Medio	Medio
2<Vulnerabilidades Bajas<9		
Vulnerabilidades Bajas< 3	Bajo	Alto

Como resultado final del subproceso Realizar auditoría de seguridad, se efectúa la actividad Realizar informe de resultados y recomendaciones. esta actividad tiene como objetivo generar el informe de los resultados obtenidos en

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

las pruebas de la aplicación y las recomendaciones para disminuir o erradicar las vulnerabilidades encontradas. en la tabla 4 se enumeran los aspectos que se deberán abordar:

Tabla 4. Resumen de la estructura del Informe de resultados y recomendaciones. Elaboración propia.

Aspectos	**Finalidad**
Objetivo	Propósito general de la auditoría de seguridad.
Resumen Ejecutivo	Enumerar las vulnerabilidades encontradas y las recomendaciones generales para mitigar las vulnerabilidades, de una manera clara y sencilla. Este resumen debe ser entendido por cualquier directivo. Al final de esta sección se debe responder a la siguiente interrogante: ¿Puede salir la aplicación móvil sobre plataforma Android a producción?
Detalle de Resultados Técnicos	Nombre y versión del paquete (APK), versión mínima del SDK y los permisos solicitados al dispositivo móvil sobre plataforma Android. Otras informaciones técnicas de interés.
Enumeración de Vulnerabilidades y Recomendaciones	Vulnerabilidades encontradas, el riesgo asociado y las recomendaciones para erradicar o disminuir el impacto que pudiera ocasionar. Aspectos técnicos e impacto al negocio. Pruebas realizadas y las capturas de pantalla o ficheros de escaneos de las herramientas utilizadas que demuestren la vulnerabilidad encontrada, con sus referencias de ser necesario.

El último subproceso, denominado Aprobar o rechazar la aplicación, tiene como ejecutores los superiores o directivos. Está destinado para revisar el informe final de trabajo realizado y sus recomendaciones, actualizando la información a partir de otros criterios que pudieran existir. Ellos son los responsables de aprobar o rechazar el despliegue de la aplicación y de dirigir el encuentro de discusión de resultados con los desarrolladores y/o responsables de la aplicación en la Empresa. La actualización del informe se realiza a través de la consulta con otros especialistas o desarrolladores, la valoración personal de la propia práctica profesional del directivo y concluye, con su aceptación o rechazo para el despliegue de la aplicación. Si la aplicación es rechazada los desarrolladores o responsables de la aplicación en ETECSA tendrán que solicitar una nueva prueba de seguridad, posterior a su perfeccionamiento.

Validación de la Metodología propuesta

Los resultados de la consulta con los expertos indican que existió la tendencia de ser valorada la metodología de bastante adecuada (BA). Con respecto a la variable independiente (metodología para evaluar el nivel de seguridad de las aplicaciones móviles sobre plataforma Android), en la aplicación de su primera etapa, se estableció que la preparación del entorno de trabajo resultó sencilla la adquisición, instalación y utilización de las herramientas a emplear. En el indicador precisión se identificó que la entrega de la documentación constituye un elemento necesario

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

en la metodología descrita, al impactar la no presentación o su demora en los tiempos previstos para su presentación final. En la variable dependiente (evaluar el nivel de seguridad de las aplicaciones móviles sobre plataforma Android) se obtuvieron los resultados los siguientes:

- Indicador detección de vulnerabilidades: Las vulnerabilidades más frecuentes encontradas en las aplicaciones fueron las relacionadas con la Calidad del código (66,7%), Almacenamiento de datos inseguro (50%) y Comunicación Insegura (50%). Además, se identificó que ninguna de las aplicaciones revisadas poseía mecanismos que dificultaran los procesos de manipulación e ingeniería inversa, pero al no ser de estricto cumplimiento, sólo se valoró que debía cumplirlo una sola aplicación (figura 5).
- Indicador establecimiento del nivel de seguridad a partir de las vulnerabilidades encontradas: Las pruebas de seguridad aplicadas permitieron identificar que cuatro aplicaciones (66,7%) tenían un nivel de seguridad muy bajo; en una era bajo (16,7%) y finalmente una (16,7%) poseía un nivel alto de seguridad.

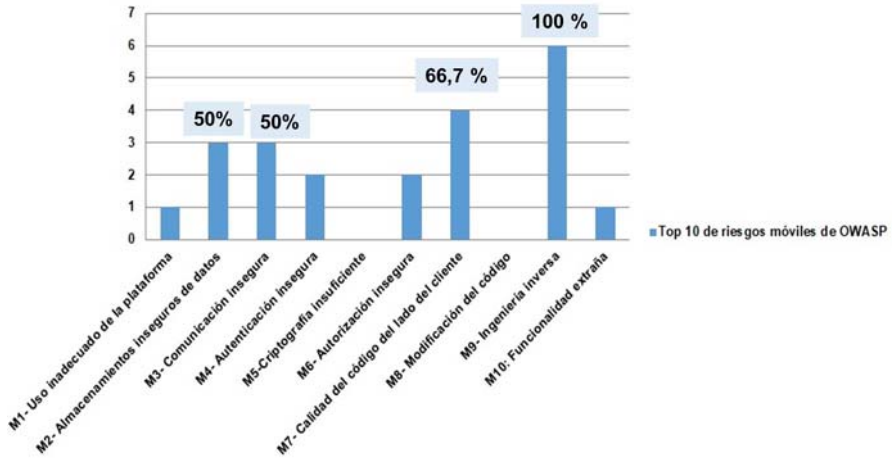

Figura 5. Cantidad de Aplicaciones que presentan vulnerabilidades. Elaboración propia.

- **Indicador contribución de resultados:** El informe de los resultados y recomendaciones discutidos con los desarrolladores o responsables, permitió dar a conocer el nivel de seguridad y de riesgo de sus aplicaciones, así como hacerlos conscientes de la necesidad de su perfeccionamiento. De las cuatro aplicaciones que fueron evaluadas por segunda vez con la metodología, las aplicaciones 3, 5 y 6 (75 %) se volvieron a presentar al mes de evaluadas y la aplicación 2 (25 %) a los tres meses. De ellas, las aplicaciones 2, 5, y 6 lograron ser clasificadas en un nivel de seguridad alto y la aplicación 3 logró un nivel medio de seguridad (figura 6):

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

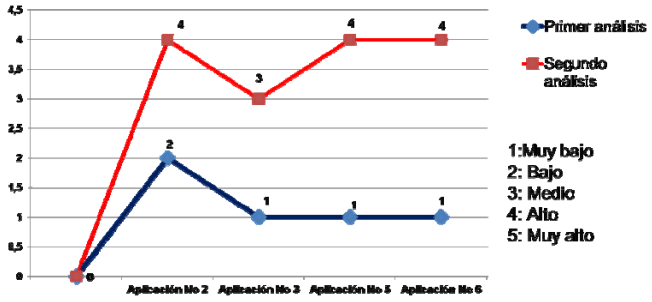

Figura 6. Comparación de los resultados de las pruebas de seguridad del primero y segundo análisis. Elaboración propia.

Conclusiones

La metodología para evaluar el nivel de seguridad de las aplicaciones móviles sobre plataforma Android que se propone, se sustentan en las mejores prácticas y estándares a nivel internacional en correspondencia con las características de ETECSA. Tiene como estructura dos etapas, tres subprocesos y 13 actividades. El análisis de los resultados de la aplicación de los métodos de las evaluaciones de los expertos y el experimento, permite concluir que la metodología que se propone es factible, precisa, detecta las vulnerabilidades y contribuye a evaluar el nivel de seguridad de las aplicaciones desarrolladas o adquiridas por la Empresa. Se recomienda continuar investigando en el perfeccionamiento de la metodología, fundamentalmente en la actualización de las pruebas de seguridad considerando las mejores prácticas y estándares a nivel internacional. Además, se debe profundizar científicamente en las vías para añadir nuevas etapas a la metodología que garantice el análisis de la seguridad durante todo el ciclo de vida del desarrollo de la aplicación.

Conflictos de intereses

Los autores de la investigación declaran no poseer conflictos de intereses.

Contribución de los autores

1. Conceptualización: Odalys Sardiñas Hernández
2. Curación de datos: Odalys Sardiñas Hernández, Raquel Hernández Borrego
3. Análisis formal: Odalys Sardiñas Hernández, Raquel Hernández Borrego
4. Adquisición de fondos: Odalys Sardiñas Hernández, Raquel Hernández Borrego, Henry Raúl González Brito

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

5. Investigación: Odalys Sardiñas Hernández¸ Raquel Hernández Borrego, Henry Raúl González Brito
6. Metodología: Odalys Sardiñas Hernández, Raquel Hernández Borrego
7. Administración del proyecto: Odalys Sardiñas Hernández
8. Recursos: Odalys Sardiñas Hernández, Raquel Hernández Borrego, Henry Raúl González Brito
9. Software: Odalys Sardiñas Hernández
10. Supervisión: Raquel Hernández Borrego, Henry Raúl González Brito
11. Validación: Odalys Sardiñas Hernández, Raquel Hernández Borrego
12. Visualización: Odalys Sardiñas Hernández
13. Redacción – borrador original: Odalys Sardiñas Hernández, Raquel Hernández Borrego
14. Redacción – revisión y edición: Henry Raúl González Brito

Financiamiento

La investigación ha sido financiada por las instituciones de los autores y no requirió fuentes de financiación externas.

Referencias

ABUSALIM, S. W. G.; R. IBRAHIM, *et al.* Comparative Analysis of Software Testing Techniques for Mobile Applications *Journal of Physics: Conference Series*, 2021, 1793(1): 12-36.

ACHARYA, S.; B. EHRENREICH, *et al. OWASP inspired mobile security*. 2015 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 2015. 782-784 p.

ALI, M. I. and S. KAUR. *BYOD Cyber Threat Detection and Protection Model*. 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2021. 211-218 p.

BERGADANO, F.; M. BOETTI, *et al.* A modular framework for mobile security analysis *Information Security Journal: A Global Perspective*, 2020, 29(5): 220-243.

CHEN, G.; W. MENG, *et al. Revisiting Mobile Advertising Threats with MAdLife*. *The World Wide Web Conference*. San Francisco, CA, USA, Association for Computing Machinery, 2019. 207–217.

CHEN, S.; L. FAN, *et al. An Empirical Assessment of Security Risks of Global Android Banking Apps*. 2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE), 2020. 1310-1322 p. 1558-1225

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

DASHEVSKYI, S.; Y. ZHAUNIAROVICH, *et al. Dissecting Android Cryptocurrency Miners*. *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy*. New Orleans, LA, USA, Association for Computing Machinery, 2020. 191–202.

HAMMOOD, W. A.; R. ABDULLAH, *et al.* A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number *IOP Conference Series: Materials Science and Engineering*, 2020, 769: 12-61.

HOWELL, G. E.; K. R. BOECKL, *et al.* Mobile Device Security: Corporate-Owned Personally-Enabled (COPE), 2020.

HUANG, J.; N. BORGES, *et al. Up-To-Crash: Evaluating Third-Party Library Updatability on Android*. 2019 IEEE European Symposium on Security and Privacy (EuroS&P), 2019. 15-30 p.

IBRAR, F.; H. SALEEM, *et al. A Study of Static Analysis Tools to Detect Vulnerabilities of Branchless Banking Applications in Developing Countries*. *Proceedings of the Ninth International Conference on Information and Communication Technologies and Development*. Lahore, Pakistan, Association for Computing Machinery, 2017. Article 30.

JADHAV, S.; T. OH, *et al. Mobile device penetration testing framework and platform for the mobile device security course*. 2015 17th International Conference on Advanced Communication Technology (ICACT), 2015. 675-680 p. 1738-9445

JIGO, E. Development of Criteria for Mobile Device Cybersecurity Threat Classification and Communication Standards (CTC&CS), 2020.

KHOKHLOV, I. and L. REZNIK. *Android system security evaluation*. 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2018. 1-2 p. 2331-9860

LEE, K. and H. PARK. *Malicious Adware Detection on Android Platform using Dynamic Random Forest*. Innovative Mobile and Internet Services in Ubiquitous Computing, Cham, Springer International Publishing, 2020. 609-617 p. 978-3-030-22263-5

MALIK, N.; J. CHANDRAMOULI, *et al. Using network traffic to verify mobile device forensic artifacts*. 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2017. 114-119 p. 2331-9860

MUELLER, B.; S. SCHLEIER, *et al. MSTG Mobile Security Testing Guide*. The OWASP Fundation, 2019. 536 p.

OGATA, M.; J. FRANKLIN, *et al. Vetting the security of mobile applications*, National Institute of Standards and Technology, 2018.

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

PAL, D.; C. ARPNIKANONDT, *et al.* Personal Information Disclosure via Voice Assistants: The Personalization–Privacy Paradox *SN Computer Science*, 2020, 1(5): 280.

PALACIOS, J.; G. LÓPEZ, *et al.* Security Analysis Protocol for Android-Based Mobile Applications, 2019, (E19): 366-378.

PALMA, F.; N. REALISTA, *et al. Automated security testing of Android applications for secure mobile development*. 2020 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), 2020. 222-231 p.

PAN, Y. *Interactive Application Security Testing*. 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA), 2019. 558-561 p.

QAMAR, A.; A. KARIM, *et al.* Mobile malware attacks: Review, taxonomy & future directions *Future Generation Computer Systems*, 2019, 97: 887-909.

QIAN, K.; R. M. PARIZI, *et al. OWASP Risk Analysis Driven Security Requirements Specification for Secure Android Mobile Software Development*. 2018 IEEE Conference on Dependable and Secure Computing (DSC), 2018. 1-2 p.

RAHALKAR, S. Testing Mobile Apps and APIs with Burp Suite. en: *A Complete Guide to Burp Suite : Learn to Detect Application Vulnerabilities*. Berkeley, CA, Apress, 2021. 147-164.p.

SAUDI, M. M.; A. AHMAD, *et al. Mobile Malware Classification for Social Media Application*. 2019 International Conference on Cybersecurity (ICoCSec), 2019. 70-75 p.

SINGH THAKUR, M. and J. CARTER. *Top 10 Mobile Risks*, The OWASP Project, 2016. [20/01/2021]. Disponible en: https://owasp.org/www-project-mobile-top-10/

STATCOUNTER_GLOBALSTATS. *Mobile Operating System Market Share Worldwide* Statcounter_GlobalStats, 2020. [5/6/2021]. Disponible en: https://gs.statcounter.com/os-market-share/mobile/worldwide

STATISTA. *Smartphones - Statistics & Facts*, 2021. [20/5/2021]. Disponible en: https://bit.ly/3veeijW

SURESH, S.; F. DI TROIA, *et al.* An analysis of Android adware *Journal of Computer Virology and Hacking Techniques*, 2019, 15(3): 147-160.

VACHON, P. The identity in everyone's pocket *Communications of the ACM*, 2020, 64: 46–55.

WANG, C.; Y. WANG, *et al.* User authentication on mobile devices: Approaches, threats and trends *Computer Networks*, 2020, 170: 107-118.

WEICHBROTH, P. and Ł. ŁYSIK Mobile Security: Threats and Best Practices *Mobile Information Systems*, 2020, 2020: 882-8078.

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)

WHITE, T. *IT Managers' and IT Professionals' Mobile Device Security Strategies: A Qualitative Exploratory Case Study*, University of Phoenix, 2020. p.

Esta obra está bajo una licencia *Creative Commons* de tipo Atribución 4.0 Internacional (CC BY 4.0)