

## Evaluación de vulnerabilidades informáticas en códigos QR de la aplicación de Banca Móvil “Wallink”

*Evaluation of computer vulnerabilities in QR codes of the “Wallink” mobile banking application*

Carlos Fajardo, Marco Yamba-Yugsi, Eduardo Mauricio Campaña Ortega

### Resumen:

El crecimiento de la banca financiera en Ecuador se ha evidenciado en la digitalización de sus servicios, lo que conlleva nuevos desafíos en ciberseguridad. Las aplicaciones de banca móvil utilizan diversos métodos de autenticación, como códigos QR, que pueden presentar vulnerabilidades que deben ser descubiertas para evitar ser explotadas por delincuentes cibernéticos. Esta investigación tuvo como objetivo evaluar la seguridad de los códigos QR en la aplicación de banca móvil “Wallink” aplicando la metodología de pruebas de seguridad del estándar SP 800-115 del Instituto Nacional de Estándares y Tecnología. Se generaron 672 códigos QR durante seis días para decodificarlos y analizar patrones y cifrado, además de realizar análisis estático y dinámico de la aplicación. Los resultados revelaron un prefijo constante “PHIQR” seguido de 48 caracteres, lo que podría representar una vulnerabilidad por reducción de entropía inicial. Se determinó una probabilidad del 95.17% de que los códigos utilicen sustitución polialfabética. El análisis estático obtuvo un puntaje de riesgo medio (46/100), identificando vulnerabilidades como el “exploit Janus” y permisos considerados excesivos. El análisis dinámico mostró una configuración adecuada de protocolos TLS/SSL, pero prácticas de almacenamiento inapropiadas. Estos hallazgos permitieron medir el nivel de riesgo en 2,83/5, determinando un riesgo medio para el uso de códigos QR. La evaluación de riesgos subraya la importancia de fortalecer la seguridad mediante algoritmos de cifrado más robustos y mejores prácticas de desarrollo seguro.

Palabras clave: Ciberseguridad; Aplicaciones Financieras; Vulnerabilidades; Análisis de riesgos; Autenticación.

---

### Carlos Fajardo

Universidad Católica de Cuenca | Cuenca | Ecuador | carlos.fajardo.90@est.ucacue.edu.ec  
<http://orcid.org/0009-0008-8049-7796>

### Marco Yamba-Yugsi

Universidad Católica de Cuenca | Cuenca | Ecuador | marco.yamba@ucacue.edu.ec  
<https://orcid.org/0000-0003-4095-1444>

### Eduardo Mauricio Campaña Ortega

Universidad Católica de Cuenca | Cuenca | Ecuador | eduardo.campana@ucacue.edu.ec  
<http://orcid.org/0000-0001-7720-5213>

## Abstract

The growth of financial banking in Ecuador has been evidenced by the digitalization of its services, which brings with it new cybersecurity challenges. Mobile banking applications use various authentication methods, such as QR codes, which may present vulnerabilities that must be discovered to avoid being exploited by cybercriminals. This research aimed to evaluate the security of QR codes in the mobile banking application “Wallink” by applying the security testing methodology of the National Institute of Standards and Technology’s SP 800-115 standard. A total of 672 QR codes were generated over six days for decoding, pattern and encryption analysis, as well as static and dynamic analysis of the application. The results revealed a constant prefix “PHIQR” followed by 48 characters, which could represent an initial entropy reduction vulnerability. A 95.17% probability that the codes use polyalphabetic substitution was determined. The static analysis obtained a medium risk score (46/100), identifying vulnerabilities such as the “Janus exploit” and permissions considered excessive. The dynamic analysis showed an adequate configuration of TLS/SSL protocols, but inappropriate storage practices. These findings allowed the risk level to be measured at 2.83/5, determining a medium risk for the use of QR codes. The risk assessment underscores the importance of strengthening security through more robust encryption algorithms and better secure development practices. Keywords: Cybersecurity; Financial Applications; Vulnerabilities; Risk Analysis; Authentication.

## Introducción

La digitalización ha transformado radicalmente diversos sectores económicos, destacándose el sistema bancario por su rápida adaptación a las nuevas tecnologías (Carbó-Valverde et al., 2020). En el Ecuador, esta tendencia se ha consolidado en los últimos cinco años, marcando un período de expansión significativa en la adopción de servicios financieros digitales según el reporte 2019-2021 de la Asociación de Bancos Privados del Ecuador (ASOBANCA, 2022). La evolución tecnológica acelerada ha impulsado esta transición hacia métodos de pago electrónicos, lo cual plantea un desafío urgente en términos de seguridad cibernética (Bhosale et al., 2023).

“Wallink” es una aplicación financiera diseñada para las cooperativas de ahorro y crédito de Ecuador, con el propósito de brindar servicios financieros a través de una red de cajeros propios. La aplicación permite el proceso de autenticación de usuarios y según sus cuentas registradas, posibilita realizar transacciones de retiros de dinero. Para autenticar los movimientos en el cajero, la aplicación genera un código QR (del inglés “Quick Response”, en español “Respuesta rápida”) con un tiempo de vida limitado a 3 minutos, el cual el usuario puede utilizar para autenticarse ante los cajeros y completar el retiro de efectivo.

Las aplicaciones móviles, especialmente aquellas dedicadas a la banca móvil, buscan aplicar protocolos de autenticación que garanticen el acceso solo a usuarios autorizados (Pernpruner et al., 2023), lidiando con el desafío de aplicar medidas efectivas de seguridad sin afectar la usabilidad. Una aplicación segura pero compleja o poco intuitiva puede disuadir a los usuarios de utilizarla, limitando su alcance y efectividad (Di Nocera et al., 2023).

En busca de equilibrar la seguridad y usabilidad, aplicaciones como "Wallink", han optado por usar códigos QR, conocidos por su capacidad para almacenar información diversa que pueden generarse e interpretarse de manera rápida y eficiente, sin embargo, los códigos QR pueden presentar vulnerabilidades potenciales que podrían ser explotadas por ciberdelincuentes (Focardi et al., 2019).

La necesidad de desarrollar soluciones de ciberseguridad efectivas para proteger las transacciones en línea (Surya et al., 2023) ha sido la motivación para llevar a cabo esta investigación y contribuir al avance de prácticas seguras en el ámbito financiero digital en Ecuador.

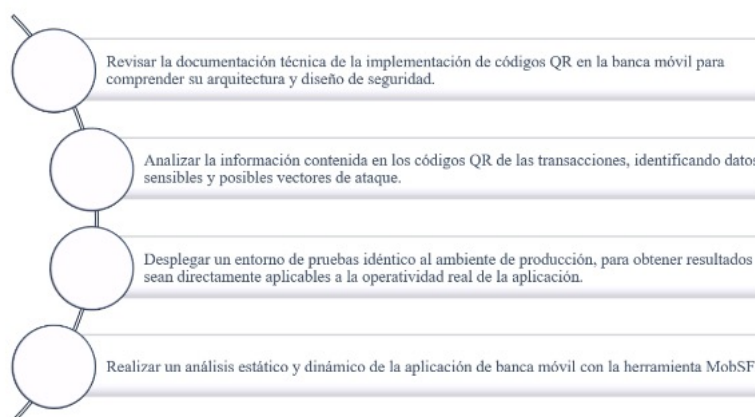
Por lo tanto, el objetivo de este estudio fue evaluar la seguridad de los códigos QR en la aplicación de banca móvil "Wallink" mediante la aplicación de la metodología de pruebas de seguridad descrita en el estándar SP 800-115 del Instituto Nacional de Estándares y Tecnología (NIST, 2008). El análisis de los códigos QR y la información que contienen tiene como objetivo identificar posibles vulnerabilidades en el sistema y evaluar la robustez de las medidas de seguridad implementadas en "Wallink".

## Metodología

El estudio adoptó un enfoque analítico experimental observacional con el objetivo de evaluar la seguridad en el uso de códigos QR en una aplicación de banca móvil. La aplicación posee una base de aproximadamente 1000 usuarios activos, quienes realizan un promedio de 40 transacciones diarias.

Para la evaluación de vulnerabilidades, el estudio se fundamentó en la guía NIST SP 800-115, donde se siguió el marco referencial que ofrece para llevar a cabo pruebas y evaluaciones de seguridad en sistemas de información. Durante la fase inicial, se establecieron objetivos específicos para la Evaluación de Seguridad de la Información (ESI), como se muestra en la figura 1.

Figura 1. Objetivos específicos para la Evaluación de Seguridad de la Información



Fuente: elaboración propia

Nota: declaración de objetivos en el proceso de Evaluación de seguridad de la información.

Para el análisis de los códigos QR, se instaló el APK (del inglés “Android Package Kit”, en español “paquete de aplicaciones de Android”) en un emulador de Android Studio versión Iguana, se registró un usuario de pruebas y se generaron 672 códigos durante 6 días, considerando el 40% de las transacciones diarias (16 transacciones). Teniendo en cuenta que el Código QR tiene un tiempo de expiración de 3 minutos y la transacción una duración de 30 minutos, se generó cada 5 minutos un nuevo código QR.

Mediante la plataforma en línea <https://zxing.org/>, se decodificó cada uno de los códigos QR para obtener el contenido de estos. Posteriormente, se utilizó <https://www.cryptool.org/>, como una herramienta de clasificación de cifrado como lo descrito por Kopal (2018), para identificar la complejidad del contenido decodificado y verificar si presentaba texto interpretable y existencia de patrones que pudieran facilitar la replicación del contenido.

En la evaluación de la aplicación, se realizó el análisis estático y dinámico con Mobile Security Framework (MobSF), como lo describe Kusreynada y Barkah (2024). Este análisis permitió obtener un primer informe que valoró la calidad, vulnerabilidades y buenas prácticas de desarrollo en el código de la aplicación, y un segundo informe del análisis dinámico que registró la actividad de la aplicación al realizar una transacción.

Previo al despliegue de MobSF, se configuró un laboratorio utilizando Docker (versión 24.0.6), donde se desplegó el servicio localmente para el análisis de la aplicación. Adicionalmente para el análisis dinámico, se configuró la ruta (PATH) del emulador de Android Studio, ejecutando los comandos de configuración correspondientes.

Como método para determinar el riesgo de los diferentes resultados de análisis, se utilizó una escala de 5 niveles, donde 1 es muy bajo y 5 muy alto, los rangos aplicados son el resultado del uso de percentiles en la escala como se observa en la tabla 1.

Tabla 1. Niveles de Riesgo de vulnerabilidades

| Tabla de Valoración |                                                                                              | Escala de valores |
|---------------------|----------------------------------------------------------------------------------------------|-------------------|
| 1                   |  Muy Bajo | 1.00 : 1.80       |
| 2                   |  Bajo     | 1.81 : 2.61       |
| 3                   |  Medio    | 2.62 : 3.41       |
| 4                   |  Alto     | 3.42 : 4.21       |
| 5                   |  Muy Alto | 4.22 : 5.00       |

Fuente: elaboración propia

Nota: escala de valores determinada para el nivel de riesgo de vulnerabilidades.

La metodología empleada para determinar la valoración del riesgo tuvo 3 principales enfoques: el análisis de los códigos QR, resultados del análisis estático y los resultados del análisis dinámico, estos dos últimos basados en el análisis a la aplicación. El análisis de los códigos QR se lo representó con un 50% de la puntuación que contempló elementos como el tiempo de vigencia

del código QR, cifrado del contenido y la complejidad de ser replicado, por el enfoque principal de esta investigación en el análisis de los Códigos QR.

La otra mitad de la puntuación se distribuyó en la evaluación de la aplicación desde donde se generan los códigos QR. A los resultados del análisis estático se consideró un veinticinco por ciento (25%) de la ponderación, en donde se evaluaron la calidad y seguridad del código, así como los permisos requeridos y el puntaje de riesgo obtenido en el informe. El veinticinco por ciento (25%) restante se asignó al análisis dinámico, incluyendo la evaluación de tráfico no cifrado, la comunicación con dominios potencialmente maliciosos y la presencia de rastreadores. Esta evaluación de

## Resultados

### Análisis de códigos QR.

El proceso de análisis de los códigos QR con la herramienta zxing, permitió identificar la estructura de su contenido, tal como se muestra en la Figura 2.

Figura 2. Texto decodificado de un código QR.

| A                                                                                                           |                                                                                                                                                                                                                                                     | B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |
|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|  <b>Decode Succeeded</b> |                                                                                                                                                                                                                                                     | <pre> PHIQR5088VYLGHVDEUQFFMUKM3ABZPYL3TYWILYPRCALTTOTWYPA3N3LCYB PHIQR5193MSWNRWMEKACUOYTTAKAMWBMXKH3AWVRAPQRREQJVFQZ PHIQR2732UDPRGEZFKLTWFXDURPXLMBRWQDP3EY2QKVSUAZOFQOGPRLX PHIQR4637YBFICKMZUJYRISWBMWSMMLBZCCUGKFKVAKFSUEEPURXAWO PHIQR2725TYVHFQWMTQWJAXEHSXULDMQQTUHGUGXYRFQKPPDDDEPXRBB PHIQR2786DABHUAFIYIY7BUQUAROTXUFQMRBSGLUCGAY3NVE3HMBCTHY PHIQR3136VZMRNSQCRCYVWYBAHFLXVXYEOWYKHPFWCUXVGAEKQDCISXJ PHIQR4029PEHUKDZTUFOKZGE1ZTAPLMGSSCMQWABKSENNW3VJ1JTTXVBQ PHIQR1692QKQVTFIBBOOERJXSZBUKJAYOHTAHMCKZHUGDVPSNLTYXWMBZD PHIQR6605DOJMARLVXEQERNEQWQGGHVLQJ3KPMHRCBFLQJEMCFBCH PHIQR4266DHLRPHPZTRWJGRCEGBTBVBTTPTKBLNBTLMDWPGZAVVREDBA PHIQR1613MNNZARZIDWZKZAEKVLQXLAQJMMISLUJADQXKNTOSOGVTRM PHIQR5546LBLZHXEJALUJLXZBVDONHYPMSHLAXLXWANHLYZVTKSCCH PHIQR1232BXWJNHRHKLWINREAYZENAOGKQNLQVFNZYEPGNGHVSXB PHIQR6774ECZGVFCFSKGUJHBTQHJ3KWHZKOG3TAVQXBRPAGBIUUDLKEFH </pre> |  |
| Raw text                                                                                                    | PHIQR5088VYLGHVDEUQFFMUKM3ABZPYL3TYWILYPRCALTTOTWYPA3N3LCYB                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
| Raw bytes                                                                                                   | <pre> 43 05 04 84 95 15 23 53 03 83 85 94 c4 74 85 64 44 04 55 14 64 84 05 54 b4 04 a4 14 25 85 05 94 c4 a5 45 95 74 94 c5 95 05 24 34 14 c5 45 44 f5 45 75 95 84 14 a4 04 a4 c4 35 94 78 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec 11 ec </pre> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
| Barcode format                                                                                              | QR_CODE                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
| Parsed Result Type                                                                                          | TEXT                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
| Parsed Result                                                                                               | PHIQR5088VYLGHVDEUQFFMUKM3ABZPYL3TYWILYPRCALTTOTWYPA3N3LCYB                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |

Fuente: elaboración propia

Nota: Sección a) Resultado de la interpretación de uno de los códigos QR con zxing. Sección b) Texto decodificado de una serie de códigos que evidencia una constante (PHIQR) en el inicio de la cadena.

El texto decodificado de los códigos QR se pudo evidenciar que contienen un prefijo "PHIQR" seguido de 4 dígitos y 39 caracteres adicionales, sumando 48 caracteres en total. La constancia del prefijo reduce la entropía inicial, pudiendo representar una vulnerabilidad. En la muestra de 672 registros examinados, no se detectaron códigos duplicados, lo cual corrobora que la vigencia de los códigos QR es inferior a 5 minutos. Transcurrido este período, el código se regenera, invalidando el anterior. Se observó que una sola transacción puede asociarse hasta con 7 códigos distintos durante su ciclo de vida.

Posteriormente, se sometió el texto decodificado de cada código QR a un análisis criptográfico utilizando la herramienta Cryptool. Los resultados de este análisis fueron promediados, concluyendo que el contenido de los códigos QR tiene una probabilidad del 95.17% de usar un método de sustitución polialfabética.

## Análisis Estático

El reporte obtenido del análisis estático en la herramienta de MobSF, como análisis a la aplicación, refleja un puntaje de riesgo de 46 sobre 100 tal como se muestra en la figura 3, categorizado como riesgo medio según los parámetros de la herramienta.

Figura 3. Resultado de análisis estático.



Fuente: elaboración propia

Nota: la calificación del Score de MobSF, como se observa es de 46/100, lo que representa un nivel de riesgo Medio.

El reporte también reveló una vulnerabilidad tipo Janus en dispositivos Android 5.0 a 8.0, lo que sugiere un punto de entrada potencial para actores maliciosos. Además, se detectó que la aplicación solicita permisos que podrían considerarse excesivos.

El análisis de APKiD (del inglés “Android Application Identifier for Packers, Protectors, Obfuscators and Oddities”, en español “Identificador de aplicaciones Android para empaquetadores, protectores, ofuscadores y rarezas”) y seguridad binaria reveló en el código mecanismos implementados para prevenir la ejecución de código arbitrario y mitigar riesgos de desbordamientos de buffer.

En cuanto a las conexiones de dominio de la aplicación, se limitan a Estados Unidos y no se comunica con entidades sancionadas por la Oficina de Control de Activos Extranjeros (OFAC). No obstante, la inclusión de claves de API (Interfaz de Programación de Aplicaciones) de Google en el código fuente puede representar un vector de amenaza significativo.

## Análisis Dinámico.

En el reporte de análisis dinámico de la aplicación, como se muestra en la figura 4, arrojó resultados satisfactorios, indicando una configuración adecuada y segura de los protocolos de TLS/SSL (del inglés “Transport Layer Security/Secure Sockets Layer”, en español “Seguridad

de la capa de transporte/Capa de sockets seguros"). Se identificaron dependencias clave para el funcionamiento de la aplicación, como bibliotecas y componentes del sistema operativo Android, incluyendo `io.flutter.embedding.android` e `io.flutter.plugin.editing`.

Figura 4. Resultado de análisis dinámico.

 TLS/SSL Security Tester

Search:

| TESTS                                            | RESULT                                                                              |
|--------------------------------------------------|-------------------------------------------------------------------------------------|
| Cleartext Traffic Test                           |  |
| TLS Misconfiguration Test                        |  |
| TLS Pinning/Certificate Transparency Bypass Test |  |
| TLS Pinning/Certificate Transparency Test        |  |

Fuente: elaboración propia

Nota: captura del reporte de MobSF de las pruebas dinámicas a la aplicación.

En este informe se confirma que la aplicación tiene interacción con dominios principalmente localizados en Estados Unidos. Asimismo, se señala que es posible acceder a archivos de bases de datos y preferencias compartidas en el almacenamiento local, tales como: Bases de datos de transporte de datos de Google; Archivos de configuración y caché de Flutter; Archivos de bloqueo y configuración de Firebase

### Evaluación de los resultados:

Tras completar los análisis de los códigos QR generados y el análisis de la aplicación estático y dinámico, se procedió a evaluar los riesgos asociados utilizando una metodología predefinida que incorpora criterios específicos con sus respectivas ponderaciones como se muestra en la tabla 2.

Tabla 2. Tabla de valoración de riesgos.

| Factores                          | Ponderación por factores | Criterios                          | Ponderación por criterios | Nivel Riesgo                                                                                  | Resultados |
|-----------------------------------|--------------------------|------------------------------------|---------------------------|-----------------------------------------------------------------------------------------------|------------|
| Características de los códigos QR | 50%                      | - Tiempo de vigencia del código QR | 33,33%                    | 2  Bajo  | 0,33       |
|                                   |                          | - Cifrado del contenido,           | 33,33%                    | 3  Medio | 0,50       |
|                                   |                          | - Complejidad de ser replicado     | 33,33%                    | 3  Medio | 0,50       |

| Factores                           | Ponderación por factores | Criterios                        | Ponderación por criterios | Nivel Riesgo |                      | Resultados       |
|------------------------------------|--------------------------|----------------------------------|---------------------------|--------------|----------------------|------------------|
| Análisis estático de la aplicación | 25%                      | - Score MobSF                    | 33,33%                    | 3            | <div></div> Medio    | 0,25             |
|                                    |                          | - Vulnerabilidades encontradas   | 33,33%                    | 4            | <div></div> Alto     | 0,33             |
|                                    |                          | - Prácticas de desarrollo seguro | 33,33%                    | 3            | <div></div> Medio    | 0,25             |
| Análisis dinámico de la aplicación | 25%                      | - Cifrado en comunicación        | 33,33%                    | 1            | <div></div> Muy Bajo | 0,08             |
|                                    |                          | - Dominios maliciosos            | 33,33%                    | 2            | <div></div> Bajo     | 0,17             |
|                                    |                          | - Almacenamiento de datos        | 33,33%                    | 5            | <div></div> Muy alto | 0,42             |
| RESULTADO DE LA VALORACIÓN:        |                          |                                  |                           |              |                      | <div></div> 2,83 |

Fuente: elaboración propia

Nota: Resultado de evaluación de nivel de riesgo del uso de códigos QR en la aplicación de banca móvil.

Cada criterio fue analizado cuidadosamente, y los riesgos fueron identificados y cuantificados basándose en los hallazgos obtenidos de los diferentes análisis. El puntaje de riesgo combinado obtenido fue de 2.83. En la tabla 1 se definió la escala de valoraciones, clasificando al uso de códigos QR en la aplicación de banca móvil con un riesgo “Medio”.

## Discusiones.

Esta investigación ha evaluado la seguridad de los códigos QR utilizados en una aplicación de banca móvil “Wallink”, así como la seguridad e integridad de la aplicación mediante análisis estático y dinámico. Los hallazgos obtenidos al aplicar la metodología propuesta han permitido conocer los posibles riesgos y vulnerabilidades, así como los niveles de seguridad implementados.

El análisis de los códigos QR decodificados ha revelado que el contenido presenta una alta probabilidad de encontrarse cifrado, factor fundamental para garantizar la seguridad de las transacciones, tal como lo sostienen Focardi et al. (2019). No obstante, se ha identificado que el algoritmo de cifrado probablemente emplea un método de sustitución polialfabética con un prefijo “PHIQR” al inicio del texto, afectando la calidad del cifrado. La adopción de múltiples algoritmos de cifrado, tales como SM2, SM3 y SM4, propuestos por Zhou et al. (2021), podría contribuir a mejorar significativamente la seguridad de las transacciones realizadas mediante este canal.

En la actualidad, se está incrementando la utilización de códigos QR en sistemas de pago electrónico. Sin embargo, muchos sistemas emplean códigos estáticos por usuario, lo que puede suponer un riesgo de seguridad según Bhosale et al. (2023). Por otro lado, los códigos QR generados por “Wallink” son de un solo uso y tienen una duración máxima de 3 minutos, lo que contribuye a reforzar la seguridad de la transacción.

La seguridad de las transacciones se ve influenciada por la aplicación responsable de generar los movimientos. Durante la revisión del código, se detectó un "exploit Janus" como una de las vulnerabilidades más críticas, el cual podría ser utilizado por potenciales agresores (Chatzoglou et al., 2021). Este exploit presenta el riesgo de permitir la manipulación de archivos de código Java (JAR) en aplicaciones de Android, lo que podría dar lugar a la ejecución o inserción de código malicioso en la aplicación "Wallink".

Otro hallazgo relevante en el análisis son los permisos de la aplicación, los cuales pueden considerarse como excesivos como lo indican Kusreynada y Barkah (2024), sin embargo, estos permisos son necesarios para la prevención de fraude y la validación de transacciones, siguiendo las regulaciones de los entes de control vigentes en el Ecuador como la Super Intendencia de economía Popular y solidaria (SEPS, 2023).

En tanto que, el reporte de las pruebas dinámicas evidenció el uso correcto de protocolos SSL/TLS. Esta buena práctica en la seguridad de la comunicación es esencial para proteger la integridad y confidencialidad de los datos transmitidos (Idris et al., 2022), sin embargo, el reporte reveló prácticas de almacenamiento de datos inapropiadas en la base de datos SQLite y los archivos de preferencias compartidas, para lo cual es necesario trabajar en el cifrado de estos datos (Wang et al., 2020).

## Conclusión

La evaluación de riesgos realizada, fundamentada en criterios predefinidos y ponderados, categorizó el riesgo asociado al uso de códigos QR en la aplicación "Wallink" con un nivel de riesgo MEDIO. Este resultado evidencia que la utilización de códigos QR en aplicaciones destinadas a generar transacciones constituye un factor de seguridad relevante, que debe ser complementado con medidas de seguridad efectivas en el cifrado del contenido de los códigos QR y la implementación de buenas prácticas de desarrollo en las aplicaciones. El objetivo primordial es elevar el nivel de seguridad de estos canales transaccionales, mitigando así potenciales vulnerabilidades y amenazas cibernéticas.

Es importante destacar que la categorización de riesgo MEDIO no implica una falla crítica en la seguridad, sino que señala áreas de mejora y la necesidad de una vigilancia continua. La implementación de técnicas de cifrado más robustas, como el uso de algoritmos de encriptación avanzados, podría contribuir significativamente a la reducción del nivel de riesgo. Asimismo, la adopción de prácticas de desarrollo seguro, incluyendo revisiones de código regulares y pruebas de penetración, podría fortalecer la integridad general del sistema.

Para futuras investigaciones, se recomienda levantar información sobre los incidentes de seguridad de diferentes aplicaciones de banca móvil que se hayan materializado. Realizar un análisis comparativo entre los diversos métodos utilizados para autenticar los movimientos permitiría determinar los enfoques más recomendables, manteniendo un equilibrio óptimo entre

seguridad y usabilidad. Este estudio comparativo podría abarcar no solo los códigos QR, sino también otras tecnologías emergentes como la autenticación biométrica, los tokens de seguridad y los sistemas de autenticación multifactor.

## Referencias

- Asociación de Bancos Privados del Ecuador [ASOBANCA]. (2022). *El avance de la banca digital en Ecuador*. <https://lc.cx/kZP0Q->
- Bhosale, V. P., Naik, P. G., Desai, S. B., & Patekar, P. (2023). Secure QR Code Transactions Using Mobile Banking App. In: T. Senjyu, C. So-In, A. Joshi, (eds). *Smart Trends in Computing and Communications*. (pp. 35–46). Springer. [https://doi.org/10.1007/978-981-99-0838-7\\_4](https://doi.org/10.1007/978-981-99-0838-7_4)
- Carbó-Valverde, S., Cuadros-Solas, P. J., & Rodríguez-Fernández, F. (2020). The Effect of Banks' IT Investments on the Digitalization of their Customers. *Global Policy*, 11(1), 9–17. <https://doi.org/10.1111/1758-5899.12749>
- Chatzoglou, E., Kambourakis, G., & Kouliaridis, V. (2021). A multi-tier security analysis of official car management apps for android. *Future Internet*, 13(3), 1–35. <https://doi.org/10.3390/fi13030058>
- Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable Security: A Systematic Literature Review. *Information*, 14(12), 641. <https://doi.org/10.3390/info14120641>
- Focardi, R., Luccio, F. L., & Wahsheh, H. A. M. (2019). Usable security for QR code. *Journal of Information Security and Applications*, 48. <https://doi.org/10.1016/j.jisa.2019.102369>
- Idris, M., Syarif, I., & Winarno, I. (2022). Web Application Security Education Platform Based on OWASP API Security Project. *EMITTER International Journal of Engineering Technology*, 10(2), 246–261. <https://doi.org/10.24003/emitter.v10i2.705>
- Kopal, N. (2018). Solving Classical Ciphers with CrypTool 2. *Proceedings of the 1st Conference on Historical Cryptology*, 29–38. <https://lc.cx/ZvacDy>
- Kusreynada, S. U., & Barkah, A. S. (2024). Android Apps Vulnerability Detection with Static and Dynamic Analysis Approach using MOBSF. *Journal of Computer Science and Engineering*, 5(1), 46–63. <https://doi.org/10.36596/jcse.v5i1.789>
- National Institute of Standards and Technology [NIST]. (2008). *Technical Guide to Information Security Testing and Assessment*. <https://doi.org/10.6028/NIST.SP.800-115>
- Pernpruner, M., Carbone, R., Sciarretta, G., & Ranise, S. (2023). An Automated Multi-Layered Methodology to Assist the Secure and Risk-Aware Design of Multi-Factor Authentication Protocols. *IEEE Transactions on Dependable and Secure Computing*, 21(4), 1935–1950. <https://doi.org/10.1109/TDSC.2023.3296210>
- Superintendencia de Economía Popular y Solidaria [SEPS]. (2023). Resolución Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009. In *Superintendencia de Economía Popular y Solidaria*. <https://lc.cx/K9JVNW>

- Surya, S., Jagtap, S. R., Ramnarayan, R., Priyadarshini, M., Ibrahim, R. K., & Alazzam, M. B. (2023). *Protecting Online Transactions: A Cybersecurity Solution Model*. 3rd International Conference on Advance Computing and Innovative Technologies in Engineering. <https://doi.org/10.1109/ICACITE57410.2023.10183282>
- Wang, Y., Shen, Y., Su, C., Ma, J., Liu, L., & Dong, X. (2020). CryptSQLite: SQLite with High Data Security. *IEEE Transactions on Computers*, 69(5), 666–678. <https://doi.org/10.1109/TC.2019.2963303>
- Zhou, Y., Hu, B., Zhang, Y., & Cai, W. (2021). Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and Its Performance. *IEEE Access*, 9, 122362–122372. <https://doi.org/10.1109/ACCESS.2021.3108189>

## Autores

Carlos Fajardo. Ingeniero de Sistemas graduado en la Universidad Católica de Cuenca, nació en la ciudad de Cuenca, Ecuador. Director General de TECSO S.A.S., una empresa de servicios informáticos ubicada en Cuenca.

Marco Yamba-Yugsi. Es doctor en Ciencias y Tecnologías Experimentales por la UVic: Universitat de Vic–Universitat Central de Catalunya, y Máster en Diseño Multimedia por la Universidad del Azuay.

Eduardo Mauricio Campaña Ortega. Docente de la Maestría en Ciberseguridad

## Declaración

Conflicto de interés

No tenemos ningún conflicto de interés que declarar.

Financiamiento

Sin ayuda financiera de partes externas a este artículo.

Nota

El artículo es original y no ha sido publicado previamente.