Revista Multidisciplinaria Prospherus

ISSN: 3091-177X

Doi: https://doi.org/10.63535/smk3pn96

Periocidad trimestral, Volumen 3, Numero 1, Años (2026), Pág. 803 - 825

Vulnerabilidades de ciberseguridad en aplicaciones móviles usadas por jóvenes profesionales ecuatorianos

Cybersecurity vulnerabilities in mobile applications used by young Ecuadorian professionals

Autor

Álvaro David Cuyan Chimbo

alvaro.cuyanchimbo1196@upse.edu.ec

https://orcid.org/0009-0007-9767-9425

Universidad Estatal Península De Santa Elena

Santa Elena – Ecuador

Ing. Diego Benavides Astudillo, Ph.D

Docente Tutor

debenavides@espe.edu.ec

https://orcid.org// 0000-0003-4543-0082

Universidad Estatal Península De Santa Elena

Santa Elena - Ecuador

Como citar:

Cuyan Chimbo, Álvaro D., & Benavides Astudillo, D. . (2026). Vulnerabilidades de ciberseguridad en aplicaciones móviles usadas por jóvenes profesionales ecuatorianos. *Prospherus*, *3*(1), 803-825. https://doi.org/10.63535/smk3pn96

Fecha de recepción: 2026-01-24

Fecha de aceptación: 2026-02-24

Fecha de publicación: 2026-03-25

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Resumen

El objetivo fue analizar el nivel de riesgo de ciberseguridad en jóvenes profesionales, integrando la evaluación de las vulnerabilidades técnicas presentes en las aplicaciones móviles y los patrones de comportamiento en materia de seguridad dentro de entornos BYOD. Desde ese enfoque se realizó un abordaje académico para conocer las brechas técnicas de un tema poco investigado. El estudio tuvo un enfoque mixto descriptivo y correlacional, analizó vulnerabilidades técnicas en aplicaciones móviles usadas por jóvenes profesionales en entornos BYOD, relacionándolas con hábitos de seguridad. Se aplicó encuesta digital a 40 participantes mediante muestreo no probabilístico, con diseño transversal no experimental. En los resultados se confirma el riesgo de ciberseguridad en entornos BYOD en la parte técnica y está condicionada por el comportamiento del usuario. La relevancia de los hallazgos técnicos del análisis basado en el marco OWASP Mobile Top 10, exponen que existen vulnerabilidades recurrentes asociadas a almacenamiento inseguro, fallos en autenticación y deficiencias criptográficas. En este mismo marco, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, lo que valida la relevancia de la protección de datos cuando los profesionales trabajan en entornos BYOD. En conclusión, el estudio aporta evidencia empírica en el contexto ecuatoriano y propone un enfoque diagnóstico que integra la dimensión técnica y conductual, contribuyendo al fortalecimiento de la gestión de riesgos en organizaciones que adoptan esquemas BYOD.

Palabras clave: Ciberseguridad; Vulnerabilidades Técnicas; Dispositivos Móviles; Entornos BYOD.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Abstract

The objective was to analyze the level of cybersecurity risk in young professionals, integrating the assessment of technical vulnerabilities present in mobile applications and security behavior patterns within BYOD environments. From that approach, an academic endeavor was undertaken to understand the technical gaps in a poorly researched topic. The study had a mixed descriptive and correlational approach, analyzing technical vulnerabilities in mobile applications used by young professionals in BYOD environments, relating them to security habits. A digital survey was administered to 40 participants using non-probabilistic sampling, with a non-experimental cross-sectional design. The results confirm the cybersecurity risk in BYOD environments on the technical side, which is conditioned by user behavior. The relevance of the technical findings from the analysis based on the OWASP Mobile Top 10 framework reveals that there are recurring vulnerabilities associated with insecure storage, authentication failures, and cryptographic deficiencies. In this same framework, the null hypothesis is rejected and the alternative hypothesis is accepted, which validates the relevance of data protection when professionals work in BYOD environments. In conclusion, the study provides empirical evidence in the Ecuadorian context and proposes a diagnostic approach that integrates the technical and behavioral dimensions, contributing to the strengthening of risk management in organizations that adopt BYOD schemes.

Keywords: Cybersecurity; Technical Vulnerabilities; Mobile Devices; BYOD Environments.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Introducción

En los últimos años, la dependencia de los dispositivos móviles ha transformado la forma en que los jóvenes profesionales gestionan sus actividades laborales. Este fenómeno ha impulsado la práctica del *BYOD* (*Bring Your Own Device*, por sus siglas en inglés), en español significa "trae tu propio dispositivo", para acceder a recursos corporativos y al sistema de la empresa, lo que incrementa la flexibilidad, pero también aumenta los riesgos de ciberseguridad por la vulnerabilidad a la seguridad informática, posible filtración de información y dificultad para controlar los dispositivos personales por la inseguridad en las contraseñas, cifrado de datos independientes utilizados en la conexión (Mahmood y Bano, 2020).

Por consiguiente, el uso intensivo de aplicaciones móviles en las diversas áreas de productividad ha incrementado la superficie de exposición a ciber amenazas, por tanto, cuando un empleado usa su propio dispositivo (BYOD) en la empresa para realizar las diversas actividades y se conecta a la red empresarial se accede a datos e información sensible y confidencial (Fortinet, 2026). Es importante señalar que entre los dispositivos utilizados se encuentran los teléfonos inteligentes, tabletas, computadoras portátiles (laptop), computadoras de escritorio, unidades USB, entre otros, que se deben administrar con seguridad para evitar vulnerabilidades en la información.

Bajo esta perspectiva, los riesgos por la práctica de utilizar dispositivos móviles personales en entornos laborales deben tener en cuenta controles centralizados y la aplicación de políticas de seguridad homogéneas en las organizaciones (INCIBE, 2020). Desde un marco más general, la necesidad de optimizar la productividad influye en que muchos jóvenes profesionales usen BOYD, sin la instalación de aplicaciones desde fuentes confiables como la autenticación de las fuentes, antivirus actualizado, se conectan a redes *WiFi* públicas inseguras y están expuestos a *phishing* (Hernández, 2022). Las vulnerabilidades exponen a ciber ataques y problemas de técnicos y compatibilidad con la información de la empresa.

En este mismo sentido, existen marcos como *OWASP Mobile* Top 10, que identifican vulnerabilidades críticas en aplicaciones móviles (OWASP, 2021), por tanto, se debe evaluar las fallas técnicas de las apps con la finalidad de establecer políticas internas para el uso de los sistemas operativos, de esa manera si el colaborador pierde su equipo, la información empresarial no quede expuesta al uso indebido de los datos (Guaña, 2024).

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Dentro de este orden de ideas, a pesar de los avances en las políticas de seguridad, aún existen vacíos en la comprensión integral de las vulnerabilidades técnicas en las aplicaciones móviles y aquellas que se relacionan con las conductas de seguridad de los jóvenes profesionales (Garcia et al., 2022). En este contexto, el presente proyecto busca diagnosticar el nivel de riesgo de ciberseguridad móvil integrando el análisis técnico de las pruebas estadísticas de seguridad de las aplicaciones (SAST) y las pruebas dinámicas de seguridad de aplicaciones (DAST) y el comportamiento del usuario en los entornos BYOD.

Cabe indicar que al conocer el problema nace la pregunta general: ¿Cuál es el nivel de riesgo de ciberseguridad que enfrentan los jóvenes profesionales ecuatorianos al combinar las vulnerabilidades técnicas presentes en las aplicaciones móviles que utilizan con sus patrones de comportamiento de seguridad en entornos BYOD?

Este planteamiento responde a la necesidad de evaluar en forma conjunta tanto las fallas técnicas identificadas en las aplicaciones como los hábitos de seguridad de los jóvenes profesionales, siguiendo lineamientos de marcos de referencia como OWASP Mobile Top 10 y de investigaciones que destacan la importancia de integrar factores técnicos y conductuales en la gestión de riesgos móviles (INCIBE, 2020).

El presente proyecto se justifica por la necesidad crítica de transformar la gestión de la ciberseguridad móvil en el entorno profesional que suele enfrentar riesgos de vulnerabilidad en las actividades cotidianas en los puestos laborales (Oke, 2024). En la parte práctica, analizar el riesgo operacional y la adopción de la práctica BYOD, permite reconocer vulnerabilidades por los fallos técnicos en el cifrado débil y la inseguridad en el *Software Development Kit* SDK; así como diversas conductas por parte del usuario calificadas como negligencia en patching que influyen en la inestabilidad de los sistemas, específicamente provocado por la descarga de fuentes no oficiales y otras acciones que amplía el vector de ataque móvil (Tatai, 2026).

La relevancia académica es aportar una base empírica que permita a las organizaciones diseñar políticas de seguridad y programas de capacitación más eficaces, así como fortalecer la cultura de ciberseguridad individual y colectiva (Montalvo et al., 2025). Con ello, se pretende contribuir al ámbito académico, laboral y profesional, llenar los vacíos en la literatura al contribuir con una publicación investigativa que promueve un enfoque integral para la gestión de riesgos digitales en esta era de la globalización.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

De lo anteriormente indicado nace el Objetivo General:

Analizar el nivel de riesgo de ciberseguridad en jóvenes profesionales, integrando la evaluación de las vulnerabilidades técnicas presentes en las aplicaciones móviles y los patrones de comportamiento en materia de seguridad dentro de entornos BYOD.

Estado de Arte

Abordaje teórico de los dispositivos móviles en el entorno BYOD (Bring Your Own Device)

En la parte conceptual, los dispositivos móviles son las herramientas portátiles que realizan multifunciones, requieren de conectividad inalámbrica, capacidad de procesamiento de datos y memoria. Están diseñados para realizar diversas funciones en la educación, lo laboral y la comunicación (Guaña, 2024).

Consecuentemente, al utilizar los dispositivos móviles hay riesgos inherentes en el uso, específicamente en la parte técnica se presentan vulnerabilidades en los mensajes de texto, productividad laboral, uso de la banca, redes sociales entre otras, debido a que puede existir permisos excesivos en el acceso a contactos, micrófono abierto en las computadores y otros dispositivo, ubicación del usuario, fallos de cifrado en tránsito y en el almacenamiento de datos y el uso de librerías obsoletas que no tienen soporte técnico seguro (Mahmood y Bano, 2020).

En el siglo XXI, la frecuente incorporación de dispositivos móviles en el entorno organizacional ha transformado la manera de gestionar los procesos productivos, la comunicación interna y externa, así como el acceso a la información en el ámbito laboral (Pérez, 2024). En el marco del modelo BYOD (Bring Your Own Device), los colaboradores utilizan dispositivos personales, entre ellos teléfonos inteligentes, reloj, tabletas y computadoras portátiles para acceder a recursos corporativos, lo que genera nuevas dinámicas de productividad y desafíos en materia de seguridad (Chou y Chen, 2020).

La modernidad y globalización en el campo laboral, los dispositivos móviles se caracterizan por su portabilidad, conectividad al internet y capacidad de almacenamiento de información sensible, constituyéndose en la principal fortaleza operativa y un punto crítico de vulnerabilidad (Rodríguez y Martínez, 2022).

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

En el campo laboral, el crecimiento sostenido en el uso de laptop y smartphones en entornos laborales ha incrementado la superficie de ataque cibernéticos en las empresas, especialmente cuando en sus políticas internas no se establecen condiciones de custodia, control y monitoreo (Dávila, 2023). En el entorno BYOD, la práctica identifica que los dispositivos móviles principalmente Android y iOS operan bajo sistemas operativos diversos, estás acciones dificulta la estandarización de controles de seguridad. Cabe considerar que la heterogeneidad tecnológica complica la aplicación uniforme de actualizaciones que resguarden la información y los mecanismos de cifrado, por lo que se incrementa la exposición a diferentes tipos de amenazas como malware móvil, phishing, accesos no autorizados y fuga de información (Loor, 2024).

Desde una perspectiva de gestión de riesgos, la International *Organization for Standardization* (ISO/IEC 27001, 2022), enfatiza la necesidad de implementar controles específicos para dispositivos móviles, incluyendo autenticación multifactor, cifrado de datos, gestión remota y políticas de borrado seguro (Dávila, 2023). En el contexto BYOD, estos controles adquieren mayor relevancia debido a la delgada línea entre el uso personal y profesional del dispositivo (Garcia et al., 2022).

Asimismo, el uso de redes públicas, aplicaciones no autorizadas y la falta de actualización de software constituyen factores que incrementan el riesgo de incidentes de ciberseguridad con el uso de dispositivos móviles bajo el modelo BYOD (Guaña, 2024). La utilización de los dispositivos móviles en entornos corporativos se ha convertido en vectores de ataque más explotados por ciberdelincuentes, especialmente en organizaciones que carecen de soluciones de gestión de dispositivos móviles (MDM) (Tatai, 2026).

Desde una visión estratégica, los dispositivos móviles en el entorno BYOD son herramientas tecnológicas y activos críticos de información (Fortinet, 2025). Su adecuada gestión requiere políticas organizacionales claras, capacitación continua del personal y la implementación de tecnologías de control que permitan equilibrar la productividad con la protección de datos corporativos.

Los dispositivos móviles en el entorno BYOD se configura como un elemento determinante dentro de la gestión de riesgos de ciberseguridad (Hernández, 2022), dado que

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

concentra los beneficios operativos de la movilidad (Akamai, 2025), y focos de vulnerabilidad en las organizaciones contemporáneas (Alshahrani et al., 2021).

Riesgos de ciberseguridad asociados al uso del modelo BYOD (Bring Your Own Device)

En otros casos se observa que se carece de conocimiento para la aplicación de herramientas de análisis, tales como escáneres de seguridad de aplicaciones (*OWASP Mobile Security Testing Guide*), se obvian las revisiones en tiendas oficiales de *Google Play, App Store*, se omiten pruebas de penetración controladas en entornos simulados utilizados en diversos entornos móviles (OWASP, 2021).

En el ámbito conceptual, los estudios destacan que la práctica BYOD presentan riesgos significativos debido a la falta de controles en los dispositivos móviles utilizados en entornos laborales (INCIBE, 2020). Asimismo, se señala que los riesgos de seguridad en dispositivos móviles y aplicaciones cuando se utilizan contraseñas repetidas y débiles, en otras ocasiones de descargan apps fuera de tiendas oficiales y otros casos cuando se accede a conexiones de redes Wi-fi públicas (Hernández, 2022). Cabe indicar que los factores de comportamiento en entornos BYOD afectan la seguridad corporativa (Alshahrani et al., 2021). Estos aportes permiten establecer la necesidad de diagnosticar riesgos por los factores técnicos y humanos.

Respecto al aspecto técnico, el componente se centra en las vulnerabilidades de las aplicaciones móviles. El marco *OWASP Mobile Top* 10 clasifica riesgos críticos como almacenamiento inseguro, comunicación no cifrada o uso de SDKs vulnerables y fáciles de intervenir por los hackers (OWASP, 2021). Como herramientas y técnicas de evaluación, tales como las pruebas de seguridad de aplicaciones móviles (SAST y DAST) son objeto de estudios recientes que sistematizan su uso (Shishkovsky y Sarnov, 2021).

Además, nuevas tecnologías como las redes 5G amplían los ataques, introduciendo amenazas emergentes (Kumar et al., 2023) Algunos informes de la industria (Verimatrix, 2025) y (Akamai, 2025) refuerzan que las aplicaciones actuales presentan fallos recurrentes en criptografía, API y autenticación. Esto demuestra que el problema técnico no es aislado sino generalizado en el ecosistema móvil.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Desde la perspectiva conductual, el comportamiento del usuario es otro vector fundamental en la seguridad móvil, por tanto, se subraya que la conciencia de ciberseguridad y la autoeficacia reducen los riesgos en trabajadores jóvenes (Morufu y Taufik , 2025). En este sentido, los factores cognitivos y emocionales como la autoconciencia influyen para frenar posibles vulneraciones a la seguridad en sus transacciones (Hansen y D'Arcy, 2021).

De forma complementaria, la seguridad de la información que reciben los usuarios depende en gran medida de los hábitos de las personas al momento de realizar sus actividades (Tsaousis y Spiliopoulou, 2020). Se confirma que las brechas de seguridad ocurren porque los usuarios no actualizan sus perfiles y a la vez incurren en prácticas inseguras al momento de utilizar sus dispositivos móviles BOYD (Sotera, 2025). Estos hallazgos confirman la necesidad de integrar el factor humano en cualquier diagnóstico de ciberseguridad móvil (Akamai, 2025), considerando que la seguridad de la información que reciben los usuarios depende de sus hábitos de protección al momento ingresar a las plataformas digitales (D'Arcy, Hovav y Galletta, 2023).

En este sentido, las brechas de defensa se producen porque los propios usuarios facilitan los ataques, en ocasiones por la falta de actualización de sus dispositivos o por la adopción de prácticas inseguras (Chou y Chen, 2020). Es así que la integración técnica-conductual requiere de acciones eficientes y efectivas para frenar ataques cibernéticos y contribuyan al resguardo de la información en el contexto laboral (Garcia et al., 2022).

El estándar ISO/IEC proporciona directrices sobre gestión de riesgos de seguridad de la información, incorporando tanto factores tecnológicos como humanos, reafirman que el eslabón más débil es el usuario móvil, pese a la sofisticación de los ataques y la custodia a los datos de la organización (Fortinet, 2025). En este marco se ratifica la necesidad de concienciar a los usuarios sobre medidas de seguridad como acción inmediata para reducir el inadecuado uso de los sistemas informáticos de las organizaciones y proteger los dispositivos móviles que se los utiliza como BOYD (D'Arcy y otros, 2023).

Este conjunto de aportes demuestra que el vacío investigativo actual se encuentra en la falta de un modelo de diagnóstico global que integre vulnerabilidades técnicas con factores conductuales en la población de jóvenes profesionales ecuatorianos.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Jóvenes profesionales en el entorno BYOD

En el contexto del modelo BYOD, los jóvenes profesionales se los identifica como parte de la generación Millennials y Z, quienes crecieron en el entorno digital y en este siglo XXI se han convertido en la fuerza laboral que forma parte de las organizaciones y usan sus dispositivos móviles en el entorno laboral (Dávila, 2023). Esta caracterización indica que la utilización de la tecnología genera hábitos de uso intensivo de dispositivos móviles, en los resultados del estudio realizado por (Deloitte, 2025), indican que 70% de la Generación Z dedican tiempo a mejorar sus habilidades profesionales con el apoyo de la tecnología,

Los jóvenes profesionales se consideran aquello colaboradores nacidos entre 1995 y 2006 (Generación Z) y los nacidos entre 1983 y 1994 (Millennials), que para el 2030 representaron el 74% de la fuerza laboral en el mundo (Deloitte, 2025). Corresponden a grupo de personas que aplican la tecnología, fundamentando que los esquemas BYOD, les permite adaptarse fácilmente a nuevos desafíos globalizados (Díaz, 2025).

Desde el punto de vista del comportamiento, varios estudios sobre seguridad de la información indican que el factor humano es uno de los elementos más débiles en los entornos de las organizaciones (Díaz, 2025), la forma en que un usuario utiliza su dispositivo afecta mucho la posibilidad de caer en peligros como el phishing, la instalación de apps sin verificar o el uso de redes Wi-Fi públicas que no tienen seguridad (Kumar et al., 2023).

Een el mundo laboral, los jóvenes profesionales al utilizar los dispositivos móviles interactúan con los riesgos de seguridad en la red (Pérez, 2024). Esto quiere decir que su nivel de conocimiento digital, su actitud hacia la seguridad, cómo usan la tecnología y cómo ven los riesgos influye en las acciones que ejecutan para resguardar la información de posibles ciberataques (D'Arcy et al., 2023). Desde el punto de vista de la organización, se destaca la importancia de que el personal esté consciente y recibiendo formación continua como parte esencial del sistema de gestión de la seguridad de la información (Morufu y Taufik , 2025).

Los jóvenes profesionales son un grupo importante para los programas de entrenamiento en ciberseguridad, porque su forma de usar la tecnología influye directamente en la seguridad de los datos y sistemas informáticos, por tanto, se debe considerar el impacto de los dispositivos móviles en el entorno BYOD, considerando los riesgos de ciberseguridad que pueden ocurrir y las acciones que deben asumir para prever estos problemas.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Métodos de investigación

Tipo de investigación

El estudio adoptó un enfoque cuantitativo con predominancia descriptiva y un componente correlacional. En la parte descriptiva se caracterizó las vulnerabilidades técnicas presentes en las aplicaciones móviles utilizadas por jóvenes profesionales y el comportamiento frente a la ciberseguridad.

La investigación fue correlacional, en la medida que analizó la relación entre las vulnerabilidades identificadas y los hábitos de uso de los dispositivos móviles en entornos BYOD.

Diseño de investigación

El diseño de la investigación fue no experimental y transversal, dado que no se manipularon variables y la información se recolectó en un único momento del tiempo.

Población y Muestra

Población: Jóvenes profesionales entre 22 y 35 años que utilizan dispositivos móviles personales para actividades laborales en un esquema BYOD (Bring Your Own Device). Este grupo se caracteriza por el uso intensivo de aplicaciones móviles de productividad, mensajería y finanzas que los convierte en un segmento vulnerable frente a riesgos de ciberseguridad.

Muestra: Se empleó un muestreo no probabilístico por conveniencia, integrado por 40 participantes que cumplieron con el perfil descrito y aceptaron voluntariamente participar en el estudio. La muestra incluyó profesionales de sectores con alto uso de aplicaciones móviles de productividad y finanzas (consultoría, startups, pymes tecnológicas).

Cálculo de la muestra N

La muestra se definió mediante un muestreo no probabilístico por conveniencia, el propósito fue encontrar hallazgos en el diagnóstico de ciberseguridad aplicada, donde la disponibilidad de los participantes constituye un factor determinante para aplicar la investigación (Zamora et al., 2025).

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Para el cálculo del tamaño muestral se empleó la fórmula para poblaciones finitas:

$$n = \frac{N * Z^2 * p * q}{e^2(N-1) + Z^2 * p * q}$$

En forma práctica, se tomó en cuenta la población estimada de 50 jóvenes profesionales de la ciudad de Guayaquil que trabajan en diferentes entornos empresariales. El detalle del cálculo y la aplicación de la fórmula se presentan en la Tabla 1.

Tabla 1 Cálculo del tamaño muestral

Parámetro	Símbolo	Valor utilizado	Descripción
Tamaño de la población	*N*	50	Estimación de jóvenes profesionales en el sector
Nivel de confianza	*Z*	1,96	95% de confianza
Proporción esperada	*p*	0,5	Máxima variabilidad
Complemento	*q*	0,5	(1–p)
Error muestral permitido	*e*	0,05	5%
Tamaño de muestra calculado	*n*	**Por caso de limitacion logistica sera 40**	Resultado de la fórmula para población finita

Nota: Elaborado por el autor

Técnicas e instrumentos de recolección de datos

Técnica: Encuesta

Instrumento: Cuestionario digital con preguntas en escala Likert, orientadas a medir prácticas de seguridad (gestión de permisos, actualización de aplicaciones, uso de contraseñas). Este instrumento permitió cuantificar las conductas de riesgo en los jóvenes profesionales.

El enfoque cuantitativo permitió aplicar la estadística descriptiva (frecuencias, porcentajes, medidas de tendencia central) y análisis correlacional (coeficiente de correlación de Spearman) para evaluar la relación entre vulnerabilidades técnicas y prácticas de seguridad. También las aplicaciones objetivo como las apps de productividad, mensajería y finanzas más usadas por los participantes.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Análisis técnico de aplicaciones móviles (cuantitativo/técnico):

Instrumento: El análisis se realizó combinando técnicas SAST (Static Application Security Testing) y DAST (Dynamic Application Security Testing), empleando herramientas de código abierto y de uso académico ampliamente reconocidas: como MobSF y QARK para el análisis estático automatizado, Apktool y JADX para la ingeniería inversa del código y revisión manual de configuraciones inseguras, Frida para la instrumentación dinámica en entorno controlado.

Alcance del análisis técnico

Solo se analizaron aplicaciones facilitadas por los participantes o versiones públicas descargadas desde tiendas oficiales (Google Play / App Store) con fines de investigación. No se realizó ingeniería inversa ni recopilación de datos en aplicaciones de terceros sin autorización explícita.

Todas las pruebas dinámicas (captura de tráfico, ejecución instrumentada) se realizaron en entorno controlado de laboratorio, con cuentas de prueba y sin acceso a sistemas productivos ni datos de terceros.

Consideraciones Éticas y de datos

El presente estudio analizó aplicaciones móviles y hábitos de uso por jóvenes profesionales; por tanto, se aplicó los principios éticos básicos: consentimiento informado, minimización de datos, seguridad en almacenamiento ante hallazgos críticos. Antes de iniciar cualquier análisis técnico o de tráfico, se solicitó la aprobación de la autoridad correspondiente.

Resultados: Análisis de resultados

Análisis de los Estadísticos descriptivos:

La variable categórica “Uso de autenticación multifactorial” mostró una distribución equilibrada, 50 % de los jóvenes profesionales indicó utilizar 2FA, mientras que 50 % no emplea esta medida de protección, reflejando una adopción parcial de buenas prácticas de ciberseguridad. Estos resultados se lo visualizan en la siguiente tabla 2:

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Tabla 2 Interpretaciones de los datos

Tipo de variable	Nombre	Descripción	Escala de medición
Categórica	Uso de autenticación multifactor (2FA)	Indica si el participante utiliza un método de autenticación adicional para acceder a sus aplicaciones móviles.	Sí / No
Ordinal (Likert)	Frecuencia de actualización de aplicaciones móviles	Mide la frecuencia con la que el usuario actualiza las aplicaciones instaladas (1 = Nunca → 5 = Siempre).	Escala Likert 1–5
Continua	Nivel de exposición a vulnerabilidades técnicas	Representa el nivel promedio de vulnerabilidades identificadas en las aplicaciones móviles (según criterios OWASP Mobile Top 10).	0 – 100

Nota: Elaborado por el autor

Tabla 3 Uso de autentificación multifactor

Variable categórica — Uso de autenticación multifactor (2FA)		
Categoría	Frecuencia	Porcentaje
Sí	20	50%
No	20	50%

Nota: Elaborado por el autor

En los resultados se observa que en la categoría de uso hay un equilibro 50% que, si lo usan vs el 50% que no lo usan como medio de protección de datos, se confirma la problemática.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Tabla 4 Frecuencia de Actualización de datos

Variable Likert — Frecuencia de actualización

Medida	Valor
n	40
Media	3.2
Desviación estándar	1.4
Mínimo / Máximo	Minimo = 1 Maximo = 5

Nota: Elaborado por el autor

En cuanto a la frecuencia de actualización de aplicaciones, se observó una media de 3.2 ± 1.4, con valores que oscilan entre 1 (nunca actualiza) y 5 (siempre actualiza). (Ver Tabla 5) Esto sugiere una tendencia intermedia en la adopción de prácticas preventivas de mantenimiento del software. En la Tabla 5 se exponen las vulnerabilidades técnicas.

Tabla 5 Nivel de exposición a Vulnerabilidades técnicas

Variable continua — Nivel de exposición a vulnerabilidades técnicas

Medida	Valor
n	40
Media	55
Desviación estándar	22.1
Mínimo / Máximo	24 / 87

Nota: Elaborado por el autor

En relación con el nivel de exposición a vulnerabilidades técnicas registró un promedio de 55 puntos ± 22.1, dentro de un rango de 24 a 87 (Ver Tabla 6). En general, los participantes que no actualizan sus aplicaciones y no emplean autenticación multifactor presentan niveles más altos de exposición.

Análisis inferencial

El propósito de este análisis fue evaluar la relación entre los hábitos conductuales de seguridad móvil y la exposición a vulnerabilidades técnicas en el contexto del uso de dispositivos personales bajo el esquema BYOD (Bring Your Own Device). Para ello se empleó una prueba de correlación de Spearman (ρ), dado que las variables presentaron niveles de medición ordinal y continua. En los resultados no se asumió una distribución normal en los datos de la investigación.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Las variables analizadas fueron:

Frecuencia de actualización de aplicaciones móviles (Likert 1–5): representa el nivel de comportamiento preventivo de los usuarios.

Nivel de exposición a vulnerabilidades técnicas (0–100): indicó el promedio de vulnerabilidades detectadas en las aplicaciones móviles, de acuerdo con las categorías OWASP Mobile Top 10.

Formulación de hipótesis

Hipótesis nula (Ho): No existe relación estadísticamente significativa entre la frecuencia de actualización de las aplicaciones móviles y el nivel de exposición a vulnerabilidades técnicas.

Hipótesis alternativa (H1): Existe una relación estadísticamente significativa e inversa entre la frecuencia de actualización de las aplicaciones móviles y el nivel de exposición a vulnerabilidades técnicas.

Resultados de la prueba de hipótesis

La aplicación de la correlación de Spearman arrojó los siguientes datos, expuesto en la Tabla 6.

Tabla 6 Prueba estadística aplicada

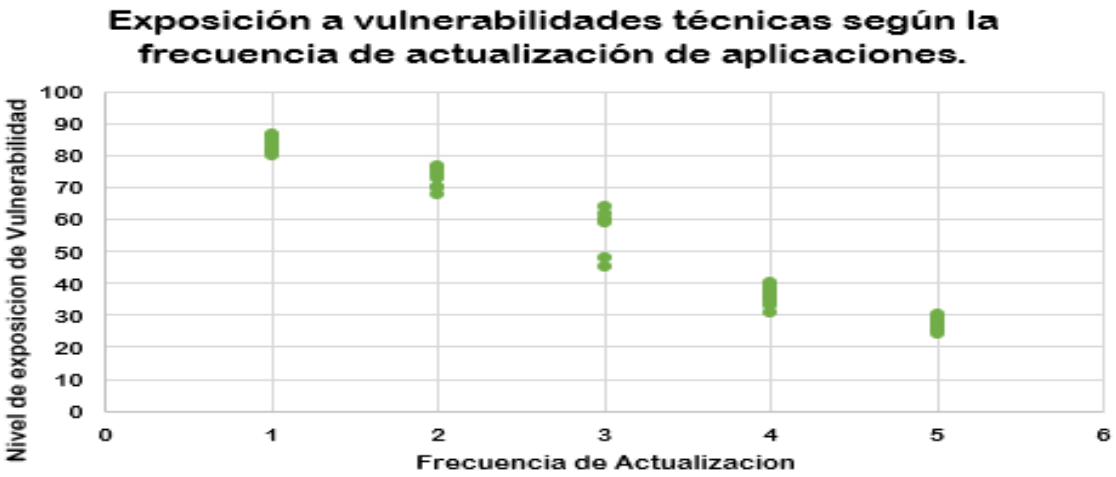
	Prueba estadística aplicada		
Prueba	Estadístico (ρ)	p (aprox.)	Decisión (α = 0.05)
Spearman	−0.61	0.001	Se rechaza H_0

Nota: Elaborado por el autor

El valor negativo del coeficiente (ρ = –0.61) indica que a medida que aumenta la frecuencia de actualización de las aplicaciones móviles, el nivel de exposición a vulnerabilidades técnicas disminuye. Este resultado es estadísticamente significativo ($p < 0.05$), por lo cual se rechaza la hipótesis nula y se acepta la hipótesis alternativa (H_1) Esta relación se observa gráficamente en la siguiente figura:

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Figura 1 Dispersión: Exposición a vulnerabilidades técnicas



Nota: Elaborado por el autor

En la figura de dispersión se ilustró de manera visual la correlación estadísticamente significativa e inversa ($\rho = -0.61$) existente entre los hábitos del usuario y el riesgo técnico. Se evidenció claramente una tendencia descendente, esto quiere decir que los participantes con una menor frecuencia de actualización de sus aplicaciones (valores 1 y 2) registraron los niveles más altos de exposición a vulnerabilidades.

En contraste, a medida que la frecuencia de actualización aumentó (valores 4 y 5), el nivel de exposición desciende en forma notable. Esto corrobora empíricamente que el comportamiento preventivo del joven profesional es un factor determinante para mitigar los riesgos de ciberseguridad en entornos BYOD.

Discusión de resultados

En los resultados de los estadísticos descriptivos se mostró una adopción parcial de buenas prácticas de seguridad, 50% de los participantes utilizó autenticación multifactorial (2FA), lo que reveló una brecha importante entre el conocimiento digital esperado en jóvenes profesionales y la aplicación real de medidas de protección. Se coincide con los hallazgos de D'Arcy et al. (2023) y Alshahrani et al. (2025), quienes sostienen que el factor humano continúa siendo el eslabón más débil en la cadena de seguridad de la información, incluso en poblaciones con alta familiaridad tecnológica como los Millennials y generación Z.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

En cuanto a la frecuencia de actualización de aplicaciones (media 3.2 ± 1.4), se observa una conducta preventiva intermedia, lo que resulta relevante con los hallazgos técnicos del análisis basado en el marco OWASP Mobile Top 10, que identifican vulnerabilidades recurrentes asociadas a almacenamiento inseguro, fallos en autenticación y deficiencias criptográficas. Se concuerda con Hernández (2022), Díaz (2025), quienes afirman que la falta de actualización constante facilita la explotación de vulnerabilidades para proteger los datos de las organizaciones.

El resultado más significativo del estudio se encuentra en el análisis inferencial. La correlación de Spearman ($\rho = -0.61$; $p < 0.05$) confirma una relación inversa estadísticamente significativa entre la frecuencia de actualización y el nivel de exposición a vulnerabilidades técnicas. Este hallazgo es consistente con los lineamientos de la *International Organization for Standardization* a través de la norma ISO/IEC 27001 (2022), que enfatiza la necesidad de controles preventivos como la gestión de actualizaciones y autenticación robusta en dispositivos móviles.

Desde una perspectiva más estratégica, los resultados confirman que el modelo BYOD no es intrínsecamente inseguro; el riesgo emerge cuando no existe una integración entre controles técnicos y cultura de seguridad. Los resultados se asemejan al enfoque del OWASP (2021), que clasifica las vulnerabilidades técnicas y a su vez promueve las prácticas seguras de desarrollo y uso de protección de los datos de las organizaciones. Estas afirmaciones son ratificadas por Chou y Chen (2020), quienes exponen que se deben proteger los datos de la empresa para salvaguardar la información empresarial.

Uno de los componentes más importantes es la confirmación de la muestra de los jóvenes profesionales de Guayaquil, pertenecientes a la Generación Millennials y Generación Z, en los resultados se coincide con lo planteado por Deloitte (2025), respecto a que estas generaciones presentan alta competencia digital, pero no necesariamente una cultura sólida de ciberseguridad. Se reafirma con lo expuesto por Shishkovsky y Sarnov (2021), cuyo estudio demuestra que la familiaridad tecnológica equivale al uso de BYOD en forma segura.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Conclusiones

Las conclusiones se desarrollaron de acuerdo al objetivo y los resultados del estudio.

Se concluye que al analizar el nivel de riesgo de ciberseguridad frente a las vulnerabilidades técnicas presentes en las aplicaciones móviles y los patrones de comportamiento de los jóvenes profesionales en entornos BYOD, se confirma que existe una relación estadísticamente significativa e inversa entre los hábitos de actualización de aplicaciones móviles y el nivel de exposición a vulnerabilidades técnicas. En consecuencia, se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

En síntesis, aunque los jóvenes profesionales, pertenecientes a las generaciones Millennials y Z, poseen alta familiaridad con la tecnología, incluso en los entornos BYOD, aún mantienen prácticas de seguridad inconsistentes, especialmente en el uso de autenticación multifactorial y en la actualización sistemática del software que genera vulnerabilidad de ciberataques, entonces se incrementa su exposición a riesgos identificados en marcos internacionales de seguridad móvil.

Los resultados confirman que el riesgo de ciberseguridad en entornos BYOD está condicionado por el comportamiento del usuario. Por tanto, se deben aplicar estrategias integrales que se relacionan con los controles técnicos cifrado, autenticación multifactor, entre otros con programas de formación en ciberseguridad.

Finalmente, los hallazgos validan el vacío investigativo identificado en el estado del arte: la necesidad de integrar vulnerabilidades técnicas y factores conductuales en un modelo diagnóstico aplicado al contexto ecuatoriano. Sus aportes desde el enfoque diagnóstico contribuyen al fortalecimiento de la gestión de riesgos en organizaciones que adoptan esquemas BYOD.

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Referencias bibliográficas

Akamai. (2025). *Estado de la seguridad de API y aplicaciones 2025, volumen 11, número 02.* Akamai Technologies.

Alshahrani, M. S., Aljuraidan, H. A., & Al-Nami, N. (2021). *User security behavior in BYOD environments: A study of professional employees. Computers & Security.*

Chou, J. T., & Chen, Y. C. . (2020). *Combining technical and behavioral factors for cybersecurity risk assessment of IoT devices.* IEEE Internet of Things Journal.

D'Arcy, J., Hovav, A., & Galletta, D. (2023). *User awareness of security countermeasures and its impact on information systems misuse: A deterrence perspective.* Information Systems Research.

Dávila, R. (1 de Agosto de 2023). Análisis cuantitativo de la relación entre el uso de dispositivos móviles y la productividad laboral en un entorno empresarial. *Revista Conrado, 19*(2). doi:https://conrado.ucf.edu.cu/index.php/conrado/article/view/3251

Deloitte. (2025). https://www.deloitte.com/content/dam/assets-zone4/latam/es/docs/campaigns/2025/Encuesta_de_las_Generaciones_Z_y_Millennials_2025_Esp.pdf. *Deloitte*. Obtenido de https://www.deloitte.com/content/dam/assets-zone4/latam/es/docs/campaigns/2025/Encuesta_de_las_Generaciones_Z_y_Millennials_2025_Esp.pdf

Díaz, C. (8 de marzo de 2025). Más allá de los millennials y la generación Z: preparando a las organizaciones para el futuro laboral. *Dictamen Libre*. doi:DOI: https://doi.org/10.18041/2619-4244/dl.36.12297

Fortinet. (2025). *Reporte Ciberseguridad 2025.*

Fortinet. (5 de enero de 2026). Obtenido de ¿Qué es Bring Your Own Device (BYOD)? Definición y explicación de BYOD: https://www.fortinet.com/lat/resources/cyberglossary/byod

Garcia, Y., Arteaga, K., Castillo, E., Zambrano, J., & Mendoza, M. (14 de diciembre de 2022). Protección de datos para el uso de bring your own device. *Revista Minerva*. doi:https://doi.org/10.47460/minerva.v1iSpecial.82

Guaña, J. (6 de mayo de 2024). Seguridad, amenazas y mecanismos de protección de los dispositivos móviles. *DATEH*, *6*(1). doi:ISSN: 2773-7527

Hansen, G. B., & D'Arcy, J. (2021). *User behavior and the mobile security*.

Hernández, Y. (2022). *Seguridad de dispositivos móviles y aplicaciones: una revisión de riesgos y desafíos actuales.* Revista Universidad y Sociedad.

INCIBE. (2020). *Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

ISO/IEC 27001. (2022). *Information security, cybersecurity and privacy protection.* https://www.iso.org/es/norma/27001.

Kumar, M., Gupta, B. B., Misra, R., & Singh, P. (2023). *Cybersecurity threats and vulnerabilities in 5G mobile networks: A state-of-the-art review. Computers & Security.*

Lee, D., & Kim, Y. (2023). *The role of cybersecurity awareness and self-efficacy in reducing mobile security risk: A study of Generation Z workers. International Journal of Information Management.*

Loor, J. (junio de 2024). Uso de dispositivos móviles en el lugar de trabajo, implicaciones sobre la productividad laboral. *Researchgate.net*. doi:DOI:10.13140/RG.2.2.17059.46888

Mahmood, M., & Bano, M. (2020). *Impact of BYOD on information security in corporate environments: A systematic literature review. Journal of Network and Computer Applications.*

Montalvo, C., Checa, M., & Cabrera , P. (3 de julio de 2025). El esquema de seguridad en el modelo BYOD y su nuevo paradigma de aplicación. *Pro Sciences*. doi:DOI: https://doi.org/10.29018/issn.2588-1000vol9iss58.2025pp378-393

Morufu, M., & Taufik , R. (10 de Julio de 2025). A Review of Bring Your Own Device on Security Issues. *Sagepub journals*. Obtenido de https://journals.sagepub.com/doi/10.1177/21582440155803372

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Oke, S. (25 de junio de 2024). The Risks and Rewards of Personal Devices and BYOD. *Coretek*. Obtenido de https://coretek.co.uk/the-risks-and-rewards-of-personal-devices-and-byod/

Organization, E. (2025). *Los ataques a dispositivos móviles y apps aumentan porque los permitimos.* Obtenido de Entrepreneur.

OWASP. (2021). Obtenido de OWASP Mobile Top 10: Principales riesgos de seguridad en aplicaciones móviles. OWASP: https://owasp.org/www-project-mobile-top-10/

Pérez, Á. (2024). *Educarse en la era digital.* Madrid : Morata .

Rodríguez, J. (2020). Revista de Innovación y Investigación en Educación. *REIRE*, 13(2), 1–13.

Rodríguez, L., & Martínez, J. (19 de Septiembre de 2022). Uso de aplicaciones móviles como herramienta de apoyo tecnológico para la enseñanza con metodología Steam. *Redalyc.org*, *18*(36). Obtenido de https://www.redalyc.org/journal/6078/607872732006/html/

Security., S. D. (2025). *Amenazas y oportunidades emergentes en 2025: Un análisis prospectivo de las tendencias en ciberseguridad*. Obtenido de Sotera Digital Security Blog.

Shishkovsky, M., & Sarnov, I. (2021). *Mobile application security testing tools and techniques: A review. Proceedings of the 2021 International Conference on Information Technology (ICIT).*

Tatai, P. (12 de enero de 2026). Política de seguridad BYOD: principales riesgos, pros y contras y mejores prácticas. *Safetica*. Obtenido de https://www.safetica.com/es/recursos/blogs/politica-de-seguridad-byod-principales-riesgos-pros-y-contras-y-mejores-practicas

Tsaousis y Spiliopoulou. (2020). *Towards a comprehensive model of information security behavior: A meta-analysis.* Computers in Human Behavior.

Verimatrix. (2025). *Principales fallos de seguridad de las aplicaciones móviles de RSAC 2025*. Obtenido de https://www.verimatrix.com/es/antipirateria/ideas-contra-la-pirateria/

Revista Multidisciplinaria Prospherus
ISSN: 3091-177X
Doi: https://doi.org/10.63535/smk3pn96

Zamora, Gutiérrez y Pérez. (4 de octubre de 2025). *Evidencias sobre la validación de los tests: una guía práctica. Revista relacionada con evaluación y salud pública*. Obtenido de https://scielo.isciii.es/scielo.php?pid=S1886-144X2023000300001&script=sci_arttext&utm_source=chatgpt.com

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés posible.

Nota:

El articulo no es producto de una publicación anterior.