Vol.9 No.4 (2025): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.9.4.2025.e1198

Home Wi-Fi security assessment: practical vulnerability analysis of commercial home routers with WPA2 and WPA3 protocols.

Evaluación de la seguridad en redes Wi-Fi domésticas: análisis práctico de vulnerabilidades en routers domésticos comerciales con protocolos WPA2 y WPA3.

Autores:

Luna-Arteaga, Alexander Paul
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca – Ecuador

alexander.luna.18@est.ucacue.edu.ec
https://orcid.org/0009-0001-3030-1002

Flores-Urgilés, Cristhian Humberto
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca – Ecuador

chfloresu@ucacue.edu.ec
https://orcid.org/0000-0002-0465-3370

Fechas de recepción: 16-OCT-2025 aceptación: 11-NOV-2025 publicación: 30-DIC-2025

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

La seguridad en redes Wi-Fi domésticas representa un desafío creciente en la era digital, especialmente ante la dependencia de protocolos como WPA2 y WPA3. Este estudio realiza un análisis práctico de vulnerabilidades en routers comerciales ampliamente utilizados en Ecuador (CNT, Netlife, Claro, Valle.net y TP-Link), mediante pruebas de penetración controladas en entornos aislados. Se emplearon herramientas especializadas como Aircrack-ng, Hashcat y Wireshark, junto con antenas Alfa AWUS036ACH en sistemas Kali Linux, para evaluar la resistencia de ambos protocolos frente a ataques de diccionario, fuerza bruta, deautenticación y vulnerabilidades específicas como KRACK y fallos en el handshake SAE de WPA3. Los resultados indican que WPA2 presenta una tasa de éxito del 64 % en ataques exitosos, principalmente debido a contraseñas débiles y configuraciones predeterminadas, mientras que WPA3 reduce significativamente este riesgo al 20 %, aunque no es inmune a errores de implementación. Se concluye que la seguridad de las redes domésticas no depende únicamente del protocolo, sino también de buenas prácticas de configuración, actualización de firmware y concienciación del usuario. Estas evidencias respaldan la necesidad de migrar progresivamente a WPA3 y reforzar la educación en ciberseguridad para entornos residenciales.

Palabras clave: Redes Wi-Fi; Protocolos de Seguridad; WPA2; WPA3; seguridad de la información; ISO/IEC 27001.

Abstract

Home Wi-Fi security remains a critical concern in the digital age, particularly regarding the use of WPA2 and WPA3 protocols. This study presents a practical vulnerability assessment of widely used commercial home routers in Ecuador (CNT, Netlife, Claro, Valle.net, and TP-Link) through controlled penetration tests in isolated environments. Specialized tools such as Aircrack-ng, Hashcat, and Wireshark, along with Alfa AWUS036ACH antennas on Kali Linux systems, were employed to evaluate both protocols against dictionary attacks, brute force, deauthentication, and specific vulnerabilities like KRACK and SAE handshake flaws in WPA3. Results show that WPA2 exhibited a 64% success rate in penetration attempts, primarily due to weak passwords and default configurations, whereas WPA3 significantly reduced this risk to 20%, though it remained susceptible to implementation errors. The findings demonstrate that home network security depends not only on the protocol but also on proper configuration, firmware updates, and user awareness. The study supports a gradual migration from WPA2 to WPA3 and emphasizes the importance of cybersecurity education for residential users to mitigate emerging threats effectively.

Keywords: Wi-Fi networks; Security protocols; WPA2; WPA3; information security; ISO/IEC 27001.

Introducción

Ahora las redes Wi-Fi en casas son muy importantes para el funcionar de las casas hoy En estos días con el aumento de trabajo desde casa y estudios en línea y el avance constante del Internet. La gente requiere cada vez más firmeza y conexión en la red con tantas cosas conectadas, así que esto pone problemas grandes a la seguridad de la red. (Cisco, 2023), esto supone un desafío crucial para proteger la distribución del desorden de estas redes alto ancho de banda (Sujay Vailshery, 2025).

Incluso con los avances significativos avances en los protocolos de seguridad inalámbrica como WPA2 (Wi-Fi Protected Access II) y su evolución hacia el WPA3, diversos estudios evidencian que las redes Wi-Fi aún presentan vulnerabilidades. Presentándose con más frecuencia en el protocolo WPA2 uno de los estándares más utilizados a nivel mundial actualmente el cual ha sido vulnerable a ataques conocidos como los KRACK (Key Reinstallation Attacks) y los ataques de diccionario, que aprovechan debilidades en el proceso de autenticación (Veroni et al., 2022). Aunque el protocolo WPA3 introduce mejoras notables como la Autenticación Simultánea de Iguales (SAE) y el cifrado individualizado por usuario, las investigaciones más recientes han demostrado que también puede verse comprometido debido a fallos en el handshake Dragonfly y a implementaciones inseguras por parte de algunos fabricantes (Ye et al., 2024).

Entendiendo que las redes Wi-Fi del hogar se hacen muy deseadas para los hackers, que siempre notan configuraciones default malas, claves débiles y la falta de buenas prácticas para cuidarse en el entorno de red (Lim et al., 2025). Desde la perspectiva ecuatoriana y más extendida en Latinoamérica, este problema es más grave porque poca gente sabe acerca métodos seguros en el mundo tecnológico y no hay revisiones técnicas en lugares caseros o no de trabajo. Esta combinación de razones hace un peligro constante ya que una red casera tocada podría ser un primer punto de entrada para ataques más complejos contra instituciones públicas o privadas (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020).

Este estudio propone un análisis técnico y práctico de las vulnerabilidades presentes en redes Wi-Fi domésticas que emplean los protocolos WPA2 y WPA3, mediante la ejecución de pruebas de penetración controladas, se utilizarán herramientas de evaluación ampliamente reconocidas, como Aircrack-ng, Hashcat y Wireshark, con el propósito de examinar la facilidad con la que pueden explotarse fallos comunes y de identificar el impacto que tienen las configuraciones predeterminadas de los routers comerciales en la seguridad de las redes (Cathcart & Mohd, 2023). Con este estudio se busca formular recomendaciones prácticas y accesibles que contribuyan a fortalecer la seguridad digital en los hogares y que puedan ser implementadas tanto por usuarios comunes como por proveedores de servicios de internet y fabricantes de equipos de red.

Material y métodos

Material

En este estudio se usan varios instrumentos y herramientas. El análisis de las debilidades en las redes Wi-Fi de los hogares está orientado a las casas. Entre ellos, se ve que la observación a usuarios que viven en casas para saber cómo ponen los enrutadores y los chequeos de seguridad hechos a equipos de los proveedores CNT, Netlife, FibraMax, Claro, Valle.net y extensores TP-Link. Para el estudio práctico, se pusieron en acto herramientas de software especiales, como Wireshark para capturar el tráfico de la red, Aircrack-ng y Hashcat para realizar ataques de diccionario y fuerza bruta, como equipos de hardware se usó una antena

Alfa AWUS036ACH compatible con sistemas operativos Linux, en este caso se usó Kali Linux para pruebas de entrada manejadas. Para la representación de los resultados se usaron formas estadísticas descriptivas e inferenciales mostradas por gráficos y tablas que se comparan con el fin de encontrar cuántas veces hay errores, el nivel de riesgo de cada uno de ellos y la dureza de cada protocolo frente a ataques falsos. Estos materiales permitieron recopilar evidencia tanto cuantitativa como cualitativa para sustentar el análisis de la seguridad en redes domésticas bajo los protocolos WPA2 y WPA3.

Métodos

Las fuentes secundarias de información utilizadas correspondieron a libros especializados, artículos científicos y publicaciones técnicas de organismos como la Wi-Fi Alliance y NIST, que fortalecieron la base teórica y permitieron estructurar el marco conceptual del estudio.

La investigación se enmarcó como aplicada, no experimental y transeccional, con enfoque mixto, ya que combinó análisis cualitativo (descripción de vulnerabilidades técnicas) y cuantitativo (medición de ataques exitosos).

El procedimiento metodológico se desarrolló en fases:

1. Configuración inicial de los routers: restablecimiento a valores de fábrica, activación de WPA2 y WPA3 y actualización de firmware.
2. Entorno de pruebas controlado: redes aisladas, sin conexión externa, con el fin de garantizar la ética del proceso.
3. Captura de tráfico: mediante Wireshark, registrando handshakes y autenticaciones.
4. Pruebas de penetración: con Aircrack-ng y Hashcat en Kali Linux, empleando ataques de diccionario como rockyou y números de cedula generados de forma automática con Python el cual es capaz de generar un secuencial desde 1 hasta n y mediante el algoritmo de validación de números de cedula verificar si es válido o no y si es válido guardar en el diccionario para su posterior uso, fuerza bruta y deautenticación.
5. Escenarios específicos: pruebas de vulnerabilidades documentadas como KRACK, PMKID, downgrade y fallos en SAE de WPA3.

Las variables analizadas incluyeron:

- Vulnerabilidades técnicas (autenticación, cifrado, gestión de claves).
- Nivel de riesgo (bajo, medio, alto).

El análisis de datos se realizó en dos niveles:

- **Descriptivo**, con tablas y gráficos que muestran frecuencia y distribución de vulnerabilidades.
- **Comparativo**, evaluando diferencias entre WPA2 y WPA3

Resultados

Descripción y análisis de las herramientas utilizadas

Las principales herramientas empleadas fueron Wireshark para captura de paquetes, Aircrack-ng para ataques de diccionario y handshakes, y Hashcat para descifrado de contraseñas mediante fuerza bruta. Estas herramientas permitieron comprobar vulnerabilidades en la autenticación y gestión de claves en routers de CNT, Netlife, Claro, Valle.net y TP-Link.

Figura 1

Número de intentos

Protocolo	Total de intentos	Ataques exitosos	Porcentaje de éxito
WPA2	50	32	64%
WPA3	50	10	20%

Fuente: Alexander Luna (2025)

Descripción de la muestra

La muestra correspondió a routers domésticos comerciales de diferentes proveedores de internet en Ecuador (CNT, Netlife, Claro, Valle.net y TP-Link), seleccionados por su amplia distribución y compatibilidad con WPA2 y WPA3. Todos los equipos estaban en estado funcional y configurados con firmware actualizado.

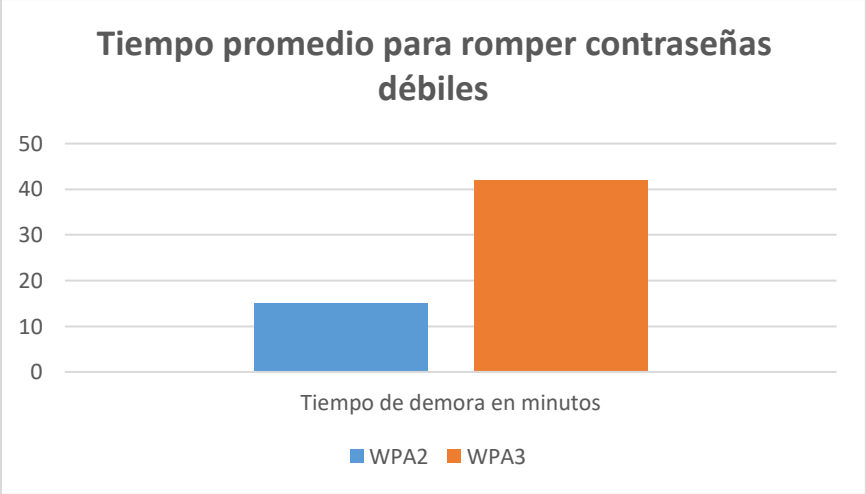
Análisis de los Resultados

Los resultados evidenciaron que WPA2 fue el protocolo más vulnerable, con una tasa de éxito del 64 % en ataques de diccionario y fuerza bruta, confirmando su susceptibilidad frente a claves débiles. WPA3 mostró mayor resistencia (20 % de éxito), pero no estuvo exento de riesgos, especialmente en el handshake SAE, donde se identificaron vulnerabilidades de downgrade y fallos de implementación en ciertos dispositivos.

El tiempo promedio de ruptura de contraseñas débiles, la **figura 2** presenta el tiempo promedio requerido para comprometer credenciales débiles en WPA2 y WPA3. WPA2 mostró tiempos más cortos de vulneración, mientras que WPA3 presentó mayor resistencia, aunque no fue completamente inmune.

Figura 2

Tiempo promedio para romper contraseñas débiles



Fuente: Alexander Luna (2025)

Se observó que las configuraciones predeterminadas con contraseñas débiles siguen siendo el principal factor de riesgo, independientemente del protocolo. Los routers de CNT y Claro resultaron más expuestos en WPA2, mientras que TP-Link y Netlife presentaron mayor robustez al implementar WPA3 con firmware actualizado, sin embargo, los routers TP-Link por también pudieron ser vulnerados por malas configuraciones de los usuarios como WPA encendido y contraseñas genéricas.

También se realizó una comparativa de routers por proveedor la **Figura 3** refleja las diferencias entre los dispositivos de cada proveedor. Se evidenció que los routers de CNT y Claro fueron más vulnerables en configuraciones predeterminadas, mientras que los equipos de Netlife y TP-Link mostraron mayor robustez al implementar WPA3 con firmware actualizado.

Figura 3

Comparativa de routers y proveedores

Proveedor / Marca	Protocolo	Vulnerabilidades detectadas	Nivel de riesgo
CNT	WPA2	Ataques de diccionario y deautenticación	Alto
Netlife	WPA3	Fallos menores en SAE	Medio
FibraMax	WPA3	Fallos menores en SAE	Medio
Claro	WPA2	Exposición a ataques de fuerza bruta	Alto
Valle.net	WPA2/WPA3	Contraseñas débiles en configuración inicial	Medio
TP-Link Extensor	WPA3	Riesgo bajo, mitigado con firmware actualizado	Bajo

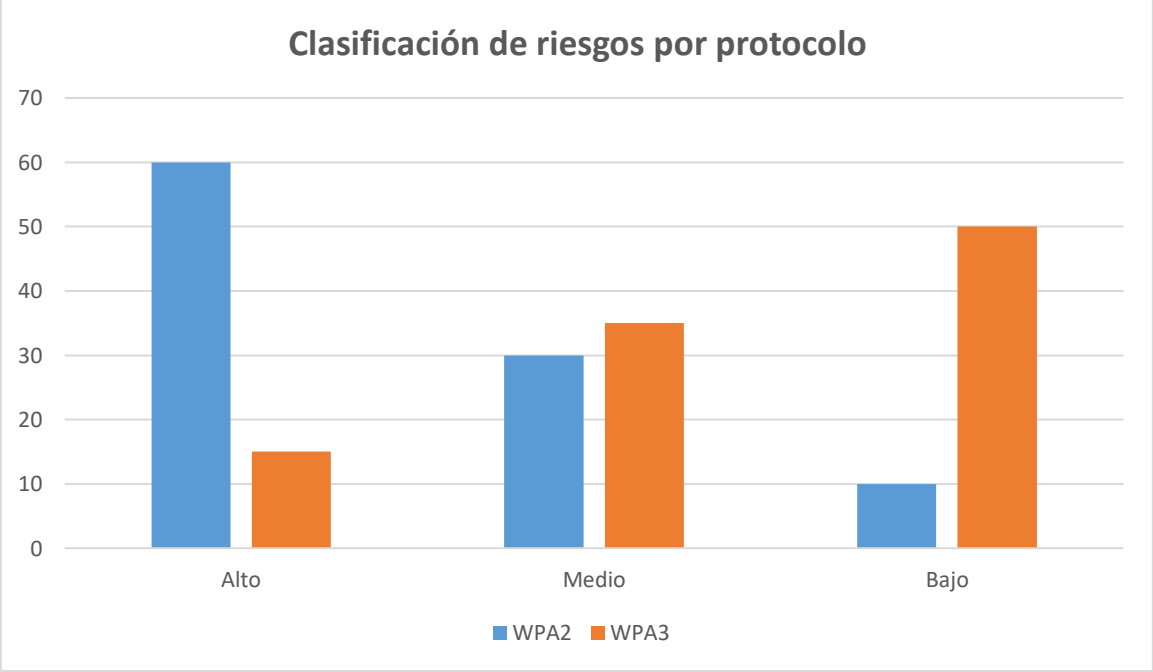
Fuente: Alexander Luna (2025)

Clasificación de riesgos

En la **Figura 4** se representa la clasificación global de riesgos encontrada en los routers evaluados. WPA2 concentró la mayor proporción de riesgos altos, mientras que WPA3 predominó en riesgos bajos y medios.

Figura 4

Clasificación global de riesgos



Fuente: Alexander Luna (2025)

Estos hallazgos refuerzan la necesidad de actualizaciones constantes, uso de contraseñas seguras y eliminación de configuraciones de fábrica como medidas críticas para mitigar riesgos en entornos domésticos.

Discusión

El presente estudio permitió evidenciar que las redes inalámbricas domésticas continúan presentando vulnerabilidades significativas, especialmente cuando utilizan el protocolo WPA2, cuya susceptibilidad a ataques de fuerza bruta y de diccionario se confirmó con una tasa de éxito del 64 %. Este hallazgo refuerza el principio ampliamente documentado en la literatura (Vanhoef & Piessens, 2017), donde se destaca que las debilidades en la gestión de claves de WPA2 lo hacen vulnerable frente a contraseñas débiles.

Por otro lado el protocolo WPA3 demostró una mayor resistencia con un 20% de éxito en los intentos de penetración, lo cual valida su incorporación de mecanismos más robustos como el handshake Simultaneous Authentication of Equals (SAE). Pero también se identificaron excepciones relevantes como en ciertos dispositivos se detectaron vulnerabilidades de downgrade y fallos de implementación, lo que indica que la seguridad no depende exclusivamente del protocolo, sino también de la correcta configuración y actualización del firmware por parte de los fabricantes.

Estos resultados concuerdan con investigaciones previas que señalan que las mejoras introducidas en WPA3 no eliminan por completo los riesgos, sino que desplazan las amenazas hacia vectores más sofisticados(Vanhoef & Ronen, 2019). También se constató que la persistencia de contraseñas débiles o configuraciones de fábrica continúa siendo el factor de riesgo más crítico, tal como lo destacan (Ye et al., 2024).

Si miramos esto desde un punto de vista realista, los resultados sugieren que tanto las compañías que nos dan internet como los que hacen los routers deberían insistir en que actualicemos el software de estos aparatos a menudo y que usemos claves complicadas sí o sí. En casa, cada uno de nosotros tiene que tomar las riendas y cuidar de la seguridad de nuestra red, haciendo cosas como cambiar las claves que vienen por defecto, usar el sistema WPA3 si podemos y apagar opciones que no necesitamos, como el WPS. En el plano de las ideas, el estudio viene a decir que, cuanto más fuertes sean los sistemas para proteger la información, menos problemas de seguridad tendremos, pero también nos enseña que la seguridad del wifi es algo que depende de muchas cosas. No solo importa cómo está hecho el sistema, sino también cómo lo ponemos en marcha, cómo lo configuramos y cómo lo usamos.

En consecuencia, se llegó a la conclusión de que:

1. En el ámbito doméstico, es hora de ir dejando atrás el WPA2 y pasarse al WPA3, ya que está bastante expuesto a ataques que ya conocemos de sobra.
2. Si bien es cierto que el WPA3 mejora bastante la seguridad, tampoco es que sea invencible. Todo depende de que se implemente bien técnicamente y de que las contraseñas sean robustas, claro.
3. Más allá de lo bueno que sea el protocolo en sí, lo que de verdad marca la diferencia para evitar problemas es que los usuarios estén bien informados y que mantengan sus dispositivos al día.

Estas conclusiones se basan en lo que vimos en las pruebas de penetración, donde quedó claro que un protocolo aguanta mejor que otro. Al igual se pudo confirmar que la seguridad de las redes wifi en casa depende mucho de cómo las configuremos.

Conclusiones

- La indagación que se hizo dejó ver que las redes Wi-Fi de las casas siguen siendo un blanco fácil, porque hay muchas cosas mal con la forma en que están hechas, cómo se ponen las cosas y lo que hace la gente que las usa.
- Se supo que WPA2 tiene puntos débiles muy grandes, que se pueden atacar probando muchas contraseñas hasta dar con la correcta. Esto hace que no sea suficiente para estar seguros hoy en día.
- WPA3 es mucho mejor porque tiene formas más fuertes de comprobar quién eres, como SAE, lo que hace que sea más difícil entrar sin permiso. Pero no es perfecto, porque se encontraron errores en cómo se usa en algunos sitios y problemas si la gente pone contraseñas fáciles.
- Se demostró que para considerar una red inalámbrica segura no solo importa cómo está hecha, sino también otras cosas como tener el firmware del router con su última actualización y sobre todo enseñar a la gente a protegerse en Internet.
- El estudio dice al final que la seguridad de las redes inalámbricas tiene que verse como algo que cambia todo el tiempo, que se adapta a los nuevos peligros y no como algo que se soluciona con una sola cosa.

Recomendaciones

- Migrar progresivamente del protocolo WPA2 a WPA3 que es el más reciente tanto en entornos domésticos como empresariales esto siempre y cuando el hardware lo permita con el fin de reducir los riesgos asociados a ataques conocidos.
- Fomentar la actualización periódica del hardware y software de routers garantizando aplicar correcciones de seguridad liberadas por los fabricantes.
- Promover el uso de contraseñas robustas evitando configuraciones predeterminadas las cuales son débiles y facilitan los ataques de diccionario.
- Deshabilitar funciones inseguras como WPS que representan una puerta de entrada para atacantes pese al uso de protocolos más modernos.
- Incorporar campañas de concientización y educación digital para usuarios finales para que comprendan la importancia de la seguridad en la red doméstica y adopten prácticas preventivas.
- Incentivar investigaciones futuras sobre vulnerabilidades emergentes en WPA3 considerando que la evolución tecnológica traerá nuevos avances y consigo nuevos retos en ciberseguridad.

Referencias bibliográficas

Banco Interamericano de Desarrollo, & Organización de los Estados Americanos. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe | Publicaciones*. https://publications.iadb.org/es/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Cathcart, J., & Mohd, T. K. (2023). Password Hacking Analysis of Kali Linux Applications. *Lecture Notes in Networks and Systems*, *665 LNNS*, 815–828. https://doi.org/10.1007/978-981-99-1726-6_63

Cisco. (2023). *2023 Annual Report*. www.cisco.com

Lim, Y. Z., Rahman, H. B. A., & Sikdar, B. (2025). *False Sense of Security on Protected Wi-Fi Networks*. http://arxiv.org/abs/2501.13363

Sujay Vailshery, L. (2025, June 25). *Global IoT and non-IoT connections 2010-2025| Statista*. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

Vanhoef, M., & Piessens, F. (2017). *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*. https://doi.org/10.1145/3133956.3134027

Vanhoef, M., & Ronen, E. (2019). *Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd*.

Veroni, E., Ntantogian, C., & Xenakis, C. (2022). A large-scale analysis of Wi-Fi passwords. *Journal of Information Security and Applications*, *67*, 103190. https://doi.org/10.1016/J.JISA.2022.103190

Ye, J., Zhao, L., Zhang, M., Wu, L., Zhang, W., & De Carné De Carnavalet, X. (2024). *Exposed by Default: A Security Analysis of Home Router Default Settings*. 17. https://doi.org/10.1145/3634737.3637671

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.