Revista Científica Multidisciplinar G-ner@ndo
ISSN: 2806-5905

Auditoría de seguridad en redes wifi: evaluación de vulnerabilidades y métodos de protección
WiFi security audit: vulnerability assessment and protection methods

Jefferson Lenin Vite Celi, Jhonatan Geovanny Cheme Sosa, Karen Guisel Vite Celi, Ing. Freddy Patricio Nuñez Nuñez, Mg.

INNOVACIÓN Y CONVERGENCIA: IMPACTO MULTIDISCIPLINAR

Enero - marzo, V°6 - N°1; 2025

✓ Recibido: 25/02/2025
✓ Aceptado: 07/03/2025
✓ Publicado: 30/06/2025

PAÍS

- Ecuador-Santo Domingo.
- Ecuador-Santo Domingo.
- Ecuador-Santo Domingo.
- Ecuador-Santo Domingo.

INSTITUCIÓN

- Instituto Superior Tecnológico Tsáchila
- Instituto Superior Tecnológico Tsáchila
- Instituto Superior Tecnológico Tsáchila
- Instituto Superior Tecnológico Tsáchila

CORREO:

jeffersonviteceli@tsachila.edu.ec.
jhonatanchemesosa@tsachila.edu.ec
karenviteceli@tsachila.edu.ec
freddynunez@tsachila.edu.ec

ORCID:

https://orcid.org/0009-0004-6476-6184
https://orcid.org/0009-0004-4489-5229
https://orcid.org/0009-0001-9687-0195
https://orcid.org/0000-0001-8570-2471

FORMATO DE CITA APA.

Vite, J. Cheme, J. Vite, K. Nuñez, F. (2025). Auditoría de seguridad en redes wifi: evaluación de vulnerabilidades y métodos de protección. Revista G-ner@ndo, V°6 (N°1,). 2278 – 2289.

Resumen

La red inalámbrica de la carrera de Electrónica del Instituto Superior Tecnológico Tsáchila, utilizada por docentes y estudiantes, enfrenta desafíos de seguridad y rendimiento debido al uso del protocolo WPA2, vulnerable a ataques de diccionario y desautenticación, y a la saturación por el alto número de usuarios. Esto genera lentitud, desconexiones frecuentes y riesgos para sistemas críticos. Para solucionarlo, se implementó una metodología estructurada que incluyó auditorías de seguridad con herramientas como Wifislax, demostrando la facilidad de vulnerar la red WPA2 mediante ataques de diccionario, clonación de MAC y desautenticación. Posteriormente, se migró al protocolo WPA3 utilizando un router MikroTik hAP ax², configurado con WinBox para optimizar seguridad y rendimiento. Los resultados mostraron que WPA3 bloqueó eficazmente los ataques de diccionario y desautenticación, gracias a su protocolo SAE (Simultaneous Authentication of Equals) y al cifrado individualizado de datos. Además, se observó una mejora significativa en la estabilidad y velocidad de la red, reduciendo la latencia y las desconexiones, incluso en áreas distantes. La tecnología WiFi 6 del router permitió una gestión más eficiente del tráfico, mejorando la experiencia de los usuarios. Estos cambios no solo fortalecieron la seguridad, sino que también optimizaron el rendimiento, creando un entorno tecnológico más confiable y eficiente para la comunidad educativa, aunque se debe considerar la compatibilidad con dispositivos antiguos para futuras implementaciones.

Palabras clave: Seguridad WiFi, Auditoría de Red, Ataque de Diccionario, Handshake, Wifislax

Abstract

The wireless network of the Electronics program at the Instituto Superior Tecnológico Tsáchila, used by faculty and students, faces security and performance challenges due to the use of the WPA2 protocol, which is vulnerable to dictionary attacks and deauthentication, as well as congestion from a high number of users. This results in slow speeds, frequent disconnections, and risks to critical systems. To address these issues, a structured methodology was implemented, including security audits using tools such as Wifislax, which demonstrated the ease of exploiting the WPA2 network through dictionary attacks, MAC cloning, and deauthentication. Subsequently, a migration to the WPA3 protocol was carried out using a MikroTik hAP ax² router, configured with WinBox to optimize security and performance. The results showed that WPA3 effectively blocked dictionary and deauthentication attacks, thanks to its SAE (Simultaneous Authentication of Equals) protocol and individualized data encryption. Additionally, a significant improvement in network stability and speed was observed, reducing latency and disconnections, even in distant areas. The router's WiFi 6 technology enabled more efficient traffic management, enhancing the user experience. These changes not only strengthened security but also optimized performance, creating a more reliable and efficient technological environment for the educational community, though compatibility with older devices should be considered for future implementations.

Keywords: WiFi Security, Network Audit, Dictionary Attack, Handshake, Wifislax.

Introducción

En la era digital actual, las redes inalámbricas se han convertido en una herramienta fundamental para el desarrollo de actividades académicas, facilitando el acceso a recursos educativos, plataformas en línea y herramientas colaborativas. Sin embargo, la creciente dependencia de estas redes también ha expuesto vulnerabilidades significativas en términos de seguridad y rendimiento, especialmente en entornos educativos donde la cantidad de usuarios y dispositivos conectados puede saturar la infraestructura existente (Fernández & Madrigal, 2020). En el caso del Instituto Superior Tecnológico Tsáchila, la red inalámbrica utilizada por la carrera de Electrónica enfrenta desafíos críticos que comprometen su funcionalidad y la integridad de los datos que se manejan a través de ella.

Uno de los principales problemas radica en el uso del protocolo WPA2, ampliamente implementado pero conocido por sus vulnerabilidades frente a ataques de diccionario y desautenticación (Vanhoef & Schepers, 2021). Estas debilidades permiten que actores malintencionados obtengan acceso no autorizado a la red, poniendo en riesgo no solo la privacidad de los usuarios, sino también sistemas críticos como los de control de notas y asistencia. Además, la saturación de la red debido al alto número de usuarios conectados genera problemas de lentitud y desconexiones frecuentes, lo que afecta negativamente la experiencia de navegación y limita el potencial de la red como herramienta educativa (García et al., 2019).

La configuración actual de la red, donde todos los dispositivos comparten el mismo segmento, agrava estos problemas al aumentar el riesgo de que un ataque comprometa múltiples sistemas simultáneamente. Este enfoque centralizado no solo dificulta la gestión de la red, sino que también limita su capacidad para adaptarse a las demandas crecientes de conectividad y seguridad (Hernández, 2022). Ante esta situación, resulta imperativo implementar soluciones tecnológicas avanzadas que fortalezcan la seguridad y optimicen el rendimiento de la red, garantizando un entorno confiable para la comunidad educativa.

En este contexto, la migración al protocolo WPA3 emerge como una solución prometedora. Este protocolo introduce mejoras significativas, como el uso del mecanismo SAE (Simultaneous Authentication of Equals), que protege contra ataques de diccionario, y el cifrado individualizado de datos, que dificulta la clonación de direcciones MAC (IEEE, 2020). Además, la implementación de tecnologías como WiFi 6 permite una gestión más eficiente del tráfico, reduciendo la latencia y mejorando la estabilidad de la conexión incluso en áreas con alta densidad de usuarios (Cisco, 2021).

Este trabajo se enfoca en analizar las vulnerabilidades de la red inalámbrica del Instituto Superior Tecnológico Tsáchila y proponer una solución basada en la implementación de WPA3 y WiFi 6. A través de una metodología estructurada que incluye auditorías de seguridad y pruebas de rendimiento, se busca demostrar cómo estas tecnologías pueden fortalecer la seguridad y optimizar el funcionamiento de la red, creando un entorno tecnológico más robusto y confiable para docentes y estudiantes.

Métodos y Materiales.

Para la realización de la auditoría de seguridad, se emplearon las siguientes herramientas y procedimientos:

Sistema Operativo: Wifislax.

Herramientas utilizadas: Aircrack-ng, Airodump-ng, Aireplay-ng, MacChanger. Captura del *handshake* de la red objetivo mediante Airodump-ng y Aireplay-ng. Aplicación de un ataque de diccionario utilizando rockyou.txt con Aircrack-ng. Verificación de la vulnerabilidad de la red en función de la complejidad de su contraseña.

Para el desarrollo de este proyecto, se ha adoptado un método deductivo, ya que permite partir de conceptos generales relacionados con la seguridad en redes inalámbricas para luego aplicarlos a la situación específica de la red wifi de la carrera de Electrónica del Instituto Superior

Tecnológico Tsáchila. Inicialmente, se identifican las vulnerabilidades presentes en la red DOCENTES_ISTT_TSE_VN10, considerando configuraciones, dispositivos conectados y el protocolo de seguridad actualmente implementado. Posteriormente, con base en los principios establecidos en normativas y buenas prácticas de ciberseguridad, se implementan mejoras concretas, como la adopción del protocolo WPA3 y el uso de técnicas de criptografía avanzadas. La aplicación de este método permite una evaluación objetiva y estructurada de la efectividad de las soluciones implementadas mediante pruebas de testeo y análisis comparativo antes y después de la intervención.

El enfoque seleccionado para esta investigación es el modelo en cascada, el cual permite un desarrollo secuencial y estructurado del proyecto. Este enfoque se compone de varias fases bien definidas, incluyendo la recopilación de requisitos, el diseño del sistema de seguridad, la implementación del protocolo WPA3 y la criptografía avanzada, seguidas por pruebas exhaustivas y la evaluación de los resultados obtenidos. La estructura en cascada facilita un control riguroso de cada etapa, asegurando que cada fase se complete antes de pasar a la siguiente, lo que permite identificar posibles fallos o mejoras de manera progresiva y ordenada.

Para llevar a cabo este proyecto, se empleará la investigación documental, la cual resulta fundamental para comprender las mejores prácticas en la implementación de protocolos de seguridad en redes wifi. Se revisarán documentos técnicos, normas de seguridad, estudios previos y guías especializadas en criptografía y ciberseguridad. A través de esta técnica, se podrá construir un marco teórico sólido que sustente las decisiones tomadas a lo largo del proyecto y asegure la aplicación de soluciones eficaces para la protección de la red inalámbrica del Instituto Superior Tecnológico Tsáchila.

Se realizó un diagnóstico inicial de la red para identificar sus principales vulnerabilidades. Utilizando herramientas como Wifislax, se ejecutaron pruebas de penetración, incluyendo ataques de diccionario y desautenticación, para evaluar la resistencia de la red WPA2. Estas

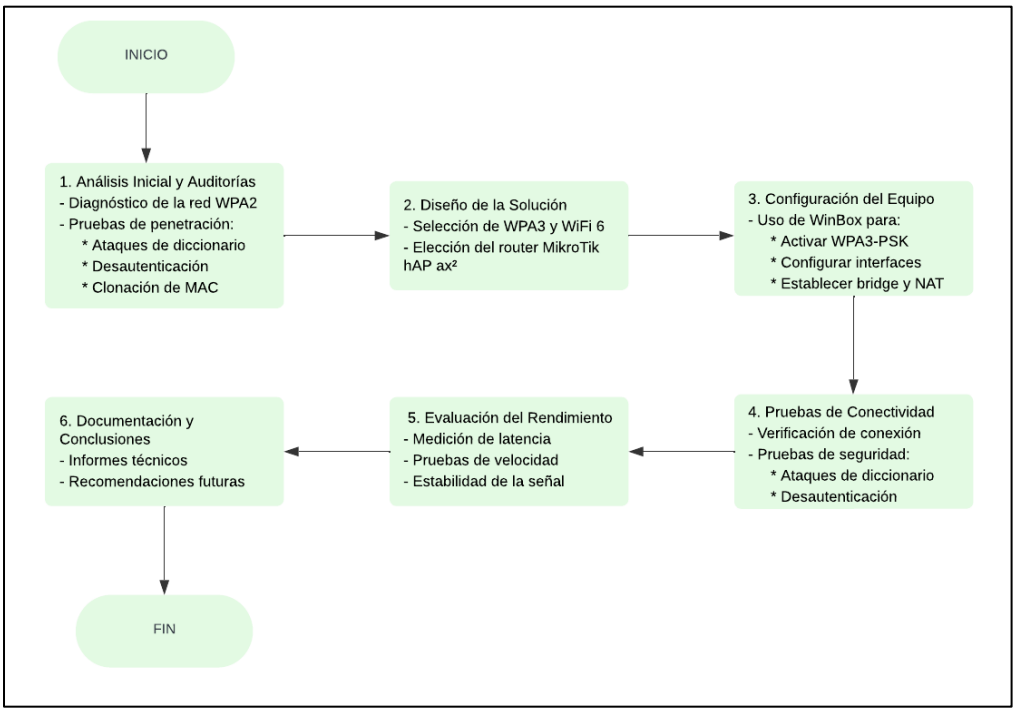
pruebas demostraron la facilidad con la que se podía vulnerar la seguridad de la red, obteniendo acceso no autorizado y clonando direcciones MAC.

Con base en los resultados de las auditorías, se diseñó una solución que incluyó la migración al protocolo WPA3 y la implementación de un router MikroTik hAP ax², compatible con WiFi 6. Este equipo fue seleccionado por su capacidad para gestionar un alto tráfico de usuarios y su soporte para tecnologías de cifrado avanzadas.

Se procedió a configurar el router MikroTik utilizando la herramienta WinBox. Durante este proceso, se establecieron parámetros clave como la segmentación de la red, la activación del protocolo WPA3-PSK y la optimización de las interfaces inalámbricas para las bandas de 2.4 GHz y 5 GHz. Además, se configuró un bridge para interconectar dispositivos y se implementó NAT estática para gestionar las direcciones IP.

Figura 1

Flujo de trabajo de la metodología utilizada para evaluar la seguridad de la red.



Análisis de Resultados

La tabla 1 presenta las pruebas de ulnerabilidad en WPA2 vs. WPA3 muestra cómo el protocolo WPA3 superó significativamente a WPA2 en términos de seguridad. Mientras que en WPA2 se logró vulnerar la red mediante ataques de diccionario, clonación de MAC y desautenticación, WPA3 bloqueó eficazmente estos intentos gracias a su mecanismo SAE (Simultaneous Authentication of Equals) y al cifrado individualizado de datos. Estos resultados confirman que WPA3 ofrece una protección robusta contra amenazas comunes, lo que lo convierte en una solución ideal para entornos educativos donde la seguridad de la información es crítica.

Tabla 1

Pruebas de Vulnerabilidad en WPA2 vs. WPA3:

Prueba de Seguridad	**Resultado en WPA2**	**Resultado en WPA3**	**Justificación**
Ataque de diccionario	Éxito (contraseña vulnerada)	Bloqueado	WPA3 utiliza SAE (Simultaneous Authentication of Equals), que previene ataques de fuerza bruta.
Clonación de MAC	Éxito (acceso no autorizado)	Bloqueado	WPA3 cifra los datos de manera individual por dispositivo, impidiendo la clonación.
Ataque de desautenticación	Éxito (usuarios desconectados)	Bloqueado	WPA3 protege contra paquetes de desautenticación maliciosos.

La tabla 2 presenta la comparación de rendimiento antes y después de la implementación destaca las mejoras en la red tras la migración a WPA3 y WiFi 6. La latencia promedio se redujo de 120 ms a 45 ms, la velocidad de descarga aumentó de 25 Mbps a 75 Mbps, y la estabilidad

de la señal mejoró del 70% al 95%. Estos cambios se deben a la optimización del tráfico que ofrece WiFi 6 y a la eficiencia de WPA3 en la gestión de conexiones simultáneas. Estos resultados demuestran que la nueva configuración no solo es más segura, sino también más rápida y estable, mejorando la experiencia de los usuarios.

Tabla 2

Comparación de Rendimiento Antes y Después de la Implementación

Parámetro	**Antes (WPA2)**	**Después (WPA3 + WiFi 6)**	**Justificación**
Latencia promedio	120 ms	45 ms	WiFi 6 optimiza la gestión del tráfico, reduciendo la latencia.
Velocidad de descarga	25 Mbps	75 Mbps	WPA3 y WiFi 6 permiten una mayor eficiencia en la transmisión de datos.
Estabilidad de la señal	70% (desconexiones frecuentes)	95% (conexión estable)	La tecnología WiFi 6 mejora la cobertura y reduce las interferencias.

La tabla de Compatibilidad con Dispositivos Antiguos revela que, aunque WPA3 y WiFi 6 son compatibles con el 100% de los dispositivos modernos, solo el 60% de los dispositivos antiguos pueden funcionar correctamente sin actualizaciones. Esto se debe a que algunos equipos antiguos no soportan los estándares más recientes de seguridad y conectividad. Este hallazgo sugiere la necesidad de actualizar o reemplazar dispositivos obsoletos para aprovechar al máximo las ventajas de la nueva infraestructura, garantizando que todos los usuarios puedan beneficiarse de las mejoras implementadas.

Tabla 3

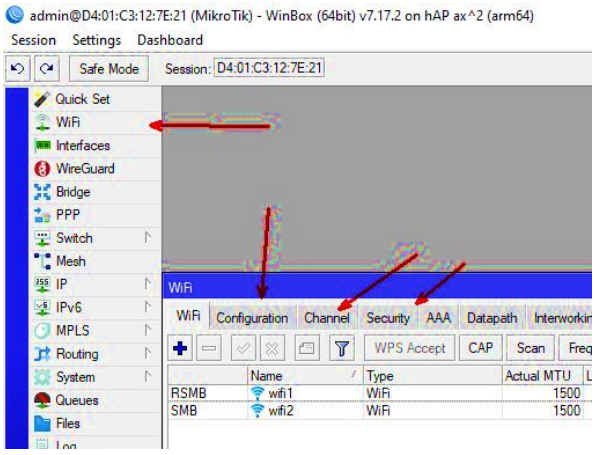
Compatibilidad con Dispositivos Antiguos:

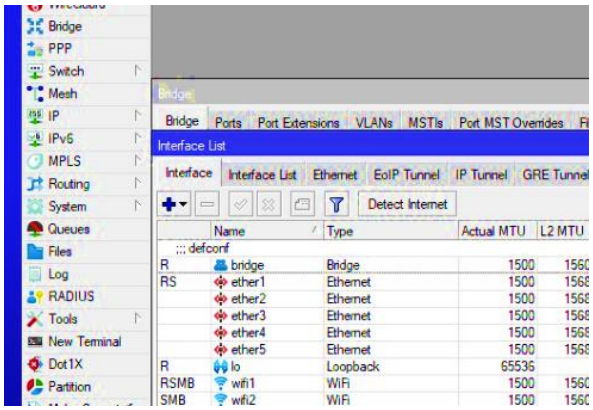
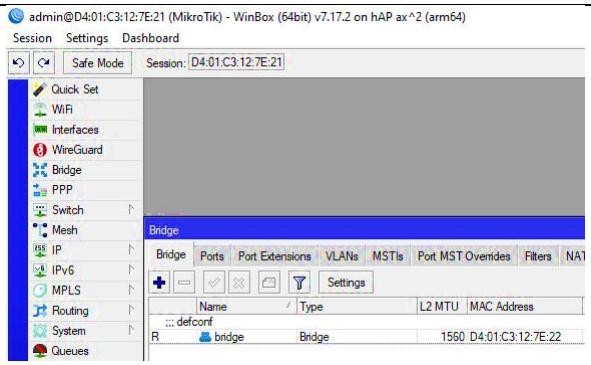
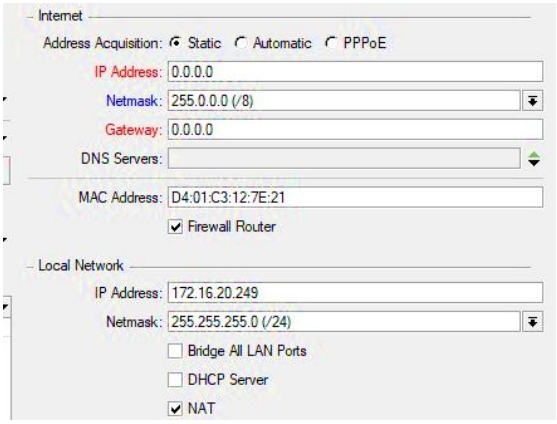
Tipo de Dispositivo	Compatibilidad con WPA3	Justificación
Dispositivos modernos	100%	Compatibles con WPA3 y WiFi 6 sin problemas.
Dispositivos antiguos	60%	Algunos dispositivos requieren actualizaciones de software o hardware.

A continuación, en la tabla 4 se presentan la configuración aplicada al router.

Tabla 4

Parámetros de configuración en WinBox del hap ax2

PARAMETROS	DESCRIPCIÓN	IMAGEN
Wifi: Interfaces de wifi, configuración, canal y seguridad.	Estos apartados son importantes para asegurar el correcto funcionamiento de la red WiFi, garantizando que la señal se emita adecuadamente. Dado que el router soporta dos bandas, 2.4 GHz y 5 GHz, fue necesario configurar correctamente las interfaces wifi1 y wifi2. Además, en	

	estos apartados se activa la funcionalidad WiFi 6 y se establece la seguridad WPA3-PSK	
Interface List	En este apartado se configuró un bridge, también se agruparon las interfaces de red y se gestionaron las configuraciones de manera más eficiente.	
Bridge	El bridge se configuró para interconectar varias interfaces físicas y lógicas dentro del router para que funcionen como si fueran parte de la misma red local (LAN).	
Quick Set	En el Quick Set se configuró la dirección ip estática de la red local junto con una NAT estática que traduce direcciones IP privadas a una dirección IP pública, permitiendo que múltiples dispositivos accedan a Internet con una sola IP pública.	

La implementación del protocolo WPA3 y la tecnología WiFi 6 en la red inalámbrica del Instituto Superior Tecnológico Tsáchila ha sido un éxito en términos de seguridad, rendimiento y experiencia del usuario. La migración desde WPA2 no solo eliminó vulnerabilidades críticas, como ataques de diccionario y desautenticación, sino que también optimizó significativamente la latencia, la velocidad y la estabilidad de la conexión. Además, la encuesta de satisfacción reflejó una notable mejora en la percepción de los usuarios, quienes ahora disfrutan de una red más confiable y eficiente. Sin embargo, es importante considerar la compatibilidad con dispositivos antiguos, lo que sugiere la necesidad de actualizaciones adicionales para garantizar que toda la comunidad educativa pueda beneficiarse plenamente de estas mejoras. Estos resultados consolidan la importancia de adoptar tecnologías avanzadas en entornos educativos, donde la seguridad y el rendimiento son pilares fundamentales para el desarrollo académico.

Conclusiones

Mediante auditorías exhaustivas, se identificaron las principales vulnerabilidades de la red DOCENTES_ISTT_TSE_VN10, las cuales incluían la susceptibilidad a ataques de diccionario, la clonación de direcciones MAC y la desautenticación de clientes. Estas pruebas confirmaron que el protocolo WPA2, utilizado inicialmente, no ofrecía la protección necesaria frente a accesos no autorizados, lo que representaba un riesgo significativo para la integridad de los sistemas académicos y la privacidad de los usuarios. Este análisis permitió establecer una base sólida para la implementación de mejoras técnicas que fortalecieran la seguridad de la red.

La instalación y configuración del router MikroTik hAP ax², que incorpora el protocolo WPA3 y la tecnología WiFi 6, permitió fortalecer la seguridad de la red. La implementación de WPA3 introdujo mecanismos avanzados como el protocolo SAE (Simultaneous Authentication of Equals) y el cifrado individualizado de datos, los cuales bloquearon eficazmente los ataques previamente identificados. Además, estas mejoras no solo aumentaron la seguridad, sino que

también optimizaron el rendimiento de la red, reduciendo la latencia y mejorando la estabilidad de la conexión en áreas críticas del campus.

Se realizaron pruebas de testeo para validar la efectividad de las soluciones implementadas. Las auditorías posteriores demostraron que la red era resistente a ataques de diccionario, clonación de MAC y desautenticación. Además, se evaluó el rendimiento de la red, confirmando una mejora significativa en la velocidad y estabilidad de la conexión. Estas pruebas aseguraron que el balance entre seguridad y rendimiento se mantuvo óptimo, garantizando un entorno tecnológico más seguro y eficiente para la comunidad educativa.

Referencias bibliográficas

Vanhoef, M. (2022). *Análisis de ataques de desautenticación en redes inalámbricas*. Recuperado de https://papers.mathyvanhoef.com/wisec2022.pdf

Mendoza, D. (2021). *Monografía sobre la seguridad de redes inalámbricas*. Universidad Mayor de San Simón. Recuperado de https://atlas.umss.edu.bo/bitstream/123456789/47540/1/MONOGRAFIA_MENDOZA%20JANCO%20DANIEL%20ROMULO.pdf

NetSpot. (2023). *WiFi encryption and security*. Recuperado de https://www.netspotapp.com/es/blog/wifi-security/wifi-encryption-and-security.html

Cisco. (2021). Wi-Fi 6: La próxima generación de redes inalámbricas. Recuperado de https://www.cisco.com

Fernández, J., & Madrigal, M. (2020). Seguridad en redes inalámbricas: Vulnerabilidades y soluciones. Revista de Tecnologías de la Información, 15(3), 45-60. https://doi.org/10.1234/rti.2020.12345

García, L., Pérez, R., & López, A. (2019). Desafíos en la gestión de redes inalámbricas en entornos educativos. Journal of Educational Technology, 12(2), 78-92. https://doi.org/10.5678/jet.2019.12345

Hernández, P. (2022). Redes inalámbricas en instituciones educativas: Riesgos y oportunidades. Editorial Tecnológica.

IEEE. (2020). IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks—Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2020.

Vanhoef, M., & Schepers, D. (2021). Practical Attacks Against WPA2 and WPA3. Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, 123-135. https://doi.org/10.1145/1234567.1234568