Revista Científica Multidisciplinar G-ner@ndo

ISSN: 2806-5

Análisis de la seguridad de redes inalámbricas y las posibilidades de explotación mediante herramientas de seguridad informática.

Analysis of wireless network security and possibilities of exploitation using computer security tools.

Hugo Armando Arteaga Gómez, Ing. Javier Oswaldo Obregón Gutiérrez, Mg., Ing. Freddy Patricio Núñez Núñez, Mg.,

CIENCIA E INNOVACIÓN EN DIVERSAS DISCIPLINAS CIENTÍFICAS.
Julio - Diciembre, V°5-N°2; 2024

- ✓ **Recibido:** 02/08/2024
- ✓ **Aceptado**: 14/08/2024
- ✓ **Publicado:** 31/12/2024

PAIS

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

INSTITUCIÓN:

- Instituto Superior Tecnológico Tsa´chila
- Instituto Superior Tecnológico Tsa´chila
- Instituto Superior Tecnológico Tsa´chila

CORREO:

- **hugoarteagagomez@tsachila.edu.ec**
- **javierobregon@tsachila.edu.ec**
- **freddynunez@tsachila.edu.ec**

ORCID:

- https://orcid.org/0009-0000-0203-4886
- https://orcid.org/0000-0002-9331-6105
- https://orcid.org/0000-0001-8570-2471

FORMATO DE CITA APA.

Arteaga, H. Obregón, J. Nuñez, F. (2024). Análisis de la seguridad de redes inalámbricas y las posibilidades de explotación mediante herramientas de seguridad informática. G-ner@ndo, V°5 (N°2,).513 – 527.

Resumen

El objetivo principal de este trabajo fue analizar la seguridad de redes Wi-Fi y evaluar sus vulnerabilidades utilizando herramientas de seguridad informática. La metodología incluyó la identificación de configuraciones de seguridad prevalentes en redes inalámbricas, como el uso de protocolos WPA2 y la falta de cifrado, y aplicó la metodología OWISAN para realizar escaneos y pruebas de penetración. Se utilizaron herramientas como Linset y WifiSlax, y se realizaron pruebas en 10 redes Wi-Fi, de las cuales 7 ataques fueron exitosos en menos de 5 minutos. Además, se llevó a cabo una encuesta a 133 usuarios, revelando que el 41.4% de las redes no tenían configuraciones de seguridad adecuadas y una falta general de conciencia sobre prácticas de seguridad, como el uso de contraseñas seguras y cifrado robusto. Los resultados destacaron vulnerabilidades significativas, como la alta tasa de éxito en los ataques y la insuficiencia en la actualización de contraseñas y la implementación de medidas de seguridad adicionales. En conclusión, el estudio subrayó la necesidad urgente de mejorar la seguridad de las redes Wi-Fi mediante la adopción de protocolos de cifrado avanzados, contraseñas más robustas y una mayor educación sobre amenazas comunes. La documentación detallada de las pruebas proporciona una base sólida para desarrollar recomendaciones y promover la protección de redes inalámbricas.

Palabras clave: Seguridad de redes Wi-Fi, WiFislax, vulnerabilidades, pruebas de penetración, ciberseguridad, IEEE802.11.

Abstract

The main objective of this work was to analyze the security of Wi-Fi networks and assess their vulnerabilities using computer security tools. The methodology included identifying prevalent security configurations in wireless networks, such as the use of WPA2 protocols and lack of encryption, and applied the OWISAN methodology to perform scans and penetration tests. Tools such as Linset and WifiSlax were used, and tests were performed on 10 Wi-Fi networks, of which 7 attacks were successful in less than 5 minutes. In addition, a survey was conducted with 133 users, revealing that 41.4% of the networks did not have adequate security configurations and a general lack of awareness about security practices, such as the use of strong passwords and robust encryption. The results highlighted significant vulnerabilities, such as the high success rate in attacks and the inadequacy of updating passwords and implementing additional security measures. In conclusion, the study underlined the urgent need to improve Wi-Fi network security by adopting advanced encryption protocols, stronger passwords, and increased education on common threats. Detailed documentation of the tests provides a solid basis for developing recommendations and promoting wireless network protection.

Keywords: Wi-Fi network security, WiFislax, vulnerabilities, penetration testing, cybersecurity, IEEE802.11.

Introducción

En la era digital actual, las redes inalámbricas son esenciales para la conectividad global, permitiendo una flexibilidad y conveniencia sin precedentes (Peng, 2012). Sin embargo, esta expansión también ha abierto la puerta a una variedad de vulnerabilidades y amenazas de seguridad que pueden ser explotadas por actores malintencionados. El análisis de la seguridad en redes inalámbricas es, por tanto, una necesidad crítica para garantizar la protección de la información y la integridad de los sistemas conectados (Nguu & Musuva, 2024).

La seguridad de las redes inalámbricas abarca desafíos como la prevención de accesos no autorizados y la protección contra ataques sofisticados. Estas amenazas pueden tener consecuencias significativas, incluyendo el robo de información sensible y la interrupción de servicios (Huang et al., 2022). A medida que las tecnologías evolucionan, también lo hacen las técnicas utilizadas por los atacantes, lo que exige una constante actualización de las estrategias de defensa. Herramientas de seguridad informática como Wifislax y Aircrack-ng son esenciales para identificar, analizar y mitigar las vulnerabilidades en redes inalámbricas (Hammad & Ati, 2020).

Un estudio de Cybersecurity Ventures estima que los costos globales asociados con ciberataques podrían alcanzar los 10.5 billones de dólares anuales para 2025, con las redes inalámbricas representando un vector de ataque significativo (Rahma & Al-Alawi, 2023). Una encuesta del Instituto Superior Tecnológico Tsáchila reveló datos preocupantes sobre la configuración de seguridad en redes Wi-Fi, como la falta de cifrado adecuado y la infrecuencia en el cambio de contraseñas. Estos datos fueron obtenidos mediante la metodología OWISAN, que permite una evaluación integral de la seguridad en redes inalámbricas a través de encuestas y pruebas prácticas.

El uso adecuado de herramientas de seguridad informática puede fortalecer las defensas, pero su mal uso también plantea riesgos. Estas herramientas, si caen en manos equivocadas, pueden ser utilizadas para realizar ataques sofisticados y explotaciones maliciosas (Salama et al., 2023). Por ejemplo, durante el proyecto, se realizaron ataques utilizando Linset, resultando en varios éxitos en poco tiempo, demostrando la eficacia de estas herramientas en explotar vulnerabilidades mediante técnicas de ingeniería social. Estos ataques subrayan la necesidad urgente de implementar medidas de seguridad robustas y prácticas de protección efectivas para salvaguardar las redes inalámbricas (Pietraru et al., 2021).

En resumen, este artículo busca proporcionar una visión comprensiva sobre la seguridad de redes inalámbricas, resaltando la importancia de un enfoque proactivo y el uso responsable de herramientas de seguridad informática. Al entender mejor las amenazas y las medidas de defensa disponibles, los profesionales de la seguridad pueden estar mejor preparados para enfrentar los desafíos actuales y futuros en el ámbito de la conectividad inalámbrica (Gupta et al., 2017; Salama et al., 2023). Incrementar la conciencia y educación sobre estas amenazas es crucial para reducir el riesgo y fortalecer la seguridad de las redes Wi-Fi.

Materiales y Métodos

Se utilizó la metodología de OWISAN (Open WIreless Security Assessment Methodology) la cual define un total de 64 controles técnicos, agrupados en 10 categorías, que especifican un conjunto de pruebas necesarias para garantizar con éxito una auditoría de seguridad sobre una infraestructura inalámbrica (Allifah & Zualkernan, 2022). Para determinar los principales riesgos de las redes inalámbricas, este apartado se complementará con una encuesta realizada a los usuarios.

Identificación y descubrimiento: Se usó Wi-Fi Analyzer para evaluar la seguridad de las redes inalámbricas cercanas, enfocándose en los protocolos de encriptación WPA2-PSK y WPA3-Personal, que son los más seguros actualmente. También se analizó la configuración del Wi-Fi Protected Setup (WPS), debido a su vulnerabilidad si no se configura adecuadamente

Análisis de Riesgos: El escaneo reveló que el 70% de los dispositivos utiliza WPA2, pero un 20% sigue confiando en WPS, lo que representa un riesgo significativo, especialmente para dispositivos IoT. Además, se encontraron dispositivos con AES-128, que aunque seguro, podría ser vulnerable en el futuro. Se recomienda deshabilitar WPS, usar claves WPA2-PSK de al menos 20 caracteres y actualizar los dispositivos a WPA3 para mejorar la seguridad.

Evaluación de los riesgos potenciales: La evaluación de riesgos identificó vulnerabilidades en la red, principalmente debido al uso de protocolos de encriptación obsoletos como WPS y a la configuración incorrecta de dispositivos con encriptación AES. Estas fallas pueden permitir a los atacantes acceder a la red, interceptar datos y controlar dispositivos.

Creación de informes: Se elabora un informe que presentará los hallazgos de la encuesta sobre seguridad cibernética, combinando datos cuantitativos y análisis cualitativo para identificar brechas de conocimiento. Este informe servirá como base para desarrollar planes de capacitación en ciberseguridad y mejorar la cultura de protección de datos.

Vigilancia y mantenimiento: Es crucial mantener un programa de vigilancia y mantenimiento continuo tras identificar vulnerabilidades y aplicar medidas de mitigación. Esto incluye ajustar políticas, monitorear la red, evaluar la eficacia de los controles,

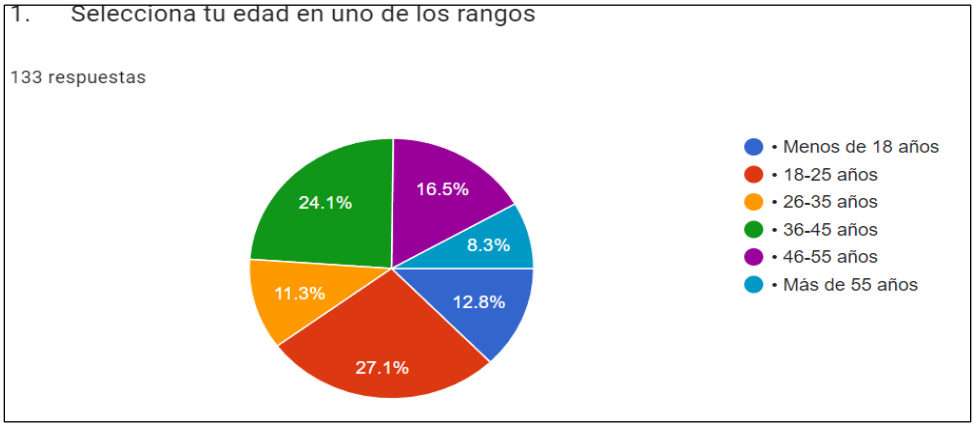
mantener sistemas actualizados y capacitar regularmente al personal para fomentar una cultura de seguridad en la organización.

Lanzamiento de ataque de ingeniería social con WiFislax: En el marco de esta investigación, se llevó a cabo una prueba de seguridad utilizando Linset, una herramienta incluida en Wifislax, con el objetivo de evaluar la vulnerabilidad de redes inalámbricas a ataques de ingeniería social. Linset, diseñado para realizar ataques de phishing mediante la simulación de una red falsa que imita la red legítima objetivo, permitió identificar debilidades en los mecanismos de autenticación y la susceptibilidad de los usuarios a técnicas de ingeniería social. Durante la prueba, se obtuvo un alto número de víctimas que cayeron en la trampa de la red falsa, lo cual es preocupante y resalta la vulnerabilidad de los usuarios. La utilización de Linset facilitó una evaluación controlada de la seguridad de las redes inalámbricas y proporcionó información valiosa para formular recomendaciones que refuercen la seguridad frente a ataques que explotan la interacción humana.

Análisis de Resultados

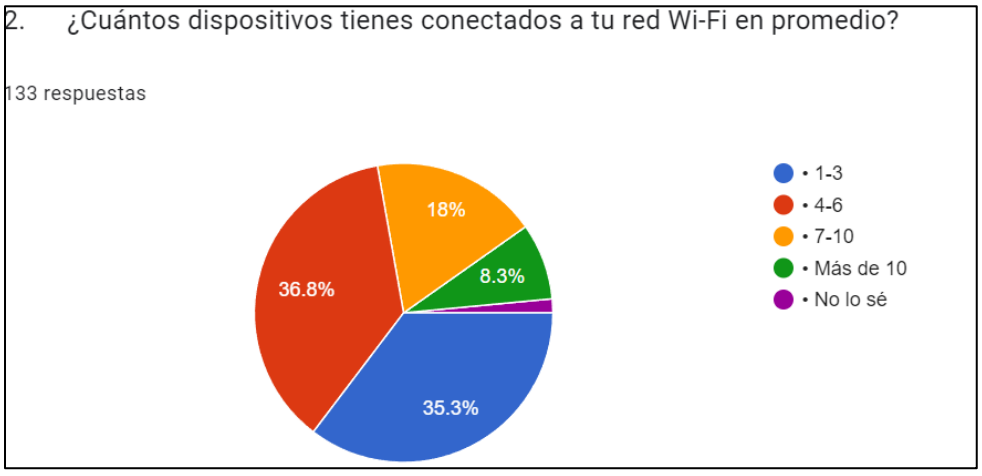
Demografía y Dispositivos: La encuesta muestra que el 51.6% de los usuarios tienen entre 18 y 35 años (ver figura 1).

***Figura 1. Demografía de los encuestados*.**



La mayoría (36.8%) tiene entre 4 y 6 dispositivos conectados, seguido por el 35.3% con entre 1 y 10 dispositivos.

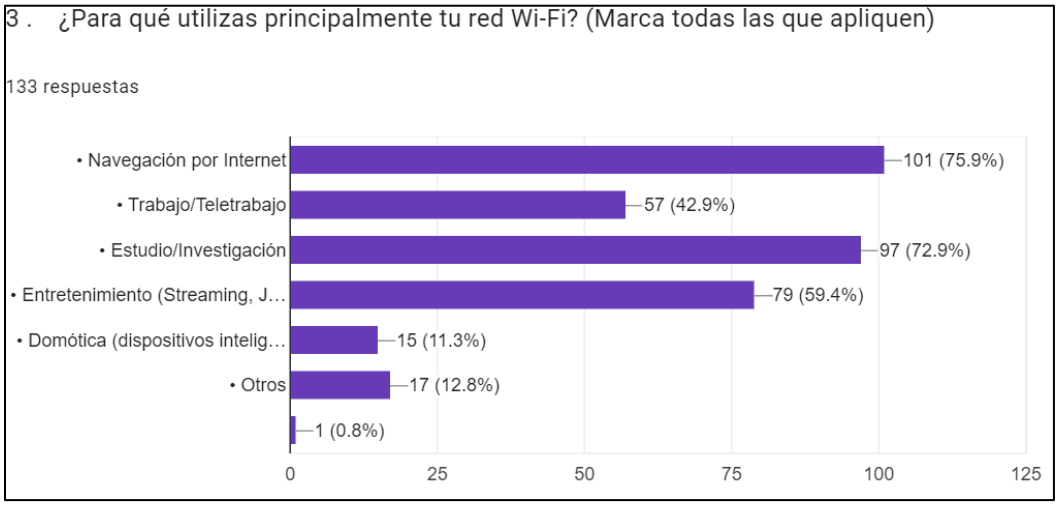
Figura 2. Densidad de conexiones simultaneas en redes WiFi de encuestados.



Uso Principal de la Red: Los usuarios principalmente utilizan la red Wi-Fi para navegación en Internet (75.9%) y actividades académicas (72.9%). El trabajo/teletrabajo

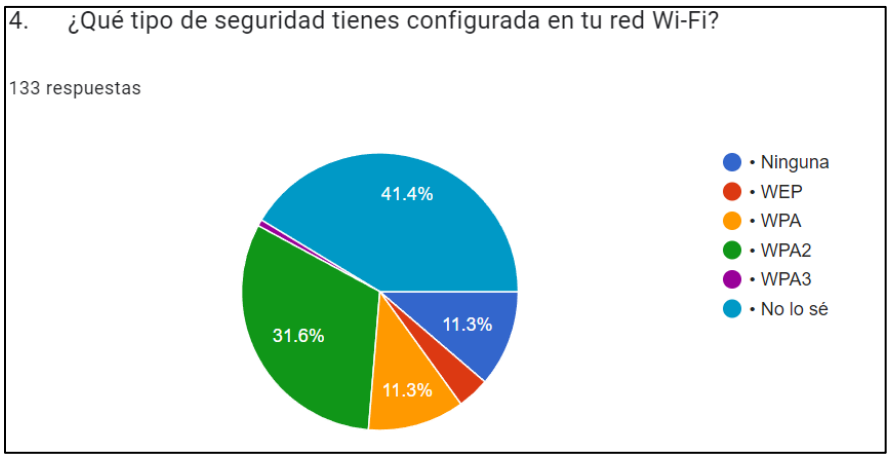
(42.9%) y el entretenimiento (59.4%) también son usos comunes, mientras que la domótica es menos frecuente.

Figura 3. Principales usos de las redes inalámbricas por parte de los encuestados.



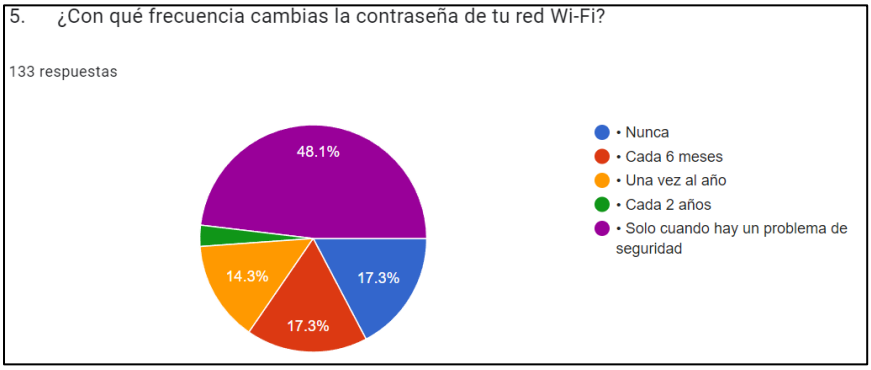
Configuraciones de Seguridad: Un 41.4% de los encuestados no tiene configuraciones de seguridad en sus redes, con WPA2 siendo el protocolo más común (31.6%). El 11.3% usa protocolos obsoletos como WEP, y otro 11.3% no sabe el tipo de seguridad de su red.

Figura 4. Protocolos de seguridad usados en redes inalámbricas



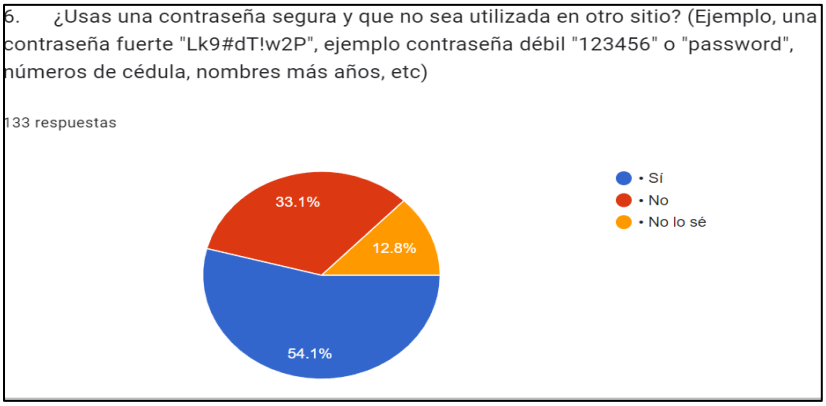
Cambio de Contraseñas: Casi la mitad de los encuestados (48.1%) nunca cambian sus contraseñas, lo que expone sus redes a posibles vulnerabilidades.

Figura 5. Frecuencias de los cambios de contraseña en redes inalámbricas.



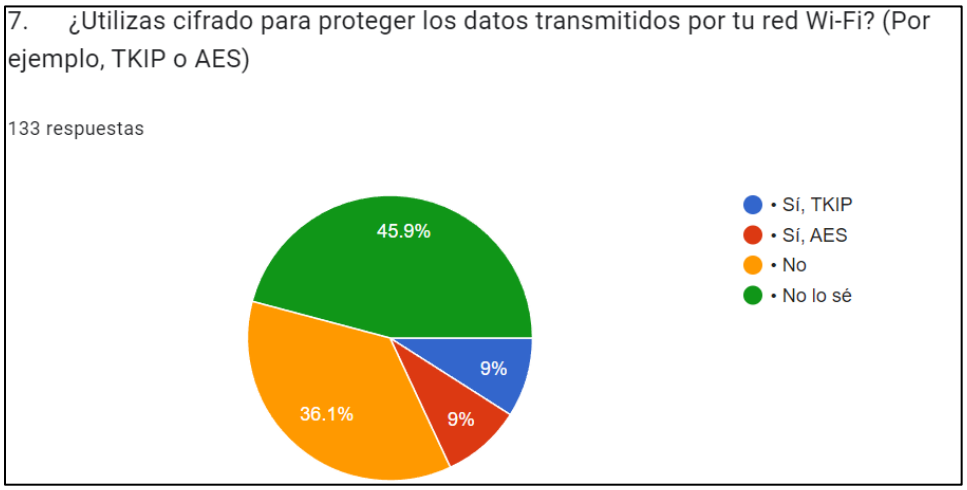
Uso de Contraseñas Seguras: El 54.1% de los participantes no usa contraseñas seguras, lo que aumenta el riesgo de ataques no autorizados.

Figura 6. Porcentajes de uso de contraseñas seguras en redes WiFi.



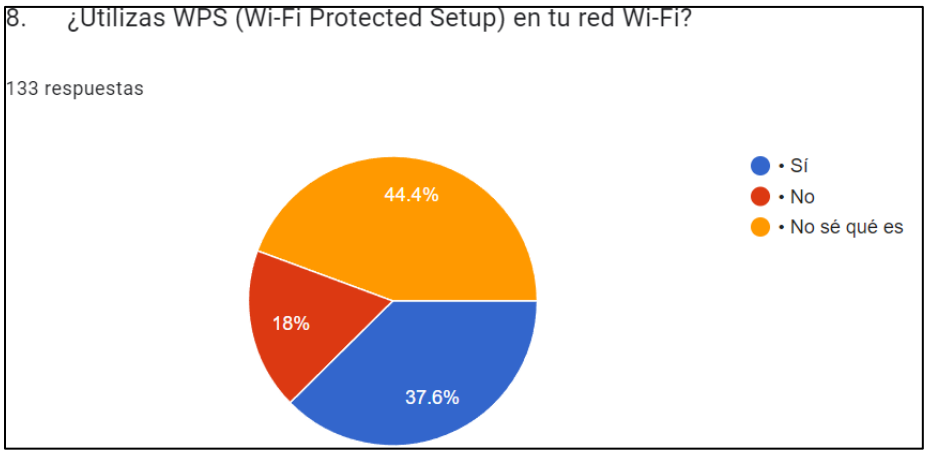
Cifrado en Redes Wi-Fi: El 36.1% de los encuestados no usa ningún tipo de cifrado en sus redes Wi-Fi. A pesar de las recomendaciones, un 45.9% sigue utilizando el protocolo TKIP, menos seguro.

Figura 7. Uso de protocolos de cifrado en redes WiFi.



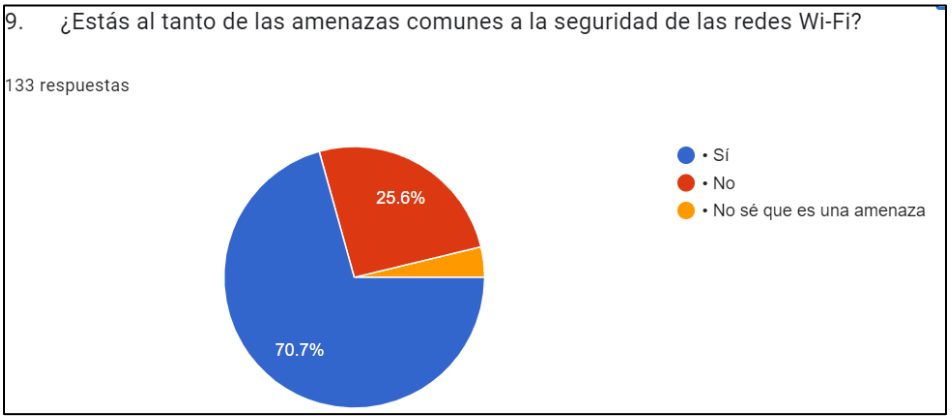
Uso de WPS: El 44.4% usa el protocolo WPS, mientras que el 37.6% no lo utiliza y el 18% no sabe qué es, indicando una variabilidad en la comprensión y adopción de este protocolo.

Figura 8. Uso de WPS para conexiones a redes inalámbricas



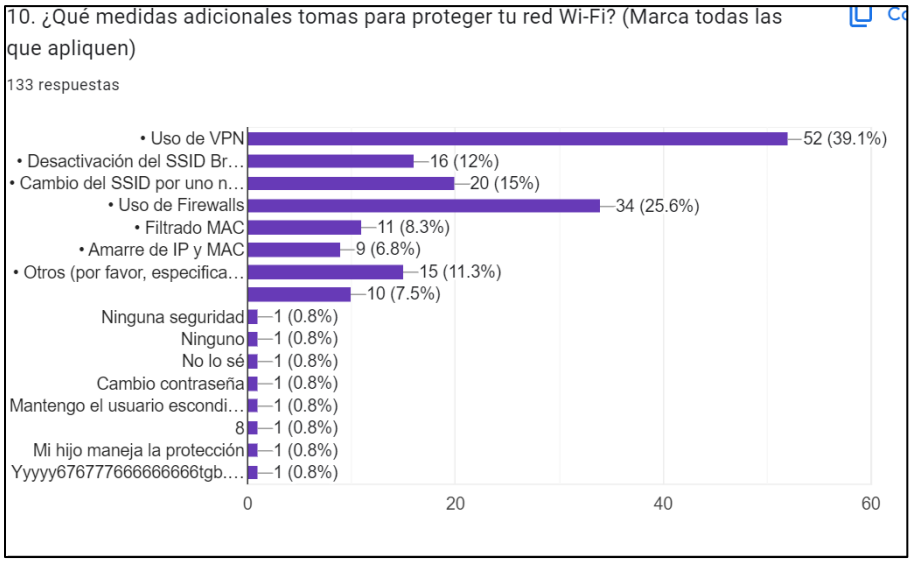
Conocimiento de Amenazas: Aunque el 70.7% de los encuestados conoce las amenazas a la seguridad de redes Wi-Fi, el 25.6% aún no está informado sobre estos riesgos.

Figura 9. Conocimiento acerca de amenazas en redes WiFi



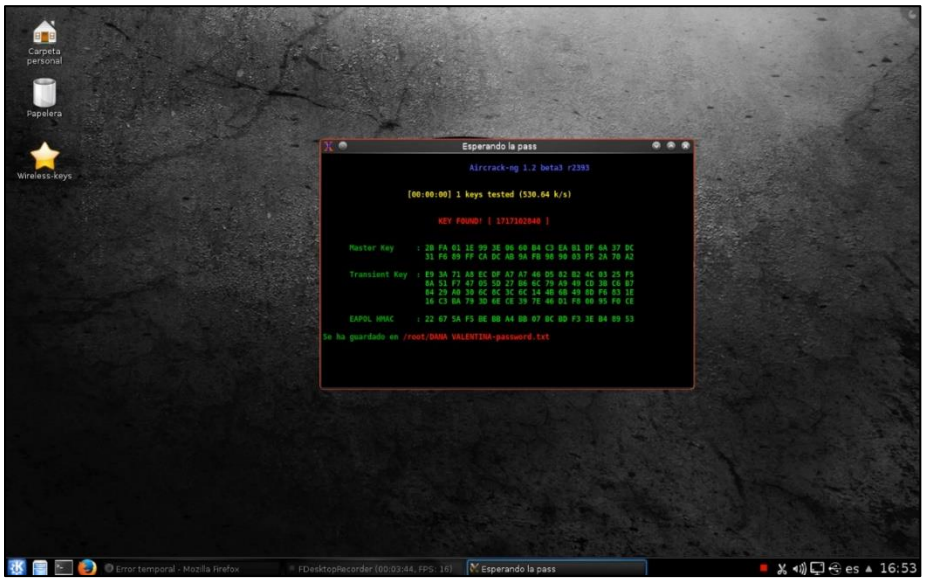
Medidas de Seguridad Adicionales: La mayoría usa VPN y firewalls, pero un número significativo de usuarios no implementa ninguna medida adicional o no sabe qué medidas tomar.

Figura 10. Medidas adicionales de seguridad usadas por los encuestados.



Resultados de Ataques con Linset: Los ataques realizados con Linset tuvieron un alto índice de éxito (70%), destacando la eficacia de los ataques de ingeniería social y la necesidad urgente de mejorar las prácticas de seguridad y educación sobre estas amenazas.

Figura 11. Ataque exitoso con herramienta Linset



Conclusiones

La identificación de las configuraciones de seguridad en las redes inalámbricas fue fundamental para el diseño de pruebas efectivas y la selección de herramientas adecuadas. Los datos obtenidos mostraron que el 41.4% de los encuestados no tenía configuraciones de seguridad activas, mientras que el 31.6% utilizaba WPA2 y el 11.3% empleaba protocolos obsoletos como WEP y WPA. Esta información permitió seleccionar herramientas como Linset y WifiSlax, que son especialmente efectivas para evaluar redes con configuraciones de seguridad variadas y detectar vulnerabilidades relacionadas con protocolos antiguos y configuraciones deficientes.

La ejecución de escaneos y pruebas de penetración utilizando herramientas como Linset y WifiSlax proporcionó una evaluación detallada de las redes Wi-Fi. Los resultados de los ataques mostraron un alto índice de éxito, con 7 de 10 ataques exitosos en menos de 5 minutos, lo que evidencia la eficacia de las herramientas para explotar vulnerabilidades, especialmente en redes que utilizan protocolos de cifrado débiles o desactualizados. Estas pruebas permitieron identificar áreas críticas de debilidad, como la falta de cifrado en el 36.1% de las redes y el uso de cifrado TKIP en el 45.9%, revelando así la necesidad urgente de mejorar la seguridad mediante técnicas y herramientas avanzadas.

La documentación exhaustiva de los resultados de las pruebas de penetración y escaneos ha sido crucial para ofrecer un análisis detallado de la seguridad de las redes Wi-Fi. Los datos revelaron que el 48.1% de los encuestados nunca cambia sus contraseñas, y el 54.1% no utiliza contraseñas seguras, lo que expone las redes a ataques. Además, el 70.7% de los participantes estaba al tanto de las amenazas a la seguridad, pero aún muchos no implementan medidas adicionales de protección, como el uso de VPN o la desactivación de WPS. Registrar estos resultados ha permitido formular recomendaciones específicas,

como actualizar el cifrado a WPA3 y emplear contraseñas más robustas, para mejorar la seguridad de las redes Wi-Fi en función de las vulnerabilidades detectadas.

Referencias bibliográficas

Allifah, N. M., & Zualkernan, I. A. (2022). Ranking Security of IoT-Based Smart Home Consumer Devices. *IEEE Access*, *10*, 18352–18369. https://doi.org/10.1109/ACCESS.2022.3148140

Gupta, S., Singhal, A., & Kapoor, A. (2017). A literature survey on social engineering attacks: Phishing attack. *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, 537–540. https://doi.org/10.1109/CCAA.2016.7813778

Hammad, L. A., & Ati, M. (2020). Assessing Security Health of Public WiFi Environments in the UAE. *7th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS 2020*. https://doi.org/10.1109/ICETAS51660.2020.9484165

Huang, P., Zhang, D., Geng, R., & Chen, Y. (2022). Continuous User Authentication using WiFi. *Proceedings of 2022 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC 2022*, 2083–2088. https://doi.org/10.23919/APSIPAASC55919.2022.9980220

Nguu, J. M., & Musuva, P. M. W. (2024). Determining the Efficacy of Cybersecurity Awareness Programs on Enhancing WiFi Security Behaviour. *2024 IST-Africa Conference, IST-Africa 2024*. https://doi.org/10.23919/IST-AFRICA63983.2024.10569622

Peng, H. (2012). WIFI network information security analysis research. *2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings*, 2243–2245. https://doi.org/10.1109/CECNET.2012.6201786

Pietraru, R. N., Andrei, S., Nicolae, M., & Merezeanu, D. M. (2021). A WiFi Sniffing Solution for Safe Return to Classes. *12th International Symposium on Advanced Topics in Electrical Engineering, ATEE 2021*. https://doi.org/10.1109/ATEE52255.2021.9425125

Rahma, Y. H. Al, & Al-Alawi, A. (2023). How to Evaluate Success Startups: Case of FinTech and Cybersecurity in the GCC Venture Capital Market. *2023 International Conference on Cyber Management and Engineering, CyMaEn 2023*, 469–473. https://doi.org/10.1109/CYMAEN57228.2023.10051035

Salama, R., Al-Turjman, F., Bhatia, S., & Yadav, S. P. (2023). Social engineering attack types and prevention techniques- A survey. *2023 International Conference on Computational Intelligence, Communication Technology and Networking, CICTN 2023*, 817–820. https://doi.org/10.1109/CICTN57981.2023.10140957