RIESGOS Y VULNERABILIDADES DE SEGURIDAD DE LA INFORMACIÓN EN REDES WLAN DOMESTICAS

LÓPEZ ARAÚJO MAICOLM ALFREDO

MUÑOZ MUÑOZ CRISTIAN GIOVANNY

PROGRAMA DE INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA
UNIVERSIDAD CESMAG
2025

RIESGOS Y VULNERABILIDADES DE SEGURIDAD DE LA INFORMACIÓN EN REDES WLAN DOMESTICAS

Autores:
LÓPEZ ARAÚJO MAICOLM ALFREDO
MUÑOZ MUÑOZ CRISTIAN GIOVANNY

Informe final de trabajo de grado presentado como requisito para optar al título de Ingeniero de Sistemas, en modalidad investigación.

Asesor
Mg. ESCOBAR HERNANDEZ LUIS ARNOBY

PROGRAMA DE INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA
UNIVERSIDAD CESMAG
2025

Nota de Aceptación

_____

_____

_____

_____

_____

Jurado 1

_____

Jurado 2

_____

San Juan de Pasto, 2025

Página de exclusión de responsabilidad intelectual

“El pensamiento que se expresa en esta obra es exclusiva responsabilidad de sus autores y no compromete la ideología de la Institución Universitaria CESMAG”

AGRADECIMIENTOS

El camino recorrido hasta la culminación de este proyecto ha estado lleno de retos, aprendizajes y experiencias enriquecedoras que han dejado una huella imborrable en nuestra vida. Es por ello que queremos expresar nuestro más profundo agradecimiento a todas las personas que, de una u otra manera, han sido parte fundamental de este proceso y han contribuido a que hoy podamos alcanzar esta meta.

En primer lugar, agradecerle a Dios, por darnos la fortaleza, la sabiduría y la perseverancia necesarias para afrontar cada desafío que se presentó en este camino. Sin su guía y bendición, nada de esto hubiera sido posible.

A nuestro asesor de proyecto, Mg. Luis Arnoby Escobar Hernández, por su paciencia, orientación y por compartir su conocimiento y experiencia con nosotros. Su guía ha sido clave en la estructuración y desarrollo de este trabajo, y le estaremos eternamente agradecidos por todo su apoyo, su tiempo y dedicación.

Agradecemos profundamente a nuestros profesores de Investigación I, II y III, cuya orientación fue clave para el desarrollo y culminación de este proyecto. Asimismo, extendemos nuestro reconocimiento a todos los docentes que, a lo largo de nuestra formación académica, nos brindaron las herramientas necesarias para nuestro crecimiento profesional y personal. Gracias por su compromiso con la enseñanza y por inspirarnos constantemente a superar nuestros propios límites.

A las personas que colaboraron con la realización de este proyecto, por brindarnos acceso a la información y los recursos necesarios para desarrollar esta investigación. Su disposición y apoyo fueron esenciales para alcanzar los objetivos propuestos.

Y, por último, a todas aquellas personas que, de una u otra manera, contribuyeron a la culminación de este proyecto. Cada palabra de aliento, cada gesto de apoyo y cada enseñanza han sido un motor que nos han impulsado a seguir adelante.

A todos ustedes, ¡muchas gracias!

DEDICATORIA

En primer lugar, doy gracias a Dios y a la Virgencita por sus bendiciones infinitas y por darme la fortaleza para seguir adelante en cada paso de mi camino.

A mi madre, por todos sus esfuerzos, sacrificios y por ser el cimiento de mis sueños. Su amor incondicional ha sido mi guía en los momentos más difíciles.

A mi esposa, mi compañera, mi apoyo inquebrantable: tus palabras de aliento, tu paciencia y tu fortaleza evitaron que desfalleciera. Eres mi refugio, mi "polo a tierra" en medio de las tormentas. Gracias por esas noches de desvelo y por cada sacrificio hecho con amor.

A mi hijo, la luz de mi vida: aunque el tiempo no siempre estuvo a nuestro favor, tu cariño y tus palabras, incluso desde pequeño, fueron el motor que me impulsó a seguir adelante. Eres mi mayor inspiración.

A mis hermanos, por sus oraciones y su apoyo incondicional; a mis suegros, que me recibieron como un hijo más y me tendieron la mano cuando más lo necesité. Su generosidad y cariño han sido un regalo invaluable; a mis profesores, quienes con su sabiduría y dedicación sembraron en mí las semillas del conocimiento y me guiaron hacia el éxito en este recorrido.

Y, finalmente, a todas aquellas personas que, de manera directa o indirecta, me brindaron una palabra de aliento, un gesto de apoyo o simplemente su compañía en los momentos clave. Cada uno de ustedes ha sido parte fundamental de esta travesía.

¡Infinitas gracias! **Att. Maicolm Alfredo López Araújo**

A Dios, mi eterno guía y fortaleza, por iluminar cada paso de este camino académico. Por darme sabiduría en los momentos de confusión, paciencia en las dificultades y bendiciones que hicieron posible este logro. Tú fuiste mi sustento cuando las fuerzas flaqueaban.

A mi madre guerrera incansable, gracias por tus madrugadas llenas de amor, por tu fe inquebrantable que me impulsaba a seguir adelante incluso cuando yo dudaba. Por ser mi primer ejemplo de resiliencia y entrega. Cada logro mío lleva el sello de tu sacrificio.

A mi Padre héroe silencioso, por trabajar sin descanso para darnos educación y valores. Por enseñarme con tu ejemplo que la disciplina y la honestidad son el camino al éxito. Tu esfuerzo diario es mi mayor motivación.

A mis hermanos cómplices de vida, por su apoyo incondicional, por las risas que aliviaban el estrés y por ser mi red de apoyo en los momentos más difíciles. Este título también es suyo.

A esa persona especial que, aunque el destino nos llevó por rumbos diferentes, dejó una huella imborrable en mi formación. Gracias por tu apoyo cuando más lo necesitaba, por tus consejos sabios y por creer en mí cuando nadie más lo hacía

A mis profesores por compartir generosamente su sabiduría, por su paciencia al responder mis infinitas dudas y por exigirme siempre dar lo mejor de mí.

A todos los que, de una forma u otra, contribuyeron a que este sueño se hiciera realidad. A quienes me tendieron la mano cuando tropecé, a quienes me inspiraron con su ejemplo y a quienes creyeron en mí incluso cuando yo no lo hacía.

"Los frutos más dulces se cosechan después de las temporadas más difíciles. Este título es prueba de ello.

Con todo mi amor y gratitud, **Cristian Giovanny Muñoz Muñoz**

RESUMEN

Este proyecto de investigación aborda los riesgos y vulnerabilidades de seguridad en redes WLAN domésticas, proponiendo estrategias y controles para mitigarlos mediante la implementación de una Guía Integral de Seguridad basada en la metodología OWISAM y respaldada por la norma ISO 27032. El estudio se enfocó en identificar las principales amenazas, tales como el uso de protocolos de cifrado obsoletos (WEP/WPA), contraseñas débiles y dispositivos mal configurados, factores que incrementan la exposición de los usuarios a posibles ataques cibernéticos.

La metodología combinó un enfoque cuantitativo y pruebas de vulnerabilidad en una muestra de 25 redes domésticas, evaluando su estado antes y después de aplicar la guía. Los resultados mostraron una reducción significativa de vulnerabilidades críticas y altas, validando la efectividad de las medidas propuestas.

Se concluyó que la implementación de controles técnicos en las redes WLAN domésticas mejora significativamente la seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información. Además, concientizar y generar una cultura de buenas prácticas en temas de ciberseguridad.

Palabras Clave: Ciberseguridad, confidencialidad, disponibilidad, integridad, ISO 27032, OWISAM.

ABSTRACT

This research project addresses the security risks and vulnerabilities in home WLAN networks, proposing strategies and controls to mitigate them through the implementation of a Comprehensive Security Guide based on the OWISAM methodology and supported by the ISO 27032 standard. The study focused on identifying the main threats, such as the use of outdated encryption protocols (WEP/WPA), weak passwords, and misconfigured devices, factors that increase users' exposure to potential cyberattacks.

The methodology combined a quantitative approach and vulnerability testing on a sample of 25 home networks, assessing their status before and after applying the guide. The results showed a significant reduction in critical and high-level vulnerabilities, validating the effectiveness of the proposed measures.

It was concluded that implementing technical controls in home WLAN networks significantly improves security, ensuring the confidentiality, integrity, and availability of information. Additionally, it raises awareness and fosters a culture of good cybersecurity practices.

Keywords: Cybersecurity, confidentiality, availability, integrity, ISO 27032, OWISAM.

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

INTRODUCCIÓN

En la actualidad, se puede observar que cada vez son más los dispositivos que tienen conexión a internet, y que en los hogares su consumo se ha convertido en una necesidad del día a día, el incremento de dispositivos tales como (portátiles, Tablet, televisores, celulares, entre otros) hacen que la transferencia de información en las redes WLAN domesticas aumente, por ende, los riesgos de ciberseguridad hacia estas redes se incrementen [1].

Para el desarrollo de este proyecto, se trabajó bajo la metodología OWISAM (Open Wireless Security Assessment Methodology) [2], la cual se basa fundamentalmente en la evaluación de controles de seguridad en redes inalámbricas, que buscan ejercer las mejores prácticas al momento de realizar una auditoria en redes WLAN, además se tendrá en cuenta el estándar ISO 27032 como marco de referencia en prácticas de Ciberseguridad para fortalecer los controles y minimizar las vulnerabilidades asociadas a estas redes [3].

Esta investigación comenzó con un análisis comparativo de las metodologías existentes para determinar cuál es la más adecuada para su aplicación en el estudio. Posteriormente, se elaboró una guía orientada a promover buenas prácticas de seguridad en redes domésticas, la cual fue implementada en una población seleccionada aleatoriamente. A este grupo se le aplicaron pruebas de vulnerabilidad y penetración en sus redes, con el fin de identificar posibles riesgos. Finalmente, se evaluó el impacto de las medidas propuestas mediante un análisis estadístico, el cual permitió verificar la efectividad de los controles de seguridad establecidos en la fase inicial.

Con este proyecto, se busca establecer o determinar las vulnerabilidades más concurrentes en las redes WLAN domésticas y por medio de una Guía Integral de Seguridad de la información, poder mitigar estas vulnerabilidades, además fortalecer la seguridad en los dispositivos inalámbricos conectados a nuestras redes residenciales y con esto blindar la disponibilidad, integridad, y confidencialidad de la información que se transfiere mediante las redes inalámbricas de nuestros hogares [4].

I. PROBLEMA DE INVESTIGACIÓN

A. OBJETO O TEMA DE ESTUDIO

El objeto de la presente investigación estará orientada a la seguridad de la información en redes WLAN domésticas.

B. LÍNEA DE INVESTIGACIÓN

La línea de investigación se centró en la **Seguridad de la Información**, la cual, por medio de controles en los dispositivos de red y usuarios, busca minimizar los riesgos y vulnerabilidades existentes en las redes WLAN[5], con el fin de proteger la Disponibilidad, Integridad y Privacidad de la Información. Además, la Seguridad Informática nos permite usar métodos y controles informáticos para mitigar los riesgos cibernéticos asociados a estas redes [6].

C. SUB LÍNEA DE INVESTIGACIÓN

La seguridad informática enmarca todos los métodos y controles tecnológicos que se pueden implementar con el fin de mitigar el riesgo relacionado a las amenazas cibernéticas que pueden comprometer la privacidad, integridad o confidencialidad de los sistemas de información, incluyendo la transmisión y almacenamiento de la información tratada por los mismos, entre las principales amenazas se encuentran: Infección por malware, ataques de denegación de servicio, suplantación de identidades, errores de los usuarios, interceptación de las comunicaciones, entre otros.

D. PLANTEAMIENTO DEL PROBLEMA

En un mundo cada vez más dependiente de las comunicaciones inalámbricas, la seguridad de las redes WLAN Domesticas se ha vuelto crucial. En este contexto, una de las vulnerabilidades más representativas son las redes inalámbricas en entornos residenciales [7]. La facilidad de acceso a estas redes, combinada con la falta de conocimiento sobre medidas de seguridad, plantea desafíos significativos para la protección de la privacidad y la integridad de los datos [8].

Las consecuencias de estas vulnerabilidades pueden ser significativas [9], desde la pérdida de privacidad personal hasta el robo de información confidencial. Además, los ataques a redes WLAN domésticas, pueden tener repercusiones más amplias como el acceso no autorizado a dispositivos conectados, interrupciones de servicios en línea, perdida o alteración de información y posibles pérdidas económicas. Esta situación resalta la necesidad urgente de abordar el problema de seguridad en redes WLAN domesticas para proteger la integridad de las comunicaciones y los datos de los usuarios [10].

La importancia de esta investigación se enfoca en la capacidad de implementar, comprender y respaldar controles de seguridad en las redes WLAN domésticas y brindar información detallada y concisa de cómo los usuarios pueden comprometer su seguridad si no toman las medidas adecuadas en sus redes inalámbricas [11].

E. FORMULACIÓN DEL PROBLEMA

¿Cómo mitigar los riesgos y vulnerabilidades de seguridad de la información en las redes WLAN domésticas?

F. OBJETIVOS

1) Objetivo general

Implementar estrategias de aseguramiento de las redes WLAN Domesticas en los dispositivos de red instalados en los hogares, basándose en la metodología OWISAM y la Norma ISO 27032 aplicada en una Guía Integral de Seguridad de la información, con el propósito de garantizar la integridad, confidencialidad y disponibilidad de la información en entornos residenciales.

2) Objetivos específicos

- ✓ Determinar los principales criterios de la metodología OWISAM, así como la arquitectura y puntos críticos de seguridad en los dispositivos de las redes WLAN domésticas.
- ✓ Diseñar una Guía Integral de Seguridad de la información basada en la metodología OWISAM y la Norma ISO 27032, adaptada específicamente para entornos residenciales, con el fin de establecer protocolos y procedimientos de aseguramiento de redes WLAN domésticas.
- ✓ Aplicar la Guía Integral de Seguridad de la información con el fin de mitigar vulnerabilidades detectadas en una muestra representativa.
- ✓ Evaluar el impacto y efectividad de la aplicación de la Guía Integral de Seguridad de la información en entornos residenciales.

G. JUSTIFICACIÓN

El estudio sobre la seguridad en redes WLAN domésticas es esencial debido al crecimiento de dispositivos conectados usando esta tecnología, lo que aumenta la vulnerabilidad de los usuarios ante posibles ataques cibernéticos [12]. La presente investigación está justificada por la necesidad urgente de proteger la privacidad y la integridad de la información personal y familiar que circula a través de estas redes [13]. La exposición a amenazas cibernéticas puede tener consecuencias graves, incluida la pérdida de datos sensibles, el robo de identidad y la intrusión en la privacidad de los usuarios. Además, la seguridad de las redes WLAN domésticas es fundamental para garantizar un entorno digital seguro para las familias, protegiendo así su bienestar y tranquilidad[14].

La literatura existente destaca la importancia de la seguridad en redes WLAN domésticas y su impacto en la protección de la privacidad y la integridad de los datos de los usuarios. Sin embargo, hay una falta de enfoque específico en las particularidades y desafíos únicos que enfrentan los usuarios de redes WLAN domésticas [15]. La investigación propuesta, se diferencia del enfoque tradicional al centrarse en el contexto residencial, lo que permite identificar y abordar de manera más efectiva las necesidades y limitaciones de los usuarios no expertos en tecnología. Además, se identifican brechas en la literatura existente, especialmente en términos de soluciones prácticas y adaptadas a entornos domésticos [16].

La investigación propuesta tiene el potencial de contribuir significativamente al conocimiento existente sobre la seguridad en redes WLAN domésticas, la cual puede proporcionar soluciones prácticas y efectivas para su protección [17] , estas soluciones podrían incluir recomendaciones de configuración segura, actualizaciones de software, implementación de nuevas tecnologías de seguridad y orientación sobre buenas prácticas de seguridad de la Información, ayudando a mejorar la integridad de los datos y promoviendo un entorno digital más seguro para las familias [18].

H. DELIMITACIÓN

1) Ámbito geográfico

Esta investigación se llevará se a cabo en hogares ubicados en zona urbana de la ciudad de San Juan de Pasto, que cuenten con servicio de internet y una conexión inalámbrica.

2) Ámbito temporal

El tiempo establecido para esta investigación, será de dos periodos académicos 2024 – 2025.

3) Tecnologías y metodologías

La presente investigación estará basada en la metodología OWISAM, la cual está orientada en la toma de decisiones basada en datos, la optimización de recursos y la mejora continua [19]. Su aplicabilidad se extiende a disciplinas como la ingeniería, la tecnología, los negocios y cualquier contexto donde se requiera una gestión sistemática y estructurada para lograr resultados exitosos. Además, esta metodología se apoyará en la norma ISO 27032 que aborda la Ciberseguridad en el contexto de la Seguridad de la Información y las TIC [20].

4) Contexto institucional

El proyecto se llevará a cabo en el contexto el contexto urbano de la ciudad de San Juan de Pasto.

5) Alcance temático

El alcance temático de esta investigación se centrará en la seguridad en redes WLAN domésticas [21], la cual abarca varios aspectos importantes para proteger la integridad, confidencialidad y disponibilidad de los datos transmitidos a través de redes inalámbricas, además, la implementación efectiva de controles y medidas de seguridad en cada uno de estos aspectos es crucial para proteger la Seguridad de la Información en los hogares [22].

II. MARCO TEÓRICO

La seguridad de la información es un tema que se ha incrementado por el alto uso de diferentes aplicaciones que requieren un tratamiento de datos de manera accesible. En diferentes estudios se contempla la implementación de seguridad en diferentes ámbitos.

A. ANTECEDENTES

1) Internacionales

- ✓ En el campo de la seguridad en redes WiFi, es fundamental comprender las diferencias entre los protocolos de cifrado WPA2 y WPA3. Según investigaciones realizadas por la (Association for Computing Machinery) fundada en la ciudad de Nueva York, WPA2 ha sido ampliamente utilizado debido a su compatibilidad con la mayoría de los dispositivos y su implementación del estándar de cifrado AES-CCMP. Sin embargo, presenta vulnerabilidades significativas, como el ataque KRACK (Key Reinstallation Attack), que compromete la seguridad de las conexiones inalámbricas. Por otro lado, WPA3 introduce mejoras sustanciales, como el uso de Simultaneous Authentication of Equals (SAE) en lugar de PSK (Pre-Shared Key), lo que refuerza la seguridad contra ataques de fuerza bruta y mejora la confidencialidad de las redes abiertas mediante Opportunistic Wireless Encryption (OWE) [23].En una configuración de red doméstica, la elección entre WPA2 y WPA3 debe considerar la compatibilidad de los dispositivos, ya que no todos los equipos soportan WPA3. No obstante, cuando es posible, se recomienda optar por WPA3 debido a sus mejoras en protección contra ataques pasivos y activos, así como su mayor resistencia ante intentos de descifrado sin autorización.

- ✓ Según Zhang et al [24]. el aumento del Internet de las Cosas (IoT) ha incrementado la exposición de redes domésticas a amenazas avanzadas, dado que muchos dispositivos carecen de mecanismos de seguridad robustos. Las redes WiFi domésticas están diseñadas principalmente para el uso particular, y en muchos casos, se subestima la importancia de su seguridad bajo la premisa de que la información transmitida es de baja relevancia. Sin embargo, estudios recientes han demostrado que estas redes pueden ser objetivos de ataques cibernéticos debido a la transferencia de datos personales y, en ocasiones, laborales, lo que las convierte en un punto crítico de vulnerabilidad.

- ✓ En el Instituto Nacional de Estándares y Tecnología (NIST, 2021), Conti et al.[25] identificaron que uno de los ataques más frecuentes en redes WiFi es el **Man-in-the-Middle (MitM)**, donde un atacante intercepta la comunicación para robar información confidencial. Otros estudios, como el de Shin et al. (2021). Destacan la importancia de implementar controles de seguridad como **WPA3-SAE**, la autenticación multifactor y la segmentación de redes mediante VLANs para minimizar riesgos. Finalmente, enfatizaron la necesidad de actualizar periódicamente el firmware de los routers, desactivar la difusión del **SSID broadcasting** y emplear listas de control de acceso para reforzar la seguridad en entornos domésticos

2) Nacionales

- ✓ En estudios realizados en la Universidad Católica de Colombia a cargo del estudiante JEISON ALEXANDER de la Facultad de Ingeniería [26], analizó el uso de herramientas informáticas para descubrir vulnerabilidades presentes en redes WLAN domésticas, con el objetivo de identificar brechas de seguridad en la información. Dichos estudios coinciden con investigaciones a nivel internacional, donde se ha demostrado que redes Wi-Fi domésticas pueden ser vulnerables a ataques como la captura de paquetes para descifrar claves, ataques de fuerza bruta sobre credenciales y técnicas de suplantación de identidad mediante evil twin attacks . Para evaluar estos riesgos, se emplean herramientas como Wireshark, Aircrack-ng y Kali Linux, que permiten realizar pruebas de penetración y auditorías de seguridad en redes inalámbricas. Además, se ha identificado que muchas de estas vulnerabilidades surgen por configuraciones incorrectas o el uso de protocolos de cifrado obsoletos como WEP y WPA en lugar de WPA2/WPA3. Como medida de mitigación, expertos recomiendan el uso de autenticación robusta, la segmentación de redes, el cifrado extremo a extremo y la actualización frecuente del firmware del router para prevenir ataques y garantizar la integridad de la información en entornos domésticos. La evolución de las tecnologías ha permitido a las universidades implementar, Herramientas que permiten proteger la información y los sistemas de telecomunicaciones.

- ✓ Según el DANE [27], las conexiones inalámbricas y el uso de dispositivos con conexión Wi-Fi han aumentado considerablemente en los últimos años, lo que ha permitido una mayor conectividad y acceso a la información. Sin embargo, este crecimiento también ha traído consigo un incremento en las amenazas cibernéticas dirigidas a redes WLAN domésticas, como los ataques de man-in-the-middle (MitM), el sniffing de paquetes y la explotación de vulnerabilidades en protocolos de seguridad obsoletos. Estudios recientes demuestran que los atacantes pueden aprovechar configuraciones débiles en los routers domésticos para llevar a cabo accesos no autorizados, robo de credenciales y distribución de malware. Ante esta problemática, se recomienda implementar cifrado WPA3, desactivar el SSID broadcasting, habilitar la autenticación multifactor (MFA) para dispositivos críticos y actualizar constantemente el firmware del router para corregir posibles vulnerabilidades Además, la concienciación de los usuarios sobre prácticas seguras en el uso de redes inalámbricas es clave para reducir los riesgos de ciberataques y garantizar la protección de la información personal y empresarial en entornos domésticos .

3) Regional

- ✓ En la empresa Panavias de la ciudad de Pasto [26] al realizar pruebas de vulnerabilidad en redes con protocolos WPA y WEP, se evidenció que estos protocolos presentan importantes fallas de seguridad, permitiendo a atacantes interceptar el tráfico, descifrar contraseñas y comprometer la privacidad de los usuarios. Estudios han demostrado que WEP (Wired Equivalent Privacy) es especialmente vulnerable debido a su uso de claves estáticas y algoritmos de cifrado débiles, lo que facilita ataques de tipo ARP Spoofing y la rápida obtención de claves mediante herramientas como Aircrack-ng y Hashcat. Por otro lado, WPA (Wi-Fi Protected Access), aunque una mejora con respecto a WEP, sigue presentando riesgos, especialmente en versiones antiguas como WPA-TKIP, que es susceptible a ataques de reinyección de paquetes y exploits de diccionario

  En este contexto, nuestra investigación busca determinar el protocolo de seguridad más adecuado para redes domésticas, siendo WPA3 la mejor opción disponible actualmente. WPA3

incorpora Autenticación Simultánea de Iguales (SAE), que reemplaza al PSK (Pre-Shared Key) utilizado en WPA2, haciendo que los ataques de fuerza bruta sean ineficaces. Además, WPA3 implementa cifrado de 192 bits, proporcionando mayor resistencia contra ataques criptográficos avanzados y reforzando la seguridad en redes Wi-Fi modernas. Como parte de las recomendaciones para mejorar la seguridad de dispositivos de red, es esencial deshabilitar protocolos inseguros como WEP y WPA-TKIP, habilitar el cifrado WPA3-Personal o WPA2-AES si no se dispone de WPA3, y realizar actualizaciones periódicas de firmware para mitigar posibles vulnerabilidades.

- ✓ Las redes Wi-Fi pueden utilizarse en diversos campos de investigación, como lo demuestra el estudio realizado en la Universidad de Nariño, donde se implementaron sistemas de gestión del ancho de banda en una red Wi-Fi para optimizar el tráfico y mejorar la eficiencia en la transmisión de datos. Esta estrategia es fundamental para el control del uso indebido de la red, la mitigación de ataques de denegación de servicio (DoS) y la prevención de congestiones que pueden comprometer la seguridad y el rendimiento de la red. Estudios recientes han evidenciado que la mala gestión del ancho de banda puede aumentar la vulnerabilidad de una red Wi-Fi, facilitando la ejecución de ataques como el deauth attack, en el cual un atacante fuerza la desconexión de dispositivos legítimos para interceptar credenciales de acceso.
  Por esta razón, la implementación de un control de ancho de banda como medida de seguridad en redes WLAN domésticas es clave para restringir el tráfico no autorizado y evitar el uso excesivo de recursos por parte de dispositivos comprometidos. Además, la aplicación de políticas de Quality of Service (QoS) y la segmentación de la red mediante VLAN pueden mejorar la administración del tráfico y reducir los riesgos de ataques internos. En el contexto de nuestra investigación, estas prácticas se integrarán en la guía de seguridad para redes WLAN domésticas, promoviendo configuraciones seguras en routers y sistemas de gestión de tráfico para garantizar la estabilidad, disponibilidad y protección de la información en entornos residenciales. [27].

- ✓ En estudios realizados en la universidad CESMAG a cargo de los estudiantes ERICK DAVID BASTIDAS MONTENEGRO Y LUIS CARLOS ZUÑIGA CHALAPUD en la facultad de ingeniería donde se llevaron estudios sobre seguridad en redes Wlan domesticas [30] , en la cual se recomienda la aplicación de controles de la metodología **OWISAM (Open Wireless Security Assessment Methodology)** para auditorías de seguridad en redes inalámbricas. Esta metodología se basa en un enfoque sistemático que permite evaluar vulnerabilidades y aplicar medidas de mitigación en entornos Wi-Fi, asegurando la confidencialidad, integridad y disponibilidad de la información transmitida. OWISAM se estructura en varias fases, incluyendo reconocimiento, identificación de amenazas, evaluación de vulnerabilidades y pruebas de penetración, lo que facilita la detección de fallas de seguridad antes de que puedan ser explotadas por atacantes. En este sentido, es crucial adoptar esta metodología en nuestra investigación, ya que proporciona parámetros claros y estructurados para la evaluación de la seguridad en redes WLAN domésticas. Diversos estudios han demostrado que la falta de auditorías regulares en redes inalámbricas incrementa la exposición a ataques como el KRACK (Key Reinstallation Attack), que compromete la seguridad en redes WPA2 al permitir la reinstalación de claves de cifrado y la interceptación de tráfico. Además, OWISAM permite evaluar aspectos como la configuración de los protocolos de cifrado, la autenticación de usuarios y la segmentación de la red, lo que resulta fundamental para reforzar la seguridad en entornos residenciales. Implementar OWISAM en auditorías de redes Wi-Fi domésticas

facilitará la identificación de brechas de seguridad y la aplicación de controles preventivos para reducir la posibilidad de intrusiones y filtraciones de datos.

B. SUPUESTOS TEÓRICOS

Vulnerabilidad

Una vulnerabilidad de seguridad es un fallo, debilidad o deficiencia en el diseño, configuración, implementación o gestión de un sistema, red o activo tecnológico que puede ser explotado por actores malintencionados, como hackers o ciberdelincuentes, para comprometer su integridad, confidencialidad o disponibilidad. Estas vulnerabilidades pueden manifestarse en software, hardware, protocolos de comunicación e incluso en prácticas humanas (como errores de usuarios), y permiten la ejecución de ciberataques, el acceso no autorizado a datos sensibles, la interrupción de servicios o el robo de información. Su identificación y mitigación proactiva son fundamentales para reducir riesgos y proteger los activos digitales de una organización[29].

Fig. 1 Vulnerabilidad

Hacker

Un hacker es un individuo con amplios conocimientos en informática, redes y sistemas, capaz de identificar y explotar vulnerabilidades en tecnologías digitales. Aunque comúnmente se asocia el término con actividades ilegales, en realidad engloba un espectro más amplio, ya que no todos los hackers actúan con malas intenciones. Su perfil técnico les permite manipular sistemas, software o hardware para distintos fines, ya sea para mejorar la seguridad, investigar fallos o, en algunos casos, cometer ciberdelitos. [32].

Tipos de Hackers

- ✓ **White hat (Sombrero blanco):** Hackers éticos que trabajan para proteger sistemas. Identifican vulnerabilidades con autorización para corregirlas antes de que sean explotadas. Suelen ser profesionales de ciberseguridad, pentesters o empleados de empresas de seguridad informática[33].
- ✓ **Black hat (Sombrero negro):** Actúan con fines maliciosos: robo de datos, fraudes, infección con malware o ataques a infraestructuras críticas[34].

Su actividad es ilegal y pueden pertenecer a grupos delictivos o actuar por motivaciones económicas, políticas o personales.

- ✓ **Grey hat (Sombrero gris):** Combinan aspectos de los dos anteriores: pueden vulnerar sistemas sin autorización, pero sin fines destructivos[35].
  A veces informan a las organizaciones afectadas para recibir recompensas (bug bounties) o reconocimiento.

- ✓ **Hacktivistas:** Usan sus habilidades para promover causas sociales o políticas (ej. Anonymous)[36].
  Sus acciones incluyen filtraciones de información o ataques a entidades que consideran injustas.

- ✓ **Script kiddies:** Principiantes sin conocimientos profundos que usan herramientas creadas por otros para atacar sistemas.
  Suelen ser menos peligrosos, pero pueden causar daños significativos por falta de experiencia[37].

Fig. 2 Hacker

Ciberdelincuente

Un ciberdelincuente es un individuo o grupo que utiliza técnicas informáticas ilegales para cometer fraudes, robos, sabotajes u otros delitos en el entorno digital. A diferencia de los hackers (que pueden tener motivaciones éticas o técnicas), los ciberdelincuentes actúan exclusivamente con fines maliciosos, buscando beneficio económico, daño reputacional o acceso a información confidencial sin autorización.
Su actividad representa una grave amenaza para personas, empresas e incluso gobiernos, ya que explotan vulnerabilidades en sistemas, redes y dispositivos a internet [38].

Tipos de ciberdelincuentes

- ✓ **Estafadores digitales (Scammers):** Engañan a víctimas mediante fraudes en línea (phishing, falsas ofertas, suplantación de identidad).
- ✓ **Desarrolladores y distribuidores de malware:** Crean virus, troyanos, spyware y ransomware para infectar sistemas.

- ✓ **Hackers de sombrero negro (Black hat hackers):** Aunque no todos los black hats son ciberdelincuentes, muchos realizan intrusiones ilegales para robar datos o venderlos en mercados clandestinos.

- ✓ **Carders (Ladrones de información bancaria):** Especializados en clonar tarjetas, realizar compras fraudulentas o vaciar cuentas bancarias.

- ✓ **Ciberespías y agentes patrocinados por estados:** Trabajan para gobiernos o grupos de interés en el robo de secretos industriales, información militar o manipulación política.

- ✓ **"Script kiddies" (Cibervándalos):** No son expertos, pero usan herramientas prefabricadas para lanzar ataques básicos (DDoS, defacement de webs).

Fig. 3 Ciberdelincuente

Seguridad de la información

La seguridad de la información es un área crítica que engloba un conjunto de medidas, políticas, procedimientos y técnicas diseñadas para proteger los datos de una organización. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información, evitando accesos no autorizados, modificaciones malintencionadas o fugas de datos. Esto incluye el control de los flujos de información dentro y fuera de los sistemas establecidos por la organización, así como la protección contra amenazas internas y externas, como ciberataques, errores humanos o fallos técnicos.

Entre las prácticas más comunes se encuentran la encriptación de datos, la implementación de firewalls, la gestión de contraseñas robustas, la autenticación multifactor (MFA) y la formación de los empleados en concienciación sobre ciberseguridad. Además, muchas organizaciones adoptan estándares internacionales como ISO 27001 para establecer un sistema de gestión de seguridad de la información (SGSI) eficaz[39].

Fig. 4 Seg. de la Información

Autenticación multifactor (MFA)

Es un sistema de seguridad que refuerza la protección de cuentas y sistemas al requerir dos o más métodos de verificación independientes para confirmar la identidad del usuario, combinando típicamente algo que el usuario sabe (como una contraseña o PIN), algo que posee (un dispositivo móvil, token físico o tarjeta inteligente) y algo que es inherente al usuario (huella digital, reconocimiento facial u otra característica biométrica). Este enfoque por capas mitiga significativamente los riesgos asociados con credenciales robadas o ataques de phishing, ya que incluso si un atacante obtiene la contraseña, necesitaría superar al menos otra barrera de autenticación para acceder ilegítimamente. Implementado ampliamente en servicios bancarios, plataformas corporativas y aplicaciones críticas, el MFA ha evolucionado para incluir métodos avanzados como códigos temporales (TOTP), notificaciones push, llaves de seguridad física (como YubiKey) y autenticación adaptativa basada en contexto, que evalúa factores como la ubicación geográfica o el dispositivo utilizado. Su adopción se ha convertido en estándar en marcos de seguridad como el NIST SP 800-63 y regulaciones como el GDPR, siendo fundamental para proteger tanto datos sensibles como infraestructuras críticas contra accesos no autorizados en un panorama de ciberamenazas cada vez más sofisticado[40].

Fig. 5 MFA

Redes WLAN domesticas

Las redes WLAN domésticas (Wireless Local Area Network) representan un sistema de conexión inalámbrica que utiliza ondas de radiofrecuencia para interconectar dispositivos electrónicos dentro de un hogar, eliminando la necesidad de cables físicos y ofreciendo mayor flexibilidad de uso. Estas redes, basadas comúnmente en los estándares IEEE 802.11 (Wi-Fi), permiten la conexión simultánea de múltiples dispositivos como smartphones, computadoras, tablets, televisores inteligentes y sistemas de domótica, creando un ecosistema digital integrado. Su popularidad en entornos residenciales se debe a su facilidad de instalación, escalabilidad y costos accesibles, aunque presentan desafíos de seguridad que requieren atención especial, como la implementación de protocolos de cifrado robustos (WPA3), el cambio de credenciales predeterminadas y la segmentación de redes para dispositivos IoT vulnerables. Además de su uso doméstico, esta tecnología sirve como base para implementaciones más avanzadas como redes mesh o sistemas de cobertura extendida, adaptándose a diferentes tamaños y necesidades de viviendas. El correcto diseño e implementación de una WLAN doméstica debe considerar factores como la ubicación estratégica del router, la selección de canales menos congestionados y la actualización periódica del firmware, aspectos que garantizan un equilibrio óptimo entre cobertura, velocidad de transmisión y seguridad en el creciente panorama de hogares inteligentes[41].

Fig. 6 Red WLAN doméstica

Ondas de radiofrecuencia (RF)

Son un tipo de radiación electromagnética dentro del espectro no ionizante, caracterizadas por longitudes de onda que van desde 1 milímetro hasta 100 kilómetros y frecuencias comprendidas entre 3 kHz y 300 GHz, utilizadas ampliamente en telecomunicaciones, sistemas de navegación, radiodifusión y tecnologías inalámbricas como Wi-Fi, Bluetooth y redes móviles (4G/5G). Estas ondas se propagan tanto en el vacío como en la atmósfera, pudiendo viajar largas distancias y atravesar ciertos obstáculos, aunque su alcance y calidad de transmisión dependen de factores como la frecuencia empleada (donde frecuencias más bajas tienen mayor alcance, pero menor ancho de banda, y viceversa), condiciones atmosféricas y la presencia de interferencias. Su aplicación en el ámbito tecnológico incluye desde sistemas de comunicación satelital y GPS hasta dispositivos médicos como resonadores magnéticos, aunque su uso también conlleva consideraciones de seguridad, como la exposición a campos electromagnéticos (regulados por estándares internacionales como los de la ICNIRP) y vulnerabilidades en transmisiones no cifradas, que pueden ser interceptadas. Además, las propiedades de las radiofrecuencias permiten innovaciones

emergentes, como la identificación por RFID en logística o la implementación de smart cities con sensores IoT, demostrando su papel fundamental en la infraestructura tecnológica moderna y su continua evolución para satisfacer demandas de conectividad global[42].

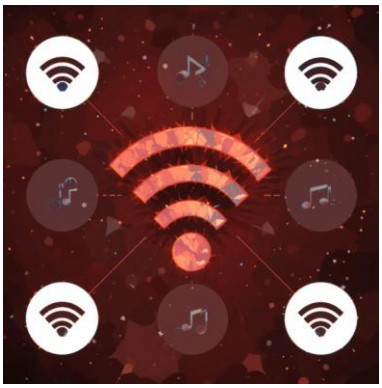


Fig. 7 Ondas RF

Firmware

El firmware es un tipo de software esencial y altamente especializado que se encuentra integrado de forma permanente en dispositivos electrónicos y hardware, actuando como un puente entre el componente físico y las capas superiores de software. A diferencia del software convencional que puede ser modificado o actualizado fácilmente por el usuario, el firmware suele almacenarse en memorias no volátiles como ROM, EPROM o flash, y contiene las instrucciones básicas que controlan el funcionamiento específico del dispositivo, desde electrodomésticos inteligentes y routers hasta sistemas complejos como placas base de computadoras, módulos de almacenamiento y componentes de automóviles. Su importancia radica en que gestiona las operaciones de bajo nivel del hardware, optimizando el rendimiento, garantizando la seguridad mediante parches que corrigen vulnerabilidades, y habilitando nuevas funcionalidades a través de actualizaciones proporcionadas por los fabricantes. Sin embargo, el firmware también puede convertirse en un vector de ataque para ciberdelincuentes (como en casos de rootkits de firmware), por lo que su protección es crítica en entornos donde la integridad del sistema es prioritaria, llevando al desarrollo de estándares como UEFI Secure Boot y tecnologías de verificación de firmware que aseguren su autenticidad y prevengan modificaciones maliciosas[43].

Fig. 8 Firmware

OWISAM (Open Wireless Security Assessment Methodology)

OWISAM (Open Wireless Security Assessment Methodology) es una metodología abierta y colaborativa diseñada específicamente para evaluar y fortalecer la seguridad de redes inalámbricas basadas en el estándar IEEE 802.11 (Wi-Fi), que surge como respuesta a la creciente necesidad de estandarizar los procesos de auditoría de seguridad en entornos wireless. Esta iniciativa, desarrollada por y para la comunidad de seguridad informática, proporciona un marco estructurado que sistematiza los controles de seguridad esenciales que deben verificarse en redes inalámbricas, incluyendo aspectos como la autenticación, cifrado, configuración de puntos de acceso, protección contra ataques de rogue AP (puntos de acceso no autorizados) y mitigación de vulnerabilidades comunes en protocolos WEP, WPA y WPA2. OWISAM se distingue por su enfoque práctico y accesible, ofreciendo a administradores de red, profesionales de seguridad TI y pentesters una guía detallada para identificar riesgos, evaluar el nivel de exposición de la infraestructura wireless y aplicar medidas correctivas que minimicen el impacto potencial de ataques como eavesdropping (escuchas ilegítimas), man-in-the-middle (hombre en el medio) o denial-of-service (denegación de servicio). Al adoptar una filosofía abierta y colaborativa, esta metodología no solo facilita la detección proactiva de vulnerabilidades en redes corporativas, educativas y gubernamentales, sino que también promueve el intercambio de conocimiento entre profesionales para elevar colectivamente los estándares de seguridad wireless en un panorama donde las amenazas evolucionan constantemente y donde la superficie de ataque se expande con la proliferación de dispositivos IoT y entornos BYOD (Bring Your Own Device)[44].

ISO 27032

La norma ISO/IEC 27032, titulada "Ciberseguridad: Directrices para la seguridad en el ciberespacio", es un estándar internacional clave dentro de la familia ISO 27000 que proporciona un marco de mejores prácticas para gestionar los riesgos cibernéticos en entornos digitales interconectados. A diferencia de normas certificables como la ISO 27001, la ISO 27032 actúa como guía de referencia para identificar y mitigar amenazas como malware, phishing y ransomware, fomentando la colaboración entre organizaciones y complementando otros frameworks de seguridad. Esta norma resulta especialmente valiosa para empresas con alta exposición digital, gobiernos que gestionan infraestructuras críticas y equipos de seguridad, ya que ofrece un enfoque proactivo para proteger ecosistemas digitales completos (incluyendo personas, procesos y tecnologías), al tiempo que facilita el cumplimiento de regulaciones como el RGPD. Su aplicación práctica incluye desde el mapeo de riesgos en aplicaciones móviles hasta la implementación de protocolos de respuesta ante incidentes y capacitación contra amenazas como el phishing, posicionándose como una herramienta complementaria que aborda específicamente los desafíos técnicos y colaborativos del ciberespacio moderno[45].

Integridad

La integridad es un principio fundamental de la seguridad de la información que garantiza su exactitud, consistencia y confiabilidad durante todo su ciclo de vida. Este concepto implica proteger los datos contra modificaciones no autorizadas, ya sean deliberadas (como alteraciones malintencionadas por hackers o empleados internos) o accidentales (errores humanos, fallos técnicos o interrupciones en los sistemas). Para preservar la integridad, las organizaciones implementan diversas medidas de control como mecanismos de autenticación robustos, sistemas

de checksum y hashing criptográfico, registros de auditoría (logs) que permiten el rastreo de cambios, y protocolos de redundancia y recuperación ante fallos. En entornos críticos como entornos residenciales, registros médicos o bases de datos gubernamentales, mantener la integridad de la información es particularmente crucial, ya que incluso pequeñas alteraciones no detectadas podrían comprometer decisiones operativas, generar pérdidas económicas significativas o afectar la seguridad pública. La norma ISO 27001 incluye específicamente la integridad como uno de los tres pilares fundamentales de la seguridad de la información (junto con la confidencialidad y disponibilidad), destacando su importancia en los sistemas de gestión de seguridad informática modernos [46].

Fig. 9 Integridad de la información

Confidencialidad

La confidencialidad es un principio fundamental de la seguridad de la información que garantiza la protección de datos sensibles mediante el control estricto de acceso, asegurando que sólo los usuarios, sistemas o procesos debidamente autorizados puedan consultarlos, procesarlos o modificarlos. Este concepto va más allá del simple ocultamiento de información, implicando un conjunto de medidas técnicas (como cifrado de datos, firewalls, sistemas de autenticación robusta y protocolos seguros de transmisión), administrativas (políticas de acceso, acuerdos de confidencialidad) y físicas (control de accesos a instalaciones) diseñadas para prevenir fugas, filtraciones o accesos indebidos, ya sean estos accidentales o malintencionados. En contextos organizacionales, la confidencialidad es particularmente crítica para proteger secretos comerciales, información financiera, datos personales (especialmente los considerados como categorías especiales bajo regulaciones como el GDPR), registros médicos o cualquier otro activo informativo cuya divulgación no autorizada podría causar daños reputacionales, económicos o legales. La norma ISO 27001 establece la confidencialidad como uno de los tres pilares esenciales de la seguridad de la información (junto con la integridad y disponibilidad), destacando su importancia en la gestión de riesgos y la continuidad del negocio en entornos cada vez más expuestos a ciberamenazas sofisticadas y requisitos regulatorios más exigentes[45].

Fig. 10 Confidencialidad de la información

Disponibilidad

La disponibilidad de la información constituye un pilar esencial de la seguridad informática que garantiza el acceso continuo, oportuno y sin restricciones a los datos y sistemas críticos cuando son requeridos por usuarios autorizados. Este principio va más allá del simple funcionamiento técnico, implicando una estrategia integral que combina redundancia de sistemas, planes de recuperación ante desastres (DRP), mantenimiento preventivo, balanceo de cargas y protección contra amenazas como ataques DDoS o fallos de hardware. En el contexto empresarial actual, donde las operaciones dependen cada vez más de entornos digitales, la pérdida de disponibilidad -incluso por períodos breves- puede generar impactos operativos severos, desde la paralización de líneas de producción y transacciones financieras hasta la interrupción de servicios esenciales en sectores como salud, transporte o energía, con consecuencias económicas, legales y reputacionales potencialmente devastadoras. Normativas como ISO 27001 y marcos como el NIST incluyen la disponibilidad como componente clave de sus estándares de seguridad, destacando la necesidad de implementar medidas proactivas que contemplen desde la tolerancia a fallos y sistemas de alimentación ininterrumpida (UPS) hasta protocolos de contingencia que aseguren la continuidad del negocio ante cualquier escenario de crisis, adaptándose así a los requerimientos de resiliencia que exige la transformación digital actual [46].

Fig. 11 Disponibilidad de la información

CVSS (Common Vulnerability Scoring System)

Es un estándar abierto utilizado para evaluar y comunicar la gravedad de las vulnerabilidades de seguridad en sistemas informáticos. Este sistema asigna una puntuación numérica, generalmente de 0 a 10, que refleja el nivel de riesgo que representa una vulnerabilidad, considerando factores como su facilidad de explotación, el impacto sobre la confidencialidad, integridad y disponibilidad, y si requiere interacción del usuario. CVSS permite a organizaciones priorizar la corrección de fallos en función de su criticidad, promoviendo una gestión eficiente de riesgos en ciberseguridad[47].

C. VARIABLES DE ESTUDIO

1) Definición nominal de variables

- ✓ **Número de vulnerabilidades detectadas**: Cantidad de debilidades o fallas encontradas en un sistema, aplicación o red informática que podrían ser explotadas por actores malintencionados para causar daños o acceder a información confidencial.

- ✓ **Nivel de riesgo**: Probabilidad de que una vulnerabilidad sea explotada y el impacto potencial que causaría.

- ✓ **Impacto de las medidas de seguridad:** Eficacia de las medidas implementadas para mitigar el riesgo asociado a las vulnerabilidades detectadas.

- ✓ **Satisfacción del usuario**: Es la percepción que tienen los usuarios sobre la seguridad y confiabilidad de los resultados después de aplicar los controles implementados en la guía de Seguridad de la Información.

2) Definición operativa de variables

- ✓ **Variable dependiente**

Guía integral de seguridad de la información: Es el artefacto que resultará del proyecto de investigación recogiendo las mejores prácticas para afianzar la seguridad en redes WLAN domésticas.

- ✓ **Variables independientes**

Número de vulnerabilidades detectadas: Se obtuvieron mediante las pruebas de vulnerabilidad y de penetración que se realizan en las redes WLAN domésticas seleccionadas.

Nivel de riesgo: El nivel de riesgo se obtiene según los parámetros de medición que propone la metodología CVSS la cual es un estándar al momento de catalogar y medir la criticidad de las vulnerabilidades encontradas.

Impacto de las medidas de seguridad: La efectividad de las medidas de seguridad implementadas se evaluará mediante el análisis comparativo de los resultados obtenidos antes y después de aplicar los controles establecidos en la Guía Integral de Seguridad de la información.

Satisfacción del usuario: Percepción y satisfacción de los usuarios después de la implementación de la guía de seguridad, utilizando encuestas y entrevistas.

D. FORMULACIÓN DE HIPOTESIS

1) Hipótesis de la investigación

Después de implementar los controles planteados y las configuraciones recomendadas en la guía de Seguridad, se logró mitigar y prevenir los riesgos y vulnerabilidades, en las redes WLAN domésticas.

2) Hipótesis nula

Después de implementar los controles planteados y las configuraciones recomendadas en la guía de Seguridad, no se logró mitigar y prevenir los riesgos y vulnerabilidades, en las redes WLAN domésticas.

3) Hipótesis alterna

Una vez implementada la guía de Seguridad las personas aprendieron a tener más control sobre las nuevas tecnologías de Información.

III. METODOLOGÍA

Para el desarrollo de esta investigación se tiene en cuenta los siguientes apartados.

A. PARADIGMA

Según [48] el paradigma positivista se caracteriza por ser preciso real y certero, en la investigación se puede observar que al analizar los posibles ataques en las redes WLAN domésticas, se encuentran que los procesos se llevan a cabo de manera efectiva logrando la materialización de los riesgos detectados.

B. ENFOQUE

De acuerdo a [49] el enfoque cuantitativo se caracteriza por utilizar datos cuantificables y medibles, por esta razón este enfoque es el más adecuado para la investigación, ya que el estudio se sustenta en el número de vulnerabilidades detectadas en el grupo muestra, antes de aplicar los controles planteados y posteriormente una vez que se aplique la guía para mitigar los riesgos y vulnerabilidades se podrá contabilizar en cuanto se redujo estos factores.

C. MÉTODO

El método que se utilizara en la investigación será el método científico [50], mediante la observación y análisis de posibles vulnerabilidades y riesgos asociados a las redes WLAN domesticas que nos permitan plantear una hipótesis con la cual se podrán generar controles técnicos y personales.

D. TIPO DE INVESTIGACIÓN

El desarrollo de la investigación se utilizó el tipo correlacional [51] el cual se desarrolla siguiendo los lineamientos dispuestos por los objetivos específicos de la misma.

E. DISEÑO DE LA INVESTIGACIÓN

La presente investigación se basó en el diseño pre experimental que según Vodniza [52]dentro de su apartado de pre experimental y de diseño de preprueba-posprueba describe que se le aplica una pre prueba antes del tratamiento experimental, después se le administra el tratamiento y, finalmente, se le aplica una prueba posterior al tratamiento. Para la investigación se realizaron pruebas antes y después de la implementación de la metodología todo con el fin de comparar si al usarla existen mejoras o se lograron contrarrestar problemas al seguir los pasos planteados por la misma.

F. POBLACIÓN Y MUESTRA

La población objetivo de este estudio está compuesta por usuarios que cuentan con servicio de internet inalámbrico en sus hogares. Sin embargo, dadas las restricciones de recursos y el tiempo disponible, se llevará a cabo con una muestra de 25 usuarios de diferentes sectores de la ciudad y operadores ISP que serán seleccionados aleatoriamente.

La muestra está dada con un nivel de confianza del 95%, un error inferior del 6% y una probabilidad del 50% corresponde a un total de 25 usuarios según la fórmula de muestreo para población infinita.

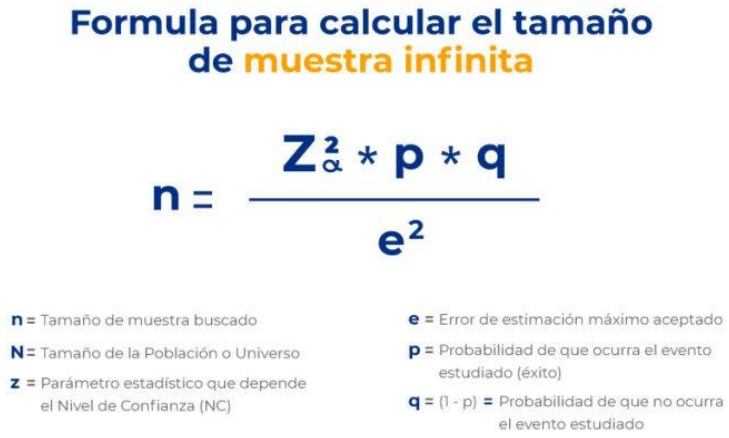


Fig. 12 Formula tamaño de muestra infinita

G. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

1) Revisión documental

Para la investigación se realizó la recopilación y el análisis de información existente sobre el tema de estudio a través de diversas fuentes documentales [53]. En estas fuentes estarán incluidos libros, artículos académicos, informes técnicos, manuales de usuario, normas, estándares, y documentos oficiales de seguridad, los cuales tendrán un papel importante dentro de la investigación.

2) Análisis de la red WLAN domestica

El análisis de la red WLAN domestica implica la evaluación directa de una red inalámbrica mediante el uso de herramientas y técnicas especializadas para identificar configuraciones, vulnerabilidades, y prácticas de seguridad. Este análisis estuvo orientado exclusivamente a redes WLAN domésticas [54].

3) Encuestas

Para la implementación de la encuesta en la investigación sobre seguridad en redes WLAN domésticas, se siguió un enfoque sistemático y detallado, para la encuesta se seleccionaron usuarios aleatoriamente que cuenten con servicio de internet inalámbrico en sus hogares, los cuales desarrollaron un cuestionario con preguntas abiertas sobre el tema de investigación, [55].

H. VALIDEZ DE LAS TECNICAS DE RECOLECCIÓN

Las técnicas de recolección de información anteriormente mencionadas son válidas para la investigación porque abarcan diversas fuentes de información, documentación especializada y estándares técnicos vigentes aplicadas a las redes WLAN tales como la norma ISO 27032, IEEE 802.11i entre otras [56]para comprender los requisitos mínimos de seguridad y las mejores prácticas recomendadas por la industria, además se tendrá en cuenta los resultados obtenidos en las diferentes pruebas de vulnerabilidad realizadas a estas redes y las encuestas que se realizaran a los usuarios residenciales.

I. CONFIABILIDAD DE LAS TECNICAS DE RECOLECCIÓN

Las herramientas que se utilizarán para realizar las pruebas de vulnerabilidad, son de alto grado de confiabilidad ya que son las más utilizadas para realizar auditorías a redes WLAN [46], además se utilizaran métodos, estándares y normas internacionales que se aplican para la seguridad de la información, los resultados obtenidos por las encuestas realizadas a los usuarios, serán de vital importancia para definir el estado actual de la seguridad en las redes de objeto de estudio [54].

J. INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Los instrumentos que se utilizarán para esta investigación serán:

1) Revisión documental

Se realizará la recopilación y el análisis de información existente sobre el tema de estudio a través de diversas fuentes documentales [48]. En estas fuentes estarán incluidos libros, artículos académicos, informes técnicos, manuales de usuario, normas, estándares, y documentos oficiales de seguridad, los cuales se encuentran publicados en Internet y además se realizará consulta en la biblioteca institucional de la Universidad CESMAG.

2) Análisis de la red WLAN

Para el análisis de la red WLAN, se implementará una metodología que incluirá el uso de herramientas y técnicas especializadas de auditoría de redes inalámbricas. Este proceso permitirá identificar: configuraciones inadecuadas, vulnerabilidades de seguridad, puntos de acceso no autorizados, protocolos de cifrado débiles (como WEP o WPA obsoletos), y prácticas de seguridad deficientes. Entre las herramientas a utilizar se consideran escáneres de redes Wi-Fi (como Airodump-ng o Kismet), herramientas de evaluación de cifrado (Wireshark para análisis de paquetes), adicionalmente, se evaluarán aspectos como la fuerza de las contraseñas, la segregación de redes, la correcta implementación de WPA3 (cuando esté disponible), y la exposición a ataques comunes.

3) Encuestas

El instrumento de recolección de datos se realizó mediante encuestas digitales creadas en Google Forms, plataforma que ofrece funcionalidades avanzadas para diseño de cuestionarios. La distribución se realizó a través de medios digitales como WhatsApp, asegurando una muestra representativa. Los resultados se almacenarán automáticamente en Google Drive con protocolos

de seguridad que garantizan la integridad y confidencialidad de los datos durante todas las fases de la investigación.

K. PROCESAMIENTO DE LA INFORMACIÓN

Para el procesamiento de la información, se empleó un formato de encuesta diseñado para recopilar datos relevantes de los usuarios. Una vez obtenidos, estos datos fueron cargados y organizados en un dashboard de control, lo que permitió visualizarlos de manera estructurada y facilitó su análisis. Gracias a esta herramienta, se pudieron identificar patrones, tendencias y posibles áreas de mejora, optimizando así la interpretación de la información y la toma de decisiones.

Adicionalmente, se llevaron a cabo pruebas de vulnerabilidad con el objetivo de evaluar los riesgos de seguridad a los que podrían estar expuestos los usuarios. Los resultados de estas pruebas fueron documentados en formatos previamente establecidos, asegurando un registro preciso y confiable. Posteriormente, toda esta información fue integrada en el dashboard, permitiendo una gestión centralizada y un acceso más ágil a los datos. Esto no solo mejoró la eficiencia en el análisis, sino que también facilitó la implementación de medidas correctivas basadas en información concreta y bien estructurada.

Fig. 13 Dashboard

IV. RESULTADOS DE LA INVESTIGACIÓN

Como resultado de la implementación de estrategias de aseguramiento en redes WLAN domésticas, basadas en la metodología OWISAM y la norma ISO 27032, se logró desarrollar una Guía Integral de Seguridad de la información de la información con recomendaciones prácticas para la protección de los dispositivos de red en entornos residenciales. Lo cual permitió, la aplicación de configuraciones seguras en routers y puntos de acceso, el uso de protocolos de autenticación y cifrado robustos, así como la aplicabilidad de las buenas prácticas de seguridad en redes WLAN domésticas. Además, se llevó a cabo un análisis y evaluación de riesgos para identificar vulnerabilidades y mitigar posibles amenazas, fortaleciendo la confidencialidad, integridad y disponibilidad de la información mediante el aseguramiento del tráfico de datos y la prevención de accesos no autorizados. Asimismo, se promovió la concientización y capacitación de los usuarios mediante la difusión de buenas prácticas en ciberseguridad para garantizar un entorno digital más seguro en los hogares.

A. Determinar los principales criterios de la metodología OWISAM, así como la arquitectura y puntos críticos de seguridad en los dispositivos de las redes WLAN domésticas

Como resultado de la investigación y el análisis de las diferentes metodologías de seguridad en redes, se pudo determinar algunas comparativas que se muestran en el siguiente **¡Error! No se encuentra el origen de la referencia.**TABLA I

TABLA I COMPARACIÓN DE METODOLOGÍAS DE SEGURIDAD EN REDES WLAN.

Aspecto	OWISAM	NIST CSF	ISO 27001	CIS Benchmarks	OWASP
Objetivo principal	Evaluar la seguridad de redes WLAN	Gestionar el riesgo cibernético	Establecer un SGSI	Proporcionar configuraciones seguras	Asegurar aplicaciones web
Controles específicos	Controles detallados para WLAN	Controles de alto nivel	Controles genéricos	Configuraciones detalladas	Vulnerabilidades y contramedidas web
Metodología	Basada en riesgos y controles técnicos	Basada en funciones y subfunciones	Ciclo PDCA (Planificar, Hacer, Verificar, Actuar)	Evaluación de la configuración	Ciclo de desarrollo seguro
Implementación	Auditorías de seguridad WLAN	Programas de gestión de riesgos	Implementación de un SGSI	Configuración de dispositivos	Pruebas de seguridad de aplicaciones web
Enfoque	Específico para WLAN	Marco general para gestión de riesgos	Sistema de gestión de seguridad de la información	Configuraciones de seguridad recomendadas	Seguridad de aplicaciones web
Alcance	Redes inalámbricas	Toda la infraestructura de TI	Toda la organización	Dispositivos y sistemas específicos	Aplicaciones web
Detalles técnicos	Muy detallados para WLAN	Nivel de detalle variable	Requisitos generales	Configuraciones específicas	Vulnerabilidades y amenazas webx

Flexibilidad	Alta adaptabilidad a diferentes entornos WLAN	Muy flexible y adaptable	Estructurada pero adaptable	Configuraciones predefinidas	Enfoque en aplicaciones web
Comunidad	Comunidad abierta y colaborativa	Amplia comunidad de usuarios	Comunidad global de profesionales de la seguridad	Comunidad de seguridad de TI	Gran comunidad de desarrolladores y profesionales de seguridad

Como conclusión y según la anterior comparativa, la metodología que mejor se ajusta a la investigación es OWISAM (Wireless Security Assessment Methodology) por las siguientes razones:

1. **Enfoque específico para WLAN**:
    - ✓ OWISAM está diseñado exclusivamente para evaluar la seguridad de redes inalámbricas (WLAN), a diferencia de otros marcos más genéricos como NIST CSF o ISO 27001.

2. **Controles detallados para WLAN**:
    - ✓ Proporciona controles técnicos específicos para redes inalámbricas, como autenticación, cifrado (WPA2/WPA3), gestión de puntos de acceso y detección de rogue APs.

3. **Metodología técnica y basada en riesgos**:
    - ✓ Su enfoque combina evaluación de riesgos con pruebas técnicas (ej: auditorías de seguridad WLAN), lo que es clave para investigar vulnerabilidades en redes inalámbricas.

4. **Alto nivel de detalle técnico**:
    - ✓ OWISAM incluye configuraciones y pruebas específicas para WLAN (ej: análisis de paquetes, ataques a protocolos como 802.11), mientras que otros marcos son más generales o abordan otros dominios (ej: CIS Benchmarks para configuraciones de sistemas o OWASP para aplicaciones web).

5. **Flexibilidad en entornos WLAN**:
    - ✓ Se adapta a diferentes escenarios inalámbricos (empresariales, públicos, IoT), algo crítico en investigaciones prácticas.

Por esta razón, OWISAM es la mejor opción para investigar seguridad en redes WLAN debido a su especialización, detalle técnico y metodología práctica como se muestra en la TABLA II.

TABLA II. DOMINIOS METODOLOGÍA OWISAM.

Dominio OWISAM	Objetivo	Ejemplos de Controles/Pruebas
1. Evaluación de Infraestructura	Identificar dispositivos y topología de la red WLAN.	- Inventario de APs, clientes y antenas. - Mapeo de cobertura y canales (ej: NetSpot, Ekahau).
2. Autenticación y Acceso	Evaluar mecanismos de autenticación y vulnerabilidades.	- Ataques a PSK (WPA/WPA2-Personal). - Vulnerabilidades en EAP (ej: LEAP, PEAP). - Uso de herramientas como aircrack-ng.
3. Cifrado y Privacidad	Analizar protocolos de cifrado y debilidades.	- Ataques a WEP (FMS, PTW). - Vulnerabilidades en TKIP (Michael). - Validación de AES-CCMP (WPA2/WPA3).
4. Gestión de Dispositivos	Verificar configuraciones seguras en APs y clientes.	- SSID ocultos (inefectivos). - MAC filtering (spoofing). - Firmware desactualizado (ej: CVE en routers).
5. Redes Rogue/Evil Twin	Detectar APs no autorizados o maliciosos.	- Herramientas: Kismet, airodump-ng. - Técnicas para identificar Evil Twins (ej: comparación de BSSID/ESSID).
6. Análisis de Tráfico	Capturar y analizar tráfico inalámbrico.	- Sniffing con Wireshark/TShark. - Extracción de credenciales en redes abiertas.
7. Pentesting WLAN	Simular ataques activos para explotar vulnerabilidades.	- Ataques de deautenticación (aireplay-ng). - KRACK (WPA2). - WPS (Pixie Dust con Reaver).
8. Redes Públicas/Guest	Evaluar riesgos en redes Wi-Fi públicas.	- MITM en hotspots. - Uso de VPNs como contramedida. - Segmentación de tráfico guest.
9. Cumplimiento y Políticas	Alinear con estándares y políticas de seguridad.	- Comparación con NIST SP 800-153. - Políticas de contraseñas y monitoreo.
10. Herramientas y Reportes	Documentar hallazgos y generar recomendaciones.	- Uso de Aircrack-ng, Wifite. - Reportes con riesgos clasificados (ej: CVSS) y planes de remediación.

B. Diseñar una Guía Integral de Seguridad de la información de la información basada en la metodología OWISAM y la Norma ISO 27032, adaptada específicamente para entornos residenciales, con el fin de establecer protocolos y procedimientos de aseguramiento de redes WLAN domésticas

En la Guía Integral de Seguridad de la información en redes WLAN Domesticas, se puede acceder desde el siguiente enlace: https://goo.su/RzvOz

Existe un apartado en el cual se relacionan las principales amenazas a las que están expuestas las redes Wi-Fi domésticas, estas están clasificadas por su nivel de riesgo, lo que permite que se pueda identificar las acciones necesarias para mejorar la seguridad de una red, minimizando el riesgo de intrusiones no deseadas y garantizando una conexión más segura. Las amenazas se describen según su riesgo tal como se muestra en la siguiente TABLA IIITABLA III.

TABLA III. VULNERABILIDADES.

Vulnerabilidad	Descripción	Nivel de Riesgo
Uso de WPA o WEP en lugar de WPA2/WPA3	Los protocolos WPA y WEP tienen fallos conocidos y pueden ser descifrados fácilmente por atacantes.	Alto
Contraseña débil del Wi-Fi	Las contraseñas simples son vulnerables a ataques de fuerza bruta, facilitando el acceso no autorizado.	Alto
Uso del SSID predeterminado	Un SSID predeterminado puede revelar el fabricante del router, facilitando ataques específicos.	Medio
Contraseña del router sin cambiar	Mantener la contraseña de administración del router por defecto facilita que los atacantes tomen control del dispositivo.	Alto
WPS activado	WPS es susceptible a ataques de fuerza bruta debido a la debilidad en su PIN, lo que puede dar acceso fácil a la red.	Alto
Firmware desactualizado	Los routers con firmware antiguo pueden tener vulnerabilidades que ya han sido corregidas en versiones más recientes.	Alto
Red Wi-Fi sin cifrado	Una red sin cifrado (abierta) permite que cualquier persona dentro del rango pueda conectarse y espiar el tráfico de la red.	Crítico
Falta de cortafuegos en el router	Un cortafuegos ayuda a bloquear accesos no autorizados desde el exterior. Su ausencia facilita ataques remotos.	Medio
Red de invitados no configurada	Si no se aísla a los invitados en una red separada, pueden tener acceso a dispositivos y datos en la red principal.	Medio
MAC Address Filtering desactivado	No habilitar el filtrado de direcciones MAC permite que cualquier dispositivo que conozca la contraseña se conecte.	Bajo
Phishing o ingeniería social	Los usuarios pueden ser engañados para dar sus credenciales a través de técnicas de phishing.	Alto
Ataques de hombre en el medio (MITM)	Si la red no está bien asegurada, los atacantes pueden interceptar la comunicación entre dispositivos.	Crítico

Vulnerabilidad	Descripción	Nivel de Riesgo
Antivirus/Antimalware desactualizado	Si los dispositivos conectados a la red no tienen protección actualizada, pueden ser vulnerables a infecciones y comprometer la red.	Medio
Acceso físico al router	Si el router está en un lugar accesible, un atacante podría restablecerlo físicamente y obtener acceso.	Medio
Sin monitoreo de tráfico	No supervisar el tráfico de la red puede permitir que dispositivos desconocidos permanezcan conectados sin ser detectados.	Bajo

Para analizar la criticidad de las vulnerabilidades se tuvo en cuenta el estándar CVSS (Common Vulnerability Scoring System) el cual es un marco abierto y ampliamente adoptado para evaluar la gravedad de vulnerabilidades de seguridad en sistemas informáticos. Está mantenido por el FIRST (Forum of Incident Response and Security Teams) y se utiliza para asignar una puntuación numérica (de 0 a 10) a vulnerabilidades, facilitando la priorización de parches y mitigaciones.

Crítico CVSS 9.0-10.0	Alto CVSS 7.0-8.9	Medio CVSS 4.0-6.9	Bajo CVSS 0.1-3.9
En esta clasificación se encuentran las vulnerabilidades de seguridad que pueden comprometer un sistema.	En esta clasificación se encuentran las vulnerabilidades de seguridad que pueden otorgar privilegios a un atacante sobre el sistema.	En esta clasificación se encuentran las vulnerabilidades de seguridad que individualmente no afectan de forma grave el sistema pero que pueden llevar a un ataque al combinarse con otras.	En esta clasificación se encuentran las vulnerabilidades de seguridad que suministran información a un atacante, pero no genera un riesgo para la integridad o disponibilidad del sistema.

Fig. 14 Niveles de criticidad CVSS

Además, en la guía también se definen algunos controles o acciones que permiten minimizar el riesgo a una de estas vulnerabilidades, estos controles son:

1. Configuración de contraseña segura.
2. Configuración de Cifrado WPA3 o WPA2.
3. Actualización de router.
4. Crea una red de invitados.

La norma **ISO/IEC 27032:2012** (Ciberseguridad o *Cybersecurity*) se aborda los riesgos asociados a las redes inalámbricas (Wi-Fi) en el contexto de la seguridad cibernética, aunque no se enfoca exclusivamente en ellos. Sin embargo, dentro de su marco, se pueden identificar riesgos relacionados con Wi-Fi y su impacto en los dominios de seguridad que la norma considera.

Principales riesgos asociados a Wi-Fi según ISO 27032

1. **Interceptación de datos (Sniffing)**
    - ✓ Transmisión no cifrada de información sensible.
    - ✓ Uso de protocolos inseguros (WEP, WPA obsoletos).
2. **Ataques de suplantación (Spoofing / Evil Twin)**
    - ✓ Puntos de acceso falsos (rogue APs) que imitan redes legítimas.
    - ✓ Ataques *Man-in-the-Middle* (MitM).
3. **Denegación de servicio (DoS / Jamming)**
    - ✓ Sobrecarga de la red mediante inundación de paquetes.
    - ✓ Bloqueo de señales Wi-Fi mediante interferencia.
4. **Acceso no autorizado**
    - ✓ Contraseñas débiles o por defecto en routers.
    - ✓ Explotación de vulnerabilidades en dispositivos IoT conectados.
5. **Exposición de dispositivos (Fuga de información)**
    - ✓ Configuraciones incorrectas que permiten acceso a recursos internos.
    - ✓ Dispositivos con servicios vulnerables expuestos a la red Wi-Fi.
6. **Malware y propagación de amenazas**
    - ✓ Infección a través de redes Wi-Fi públicas (ej. aeropuertos, cafés).
    - ✓ Propagación lateral en redes corporativas mal segmentadas.

Tanto la metodología OWISAM como la norma ISO 27032, previamente mencionadas, proporcionan un marco sólido para establecer protocolos específicos que se encuentran detallados en la Guía Integral de Seguridad de la información para redes WLAN domésticas. Esta guía resulta fundamental, ya que ofrece una serie de directrices claras que permiten tomar decisiones informadas al momento de aplicar controles de seguridad efectivos. Estos controles están diseñados para mitigar las vulnerabilidades identificadas en una red WLAN doméstica, asegurando así la protección frente a amenazas y posibles ataques.

La implementación adecuada de estos protocolos no solo mejora la seguridad de la red, sino que también facilita una gestión proactiva y eficiente de los riesgos asociados con el uso de redes inalámbricas en entornos domésticos.

A continuación, se detalla los dominios que aportan la norma según los principales riesgos en redes WLAN como se muestra en la siguiente TABLA IV

TABLA IV. DOMINIOS ISO 27032.

Dominio (Enfoque ISO 27032)	**Riesgos Wi-Fi Asociados**	**Controles / Buenas Prácticas**
Seguridad de Redes	- Interceptación de datos (sniffing).	- Uso de WPA3 (evitar WEP/WPA2 obsoletos).
	- Ataques de suplantación (Evil Twin).	- Segmentación de redes (VLANs para invitados y empleados).
	- Denegación de servicio (DoS).	- Monitoreo con IDS/IPS para redes inalámbricas.
Seguridad de la Información	- Fuga de datos por transmisión no cifrada.	- Cifrado AES-256 en redes Wi-Fi.
	- Acceso no autorizado a información sensible.	- Uso de VPN en redes públicas.
		- Políticas de autenticación fuerte (802.1X, certificados).
Seguridad de Aplicaciones	- Explotación de vulnerabilidades en apps expuestas a Wi-Fi.	- Parcheo regular de aplicaciones.
	- Malware propagado por conexiones inseguras.	- Uso de firewalls de aplicación (WAF).
		- Restricción de acceso a servicios internos.
Gestión de Identidad y Acceso	- Acceso no autorizado por credenciales débiles.	- Autenticación multifactor (MFA).
	- Suplantación de usuarios (MITM).	- Rotación periódica de contraseñas.
		- Control de dispositivos conectados (NAC).
Concienciación y Formación	- Usuarios que se conectan a redes inseguras.	- Capacitación en riesgos de Wi-Fi público.
	- Falta de conocimiento sobre phishing en Wi-Fi público.	- Simulacros de ataques (ej. Evil Twin).
		- Políticas claras de uso de redes inalámbricas.
Respuesta a Incidentes	- Detección tardía de intrusiones en Wi-Fi.	- Plan de respuesta para ataques a redes inalámbricas.
	- Ataques persistentes en la red.	- Herramientas de detección de rogue APs.
		- Registros (logs) de acceso y auditorías.
Protección de Dispositivos	- Dispositivos IoT vulnerables conectados a Wi-Fi.	- Inventario de dispositivos conectados.
	- Exposición de endpoints a ataques.	- Actualización de firmwares en routers y equipos.
		- Aislamiento de dispositivos IoT en red separada.

C. Aplicar la Guía Integral de Seguridad de la información de la información con el fin de mitigar vulnerabilidades detectadas en una muestra representativa

Para aplicar la guía inicialmente se realizaron pruebas de vulnerabilidad a la población objetivo de este estudio las cuales estuvieron compuestas por usuarios que cuentan con servicio de internet inalámbrico en sus hogares, diferentes proveedores de servicio y diferentes dispositivos de red.

A continuación, se muestra una de las pruebas de vulnerabilidad y su respectiva remediación después de aplicar la Guía Integral de Seguridad de la información en redes WLAN domésticas.

1) Pruebas de vulnerabilidad

Introducción

Es una plantilla diseñada para realizar pruebas de vulnerabilidades y pruebas de penetración en redes WLAN domésticas, con el objetivo de identificar posibles fallos de seguridad en la configuración de la red, los dispositivos conectados y los servicios expuestos. Las redes domésticas suelen ser el punto de entrada para ciberataques, ya que muchos usuarios no son conscientes de los riesgos asociados a una configuración insegura o a dispositivos con vulnerabilidades conocidas: ataques como el robo de contraseñas, la interceptación de comunicaciones, el acceso no autorizado a cámaras de seguridad o el control remoto de dispositivos IoT (Internet de las Cosas) son solo algunos de los riesgos a los que se enfrentan las redes WLAN domésticas.

El propósito de esta plantilla es evaluar la seguridad de una red doméstica, identificando vulnerabilidades comunes y proponiendo medidas correctivas. A través de pruebas específicas, como el análisis de la fortaleza de las contraseñas, la detección de puertos abiertos, la evaluación de la seguridad del router y la verificación de la protección contra ataques Man-in-the-Middle (MITM), se busca ofrecer una visión clara de los puntos débiles de la red y cómo mitigarlos.

Informe técnico pruebas de vulnerabilidad

A continuación, se presenta el informe detallado de las pruebas realizadas, en él se puede observar el escenario de prueba, los resultados esperados y obtenidos, así como la conclusión y las recomendaciones final.

Con el propósito de alcanzar los objetivos esperados, el proyecto se estructura de la siguiente forma:

Fig. 15 Metodología ejecución de pruebas

Niveles de criticidad CVSS (Common Vulnerability Score System)

A continuación, se describen los niveles de criticidad bajo los que se realiza el análisis.

Crítico CVSS 9.0-10.0	Alto CVSS 7.0-8.9	Medio CVSS 4.0-6.9	Bajo CVSS 0.1-3.9
En esta clasificación se encuentran las vulnerabilidades de seguridad que pueden comprometer un sistema.	En esta clasificación se encuentran las vulnerabilidades de seguridad que pueden otorgar privilegios a un atacante sobre el sistema.	En esta clasificación se encuentran las vulnerabilidades de seguridad que individualmente no afectan de forma grave el sistema pero que pueden llevar a un ataque al combinarse con otras.	En esta clasificación se encuentran las vulnerabilidades de seguridad que suministran información a un atacante, pero no genera un riesgo para la integridad o disponibilidad del sistema.

Fig. 16 Nivel de criticidad CVSS Primer prueba

Descripción detallada de vulnerabilidades

A continuación, se presentan los resultados de las pruebas de explotación realizadas sobre la red WLAN objetivo. En la TABLA V se detalla inicialmente la caracterización de la prueba de vulnerabilidad 1, la cual no requirió preprocesamiento ni aplicación de contramedidas. Posteriormente, se enumeran los pasos ejecutados durante la prueba, junto con los niveles de criticidad asociados. Finalmente, la tabla contrasta los resultados esperados con los obtenidos tras la explotación de las vulnerabilidades identificadas.

TABLA V. MUESTRA INICIAL Y RESULTADOS DE LA PRUEBA 1.

Código de prueba:	V006-P1		
Nombre de usuario:	Andrea Hoyos	**Evaluador:**	Maicolm López A.
Protocolo de cifrado	WPA	**Proveedor de Internet:**	Legon
Barrio:	Lorenzo	**Comuna:**	4
Escenario de prueba	KF49KFOEDK		
Pruebas de Vulnerabilidad	**Herramientas a utilizar:**	Aircrack-ng, Wireshark, Reaver, Airmon-ng, Airodump-ng, hashcat, Nmap	
	Objeto de la prueba:	El objetivo de realizar pruebas de vulnerabilidad en una red WiFi doméstica es identificar y corregir posibles fallos de seguridad antes de que un atacante pueda explotarlos.	

Procedimiento

- Tener un equipo adecuado con Kali Linux u otra distribución de seguridad (ParrotOS, BlackArch).
- Identificar las redes WiFi cercanas y seleccionar la red a la que se le va a realizar las pruebas.
- Realizar la capturar de paquetes y generar el ataque de fuerza bruta a redes con cifrado WEP/WPA/WPA2.
- Proceder con el crackeo de la contraseña de la red seleccionada.
- Verificar si el WPS está activado.
- Analizar el tráfico de red.

Niveles de criticidad

Vulnerabilidades	Baja	Media	Alta	Critica
Evaluación de seguridad del cifrado WiFi				
Captura de handshake WPA/WPA2				
Crackeo de contraseña WiFi				
Ataque a WPS (Reaver o Bully)				
Detección de dispositivos conectados				
Análisis de tráfico de red (Wireshark)				
Revisión de configuraciones del router				

Resultados esperados

1. Evaluación de seguridad del cifrado WiFi

Prueba: Analizar el tipo de cifrado usado (WEP, WPA, WPA2, WPA3)
Resultado esperado:
Segura: WPA2-PSK con AES o WPA3 detectado
Riesgosa: WPA con TKIP o WEP detectado (fácilmente hackeable)

Resultados obtenidos

	Cifrado Débil		Cifrado Fuerte	
Evaluación de seguridad del cifrado WiFi	**WEP**	**WPA**	**WPA2**	**WPA3**

2. Captura de handshake WPA/WPA2

Prueba: Capturar el proceso de autenticación de un dispositivo legítimo con Airodump-ng.
Resultado esperado:
Segura: No se logra capturar el handshake fácilmente.
Vulnerable: Se captura el handshake con éxito, lo que significa que se puede intentar crackear la clave.

Resultados obtenidos

	Cifrado Débil	Cifrado Fuerte
Captura de handshake WPA/WPA2	**Handshake alcanzable**	**Handshake inalcanzable**

Resultados esperados

3. Crackeo de contraseña WiFi

Prueba: Intentar descifrar la clave con Aircrack-ng o Hashcat.
Segura: No se logra descifrar la contraseña en un tiempo razonable.
Vulnerable: Se obtiene la contraseña en minutos u horas, indicando que es débil.

Resultados obtenidos		
Crackeo de contraseña WiFi	**Cifrado Débil**	**Cifrado Fuerte**
	Contraseña descifrada	**Contraseña no descifrada**
Resultado esperado:		

4. Ataque a WPS (Reaver o Bully)

Prueba: Intentar obtener la clave WiFi mediante el PIN de WPS.
Segura: El router bloquea los intentos después de algunos intentos fallidos.
Vulnerable: Se obtiene el PIN WPS y con ello la clave WiFi.

Resultados obtenidos		
Ataque a WPS (Reaver o Bully)	**Cifrado Débil**	**Cifrado Fuerte**
	WPS Activo	**WPS Inactivo**
Resultado esperado		

5. Detección de dispositivos conectados

Prueba: Usar herramientas como Fing o Nmap para ver quién está conectado.
Segura: Solo aparecen dispositivos autorizados.
Vulnerable: Se detectan dispositivos desconocidos en la red.

Resultados obtenidos		
Detección de dispositivos conectados	**Cifrado Débil**	**Cifrado Fuerte**
	Presencia de dispositivos desconocidos	**Solo dispositivos autorizados**
Resultado esperado:		

6. Análisis de tráfico de red (Wireshark)

Prueba: Capturar paquetes de datos para ver si la información está cifrada.
Segura: Los datos aparecen cifrados y no se pueden leer.
Vulnerable: Se capturan contraseñas en texto plano o información sensible.

Resultados obtenidos		
Análisis de tráfico de red (Wireshark)	**Cifrado Débil**	**Cifrado Fuerte**
	Contraseñas en texto plano o información sensible expuesta	**Datos cifrados, no se detecta información expuesta**
Resultado esperado		

7. Revisión de configuraciones del router

Prueba: Comprobar si el router tiene vulnerabilidades configuradas.
Segura: Acceso remoto desactivado, firmware actualizado, buena seguridad.
Vulnerable: Se encuentra acceso remoto activo, WPS habilitado, firmware antiguo.

Resultados obtenidos		
Revisión de configuraciones del router	**Cifrado Débil**	**Cifrado Fuerte**
	Firmware desactualizado	**Firmware actualizado**

De acuerdo a lo relacionado en la tabla anterior se tienen los siguientes resultados en términos de riesgos como se muestra en la TABLA VI.

TABLA VI. RESULTADOS DE CRITICIDAD DE LA PRUEBA.

Riesgo	Cantidad
Baja	1
Media	1
Alta	2
Critica	3

Según los resultados obtenidos en la primera prueba de vulnerabilidad ejecutada, se puede analizar que el **71%** (5/7) se clasifica como alta o crítica, señalando un riesgo elevado en la red.

Por esta razón se requiere tomar acciones inmediatas sobre esas vulnerabilidades y se sugiere un plan de remediación enfocado en la aplicabilidad de la Guía Integral de Seguridad de la información en redes WLAN domésticas.

Después de analizar los resultados obtenidos durante las primeras pruebas de vulnerabilidad, se procedió a implementar los controles de remediación recomendados en la Guía Integral de Seguridad de la información en redes inalámbricas domésticas con los cuales se obtuvieron los siguientes registros representados en la TABLA VII**.**

TABLA VII. APLICACIÓN DE LA GUÍA Y RESULTADOS DE LA PRUEBA 2.

Código de prueba:	V006-P2		
Nombre de usuario:	Andrea Hoyos	**Evaluador:**	Maicolm López A.
Protocolo de cifrado	WPA	**Proveedor de Internet:**	Legon
Barrio:	Lorenzo	**Comuna:**	4
Escenario de prueba	Wifi_ah		
Pruebas de Vulnerabilidad	**Herramientas a utilizar:**	Aircrack-ng, Wireshark, Reaver, Airmon-ng, Airodump-ng, hashcat, Nmap	
	Objeto de la prueba:	El objetivo de realizar pruebas de vulnerabilidad en una red WiFi doméstica es identificar y corregir posibles fallos de seguridad antes de que un atacante pueda explotarlos.	
Procedimiento			
✓ Tener un equipo adecuado con Kali Linux u otra distribución de seguridad (ParrotOS, BlackArch). ✓ Identificar las redes WiFi cercanas y seleccionar la red a la que se le va a realizar las pruebas. ✓ Realizar la capturar de paquetes y generar el ataque de fuerza bruta a redes con cifrado WEP/WPA/WPA2. ✓ Proceder con el crackeo de la contraseña de la red seleccionada. ✓ Verificar si el WPS está activado. ✓ Analizar el tráfico de red.			

Niveles de criticidad				
Vulnerabilidades	**Baja**	**Media**	**Alta**	**Critica**
Evaluación de seguridad del cifrado WiFi				
Captura de handshake WPA/WPA2				
Crackeo de contraseña WiFi				
Ataque a WPS (Reaver o Bully)				
Detección de dispositivos conectados				
Análisis de tráfico de red (Wireshark)				
Revisión de configuraciones del router				

Resultados esperados
1. Evaluación de seguridad del cifrado WiFi
Prueba: Analizar el tipo de cifrado usado (WEP, WPA, WPA2, WPA3) **Resultado esperado:** **Segura:** WPA2-PSK con AES o WPA3 detectado **Riesgosa**: WPA con TKIP o WEP detectado (fácilmente hackeable)
Resultados obtenidos

Evaluación de seguridad del cifrado WiFi	Cifrado Débil		Cifrado Fuerte	
	WEP	WPA	WPA2	WPA3

2. Captura de handshake WPA/WPA2

Prueba: Capturar el proceso de autenticación de un dispositivo legítimo con Airodump-ng.
Resultado esperado:
Segura: No se logra capturar el handshake fácilmente.
Vulnerable: Se captura el handshake con éxito, lo que significa que se puede intentar crackear la clave.

Resultados obtenidos		
Captura de handshake WPA/WPA2	Cifrado Débil	Cifrado Fuerte
	Handshake alcanzable	Handshake inalcanzable

3. Crackeo de contraseña WiFi

Prueba: Intentar descifrar la clave con Aircrack-ng o Hashcat.
Resultado esperado:
Segura: No se logra descifrar la contraseña en un tiempo razonable.
Vulnerable: Se obtiene la contraseña en minutos u horas, indicando que es débil.

Resultados obtenidos		
Crackeo de contraseña WiFi	Cifrado Débil	Cifrado Fuerte
	Contraseña descifrada	Contraseña no descifrada

4. Ataque a WPS (Reaver o Bully)

Prueba: Intentar obtener la clave WiFi mediante el PIN de WPS.
Resultado esperado:
Segura: El router bloquea los intentos después de algunos intentos fallidos.
Vulnerable: Se obtiene el PIN WPS y con ello la clave WiFi.

Resultados obtenidos		
Ataque a WPS (Reaver o Bully)	Cifrado Débil	Cifrado Fuerte
	WPS Activo	WPS Inactivo

5. Detección de dispositivos conectados

Prueba: Usar herramientas como Fing o Nmap para ver quién está conectado.
Resultado esperado:
Segura: Solo aparecen dispositivos autorizados.
Vulnerable: Se detectan dispositivos desconocidos en la red.

Resultados obtenidos		
Detección de dispositivos conectados	Cifrado Débil	Cifrado Fuerte
	Presencia de dispositivos desconocidos	Solo dispositivos autorizados

6. Análisis de tráfico de red (Wireshark)

Prueba: Capturar paquetes de datos para ver si la información está cifrada.
Resultado esperado:

Segura: Los datos aparecen cifrados y no se pueden leer. **Vulnerable:** Se capturan contraseñas en texto plano o información sensible.

Resultados obtenidos		
Análisis de tráfico de red (Wireshark)	**Cifrado Débil**	**Cifrado Fuerte**
	Contraseñas en texto plano o información sensible expuesta	**Datos cifrados, no se detecta información expuesta**

7. Revisión de configuraciones del router

Prueba: Comprobar si el router tiene vulnerabilidades configuradas. **Resultado esperado:** **Segura:** Acceso remoto desactivado, firmware actualizado, buena seguridad. **Vulnerable:** Se encuentra acceso remoto activo, WPS habilitado, firmware antiguo.

Resultados obtenidos		
Revisión de configuraciones del router	**Cifrado Débil**	**Cifrado Fuerte**
	Firmware desactualizado	**Firmware actualizado**

De acuerdo a lo relacionado en la tabla anterior se tienen los siguientes resultados en términos de riesgos, tal como se muestra en la siguiente TABLA VIII.

TABLA VIII. RESULTADOS DE CRITICIDAD DE LA PRUEBA 2.

Riesgo	Cantidad
Baja	5
Media	1
Alta	0
Critica	1

Tras la implementación de los controles propuestos de seguridad en la red WLAN analizada y según lo establecido en la Guía Integral de Seguridad de la información en redes WLAN domésticas, se observa una reducción significativa de riesgos críticos y altos, pasando de **5 vulnerabilidades críticas**/altas iniciales a solo **1 crítica residual**.

Además, se puede concluir que el 71% de los riesgos actuales son bajos, lo que indica un entorno predominantemente seguro en la red WLAN.

Comparativo antes vs. después de aplicar la guía y realizar las pruebas

TABLA IX COMPARATIVO PRUEBA1 Y PRUEBA2

Nivel de Riesgo	Antes	Después	Reducción
Crítico	3	1	**66% ↓**
Alto	2	0	**100% ↓**
Medio	1	1	0%
Bajo	1	5	400% ↑

En la TABLA IX podemos observar que los controles de seguridad implementados en la red WLAN han logrado una reducción significativa de los riesgos identificados, mejorando notablemente su nivel de protección. En particular, se ha eliminado por completo el 100% de las vulnerabilidades clasificadas como de alto riesgo (2 de 2), y se ha reducido en un 66% la cantidad de vulnerabilidades críticas, pasando de tres a una sola. Como resultado de estas acciones correctivas, se ha logrado que el 86% de los riesgos presentes en la red sean ahora de bajo o medio impacto. Este avance no solo refleja la efectividad de los controles aplicados, sino también una mejora considerable en la postura de seguridad de la red WLAN, lo que reduce significativamente las probabilidades de que la red sea objeto de un ataque o incidente de seguridad.

D. Evaluar el impacto y efectividad de la aplicación de la Guía Integral de Seguridad de la información de la información en entornos residenciales

Para evaluar adecuadamente el impacto y la efectividad de la implementación de la Guía Integral de Seguridad de la información en redes WLAN domésticas, es esencial realizar un análisis detallado de la evolución de la seguridad, comparando el estado de la red antes y después de aplicar los controles recomendados. En la fase inicial de evaluación, se observó que una gran parte de los usuarios desconocía los riesgos inherentes a una red inalámbrica sin protección, lo que los dejaba expuestos a diversas amenazas, como ataques cibernéticos, accesos no autorizados, robo de información sensible y violaciones a la privacidad.

A partir de este diagnóstico preliminar, se implementaron las medidas correctivas sugeridas por la guía, cuyo objetivo era fortalecer la seguridad de las redes domésticas. Entre las acciones adoptadas se incluyó la actualización de credenciales de acceso, utilizando contraseñas robustas y únicas; la configuración de protocolos de cifrado avanzado, como WPA3 (cuando estaba disponible); la desactivación de protocolos inseguros; la activación de firewalls; y la revisión minuciosa de las configuraciones de seguridad en routers y puntos de acceso.

Una vez implementadas estas medidas, se procedió a una segunda evaluación para medir el impacto real de las acciones tomadas. Los resultados obtenidos mostraron una mejora sustancial en la seguridad de las redes domésticas, con una notable reducción en los riesgos de intrusión y un refuerzo significativo en la protección de los dispositivos conectados. Además, se observó un incremento en el nivel de conciencia de los usuarios sobre la importancia de mantener sus redes

seguras, lo que se reflejó en la adopción de hábitos más responsables y mejores prácticas en la gestión de sus redes inalámbricas.

Para facilitar la comprensión de estos resultados y visualizar de manera clara el impacto de las medidas implementadas, se desarrolló un dashboard de control interactivo. Esta herramienta permite comparar de manera sencilla ambos escenarios, identificar las áreas de mejora y detectar posibles puntos débiles que aún requieren atención en términos de seguridad. Además, proporciona una visión detallada del nivel de protección alcanzado tras la aplicación de la guía, lo que facilita la toma de decisiones informadas y la continuidad en la mejora de la seguridad de las redes WLAN domésticas.

A continuación, se presentan las imágenes que ilustran estos hallazgos, destacando la evolución positiva de la seguridad en las redes y el impacto tangible de las medidas adoptadas.

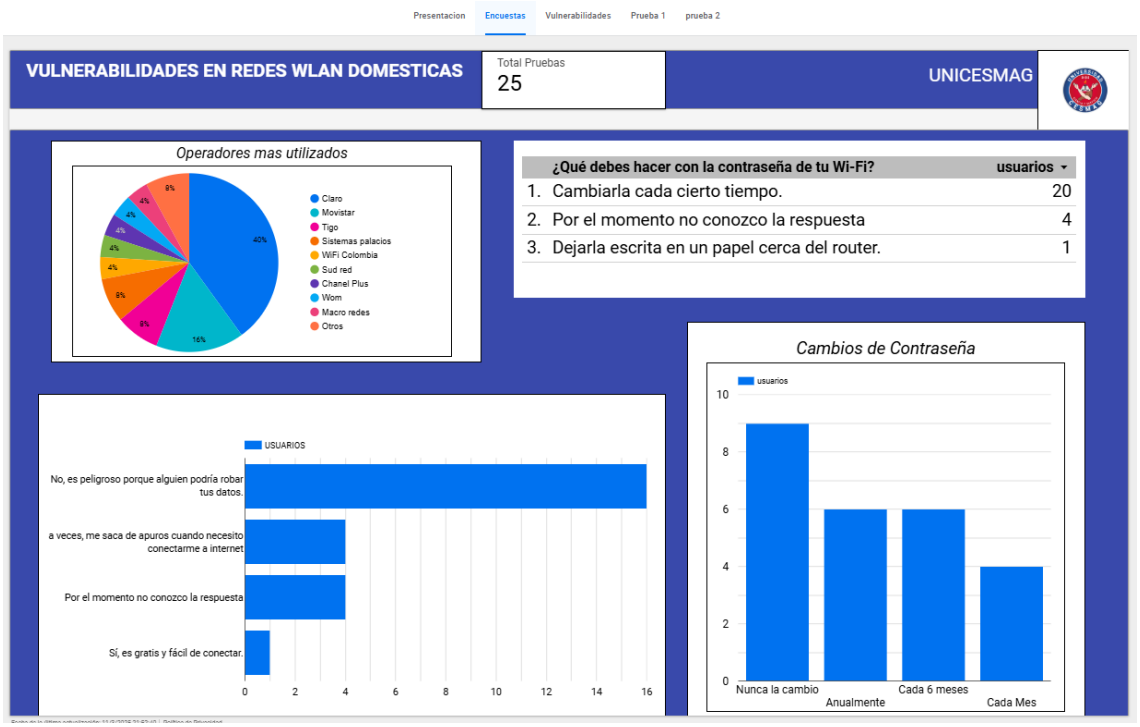


Fig. 17 Tablero encuestas

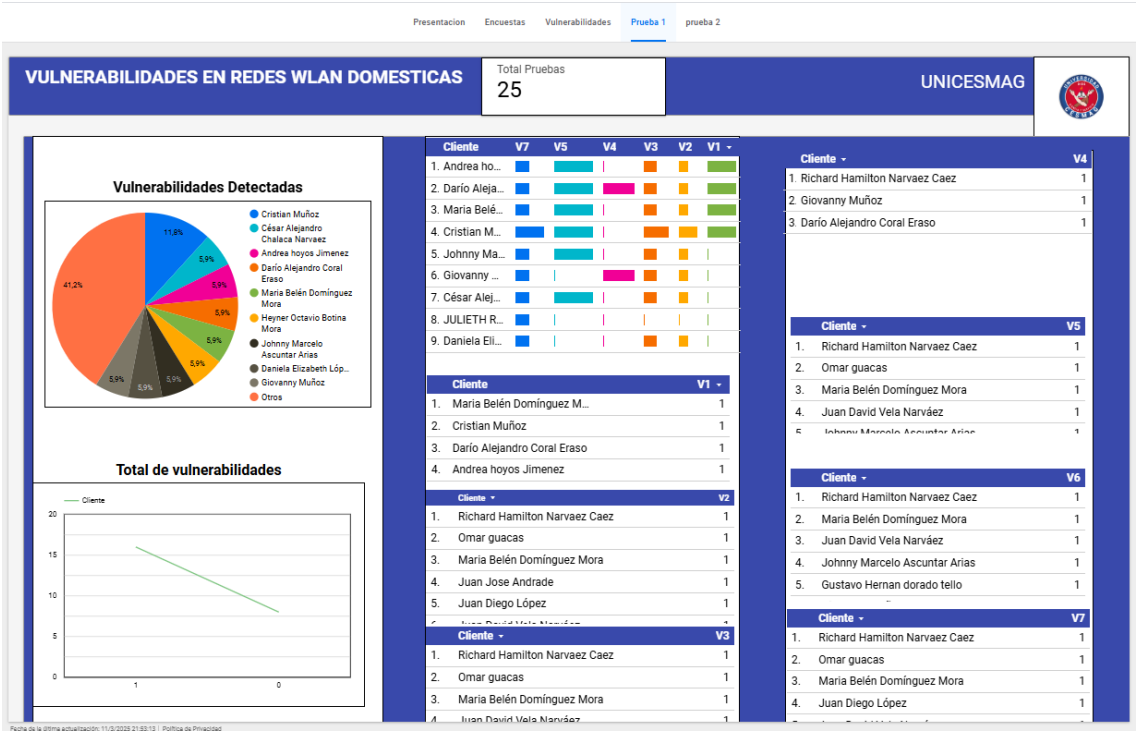


Fig. 18 Resultado Prueba 1

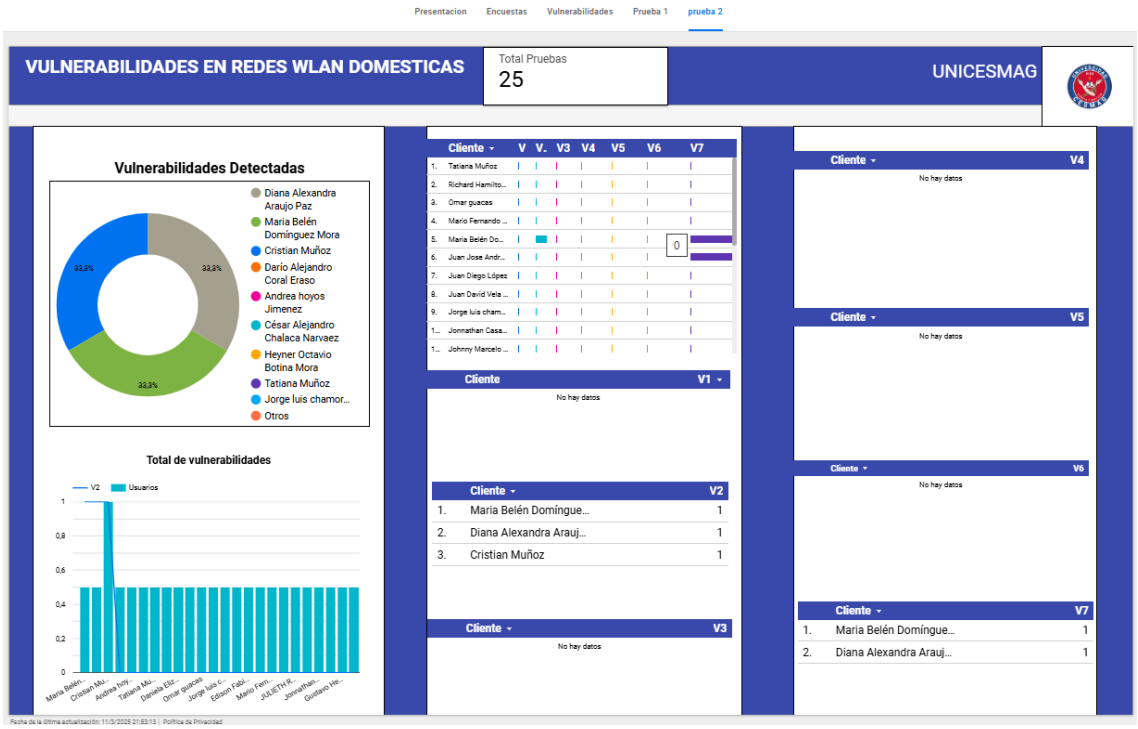


Fig. 19 Resultado prueba 2

V. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

Tras una exhaustiva investigación basada en el análisis de diversas fuentes tanto digitales como físicas, se identificó que existen múltiples metodologías diseñadas para implementar medidas de control y mitigación frente a incidentes de seguridad en redes de datos.

Estas técnicas están orientadas a salvaguardar la información en sus tres pilares fundamentales: **confidencialidad** (garantizar que solo usuarios autorizados accedan a los datos), **integridad** (evitar modificaciones no autorizadas) y **disponibilidad** (asegurar el acceso continuo a la información). Entre las metodologías evaluadas, **OWISAM** (Open Wireless Security Assessment Methodology) surgió como la opción más adecuada para auditar y fortalecer redes inalámbricas (Wi-Fi), debido a su enfoque especializado en vulnerabilidades propias de este tipo de entornos. Para maximizar su eficacia, se propuso complementar e integrar OWISAM con los lineamientos de la **norma ISO/IEC 27032**, que aborda específicamente la ciberseguridad en espacios digitales.

De acuerdo con los controles y dominios establecidos por la metodología OWISAM (Open Wireless Security Assessment Methodology), y fundamentados en los principios de seguridad cibernética propuestos por la norma ISO/IEC 27032, se desarrolló una Guía Integral de Seguridad de la información para la implementación de medidas de seguridad en redes WLAN domésticas. Esta guía técnica establece un conjunto de controles específicos diseñados para:

1. Fortalecer la postura de seguridad en redes inalámbricas residenciales, abordando vulnerabilidades críticas como:
    - ✓ Configuraciones inseguras en puntos de acceso.
    - ✓ Mecanismos de autenticación débiles.
    - ✓ Cifrado insuficiente en la transmisión de datos.
2. Proteger a los usuarios finales contra potenciales brechas de seguridad que podrían comprometer:
    - ✓ La disponibilidad del servicio de Internet.
    - ✓ La confidencialidad de información personal.
    - ✓ La integridad de datos sensibles (incluyendo información empresarial transmitida a través de redes domésticas).

La implementación de la Guía Integral de Seguridad de la información desarrollada en esta investigación demostró una eficacia significativa en la mitigación de riesgos. El análisis comparativo pre y post intervención, reveló una reducción sustancial en las vulnerabilidades identificadas inicialmente, particularmente en lo concerniente a vectores de ataque externo, para las vulnerabilidades más significativas que son las críticas y altas se logró pasar de 3 vulnerabilidades críticas a una sola y de 2 vulnerabilidades altas reducirlas en un 100%.

Nivel de Riesgo	Antes	Después	Reducción
Crítico	3	1	**66% ↓**
Alto	2	0	**100% ↓**

Este resultado no solo valida la efectividad de los controles propuestos, sino que evidencia la urgente necesidad de programas de capacitación para usuarios residenciales, particularmente en contextos donde la creciente adopción de IoT amplía significativamente la superficie de ataque.

Tras el análisis sistemático de los resultados y su contrastación con el marco teórico de referencia, se confirma la validez de la hipótesis central de esta investigación. La implementación de la metodología propuesta demostró ser efectiva para reducir de manera significativa los riesgos y vulnerabilidades detectadas en redes WLAN domésticas, validando así su aplicabilidad práctica en entornos residenciales.

Además, el componente educativo de la intervención resultó particularmente relevante, ya que permitió establecer un proceso de concientización efectivo sobre la importancia de mantener los controles de seguridad implementados y la necesidad de actualizar periódicamente las medidas de protección. Este aspecto resulta crucial si consideramos que, en entornos domésticos, el factor humano sigue siendo el eslabón más vulnerable en la cadena de seguridad informática.

CONCLUSIONES

- ✓ Con esta investigación se logró implementar con éxito un modelo integral de aseguramiento para redes WLAN domésticas mediante la articulación de la metodología OWISAM con los lineamientos de la norma ISO/IEC 27032. Esta integración nos permitió desarrollar un marco de seguridad adaptable que garantiza efectivamente la integridad, confidencialidad y disponibilidad de la información en entornos residenciales, demostrando que los estándares profesionales de ciberseguridad pueden ser contextualizados para aplicaciones no empresariales sin perder rigor técnico.

- ✓ Al aplicar la metodología OWISAM para evaluar redes WiFi caseras, se pudo identificar que los principales riesgos provienen de configuraciones básicas descuidadas, como mantener las contraseñas predeterminadas del router, usar cifrados débiles o dejar accesos administrativos expuestos. Los puntos más críticos se concentran en el router principal y los dispositivos IoT (cámaras, altavoces inteligentes, luces entre otros), que suelen estar mal configurados y desconectados de actualizaciones de seguridad.

- ✓ Al poner a prueba la Guía Integral de Seguridad de la información en redes WiFi de hogares cotidianos, comprobamos que, si funciona y es aplicable, las familias que siguieron los controles propuestos lograron corregir problemas graves como que tenían en sus redes contraseñas débiles, configuraciones peligrosas y dispositivos expuestos. La guía demostró ser un "manual de primeros auxilios" para una red casera, con pasos sencillos como actualizar el router o separar dispositivos, incluso usuarios sin conocimientos técnicos pudieron eliminar las vulnerabilidades más comunes.

- ✓ El análisis comparativo realizado antes y después de aplicar la Guía Integral de Seguridad de la Información evidenció una mejora significativa en la protección de las redes WiFi evaluadas. La implementación de medidas sencillas, como el cambio de contraseñas por defecto, la actualización del firmware del router y la configuración de cifrado robusto, permitió fortalecer notablemente la seguridad, reduciendo de manera efectiva los riesgos de intrusión y exposición de datos.

RECOMENDACIONES

- ✓ Sería valioso estudiar cómo aplicar esta guía de seguridad en diferentes tipos de hogares, desde casas en zonas rurales con internet limitado hasta departamentos con muchos dispositivos conectados (como cámaras, altavoces inteligentes o electrodomésticos con WIFI etc.).

- ✓ Desde la parte técnica, se podría pensar en el desarrollo aplicaciones móviles o asistentes virtuales que guíen paso a paso a los usuarios en la implementación de la guía, con recordatorios para mantenimiento periódico (ej.: actualizar contraseñas o firmas del router), además, integrar sistemas de diagnóstico automático que alerten sobre vulnerabilidades sin requerir conocimientos técnicos.

- ✓ Dado que el estudio se ha realizado en una población relativamente pequeña, sería recomendable sectorizar la muestra y extrapolar los resultados a una región más amplia con fines investigativos. Este enfoque permitiría analizar con mayor profundidad el nivel de alfabetización en ciberseguridad entre los participantes, así como evaluar el estado actual de la seguridad informática en comunidades específicas.

BIBLIOGRAFÍA

[1] V. A. M. Luisa F. Sicajá and O. Velásquez, "EL IMPACTO DE LAS REDES DOMÉSTICAS EN LA SEGURIDAD IOT." Accessed: May 22, 2024. [Online]. Available: https://www.researchgate.net/profile/Marvin-Leon-3/publication/376033661_Impacto_redes_domesticas_en_seguridad_IoT/links/6567d5d2b1398a779dc70b17/Impacto-redes-domesticas-en-seguridad-IoT.pdf

[2] C. DE Tecnologías La Información Proyecto De Titulación Previo A La Obtención Del Título De, "UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ FACULTAD DE CIENCIAS TÉCNICAS".

[3] C. De Telecomunicaciones, "UNIVERSIDAD NACIONAL DE CHIMBORAZO FACULTAD DE INGENIERIA".

[4] C. DE Tecnologías La Información Proyecto De Titulación Previo A La Obtención Del Título De, "UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ FACULTAD DE CIENCIAS TÉCNICAS".

[5] E. Jhordany Serna Valdivia and J. Mejia Miranda, "Propuesta de un Agente Inteligente para el Manejo y MitigaciÃn de Riesgos de Ciberseguridad en Entornos IoT," in *Applications in Software Engineering - Proceedings of the 9th International Conference on Software Process Improvement, CIMPS 2020*, 2020. doi: 10.1109/CIMPS52057.2020.9390153.

[6] G. Suárez and J. Luis, "IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD EN EL MUNDO ACTUAL".

[7] "EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA PREVIO A LA OBTENCIÓN DEL TÍTULO DE".

[8] D. Alejandro and V. Salazar, "Hardening en Enrutadores de Redes Domésticas: Mejores Prácticas y Técnicas de Seguridad".

[9] "UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES TÍTULO DEL TRABAJO DE TITULACIÓN".

[10] "Vista de Impacto en la seguridad de las redes inalámbricas." Accessed: Apr. 20, 2024. [Online]. Available: https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/43/73

[11] I. Pellejero, F. Andreu, and A. Lesta, "Fundamentos y aplicaciones de seguridad en redes WLAN : de la teoría a la práctica".

[12] J. Salazar, "REDES INALÁMBRICAS." [Online]. Available: http://www.techpedia.eu

[13] M. Gonzalez, "Velocidad de las redes WiFi N en entornos residenciales | Redes Telemáticas," Online.

[14] J. Johanna Morales Carrillo, N. Avellán Zambrano, T. Javier Lectong Zambrano, and I. María Zambrano Bravo, "Proceso de Ciberseguridad: Guía Metodológica para su implementación," *Revista Ibérica de Sistemas y Tecnologías de la Información*, vol. E29, pp. 41–50, 2020.

[15] “EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA PRÁCTICA PREVIO A LA OBTENCIÓN DEL TÍTULO DE”.

[16] M. Camila and A. Sarmiento, “ANÁLISIS DE LA SEGURIDAD A LA RED WIFI EVENTOS_COOP DE LA UNIVERSIDAD COOPERATIVA DE COLOMBIA CAMPUS ARAUCA. Nayibe Carreño García”.

[17] “Seguridad informática (Edición 2020) - POSTIGO PALACIOS, ANTONIO - Google Libros.” Accessed: Apr. 20, 2024. [Online]. Available: https://books.google.com.mx/books?hl=es&lr=&id=UCjnDwAAQBAJ&oi=fnd&pg=PR5&dq=seguridad+de+una+red+inform%C3%A1tica&ots=-IVXpl8Xc3&sig=i2f1QJyp83-IProXhpR6yrL8ZzA#v=onepage&q=seguridad%20de%20una%20red%20inform%C3%A1tica&f=false

[18] Cesmag, “Formato lineas de Investigación A-2020,” San Juan de Pasto - Nariño.

[19] S. Informáticos, Y. De, C. Jéssica, E. M. Bonilla, and G. Suntaxi, “ESCUELA POLITÉCNICA NACIONAL FACULTAD DE SISTEMAS APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES DE LA RED INALÁMBRICA DE UNA INSTITUCIÓN PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN”.

[20] H. Cruz Luz María, A. Salgado Felipe Angel, D. Chan Carlos Alberto, and G. Kú Ricardo, “Implementación de la Norma ISO 27032 frente al riesgo de inseguridad para la comunidad estudiantil en tiempos de pandemia”.

[21] E. A. Casarrubias Márquez, J. F. Castro Domínguez, R. F. Hernández Alarcón, and J. V. Galarce, “Vulnerabilidades de las Redes IoT,” *Revista Innova Ingeniería*, vol. 1, no. 6, 2021.

[22] M. Monzon and G. Angulo, “Guía metodológica para la implementación de parámetros de instalación o mantenimiento de redes WLAN,” 2020.

[23] M. Vanhoef and F. Piessens, “Key reinstallation attacks: Forcing nonce Reuse in WPA2,” *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 1313–1328, Oct. 2017, doi: 10.1145/3133956.3134027/SUPPL_FILE/MATHYVANHOEF-KEYREINSTALLATION.MP4.

[24] M. Souppaya and K. Scarfone, “Guidelines for Securing Wireless Local Area Networks (WLANs) Recommendations of the National Institute of Standards and Technology”, doi: 10.6028/NIST.SP.800-153.

[25] T. Ylonen, P. Turner, K. Scarfone, and M. Souppaya, “Security of Interactive and Automated Access Management Using Secure Shell (SSH)”, doi: 10.6028/NIST.IR.7966.

[26] “UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA-ECBTI ESPECIALIZACIÓN EN SEGURIDAD”.

[27] “Hogares colombianos con acceso a internet ya van en 60%, según el Dane.” Accessed: Nov. 28, 2024. [Online]. Available: https://www.larepublica.co/economia/hogares-colombianos-con-acceso-a-internet-ya-van-en-60-segun-encuesta-del-dane-3413775

[28] J. G. Cortés Camacho, “Auditoria a la Seguridad de la red de datos de la empresa Panavias S.A.,” https://repository.unad.edu.co/handle/10596/11941.

[29] A. J. Chaves Villota and O. J. Jossa Bastidas, “Diseño e implementación de un sistema de gestión de ancho de banda para redes wlan basado en aprendizaje de máquina,” https://sired.udenar.edu.co/7800/.

[30] ERICK DAVID BASTIDAS MONTENEGRO and LUIS CARLOS ZUÑIGA CHALAPUD, “APLICACION DE LA METODOGLOGIA OWISAM EN LA RED INALAMBRICA DE LA INSTITUCION UNIVERSITARIA CESMAG,” UNIVERSIDAD CESMAG, SAN JUAN DE PASTO, 2018.

[31] “ABOUT ENISA”, doi: 10.2824/324797.

[32] R. A. Castiblanco Carrasco, “Interfaz hack - lo hacker como interfaz y la propiedad intelectual como fricción,” p. 1, 2016, Accessed: Apr. 13, 2025. [Online]. Available: https://dialnet.unirioja.es/servlet/tesis?codigo=335547&info=resumen&idioma=SPA

[33] M. Á. de Arriba Martín, E. García García, A. S. Reillo Redón, and I. Sanz Hernando, “Herramientas de gestión de la seguridad: Más allá de los servicios de protección contra ‘hackers,’” *Comunicaciones de Telefónica I+D, ISSN 1130-4693, Nº. 30, 2003 (Ejemplar dedicado a: Tecnologías y plataformas para productos y servicios multimedia), págs. 151-166*, no. 30, pp. 151–166, 2003, Accessed: Apr. 13, 2025. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=4407052&info=resumen&idioma=SPA

[34] C. Alberto Flores Quispe, “TIPOS DE HACKERS”, Accessed: Apr. 13, 2025. [Online]. Available: http://www.axelsanmiguel.com

[35] C. A. Flores Quispe, “Revista de Información, Tecnología y Sociedad,” *Revista de Información, Tecnología y Sociedad*, p. 16, Accessed: Apr. 13, 2025. [Online]. Available: http://revistasbolivianas.umsa.bo/scielo.php?script=sci_arttext&pid=&lng=es&nrm=iso&tlng=

[36] M. L. Castro and P. León, “Hacking ético en el sector financiero,” *Sur Academia: Revista Académica-Investigativa de la Facultad Jurídica, Social y Administrativa*, vol. 8, no. 15, pp. 83–89, Jan. 2021, doi: 10.54753/SURACADEMIA.V8I15.927.

[37] A. E. R. Llerena, “Herramientas fundamentales para el hacking ético,” *Revista Cubana de Informática Médica*, vol. 12, no. 1, pp. 116–131, 2020, Accessed: Apr. 13, 2025. [Online]. Available: http://scielo.sld.cu

[38] S. Cámara Arroyo, “La Cibercriminología y el perfil del ciberdelincuente,” *Derecho y Cambio Social, ISSN-e 2224-4131, Nº. 60, 2020, págs. 470-512*, no. 60, pp. 470–512, 2020, Accessed: Apr. 13, 2025. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=7524987&info=resumen&idioma=SPA

[39] J. A. Figueroa-Suárez, J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando, and J. A. Saltos-Gómez, “La seguridad informática y la seguridad de la información,” *Polo del Conocimiento*, vol. 2, no. 12, pp. 145–155, Mar. 2018, doi: 10.23857/pc.v2i12.420.

[40] J. Antonio *et al.*, “Implementar MultiFactor de Autenticación con Microsoft 365 como estrategia de mejora en la ciberseguridad.,” *Revista Aristas*, vol. 10, no. 18, pp. 139–144, May 2023, Accessed: Apr. 13, 2025. [Online]. Available: http://revistaaristas.tij.uabc.mx/index.php/revista_aristas/article/view/287

[41] “Vista de Firewall de una red doméstica en Cisco Packet Tracer Caso de Estudio.” Accessed: Apr. 13, 2025. [Online]. Available: http://investigacion.utc.edu.ec/index.php/ciya/article/view/794/1123

[42] J. de Andrés, G. Roca, A. Perucho, C. Nieto, and D. López, “Generadores de radiofrecuencia disponibles en el mercado español,” *Revista de la Sociedad Española del Dolor*, vol. 19, no. 3, pp. 157–164, 2012, Accessed: Apr. 13, 2025. [Online]. Available: https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1134-80462012000300007&lng=es&nrm=iso&tlng=en

[43] L. Yesid and H. Fuyo, “Automatización y orquestación de herramientas en el proceso de búsqueda de vulnerabilidades en firmware de dispositivos de IoT,” Dec. 03, 2021, *Universidad de los Andes*. Accessed: Apr. 13, 2025. [Online]. Available: http://hdl.handle.net/1992/54941

[44] “OWITest: Metodología de test de penetración en redes inalámbricas - ProQuest.” Accessed: Apr. 13, 2025. [Online]. Available: https://www.proquest.com/openview/87fbbc93f144b58868fb9980dfac0a49/1?cbl=1006393&pq-origsite=gscholar

[45] S. L. Guzmán-Solano, “Guía para la implementación de la norma ISO 27032,” 2019. Accessed: Apr. 13, 2025. [Online]. Available: https://hdl.handle.net/10983/23385

[46] D. G. Muñoz Villa, “Seguridad en redes WLAN,” 2006, Accessed: Apr. 13, 2025. [Online]. Available: http://dspace.ups.edu.ec/handle/123456789/217

[47] “CVSS v4.0 Specification Document.” Accessed: Apr. 13, 2025. [Online]. Available: https://www.first.org/cvss/specification-document

[48] A. J. Quijano and V. Parte, “Guía de Investigación Cuantitativa”.

[49] Yolanda Castán, “INTRODUCCIÓN AL MÉTODO CIENTÍFICO Y SUS ETAPAS.” Accessed: May 22, 2024. [Online]. Available: https://gc.scalahed.com/recursos/files/r161r/w25794w/Introduccion%20al%20metodo.pdf

[50] A. Guillen Valle, O. Rafael, S. Camargo, M. Rodolfo, B. De Bedoya, and L. Hernando, “PASOS PARA ELABORAR UNA TESIS DE TIPO CORRELACIONAL Bajo el enfoque cuantitativo, variable categórico, escala ordinal y la estadística no paramétrica”.

[51] A. VODNIZA, “Guía de Investigación Cuantitativa,” Cesmag, PASTO, 2009.

[52] P. Inga Mariela Torres and I. Karim Paz, “METODOS DE RECOLECCION DE DATOS PARA UNA INVESTIGACIÓN”.

[53] M. Guillermo Monzon Sanchez Gustavo Alberto Angulo Justinico Universidad Santo Tomas and I. H. Juan Carlos Ramírez, “GUÍA METODOLÓGICA PARA LA DEFINICIÓN DE PARÁMETROS DE INSTALACIÓN O MANTENIMIENTO DE

REDES WLAN PROYECTO DIRIGIDO II ESPECIALIZACIÓN GESTIÓN DE REDES DE DATOS".

[54] "Vista de Las Técnicas y métodos de recolección de datos en modalidad virtual." Accessed: May 23, 2024. [Online]. Available: https://ojs33.pkpschool.publicknowledgeproject.org/index.php/jjm/article/view/1017/cunsurori

[55] Eduardo José Ocaña Rosero1 ; Neiser Stalin Ortiz Mosquera2 ; Ximena Fabiola Trujillo Borja3, "Análisis de desempeño de una red WLAN implementando el estándar IEEE 802.11ax orientado a redes de acceso múltiple y aplicaciones sensibles a latencia," *el Conocimiento REVISTA: RECIAMUC*, 2023.

[56] D. Salcedo, D. Pérez, D. Escalante, G. Vega, J. Mardini, and E. Esmeral, "METODOLOGÍA PARA EVALUACIÓN DE SISTEMAS INFORMÁTICOS UTILIZANDO TÉCNICAS DE ETHICAL HACKING EN PLATAFORMAS DE HARDWARE Y SOFTWARE LIBRE," 2022. doi: 10.26507/ponencia.851.

ANEXOS

Guía integrad de seguridad de la información en redes WLAN domesticas

UNIVERSIDAD CESMAG NIT: 800.109.387-7 VIGILADA MINEDUCACIÓN	**CARTA DE ENTREGA TRABAJO DE GRADO O TRABAJO DE APLICACIÓN – ASESOR(A)**	**CÓDIGO:** AAC-BL-FR-032
		VERSIÓN: 1
		FECHA: 09/JUN/2022

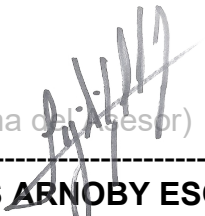
San Juan de Pasto, 04 de junio de 2025

Biblioteca
REMIGIO FIORE FORTEZZA OFM. CAP.
Universidad CESMAG
Pasto

Saludo de paz y bien.

Por medio de la presente se hace entrega del Trabajo de Grado / Trabajo de Aplicación denominado **Riesgos y Vulnerabilidades de Seguridad de la Información en redes WLAN Domesticas**, presentado por el (los) autor(es) **Maicolm Alfredo López Araújo** y **Cristian Giovanny Muñoz Muñoz**, del Programa Académico **Ingeniería de Sistemas**, al correo electrónico biblioteca.trabajosdegrado@unicesmag.edu.co. Manifiesto como asesor(a), que su contenido, resumen, anexos y formato PDF cumple con las especificaciones de calidad, guía de presentación de Trabajos de Grado o de Aplicación, establecidos por la Universidad CESMAG, por lo tanto, se solicita el paz y salvo respectivo.

Atentamente,



(Firma del Asesor)

LUIS ARNOBY ESCOBAR HERNANDEZ
98.388.299
Ingeniería de Sistemas
3154671444
laescobar@unicesmag.edu.co

INFORMACIÓN DEL (LOS) AUTOR(ES)	
Nombres y apellidos del autor: Maicolm Alfredo López Araújo	**Documento de identidad:** 12.754.631
Correo electrónico: malopez.4631@unicesmag.edu.co	**Número de contacto:** 3043830619
Nombres y apellidos del autor: Cristian Giovanny Muñoz Muñoz	**Documento de identidad:** 1.193.235.555
Correo electrónico: cgmunoz.5555@unicesmag.edu.co	**Número de contacto:** 3187431872
Nombres y apellidos del asesor: Luis Arnoby Escobar Hernandez	**Documento de identidad:** 98.388.299
Correo electrónico: laescobar@unicesmag.edu.co	**Número de contacto:** 3154671444
Título del trabajo de grado: **RIESGOS Y VULNERABILIDADES DE SEGURIDAD DE LA INFORMACIÓN EN REDES WLAN DOMESTICAS**	
Facultad y Programa Académico: Facultad de Ingeniería, Programa Ingeniería de Sistemas	

En mi (nuestra) calidad de autor(es) y/o titular (es) del derecho de autor del Trabajo de Grado o de Aplicación señalado en el encabezado, confiero (conferimos) a la Universidad CESMAG una licencia no exclusiva, limitada y gratuita, para la inclusión del trabajo de grado en el repositorio institucional. Por consiguiente, el alcance de la licencia que se otorga a través del presente documento, abarca las siguientes características:

a) La autorización se otorga desde la fecha de suscripción del presente documento y durante todo el término en el que el (los) firmante(s) del presente documento conserve (mos) la titularidad de los derechos patrimoniales de autor. En el evento en el que deje (mos) de tener la titularidad de los derechos patrimoniales sobre el Trabajo de Grado o de Aplicación, me (nos) comprometo (comprometemos) a informar de manera inmediata sobre dicha situación a la Universidad CESMAG. Por consiguiente, hasta que no exista comunicación escrita de mi(nuestra) parte informando sobre dicha situación, la Universidad CESMAG se encontrará debidamente habilitada para continuar con la publicación del Trabajo de Grado o de Aplicación dentro del repositorio institucional. Conozco(conocemos) que esta autorización podrá revocarse en cualquier momento, siempre y cuando se eleve la solicitud por escrito para dicho fin ante la Universidad CESMAG. En estos eventos, la Universidad CESMAG cuenta con el plazo de un mes después de recibida la petición, para desmarcar la visualización del Trabajo de Grado o de Aplicación del repositorio institucional.
b) Se autoriza a la Universidad CESMAG para publicar el Trabajo de Grado o de Aplicación en formato digital y teniendo en cuenta que uno de los medios de publicación del repositorio institucional es el internet, acepto(amos) que el Trabajo de Grado o de Aplicación circulará con un alcance mundial.
c) Acepto (aceptamos) que la autorización que se otorga a través del presente documento se realiza a título gratuito, por lo tanto, renuncio(amos) a recibir emolumento alguno por la publicación, distribución, comunicación pública y/o cualquier otro uso que se haga en los términos de la presente autorización y de la licencia o programa a través del cual sea publicado el Trabajo de grado o de Aplicación.
d) Manifiesto (manifestamos) que el Trabajo de Grado o de Aplicación es original realizado sin violar o usurpar derechos de autor de terceros y que ostento(amos) los derechos patrimoniales de autor

sobre la misma. Por consiguiente, asumo(asumimos) toda la responsabilidad sobre su contenido ante la Universidad CESMAG y frente a terceros, manteniéndose indemne de cualquier reclamación que surja en virtud de la misma. En todo caso, la Universidad CESMAG se compromete a indicar siempre la autoría del escrito incluyendo nombre de(los) autor(es) y la fecha de publicación.

e) Autorizo(autorizamos) a la Universidad CESMAG para incluir el Trabajo de Grado o de Aplicación en los índices y buscadores que se estimen necesarios para promover su difusión. Así mismo autorizo (autorizamos) a la Universidad CESMAG para que pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

NOTA: En los eventos en los que el trabajo de grado o de aplicación haya sido trabajado con el apoyo o patrocinio de una agencia, organización o cualquier otra entidad diferente a la Universidad CESMAG. Como autor(es) garantizo(amos) que he(hemos) cumplido con los derechos y obligaciones asumidos con dicha entidad y como consecuencia de ello dejo(dejamos) constancia que la autorización que se concede a través del presente escrito no interfiere ni transgrede derechos de terceros.

Como consecuencia de lo anterior, autorizo(autorizamos) la publicación, difusión, consulta y uso del Trabajo de Grado o de Aplicación por parte de la Universidad CESMAG y sus usuarios así:

- Permito(permitimos) que mi(nuestro) Trabajo de Grado o de Aplicación haga parte del catálogo de colección del repositorio digital de la Universidad CESMAG por lo tanto, su contenido será de acceso abierto donde podrá ser consultado, descargado y compartido con otras personas, siempre que se reconozca su autoría o reconocimiento con fines no comerciales.

En señal de conformidad, se suscribe este documento en San Juan de Pasto a los 04 días del mes de junio del año 2025

Firma del autor	Firma del autor
Nombre del autor: Maicolm Alfredo López Araújo	Nombre del autor: Cristian Giovanny Muñoz Muñoz
Firma del asesor Luis Arnoby Escobar Hernandez	