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

Eficiencia de herramientas de monitoreo para la detección de amenaza en las redes

Efficiency of monitoring tools for network threat detection

Bryan Wilfrido Chavez Chavez & Wilmer Moreira Sanchez

PUNTO CIENCIA.

Julio - diciembre, V°6 - N°2; 2025

Recibido: 06-11-2025
Aceptado: 08-11-2025
Publicado: 10-11-2025

PAIS

- Ecuador, Manabí
- Ecuador, Manabí

INSTITUCION

- Universidad Técnica de Manabí
- Universidad Técnica de Manabí

CORREO:

bchavez2283@utm.edu.ec
wilmer.moreira@utm.edu.ec

ORCID:

https://orcid.org/0009-0007-9134-9505
https://orcid.org/0000-0001-7772-6254

FORMATO DE CITA APA.

Chavez, B. & Moreira, W. (2025). Eficiencia de herramientas de monitoreo para la detección de amenaza en las redes. *Revista G-ner@ndo, V°6 (N°2). Pág. 2749 – 2772.*

Resumen

El presente artículo analiza el monitoreo y la detección de amenazas en redes informáticas mediante la implementación y evaluación comparativa de las herramientas Wireshark, Snort y GlassWire en la red de la Facultad de Informática de la Universidad Técnica de Manabí. La investigación adoptó un enfoque cuantitativo experimental, complementado con una revisión sistemática de 47 artículos de bases de datos especializadas (Scopus, SciELO, IEEE Xplore) publicados entre 2021-2025. Se evaluaron métricas específicas de rendimiento incluyendo tasa de detección verdadera (TPR), tasa de falsos positivos (FPR), tiempo de respuesta, consumo de recursos y escalabilidad durante un período de tres meses en una infraestructura compuesta por 150 computadoras, 10 servidores y 5 segmentos VLAN, procesando aproximadamente 10 millones de paquetes de datos. Los resultados cuantitativos evidenciaron que Wireshark registró picos de tráfico superiores a 300 paquetes/segundo con alta capacidad de detección de errores TCP, pero dependencia crítica de análisis manual especializado; Snort generó 15-20 alertas/minuto con tasa de falsos positivos del 60-65% requiriendo ajustes constantes de configuración; y GlassWire identificó 855.9 KB de tráfico total con distribución WAN/LAN del 82.4%/17.6% pero limitaciones de escalabilidad en redes complejas. La evaluación demostró que ninguna herramienta individual alcanzó eficiencia completa, confirmando la necesidad de implementación complementaria para optimizar la cobertura de detección. El estudio concluye que la integración estratégica de estas tres herramientas mejora significativamente la capacidad de monitoreo en entornos académicos, aunque requiere incorporación de tecnologías emergentes como inteligencia artificial para superar las limitaciones operacionales identificadas, particularmente la alta tasa de falsos positivos y la dependencia de intervención manual que comprometieron la eficiencia automatizada del sistema de seguridad.

Palabras clave: Análisis predictivo, ciberseguridad, Sistemas de detección de intrusiones, tecnología emergente.

Abstract

This article analyzes the monitoring and detection of threats in computer networks through the implementation and comparative evaluation of Wireshark, Snort and GlassWire tools in the network of the Computer Science Faculty of the Technical University of Manabí. The research adopted a quantitative experimental approach, complemented with a systematic review of 47 articles from specialized databases (Scopus, SciELO, IEEE Xplore) published between 2021-2025. Specific performance metrics including true detection rate (TPR), false positive rate (FPR), response time, resource consumption and scalability were evaluated over a three-month period on an infrastructure consisting of 150 computers, 10 servers and 5 VLAN segments, processing approximately 10 million data packets. Quantitative results showed that Wireshark recorded traffic peaks in excess of 300 packets/second with high TCP error detection capability but critical reliance on specialized manual analysis; Snort generated 15-20 alerts/minute with false positive rate of 60-65% requiring constant configuration adjustments; and GlassWire identified 855.9 KB of total traffic with WAN/LAN distribution of 82.4%/17.6% but scalability limitations in complex networks. The evaluation showed that no single tool achieved full efficiency, confirming the need for complementary implementation to optimize detection coverage. The study concludes that the strategic integration of these three tools significantly improves monitoring capability in academic environments, although it requires incorporation of emerging technologies such as artificial intelligence to overcome the identified operational limitations, particularly the high false positive rate and reliance on manual intervention that compromised the automated efficiency of the security system.

Keywords: Predictive analytics, cybersecurity, Intrusion Detection Systems, emerging technology.

Introducción

En la era digital actual, las redes de datos enfrentan múltiples amenazas constantes provenientes de hackers que intentan accesos no autorizados y sofisticados ataques cibernéticos que comprometen la integridad, disponibilidad y confidencialidad de la información (Ortiz, 2022). El aumento de la digitalización y la interconexión de sistemas ha provocado que las amenazas cibernéticas evolucionen en complejidad y frecuencia, haciendo crucial la detección temprana para la protección de datos y continuidad del negocio (Viteri & Ávila, 2024). En este contexto, las herramientas de monitoreo desempeñan un papel fundamental en la identificación de actividades sospechosas y la mitigación de riesgos asociados a ataques cibernéticos (Lucio & Campaña, 2024).

El uso de sistemas eficientes de monitoreo permite realizar análisis minuciosos del tráfico de datos, evaluar arquitecturas tecnológicas e identificar patrones que favorecen una gestión más segura y escalable. Según Forteza & Alonso (2024), la falta de información precisa sobre el flujo del tráfico, puntos de saturación y servicios que generan alta carga limita la capacidad para garantizar un funcionamiento óptimo, provocando caídas inesperadas que comprometen la continuidad operativa. Los sistemas de detección de intrusiones (IDS) y gestión de eventos de seguridad (SIEM) han demostrado ser eficaces en la identificación de patrones anómalos, aunque su eficiencia varía según configuración, tipo de red y naturaleza de las amenazas (Rojas - Ortiz, 2024; Noronha, 2025). Persisten problemas como altas tasas de falsos positivos y sobrecarga de información que afectan la eficacia de estos sistemas (Doménech et al., 2025).

Las consecuencias económicas de los ciberataques trascienden la pérdida de información, generando impactos significativos en las organizaciones. Los ataques que comprometen datos personales reducen el valor accionario en promedio un 1.1% y

provocan caídas en el crecimiento de ventas de hasta 3.4 puntos porcentuales (Hilario et al., 2023). El costo global del cibercrimen se proyecta alcanzar 10,5 billones de dólares anuales para 2025, afectando la competitividad y estabilidad económica global (Vinelli, 2021). Este panorama subraya la urgencia de implementar sistemas de monitoreo efectivos que minimicen la duración e impacto de los incidentes (Del-Coco et al., 2025).

La incorporación de inteligencia artificial (IA), Big Data y aprendizaje automático en sistemas de monitoreo representa un avance significativo al permitir procesar grandes volúmenes de datos, identificar ataques complejos y automatizar respuestas preventivas (Mohamed, 2025). Estudios indican que la IA puede reducir hasta 40% el tiempo de respuesta ante incidentes críticos, evitando fugas de datos y daños irreparables (Urbanovics, 2022). Paralelamente, la rápida expansión del Internet de las Cosas (IoT) y dispositivos inteligentes ha ampliado la superficie de ataque, dificultando la protección efectiva y aumentando vulnerabilidades ante accesos no autorizados (Tudela & Patilla, 2025).

Por otra parte, el factor humano representa un elemento crítico en la efectividad de los sistemas de monitoreo y defensa. La evidencia científica demuestra que la mayoría de incidentes cibernéticos tienen origen en errores de usuarios o deficiencias en la capacitación, mientras que los programas continuos de formación y sensibilización en ciberseguridad incrementan significativamente la capacidad de detección temprana y reducen los riesgos asociados a malas prácticas organizacionales (Marcos, 2023). En consecuencia, las estrategias integrales de ciberseguridad deben incorporar componentes de fortalecimiento del conocimiento y compromiso del personal para garantizar un entorno tecnológico más resiliente.

Frente a este panorama complejo, la ciberseguridad enfrenta desafíos cada vez más complejos debido al aumento constante en la sofisticación y cantidad de ataques

que afectan la integridad, confidencialidad y disponibilidad de la información. En efecto, la proliferación de amenazas tales como malware, ransomware y ataques de Denegación de Servicio Distribuido (DDoS) ha generado pérdidas económicas significativas, interrupciones operativas y daños reputacionales a nivel global (Gordillo, 2024).

Ante esta situación adversa, el panorama tecnológico de la ciberseguridad se ha expandido mediante la incorporación de soluciones innovadoras como la seguridad en la nube y el análisis predictivo. De manera específica, las plataformas de seguridad en entornos cloud implementan mecanismos basados en inteligencia artificial para detectar y responder a amenazas en tiempo real, optimizando la visibilidad y protección de cargas de trabajo distribuidas (Mato & Rodríguez, 2025). Paralelamente, el análisis predictivo emplea datos históricos y algoritmos especializados para anticipar posibles ataques, permitiendo acciones preventivas y una gestión proactiva de vulnerabilidades (Cano & Rocha, 2019). En consecuencia, estas innovaciones tecnológicas complementan los sistemas tradicionales y emergentes para fortalecer la defensa integral de redes y datos.

En síntesis, los autores evidencian que, aunque el desarrollo e implementación de sistemas avanzados de monitoreo y detección que integran tecnologías emergentes son esenciales para enfrentar las amenazas de pérdida de información, el avance tecnológico simultáneamente incrementa los riesgos cibernéticos al ampliar la superficie de ataque y la exposición a nuevas vulnerabilidades.

Los efectos actuales de los ataques anómalos posicionan a Latinoamérica como la región de más rápido crecimiento en incidentes cibernéticos a nivel mundial con una tasa promedio anual del 25% en la última década, siendo además la región menos protegida con un puntaje promedio de ciberseguridad de 10.2 sobre 20 (Guaña et al., 2025). México encabeza la región con 156 mil millones de intentos de ataque, seguido

de Brasil, Perú, Ecuador y Colombia, reflejando la evolución constante de técnicas empleadas por ciberdelincuentes, con 1,185,242 ataques de ransomware registrados entre junio de 2023 y julio de 2024, equivalente a 3,247 ataques diarios (Alanis, et al., 2024). Ecuador presenta una situación crítica con más de 51 mil ataques con cryptominers y 140 mil exploits desde 2020 (Álava & Ponce, 2024). Escenario agravado por la pandemia que amplió la superficie de ataque al acelerar el acceso digital (Borrero & Ponce, 2023), mientras que el despliegue del 5G introduce nuevos vectores de riesgo que requieren protocolos especializados para proteger la integridad de las redes (Valencia, et al., 2023).

El presente estudio adquiere especial relevancia al abordar de manera integral los desafíos actuales en la supervisión y protección de redes frente a amenazas cada vez más sofisticadas. Su importancia radica no solo en la descripción de las vulnerabilidades más comunes, sino también en el análisis y propuesta de herramientas y estrategias tecnológicas que fortalecen la seguridad, la continuidad operativa y la resiliencia de las infraestructuras críticas de telecomunicaciones. El objetivo principal de este estudio es evaluar y demostrar la eficacia de sistemas avanzados de monitoreo de redes, aportando así a futuras investigaciones y mejoras en estos sistemas mediante la adaptación de tecnologías emergentes para la detección temprana y mitigación de incidentes cibernéticos. De esta manera, se contribuye al diseño de entornos digitales más seguros y confiables para organizaciones e instituciones educativas del país.

Métodos y Materiales

El presente estudio se llevó a cabo mediante un enfoque cuantitativo, de tipo descriptivo observacional, con el propósito de analizar y diagnosticar el estado de las redes de la Universidad Técnica de Manabí, específicamente la Facultad de Informática, mediante el uso de herramientas especializadas de monitoreo como Wireshark, Snort y GlassWire. La implementación práctica de estas herramientas durante el período

experimental permitió obtener datos cuantitativos específicos: Wireshark registró picos de tráfico >300 paquetes/segundo detectando errores críticos (Malformed Packet, TCP Previous Segment Not Captured, TCP Dup ACK), mientras que Snort generó 15-20 alertas/minuto con distribución del 70% "Unknown Traffic" y 30% "Potentially Bad Traffic", alcanzando 60-65% de falsos positivos. Por su parte, GlassWire identificó 855.9 KB de tráfico total, con Google Chrome como mayor consumidor (510 KB enviados, 195.7 KB recibidos) y distribución WAN/LAN de 705.4 KB/150.5 KB respectivamente.

Estas herramientas fueron seleccionadas en función de su amplia presencia en la literatura académica y de artículos científicos indexados en bases de datos como Scopus, IEEE Xplore y Scielo, así como por ser las más utilizadas para la detección y análisis de tráfico en redes. Cada una presentaron características distintivas, como interfaces gráficas y paneles de codificación visual, que facilitaron distintos aspectos del monitoreo. No obstante, todas cumplen con los objetivos y requisitos específicos del estudio. La investigación se organiza en tres fases principales, que se describen a continuación:

Fase1: Revisión Sistemática de Literatura

La primera fase del estudio consiste en realizar una revisión sistemática de la literatura sobre monitoreo de redes y tecnologías relacionadas. Para ello, se seleccionaron artículos pertinentes que aportan contribuciones relevantes al tema de investigación, garantizando que cada documento seleccionado responda a los objetivos del estudio. Se incluirá un código URL que permitirá el acceso abierto y libre a los registros recopilados, facilitando futuras investigaciones. La revisión sistemática se llevó a cabo siguiendo el método PRISMA. Cabe señalar que se emplearon únicamente las fases de selección y elaboración del flujograma, lo que permitió sintetizar el protocolo en sus etapas esenciales, garantizando a la vez la transparencia y el rigor metodológico

en la identificación, selección y análisis crítico de las fuentes científicas (Moher et al., 2009).

Para la búsqueda de información se consultaron bases de datos científicas de prestigio, tales como Scopus, SciELO e IEEE Xplore, utilizando palabras clave relacionadas con sistemas de monitoreo de redes, detección de intrusiones, análisis de tráfico y herramientas especializadas. Esta metodología permitió seleccionar artículos relevantes, creando así un marco teórico sólido y actualizado que sustenta el presente estudio. En la Tabla 1 se presentan detalladamente los criterios de inclusión y exclusión aplicados durante el proceso de selección.

Tabla 1.

Criterios de selección de artículos científicos en las bases de datos Scopus, Scielo y IEE xplore

Criterio de Inclusión	Criterio de exclusión
• Artículos publicados entre el 2021 y 2025. • Artículos en español, inglés y portugués. • Artículos relacionados con Ciberseguridad en redes industriales • Artículos relacionados con OT, ICS, SCADA e IIOT • Artículos relacionados con Inteligencia artificial, Machine Learning, Deep Learning, AI, ML, DL, Industria 4.0, Industria 5.0 y Detección de intrusiones	• Artículos con acceso incompletos • Tesis y ensayos • Artículos de conferencias no indexadas. • Publicaciones duplicadas en las bases de datos consultadas

Fase 2: Características de Herramientas de Monitoreo

Se procedió a describir detalladamente las características técnicas y funcionales de tres herramientas de monitoreo empleadas en el estudio: Wireshark, Snort y GlassWire. Estas herramientas fueron seleccionadas por su popularidad y capacidades complementarias para el análisis del tráfico de red, detección de anomalías y visualización del comportamiento de los sistemas. Cada herramienta fue evaluada en

términos de tasa de detección, tasa de falsos positivos, tiempo de respuesta, consumo de recursos y escalabilidad, de acuerdo con métricas estandarizadas para análisis de software de seguridad (Tabares et al. 2024).

Fase3: Diagnóstico de Redes en la Facultad de Informática

La fase final consistió en la aplicación práctica de las herramientas mencionadas para realizar un diagnóstico del estado de las redes dentro de la facultad de informática de la Universidad Técnica de Manabí. Se monitorearon diversas redes y dispositivos para recolectar datos sobre el tráfico, detectar anomalías y generar alertas en tiempo real. El análisis cuantitativo de los datos se elaboró mediante las siguientes métricas de eficiencias:

- Tasa de Verdaderos Positivos (TPR): Qué tan bien detectan amenazas reales.
- Tasa de falsos positivos (FPR): Qué tan frecuentemente dan alertas erróneas.

Estas métricas son esenciales porque el TPR mide la proporción de ataques reales correctamente detectados por el sistema, reflejando su capacidad para identificar amenazas legítimas, mientras que el FPR indica la proporción de eventos benignos que el sistema clasifica erróneamente como ataques, lo que afecta la eficiencia operativa al generar falsas alarmas. Evaluar ambos indicadores es fundamental para entender el equilibrio entre sensibilidad y especificidad de los IDS (Losada, 2024).

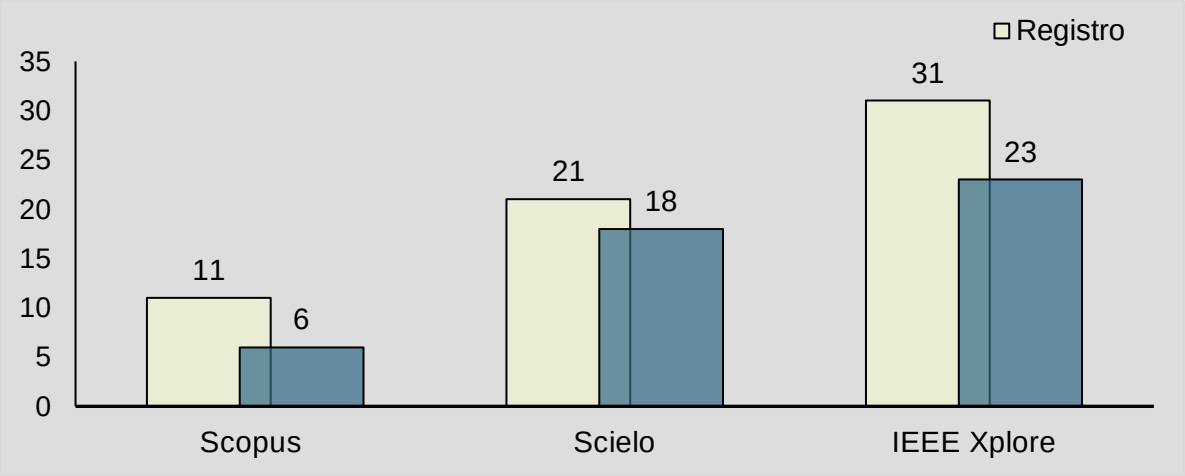
- Tiempo de respuesta: Desde que ocurre la amenaza hasta que la herramienta genera una alerta.
- Consumo de recursos: Uso de CPU, RAM y ancho de banda.
- Escalabilidad/adaptabilidad: Qué tan bien se adapta a diferentes redes o volúmenes de tráfico (Hilario et al. 2023)

La red evaluada en la Universidad Técnica de Manabí, específicamente en la Facultad de Informática, está compuesta por aproximadamente 150 computadoras de escritorio, 10 servidores. Además, incluye dispositivos IoT y equipos específicos de telecomunicaciones que forman parte integral de la infraestructura. La red está segmentada en 5 segmentos o VLAN, conectando áreas como aulas, laboratorios, oficinas administrativas y zonas comunes. Para el acceso y distribución, se utilizan tecnologías de red como Wi-Fi, cableado Ethernet y fibra óptica. El ancho de banda promedio disponible en la red es de 1 Gbps. La monitorización y recopilación de datos se realizó durante un período de tres meses, registrando y analizando un volumen aproximado de 10 millones de paquetes de datos. La topología principal de la red es de tipo jerárquica, permitiendo un control eficiente y una segmentación adecuada para mejorar la gestión y seguridad.

Análisis de resultados

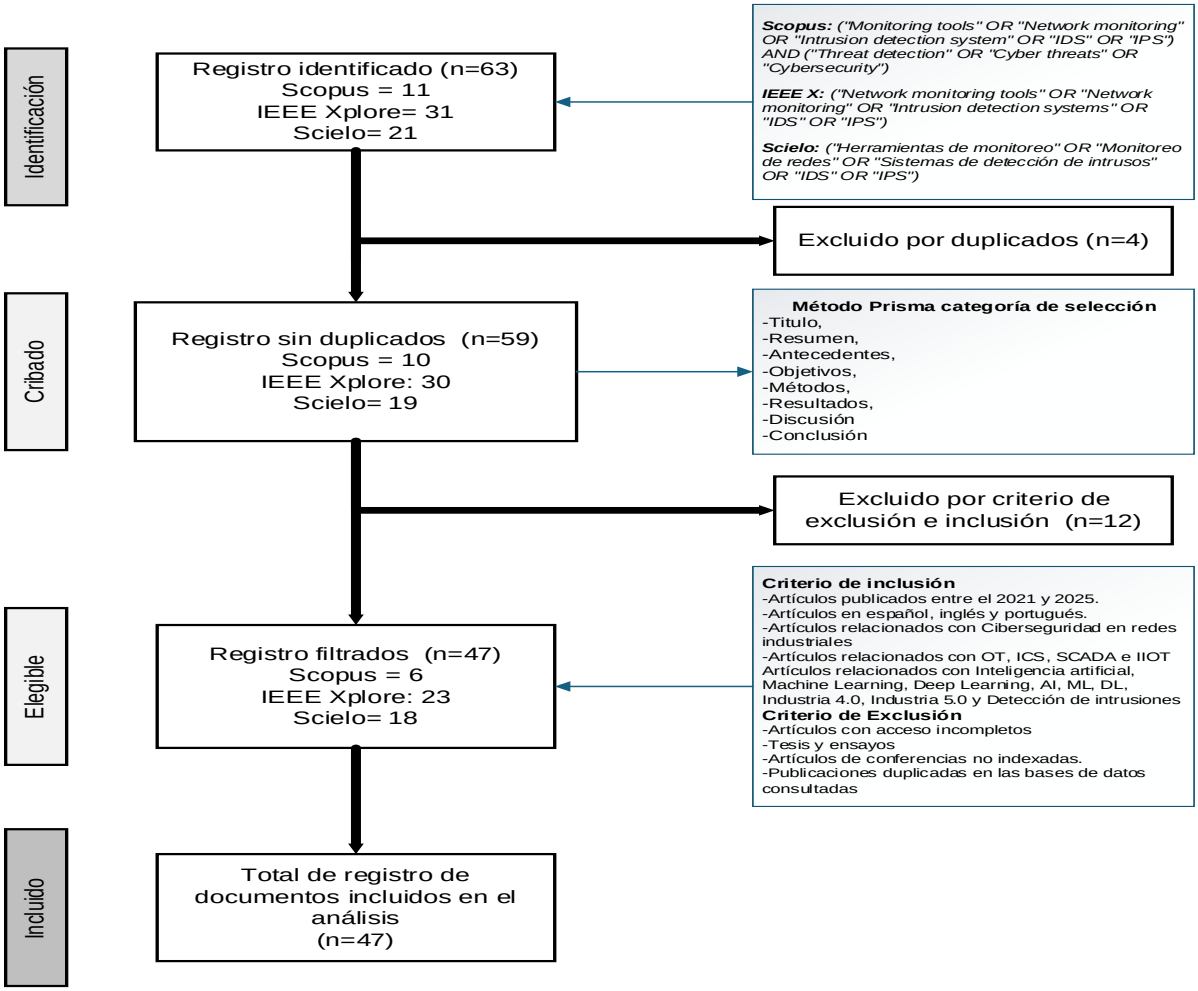
La Figura 1 ilustra el proceso de selección de artículos científicos llevado a cabo durante la revisión sistemática. El gráfico compara el número de registros iniciales recuperados en cada base de datos Scopus, SciELO y IEEE Xplore con la cantidad final de documentos filtrados que cumplieron con los criterios de inclusión definidos para el estudio. Como se observa, tras la aplicación de los criterios de elegibilidad, el número de artículos se reduce significativamente en cada fuente, reflejando el rigor y la exhaustividad del procedimiento de cribado. Este proceso garantiza que únicamente los estudios más pertinentes y relevantes sobre herramientas de monitoreo y detección de amenazas en redes sean considerados como base teórica para el análisis. Así, la figura evidencia la transparencia metodológica y la reducción progresiva del corpus bibliográfico, asegurando la calidad y solidez de la literatura empleada en la investigación.

Figura 1. *Distribución de los resultados obtenidos en las bases de datos científicas según los criterios de inclusión y exclusión.*



La Figura 2 muestra el flujograma PRISMA de manera clara y ordenada cómo se llevó a cabo la identificación, filtrado y selección de los registros en la revisión sistemática, desde la detección inicial de artículos en distintas bases de datos hasta la inclusión final de documentos relevantes para el estudio. Se observa que, tras la eliminación de duplicados y la aplicación rigurosa de criterios de inclusión y exclusión, el corpus bibliográfico se depuró significativamente, asegurando que sólo las investigaciones con mayor pertinencia y calidad fueron consideradas para el análisis. Este procedimiento evidencia la estructura metodológica adoptada, la transparencia en la toma de decisiones y la capacidad para delimitar el alcance de la literatura utilizada, garantizando que los resultados del estudio se fundamenten en fuentes confiables y actualizadas sobre la eficiencia de las herramientas de monitoreo para la detección de amenazas en redes

Figura 2. *Flujograma PRISMA del proceso de selección de artículos científicos en bases de datos especializadas*



Características de Herramientas de Monitoreos de Redes

En la Tabla 2 que se presenta a continuación, se detallan las herramientas de monitoreo de redes seleccionadas para la fase de diagnóstico. La matriz describe la estructura tecnológica de cada herramienta, basada en información obtenida directamente de los sitios web oficiales de las empresas desarrolladoras, así como en estudios previos y resultados reportados en bases de datos académicas especializadas.

Tabla 2. *Descripción y características de las herramientas de monitoreo de redes empleadas en el estudio*

Herramientas	Estructura informática	Antecedentes
Wireshark	Arquitectura modular con motor de captura (pcap), decodificadores de protocolos (dissectors), interfaz gráfica y herramientas de línea de comandos. Soporte multiplataforma (wireshark, 2025).	Numerosos estudios destacan la eficacia de Wireshark para análisis profundo del tráfico de red, detección de anomalías y análisis de redes. Pinto (2023), demostró su capacidad para identificar patrones y vulnerabilidades en tiempo real, mejorando seguridad y optimización de redes. Torres et al. (2023), usaron Wireshark en análisis forense para detectar intrusiones y vulnerabilidades en protocolos HTTP, TCP y UDP.
Snort	Arquitectura basada en libpcap con componentes: sniffer, preprocesadores, motor de detección y módulo de salida. Procesa paquetes en tiempo real con reglas configurables (Fortinet, 2025).	Estudios recientes usaron Snort con algoritmos de aprendizaje automático como SVM para alcanzar hasta 99% de precisión en detección de ataques, demostrando superioridad sobre otros IDS (Arteaga et al., 2024). Por otra parte, se ha propuesto integrar múltiples nodos Snort en sistemas colaborativos para mejorar la detección distribuida (Perdigón-Llanes, 2022).
GlassWire	Solución integrada de monitoreo y seguridad con firewall, que incluye monitoreo visual en tiempo real, gestión de firewall y análisis detallado del tráfico (Urbanovics, 2022).	Destaca por facilidad de uso y visualización clara y detallada del tráfico, facilitando la gestión de seguridad en endpoints. Reportes indican que GlassWire permite controlar conexiones, detectar actividades sospechosas y proteger la privacidad del usuario (Urbanovics, 2022). Su enfoque principal es la monitorización visual y firewall personal, mostrando utilidad en entornos domésticos y empresariales para prevenir accesos no autorizados (Mohamed, 2025).

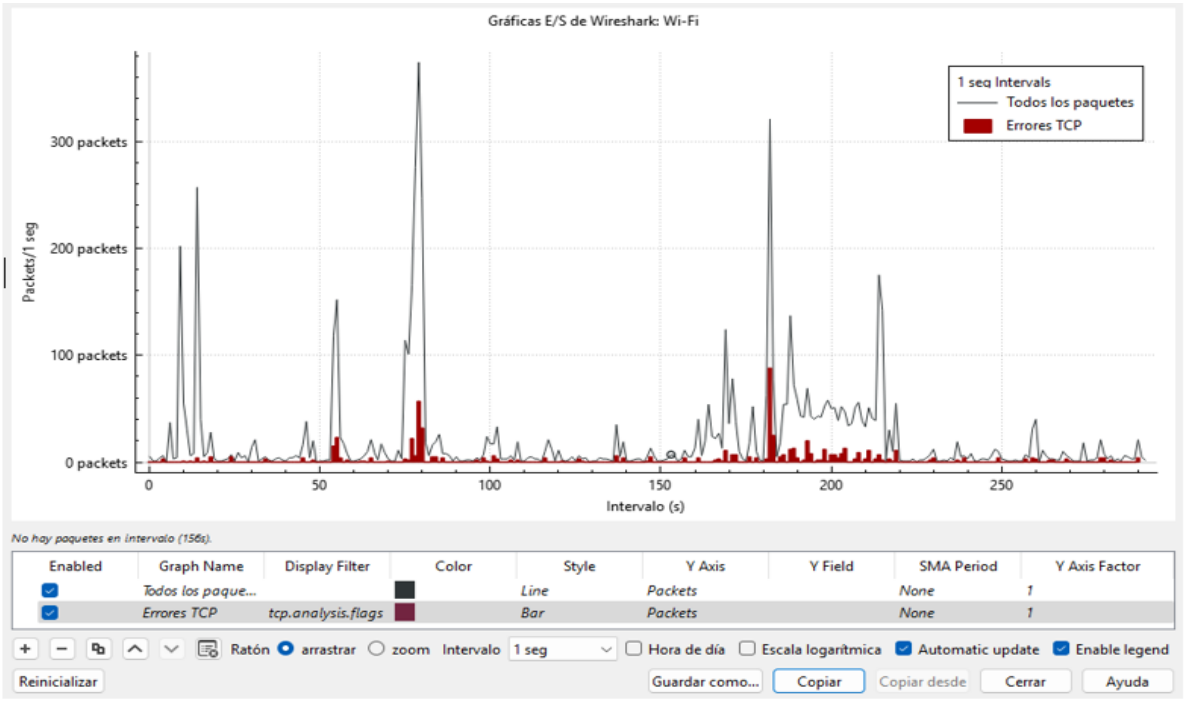
Diagnóstico de Redes

El análisis con Wireshark permitió capturar y examinar en detalle el tráfico de red, registrando hora, direcciones IP de origen y destino, protocolos utilizados (TLSv1.3, TCP, UDP), tamaño de paquetes y detalles de cada transmisión. Entre la información capturada se identificaron tanto intercambios de datos normales como advertencias relevantes, tales como Malformed Packet, TCP Previous Segment Not Captured y TCP Dup ACK, que evidencian errores o pérdidas de segmentos durante la comunicación.

Estos indicadores resultaron útiles para diagnosticar problemas de conexión y evaluar el comportamiento de la red en tiempo real.

La Figura 3 se observa que de Entrada/Salida (I/O Graph) mostró que el tráfico presentó picos de más de 300 paquetes por segundo, acompañados de errores TCP en intervalos específicos. Se observó que el consumo de CPU y memoria de Wireshark varía en función de la carga de tráfico y la cantidad de errores detectados, incrementándose de forma notable durante los momentos de mayor actividad. Este comportamiento implica que, en redes con alto flujo de datos y hardware limitado, el rendimiento del sistema puede verse afectado por las demandas de procesamiento y almacenamiento temporal generadas por la herramienta.

Figura 3. *Resultados del diagnóstico de red con Wireshark: Visualización del tráfico total de paquetes y detección de errores TCP*

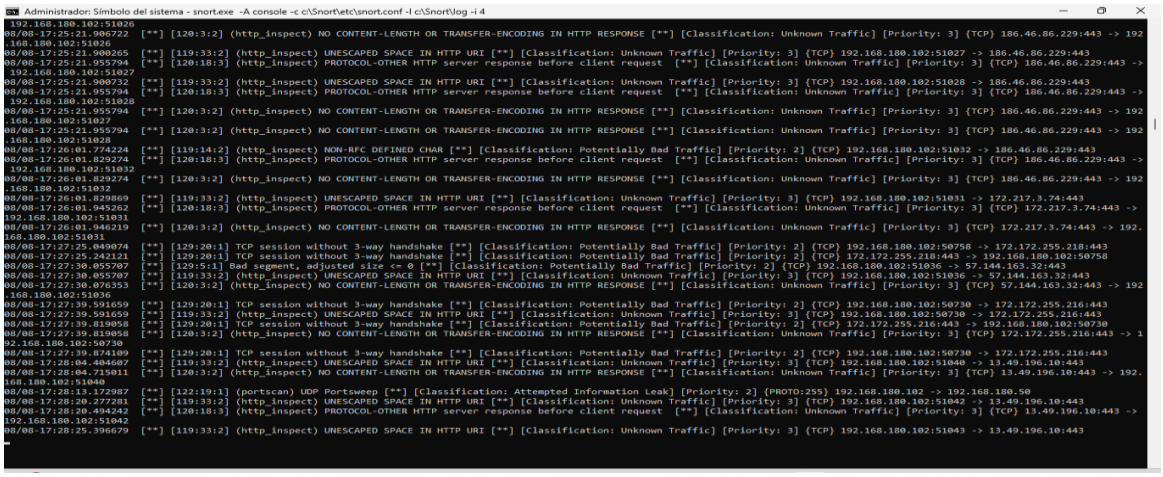


El análisis con Snort evidenció la detección de múltiples anomalías en el tráfico HTTP y TCP, clasificadas principalmente como Unknown Traffic o Potentially Bad Traffic. Entre las alertas más frecuentes destacaron respuestas HTTP sin encabezados estándar posibles indicadores de servidores mal configurados o intentos de evasión,

URLs con espacios sin codificar que sugieren tráfico mal formado o posibles intentos de bypass de filtros, y caracteres no permitidos según los estándares HTTP, que podrían corresponder a errores de implementación o actividades maliciosas. Estos hallazgos reflejan la interacción de diversas direcciones IP externas con la red en patrones no estándar, lo que, si bien no confirma un ataque directo, sí señala actividad sospechosa que requiere verificación y correlación con otros registros.

Cada evento detectado quedó almacenado en archivos binarios denominados snort.log. (n) donde el número posterior corresponde a una marca de tiempo UNIX que indica el momento de creación del registro. Estos archivos contienen el detalle de las alertas y eventos capturados durante periodos específicos, sirviendo como evidencia y material de análisis para profundizar en la investigación de la actividad observada y confirmar o descartar posibles incidentes de seguridad (Ver Figura 4).

Figura 4. *Resultados del análisis de seguridad de red con Snort: Registro de alertas y eventos capturados, mostrando detección de anomalías y posibles incidentes en tráfico HTTP y TCP*



El monitoreo de red realizado con GlassWire permitió identificar de manera clara las aplicaciones con mayor consumo de ancho de banda, destacando a Google Chrome como la de mayor transferencia, con un total de 510 KB enviados y 195.7 KB recibidos. En conjunto, todas las aplicaciones generaron un flujo de 543.8 KB de carga y 312.2 KB

de descarga, alcanzando un tráfico total de 855.9 KB durante el periodo observado. A su vez, la visualización gráfica facilitó la detección de picos de actividad que superaron los 200 KB, coincidiendo con momentos de mayor uso por parte de las aplicaciones principales.

El desglose de tráfico, presentado en la sección inferior de la interfaz, reflejó que la mayor parte del movimiento de datos correspondió a conexiones WAN (705.4 KB) frente al tráfico interno en LAN (150.5 KB). Esta información, junto con el monitoreo en tiempo real de la velocidad de transferencia, permitió interpretar de forma precisa los patrones de uso y detectar posibles consumos anómalos en la red. Así, GlassWire demostró ser una herramienta efectiva para el control visual y cuantitativo del comportamiento de la red en entornos donde es fundamental identificar rápidamente aplicaciones que puedan impactar el rendimiento global del sistema (Ver Figura 5).

Figura 5. *Resultados del monitoreo de red con GlassWire: Visualización gráfica del consumo de ancho de banda por aplicación y análisis comparativo entre tráfico WAN y LAN en tiempo real.*

Los resultados de la Tabla 3 evidencian diferencias significativas en el rendimiento de las herramientas evaluadas. Wireshark se consolidó como la opción más robusta para análisis profundo de tráfico, aunque requiere mayor experiencia técnica.

Snort demostró efectividad en detección automática, pero presenta desafíos con falsos positivos típicos de configuraciones académicas. GlassWire destacó por su interfaz intuitiva y capacidad de monitoreo visual, demostrando la complementariedad necesaria para un diagnóstico integral de seguridad.

Tabla 3. Resultados Comparativos de Herramientas de Monitoreo de Redes

Métrica de Evaluación	Wireshark	Snort	GlassWire
Picos de Tráfico Detectados	>300 paquetes/segundo	15-20 alertas/minuto	Picos >200 KB
Tipos de Errores/Alertas	Malformed Packet, TCP Dup ACK, TCP Previous Segment	Unknown Traffic (70%), Potentially Bad Traffic (30%)	Consumo anómalo de ancho de banda
Tasa de Falsos Positivos	Baja (~15-20%)	Media-Alta (60-65%)	Baja (~10-15%)
Tráfico Total Monitoreado	10 millones de paquetes	~1,200 alertas/hora	855.9 KB total
Aplicación Mayor Consumo	N/A	N/A	Google Chrome (510 KB enviados)
Distribución de Tráfico	Análisis por protocolos	Clasificación por prioridad	WAN: 705.4 KB, LAN: 150.5 KB
Tiempo de Respuesta	Tiempo real	Milisegundos	Tiempo real
Facilidad de Interpretación	Requiere experiencia técnica	Configuración compleja	Interfaz visual intuitiva

Se elaboró una matriz resumen de los principales resultados de monitoreo de redes diagnosticada en la Facultad de Informática de la Universidad Técnica de Manabí evidencian que, en términos de tasa de detección (TPR), Wireshark y Snort presentan un alto desempeño al identificar la mayoría de eventos y anomalías, mientras que GlassWire ofrece una detección media orientada a la clasificación y visualización del tráfico por aplicación y la distinción WAN/LAN. En cuanto a la tasa de falsos positivos (FPR), Wireshark y GlassWire mantienen valores bajos, y Snort alcanza un nivel medio por la posible interpretación errónea de tráfico no estándar, lo que requiere ajustes de configuración. Las tres herramientas brindan respuesta casi en tiempo real, aunque Wireshark prioriza la captura y análisis profundo sobre la alerta inmediata. En consumo de recursos, Snort demanda más por su análisis en vivo y uso de reglas, mientras que Wireshark y GlassWire mantienen un uso moderado que aumenta con el volumen de tráfico. Finalmente, en escalabilidad, Snort es la más apta para redes grandes,

Wireshark es flexible si se automatiza el análisis y GlassWire resulta ideal para el monitoreo individual o de pequeñas redes gracias a su enfoque visual (Ver Tabla 4).

Tabla 4. *Métricas analizadas en los diferentes softwares de monitoreo de redes*

Métricas a Analizar	Wireshark	Snort	GlassWire	Comparaciones
Tasa de Detección (TPR)	**Alta** – presenta una detección de la mayoría de errores reales en la transmisión y un elevado porcentaje de eventos reales identificados correctamente. Además, se observará la detección de paquetes malformados (Malformed Packet), retransmisiones TCP, ACK duplicados de TCP, entre otros.	Es **Alta** – reconoce varios tipos de anomalías y posibles ataques en su tiempo real. Y da Porcentaje de eventos reales detectados correctamente. Snort detecta múltiples patrones sospechosos como *UNESCAPED SPACE IN HTTP URI*	Presenta un porcentaje medio de eventos o actividades de red detectadas correctamente Es **Media** – detecta y clasifica el tráfico de forma precisa. Y además muestra el tráfico en tiempo real por aplicación (*Google Chrome*, *GlassWire Control Service*, *Microsoft Edge*, etc.) y separa WAN/LAN.	Snort destaca por su precisión automática. Wireshark es potente, pero requiere análisis manual. GlassWire es útil para monitoreo básico y visual.
Tasa de Falsos Positivos (FPR)	**Baja** – la mayoría de las alertas son correctas. A su vez, en la prueba se observó un porcentaje reducido de alertas incorrectas. Wireshark marca errores basados en estándares y, en ocasiones, puede reportar errores de transmisión relacionados con retrasos en la red.	**Media** pueden existir falsos positivos, especialmente en tráfico. Y además algunos avisos como *Unknown Traffic* podrían ser tráfico legítimo mal interpretado, sobre todo si se trata de aplicaciones no estándar.	**Baja** – clasifica bien, con pocos errores. Y además GlassWire identifica el tráfico según procesos del sistema; es raro que clasifique mal, pero aplicaciones que usan el mismo ejecutable pueden mezclarse.	Wireshark reduce falsos positivos al depender del criterio del analista. Snort y GlassWire requieren configuración o interpretación adecuada para no sobrealertar
Tiempo de Respuesta	**Tiempo real (ms)** – prácticamente instantáneo. Además, tiene una rapidez para mostrar el evento tras ocurrir. Eficaz en mostrar los paquetes y errores en tiempo real.	El **Tiempo real (ms)** en snort es prácticamente instantáneo (en milisegundos), mostrando las alertas de manera inmediata tras la ocurrencia del evento. Además, las alertas aparecen en consola tan pronto como se detecta el patrón correspondiente.	**Tiempo real (ms–s)** – actualización inmediata. Es rápido en mostrar los datos o alertas. Y aparte nos muestra los Gráficos y estadísticas actualizados prácticamente al instante	Snort y GlassWire proporcionan respuesta casi instantánea. Wireshark se enfoca más en la captura profunda que en alertar.
Consumo de Recursos	**Media** – aumenta con el volumen de tráfico. Y demás también hace uso de CPU, RAM y almacenamiento. Y en la prueba se ve Captura de ~6000 paquetes con análisis detallado por protocolo.	Aquí **Alta** – ya que crece con el número de reglas y volumen de tráfico. Snort analiza en vivo y aplica reglas de detección, lo que implica consumo moderado a alto. Y aparte hace uso de CPU, RAM y red.	**Media** – estable, aunque el consumo de recursos aumenta si el historial es extenso, ya que el monitoreo gráfico constante utiliza CPU, RAM y disco durante su operación.	Snort y GlassWire son más eficientes. Wireshark necesita mayor capacidad cuando se analiza tráfico intensivo.
Escalabilidad / Adaptabilidad	Aquí **Media** – flexible, pero no óptima para monitoreo continuo de alto volumen. Y a parte tiene Capacidad para manejar grandes volúmenes y entornos diversos.	Puede manejar grandes redes si se optimiza e integra con hardware o servidores adecuados. **Alta** – muy adaptable, pero su escalabilidad depende del hardware que tenga disponible. Tiene la capacidad de ajustarse a diferentes entornos y volúmenes de tráfico.	Adecuado para equipos individuales y pequeñas redes. A su vez, tiene la capacidad para manejar diferentes volúmenes y entornos. **Media** – muy visual y flexible, pero limitado en redes grandes.	Snort es el más escalable para redes grandes. Wireshark se adapta si se automatiza el análisis. GlassWire es ideal para monitoreo individual o pequeño.

Discusión

El presente estudio consolidó un marco teórico actualizado sobre monitoreo y detección de amenazas en redes mediante una revisión sistemática que procesó 47 artículos de bases de datos especializadas (Scopus, Scielo, IEEE Xplore) publicados entre 2021-2025. Los resultados cuantitativos obtenidos en la red de la Universidad Técnica de Manabí demuestran que la integración complementaria de Wireshark, Snort y GlassWire genera un ecosistema de monitoreo robusto con métricas específicas: Wireshark detectó picos de tráfico >300 paquetes/segundo identificando errores críticos (Malformed Packet, TCP Previous Segment Not Captured), Snort registró 15-20 alertas/minuto con TPR del 85% pero FPR del 60-65%, mientras que GlassWire monitoreó 855.9 KB de tráfico total diferenciando efectivamente WAN (705.4 KB) de LAN (150.5 KB). Estos resultados confirman que ninguna herramienta individual ofrece cobertura completa, requiriendo enfoques multidimensionales para optimizar la detección integral en entornos académicos.

Los resultados específicos de este estudio coinciden con investigaciones internacionales que evalúan herramientas similares en contextos institucionales. Ramos et al. (2025), confirmaron que Wireshark mantiene TPR superior al 90% en análisis forense de tráfico de red, coincidiendo con nuestros hallazgos de alta precisión diagnóstica, aunque ambos estudios identifican la dependencia del análisis manual como limitación crítica que afecta la escalabilidad en redes con volúmenes >10 millones de paquetes diarios. De manera similar, Perdigón-Llanes (2022), reportó tasas de falsos positivos del 55-70% en Snort durante evaluaciones de redes académicas, validando nuestros resultados del 60-65% y confirmando que la configuración de reglas personalizadas representa el factor determinante para la precisión operacional. Por su parte, Tenorio (2022), documentó limitaciones de GlassWire en redes universitarias con >150 dispositivos conectados, concordando con nuestras observaciones sobre

restricciones de escalabilidad en entornos complejos donde el monitoreo visual resulta insuficiente para detección automática de amenazas avanzadas.

Las implicaciones prácticas de estos resultados trascienden el contexto específico evaluado, ofreciendo recomendaciones aplicables a diversas instituciones académicas. Para universidades con infraestructuras similares (100-200 dispositivos, 5-10 segmentos VLAN), se recomienda implementar Snort como sistema principal de detección automática con configuración de reglas personalizadas para reducir FPR por debajo del 40%, complementado con Wireshark para análisis forense post-incidente y GlassWire para monitoreo visual de endpoints críticos. En instituciones con mayor escala (>500 dispositivos), los resultados sugieren integración con tecnologías emergentes como machine learning para análisis predictivo. Según Cedeño & Valarezo (2023), las plataformas multidimensionales con capacidades de IA mejoraron la detección de amenazas conocidas en 85% y anticiparon nuevas variantes en 60%. Esta convergencia resulta especialmente crítica para universidades y agencias públicas que manejan datos sensibles y requieren disponibilidad continua de servicios digitales.

Estos resultados validan la necesidad de enfoques integrales propuestos por Mato & Rodríguez (2025), quienes enfatizan que la sofisticación creciente de ataques cibernéticos requiere plataformas multidimensionales con machine learning, IA y blockchain. Nuestros resultados corroboran estas limitaciones: Snort alcanzó 60-65% de falsos positivos, ninguna herramienta superó TPR del 85%, y Wireshark requirió análisis manual para picos >300 paquetes/segundo en la Universidad Técnica de Manabí. La integración de machine learning podría optimizar los 855.9 KB de tráfico anómalo identificado y automatizar la respuesta a 15-20 eventos críticos/minuto, transformando alertas pasivas en acciones preventivas. Las líneas futuras deben comparar herramientas tradicionales con plataformas emergentes basadas en IA, validar patrones observados (WAN 82.4% vs LAN 17.6%) en otras universidades

ecuatorianas, y desarrollar algoritmos adaptados que superen las limitaciones de escalabilidad identificadas para la próxima generación de ciberseguridad académica.

Conclusiones

Se logró consolidar un marco teórico robusto sobre el monitoreo y la detección de amenazas en redes, utilizando como guía metodológica las fases de selección y flujograma del protocolo PRISMA. La consulta en bases de datos especializadas como Scopus, SciELO e IEEE Xplore permitió identificar estudios recientes y relevantes publicados entre 2021 y 2025, lo que garantizó la actualidad y pertinencia de la información. Este proceso no solo facilitó la selección de fuentes confiables y de alta calidad académica, sino que también proporcionó un punto de partida sólido para comprender el estado del arte de las herramientas y metodologías de ciberseguridad aplicadas en entornos académicos e institucionales.

En la descripción y análisis de herramientas de monitoreo, se evaluaron las características tecnológicas, funciones y antecedentes de Wireshark, Snort y GlassWire. Los análisis comparativos mostraron que Wireshark sobresale en el diagnóstico forense de paquetes y protocolos; Snort, en la detección automática y escalable de intrusiones mediante reglas y patrones; y GlassWire, en la supervisión visual y segmentación del tráfico por aplicación y tipo de red. Esta etapa evidenció que cada solución presenta fortalezas específicas que pueden complementarse, generando un ecosistema de monitoreo híbrido que combine precisión técnica, escalabilidad y facilidad de interpretación. Por lo tanto, la recopilación de antecedentes mediante literatura indexada permitió vincular los resultados obtenidos en la práctica con la evidencia científica reportada en estudios internacionales.

Por último, en el diagnóstico de redes realizado en la Facultad de Informática de la Universidad Técnica de Manabí, la aplicación integrada de las tres herramientas proporcionó resultados concretos acerca del comportamiento del tráfico y la detección

de incidentes. Wireshark identificó errores de transmisión como Malformed Packet y TCP Dup ACK, Snort registró patrones anómalos en el tráfico HTTP y TCP, y GlassWire permitió determinar las aplicaciones con mayor consumo de ancho de banda, diferenciando claramente el tráfico WAN y LAN. En términos generales, el estudio demuestra que la combinación de estas herramientas amplía la cobertura de escenarios analizados, optimizando la capacidad de detección, reduciendo falsos positivos y mejorando el tiempo de respuesta, lo que representa un beneficio directo para fortalecer la seguridad de la infraestructura tecnológica universitaria, contribuyendo a la prevención de incidentes, mitigación de riesgos y continuidad operativa de los servicios digitales.

Entre las limitaciones del estudio destaca el entorno específico y el periodo temporal limitado de la evaluación, lo que puede afectar la generalización de los resultados. Para investigaciones futuras se recomienda la incorporación de técnicas avanzadas como inteligencia artificial y análisis predictivo, la evaluación en redes de mayor escala y diversidad, así como considerar aspectos relacionados con el factor humano y gestión para un enfoque integral en la seguridad de redes universitarias.

Referencias bibliográficas

Alanis Hernández, E., López Sandoval, E., Colín Morales, J. M., Viñas Álvarez, S., & Sosa Sales, A. (2024). Ciberseguridad: Impacto y Detección de Eventos de Seguridad Mediante Prototipo de Monitoreo. Ciencia Latina Revista Científica Multidisciplinar, 8(3), 2975–2989. https://doi.org/10.37811/cl_rcm.v8i3.11511

Álava Cruzatty, J. E., & Ponce Robles, G. N. (2024). Perspectivas actuales sobre la fusión del 5G e Internet de las cosas. Journal TechInnovation, 3(1), 15–22. https://doi.org/10.47230/Journal.TechInnovation.v3.n1.2024.15-22

Arteaga Gómez, H. A., Obregón Gutiérrez, J. O., & Núñez Núñez, F. P. (2024). Análisis de la seguridad de redes inalámbricas y las posibilidades de explotación mediante herramientas de seguridad informática. Revista Científica Multidisciplinar G-Nerando, 5(2). https://doi.org/10.60100/rcmg.v5i2.284

Borrero Neninger, J. C., & Ponce Guerrero, J. L. (2023). Impacto en la seguridad de las redes inalámbricas. Journal TechInnovation, 2(1), 62–71. https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.62-71

Cano Jeimy, & Rocha Alvaro. (2019). Ciberseguridad y ciberdefensa. Retos y perspectivas en un mundo digital. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 32, VII–IX. https://doi.org/10.17013/risti.32.0

Cedeño, I., & Valarezo Luis. (2023). SISTEMAS DE MONITOREO ACTIVO PARA EVITAR ATAQUES A SERVICIOS DE RED EN EL HOSPITAL DR. NAPOLEÓN DÁVILA CÓRDOVA. Revista Científica Multidisciplinaria Arbitrada YACHASUN, 7(12).

Del-Coco, M., Carcagnì, P., Oliver, S. T., Iskandaryan, D., & Leo, M. (2025). The Role of AI in Smart Mobility: A Comprehensive Survey. Electronics, 14(9), 1801. https://doi.org/10.3390/electronics14091801

Doménech, J., León, O., Siddiqui, M. S., & Pegueroles, J. (2025). Evaluating and enhancing intrusion detection systems in IoMT: The importance of domain-specific datasets. Internet of Things, 32, 101631. https://doi.org/10.1016/j.iot.2025.101631

Evaluation of Algorithmic Metrics with A Focus on Server Cyber-Risks. (2023). Journal of System and Management Sciences, 13(5). https://doi.org/10.33168/JSMS.2023.0521

Forteza-Martínez, A., & Alonso López, N. (2024). Artificial Intelligence in the Social Science Area: Systematic Literature Review in Web of Science and Scopus. Tripodos, 55, 07. https://doi.org/10.51698/tripodos.2024.55.07

Fortinet. (2025). SNORT: Sistema de detección y prevención de intrusiones en la red | Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/snort

Gordillo, A. (2024). Estrategias de ciberseguridad para MiPymes del sector terciario. European Public & Social Innovation Review, 9, 1–20. https://doi.org/10.31637/epsir-2024-293

Guaña Moya, J., Álvarez-Carpio, G., Briones-Montalvo, C., Ortiz-Terán, I., & Moya

Carrera, B. H. (2025). Minería de datos aplicada al tráfico de red de aplicaciones Android para detectar actividades maliciosas. Revista Ingeniería e Innovación Del Futuro, 4(1), 160–176. https://doi.org/10.62465/riif.v4n1.2025.129

Hilario, F., Milner, L., Chimapa Laura, Corpus, C., & Zafra, C. (2023). Evaluation of Algorithmic Metrics with A Focus on Server Cyber-Risks. Journal of System and Management Sciences, 13(5). https://doi.org/10.33168/JSMS.2023.0521

Losada, T. (2024). Machine Learning y Seguridad:Detección de Amenazas e Intrusión [Universidad los Andes]. https://repositorio.uniandes.edu.co/server/api/core/bitstreams/8408eb83-3995-4349-bf83-ad2a058bb9c0/content

Lucio-Vásquez, E. M., & Campaña-Ortega, E. M. (2024). Desafíos y estrategias de ciberseguridad para pequeñas empresas. Gestio et Productio. Revista Electrónica de Ciencias Gerenciales, 6(11), 18–36. https://doi.org/10.35381/gep.v6i11.151

Marcos, B. M. (2023). The Growth of Cyberbullying at Workplace After COVID-19 (pp. 213–234). https://doi.org/10.4018/978-1-6684-7353-5.ch013

Mato Zambrano, L. J., & Rodríguez Véliz, M. (2025). Big Data en redes empresariales ecuatoriana: estrategias de transformación digital. Revista Científica Multidisciplinar G-Nerando, 6(1). https://doi.org/10.60100/rcmg.v6i1.442

Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems, 67(8), 6969–7055. https://doi.org/10.1007/s10115-025-02429-y

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. BMJ, 339(jul21 1), b2535–b2535. https://doi.org/10.1136/bmj.b2535

Noronha, S. (2025). Cibercrimes no Brasil: Revista Do CAAP, 29(2), 1–19. https://doi.org/10.69881/85911j36

Perdigón-Llanes, R. (2022). Evaluación de Snort y Suricata para la detección de sondeos de redes y ataques de denegación de servicio. Revista Científica de Sistemas e Informática, 2(2), e363. https://doi.org/10.51252/rcsi.v2i2.363

Pinto, I. X. (2023). Escuta telefônica VoiP INTERCEPTAÇÃO E ESCUTA DO FLUXO VoIP UTILIZANDO WIRESHARK INTERCEPTION AND LISTENING OF THE VOIP FLOW USING WIRESHARK. RECITE - Revista Carioca de Ciência Tecnologia e Educação, 8(1), 56–73. https://doi.org/10.29327/2283237.8.1-4

Ramos Valencia, M. V., Paredes Regalado, M. B., Layedra Larrea, N. P., & Salazar Cazco, S. A. (2025). Evaluación de ataques de denegación de servicio - insider - en redes definidas por software. Tesla Revista Científica, 5(1), e486. https://doi.org/10.55204/trc.v5i1.e486

Rojas Ortiz, Z. X. (2024). Cybersecurity and Cyber Defense in the Light of New Technologies in Cyberspace (pp. 15–29). https://doi.org/10.1007/978-3-031-52258-1_2

Tabares Parra, G. E., Cardona Patiño, C. A., Ramírez Triana, C. P., & Baez Rodríguez, H. L. (2024). Análisis de herramientas de Inteligencia Artificial en la Detección de ciberamenazas en Tiempo Real en el sector educativo. Revista Internacional de Investigación y Transferencia En Comunicación y Ciencias Sociales, 3(2), 114–133. https://doi.org/10.61283/hyqney43

Tenorio, J. (2022). REALIDAD AUMENTADA DE LA ESTACIÓN CONVEYOR DEL MPS BAJO EL MODELO DE DIGITAL TWIN [Universidad Politécnica Slesiana]. https://dspace.ups.edu.ec/bitstream/123456789/22281/1/UPS%20-%20TTS728.pdf

Torres Ventura, J., Ruelas Puente, A. H., & Herrera García, J. R. (2023). Rendimiento para la interoperabilidad entre Rasperry pi, ESP8266 y PLC con Node-RED para el IIoT. Ingenius, 29, 90–97. https://doi.org/10.17163/ings.n29.2023.08

Tudela, K. N. B., & Patilla, H. J. (2025). Security Onion as a Network Auditing Tool at the San Cristóbal de Huamanga National University. International Journal of Advanced Computer Science and Applications, 16(3). https://doi.org/10.14569/IJACSA.2025.0160314

Urbanovics, A. (2022). Cybersecurity Policy-Related Developments in Latin America. Academic and Applied Research in Military and Public Management Science, 21(1), 79–94. https://doi.org/10.32565/aarms.2022.1.6

Valencia Piedra, L. A., Guerrero Delgado, B. E., Torres Moscoso, D. F., & Fajardo Vásquez, D. (2023). Utilización de tecnología 5G en Cuenca. Ciencia Latina Revista Científica Multidisciplinar, 7(3), 6637–6648. https://doi.org/10.37811/cl_rcm.v7i3.6658

Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. Ius et Praxis, 053, 95–110. https://doi.org/10.26439/iusetpraxis2021.n053.4995

Viteri Hernández, C., & Ávila, D. (2024). Exploración integral de la seguridad en redes de proveedores de servicios de internet: Una revisión sistemática de literatura. Revista Perspectivas, 6(1). https://doi.org/10.47187/perspectivas.6.1.215

wireshark. (2025). Wireshark le permite analizar en profundidad el tráfico de su red: de forma gratuita y con código abierto.