UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE COMPUTACION

Evaluación de la efectividad de los sistemas de detección de intrusiones en redes, sus amenazas y vulnerabilidades

Trabajo de titulación previo a la obtención del
Título de Ingeniero/a en ciencias de la computación

AUTOR: JUAN DANIEL SANTILLAN CAMPUZANO

TUTOR: JOE FRAND LLERENA IZQUIERDO

Guayaquil – Ecuador

2025

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Juan Daniel Santillán Campuzano con documento de identificación N° 0952066116 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 14 de Julio del año 2025

Atentamente,

Juan Daniel Santillán Campuzano
0952066116

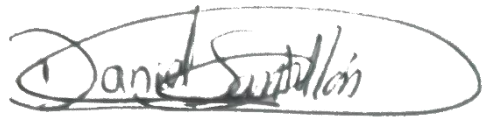
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Juan Daniel Santillán Campuzano con documento de identificación No. 0952066116, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del Artículo Académico: "Evaluación de la efectividad de los sistemas de detección de intrusiones en redes, sus amenazas y vulnerabilidades", el cual ha sido desarrollado para optar por el título de: Ingeniero de Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 14 de Julio del año 2025

Atentamente,



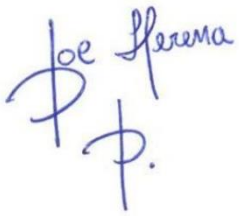
Juan Daniel Santillán Campuzano
0952066116

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Joe Frand Llerena Izquierdo con documento de identificación N° 0914884879, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: Evaluación de la efectividad de los sistemas de detección de intrusiones en redes, sus amenazas y vulnerabilidades, realizado por Juan Daniel Santillán Campuzano con documento de identificación N° 0952066116, obteniendo como resultado final el trabajo de titulación bajo la opción Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 14 de Julio del año 2025

Atentamente,



Joe Frand Llerena Izquierdo
0914884879

DEDICATORIA

Dedico este trabajo antes que todo a Dios el cual ha sido mi guía y fuerza para seguir adelante y no rendirme pese cualquier circunstancia y obstáculo que he enfrentado, a mis padres Juan Santillán y Annabelle Campuzano han sido mi motor para jamás rendirme, recibiendo su apoyo condicional constantemente, han sido mi inspiración, a ambos les agradezco infinitamente por ser ejemplo de amor, dedicación y sacrificio, quienes han sido un soporte inigualable en mi trayecto universitario, me han inculcado desde pequeño sus buenos valores y gracias a eso que ahora estoy culminando mi proyecto.

AGRADECIMIENTO

Agradezco en especial a Dios por ser siempre mi guía y camino ya que, sin Él, este logro no hubiera sido posible. A mis padres Juan Santillan y Annabelle Campuzano por ser siempre mi apoyo incondicional y a mi tutor Joe Frand Llerena por su gran orientación y apoyo constante.

RESUMEN

La evolución en tecnología ha traído un gran avance científico lo que consigo mismo ha llevado un aumento de amenazas y vulnerabilidades en las redes. Ante estas amenazas todas las organizaciones han implementado sistemas de seguridad cada vez más complejas, donde los sistemas de detección de intrusiones hacen un papel importante en proteger datos e infraestructura de la organización. Mientras tanto cabe recalcar que no todos los sistemas de detección son igualmente efectivos frente a la diversidad de ciber ataques que se presentan en el entorno.

En plena actualidad la mayoría de las organizaciones añaden IDS sin antes evaluarlos de una manera comparativa ante las circunstancias de las amenazas y vulnerabilidades la cual se vive en el presente. Esto provoca una percepción errónea de seguridad y la posibilidad de brechas que comprometan los activos críticos.

Es importante revisar en detalle cuánto realmente funcionan los sistemas de detección de intrusiones (IDS). Esto incluye cuánto detectan correctamente, cuántos errores cometen, qué tan resistentes son ante ataques y qué tan bien pueden adaptarse a las nuevas amenazas que van apareciendo.

Palabras claves: Evolución Tecnológicas, Avances científicos, Amenazas, Vulnerabilidades. Redes, Sistemas de detección de intrusos IDS

ABSTRACT

The evolution of technology has brought about great scientific advancements, which has led to an increase in network threats and vulnerabilities. In response to these threats, all organizations have implemented increasingly complex security systems, where intrusion detection systems play an important role in protecting the organization's data and infrastructure. It should be noted, however, that not all detection systems are equally effective against the diverse range of cyberattacks present in the environment.

Today, most organizations add IDS without first evaluating them comparatively against the current threat and vulnerability landscape. This leads to a misperception of security and the possibility of breaches that compromise critical assets. Therefore, there is a need for a comprehensive evaluation of the effectiveness of available IDS, considering their actual detection capacity, error rate, robustness against attacks, and adaptability to emerging threats.

Keywords: Technological Evolution, Scientific Advances, Threats, Vulnerabilities, Networks, Intrusion Detection Systems (IDS)

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

Los sistemas de detección de intrusos (IDS) han evolucionado significativamente con el uso de tecnologías inteligentes, especialmente mediante el aprendizaje automático y profundo (Castro Macías, 2022). Estas herramientas han transformado la forma en que se analiza el tráfico de red, permitiendo una mayor precisión en la identificación de amenazas y ataques cibernéticos (Villao González & López Zambrano, 2024). Aunque estos sistemas pueden funcionar bien en pruebas, todavía hay dudas sobre cómo se desempeñan en la vida real (Rigchc Mero, 2022). Muchos de los resultados que vemos en entornos controlados no se repiten igual cuando se usan en infraestructuras más complicadas. Se ha notado que algunos sistemas de detección de intrusiones, aunque funcionan bien en pruebas de laboratorio, pueden ser engañados por ataques donde se manipulan las muestras para evitar su detección (Peng et al., 2019).

Frente a esto, es importante revisar bien los IDS, no solo desde lo técnico, sino también considerando cómo funcionan en la práctica y en el contexto real.

Este estudio busca revisar diferentes tecnologías de detección de intrusiones, centrarse en cómo reaccionan a amenazas recientes y a nuevas vulnerabilidades, especialmente en redes 4G y 5G. El objetivo principal es ofrecer información que ayude a tomar decisiones más acertadas y estratégicas a la hora de crear infraestructuras de ciberseguridad que sean resistentes y puedan adaptarse a los cambios.

Varios estudios han mostrado que las técnicas modernas, como las redes neuronales profundas (Lara Bautista, 2025), realmente mejoran cómo funcionan los sistemas de detección de intrusiones, sobre todo cuando se trata de manejar mucho data y patrones complicados (Niyaz et al., 2015). Estos modelos suelen memorizar muy bien los datos con los que los entrenan, pero en situaciones más complicadas, pueden ser atacados por agentes externos (García Pérez, 2024). Es importante determinar objetivamente qué tan bien detecta patrones, asimismo determinar falsos positivos y negativos, valorar la eficiencia y especificar cómo se adapta a amenazas que no se conocen todavía (Holguín Mendoza, 2021; Villamar Arellano, 2023).

Los sistemas de detección de intrusiones (IDS) son una herramienta importante para vigilar el tráfico de la red en tiempo real (Vintimilla Murillo & Sánchez Manzaba, 2024). Ayudan a detectar a tiempo actividades peligrosas, como exploraciones de puertos, intentos de entrar sin permiso o la presencia de malware (Liao et al., 2013)(Gallegos Manrique & Lynch Escobar, 2024).

En varios estudios se identifican a los sistemas antiguos que usan firmas para detectar intrusiones son útiles, pero no logran identificar las amenazas que van surgiendo (Aroca Cedeño, 2024). Muchas investigaciones han mostrado que las técnicas modernas, como las redes neuronales profundas, mejoran mucho cómo funcionan los sistemas de detección de intrusiones (IDS). Esto es especialmente cierto cuando se trata de manejar grandes cantidades de datos y encontrar patrones complicados (Niyaz et al., 2015).

Estos modelos también tienen sus fallos. A veces aprenden tan bien los datos con los que los entrenan que se vuelven inexactos para adaptarse a situaciones difíciles. Es importante revisar qué tan bien pueden detectar las amenazas, cuántas veces se equivoca diciendo que algo es peligroso o no lo es, cuánto funciona en realidad y qué tan bien pueden adaptarse cuando aparecen peligros y riesgos que no se conocía antes.

Los IDS son una herramienta muy importante para vigilar el tráfico de red en tiempo real. Ayudan a detectar temprano actividades peligrosas, como escaneos de puertos, intentos de entrar sin permiso o la instalación de malware (Liao, Richard Lin, et al., 2013)

Aunque son útiles, muchos sistemas tradicionales de detección de intrusiones con firmas no logran ponerse al día con las amenazas nuevas. Esto pasa porque dependen mucho de bases de datos con patrones predefinidos. Esta limitación muestra lo importante que es usar métodos para detectar anomalías (Chévez Morán, 2021). Así, podemos identificar cuando algo se sale de lo habitual, ya sea usando modelos de referencia o aprendizaje que se actualiza constantemente (Mohammadian et al., 2022).

Este trabajo no solo busca comparar cómo funcionan distintos sistemas de detección de intrusiones en situaciones complicadas, sino también ofrecer ideas prácticas para que las organizaciones puedan usarlos de forma más efectiva (Baidal Perero & Quinde Cruz, 2024; Molina Estupiñán, 2025).

Esto es especialmente importante para áreas que necesitan una seguridad muy fuerte, como el sector financiero, y también en entornos que cambian rápido, como las redes 5G (Medina Astudillo, 2024; Nazwita & Ramadhani, 2017).

2. REVISIÓN DE LITERATURA

La literatura actual sobre ciencia explica bastante bien cómo avanzan las cosas y qué dificultades surgen al poner en marcha los sistemas de detección de intrusiones en redes (Lim et al., 2024a; Mugoniwa et al., 2023; Teixeira et al., 2019).

Con lo complicado que se ha puesto el tráfico de red y lo avanzadas que están las amenazas, cada vez se investiga más en soluciones que usan inteligencia artificial, aprendizaje profundo y técnicas modernas para recopilar y analizar datos (Jackson et al., 2025; Jin et al., 2025; Liao, Lin, et al., 2013; Marsilio et al., 2025; Pretolesi et al., 2025).

Estas herramientas están diseñadas para enfrentar los nuevos desafíos en ciberseguridad, especialmente en entornos muy dinámicos como las redes 4G y 5G (Allahrakha, 2024; Y. S. Chen et al., 2025; Sekhar et al., 2025). Allí, la rapidez y la gran variedad de dispositivos conectados crean obstáculos que no siempre son fáciles de superar (Jia et al., 2021).

2.1 Evaluación basada en datos de detectores de intrusiones: Un marco metodológico

15º Simposio Internacional sobre Prácticas de Seguridad en 2022, que tuvo lugar en Ottawa, Canadá, incluyó una charla donde se explicó un método para usar datos al evaluar los IDS (Jamal et al., 2023a). La investigación señala que, aunque se han probado varias técnicas de aprendizaje automático, muchas de ellas no han cambiado mucho con el tiempo, lo que hace que a veces no sean tan efectivas en situaciones nuevas. Es importante contar con métodos sólidos para evaluar qué tan bien funcionan los sistemas de detección de intrusiones. Esto incluye tener en cuenta diferentes tipos de ataques, los cambios en el tráfico de red y las distintas configuraciones de los entornos donde se usan (Alawida et al., 2024; Y. S. Chen et al., 2025; Huma et al., 2021; Nevmerzhitskaya et al., 2019).

El estudio dice que, para evaluar bien los IDS, hay que usar conjuntos de datos que muestren cómo funcionan en situaciones reales, con tráfico normal y sospechoso mezclados. Ejemplos de estos conjuntos son NSL-KDD, CICIDS2017 y UNSW-NB15 (Maseer et al., 2024). Estos conjuntos de datos permiten simular diferentes situaciones, incluyendo ataques de denegación de servicio (DoS), intrusiones internas y métodos para evadir detecciones, todo con características estadísticas importantes. También se habla de lo importante que es usar más que solo precisión para medir cómo funciona el sistema. Mencionan cosas como la tasa de falsos positivos, la tasa de aciertos verdaderos y el valor F1, porque así se obtiene una evaluación más justa y realista del rendimiento. Además, (Jamal et al., 2023a) recomienda agregar entornos de prueba que usen tráfico cifrado y que tengan cambios en la estructura de la red. Así, las pruebas reflejarán mejor cómo son las infraestructuras en la realidad hoy en día.

Esto demuestra que el IDS puede seguir funcionando bien incluso cuando hay más uso de VPN, HTTPS y otros túneles cifrados, que son bastante comunes en las redes de las empresas.

El estudio también señala que no hay un método y uniforme para evaluar los IDS, lo que hace que los resultados de diferentes investigaciones no sean muy comparables. Esto complica el progreso en el área.

2.2 Evaluación de IDS en entornos adversarios mediante aprendizaje profundo

El trabajo de (Peng et al., 2019) muestra que hace una contribución importante al analizar qué tan fuertes son los sistemas de detección de intrusos (IDS) que usan aprendizaje profundo (DL) cuando enfrentan ataques maliciosos.

Con el conjunto de datos NSL-KDD, que es muy conocido por tener diferentes tipos de tráfico de red y ataques simulados, los autores entrenaron y compararon cómo funcionaban cuatro modelos diferentes. Las redes neuronales profundas (DNN), máquinas de vectores de soporte (SVM), bosques aleatorios (RF) y regresión logística (LR) son modelos que fueron sometidos a pruebas bajo condiciones hostiles mediante técnicas de generación de ejemplos adversarios, como el ataque de descenso de gradiente proyectado (PGD), el método iterativo de señal de gradiente rápida (FGSM), el ataque L-BFGS y el ataque SPSA (Kovács & Ghous, 2020).

Los resultados muestran que los clasificadores pierden mucho en precisión y fiabilidad cuando se enfrentan a entradas que han sido manipuladas de forma intencional para engañarlos (Denham et al., 2012; Falowo et al., 2024; Maharani, 2022).

Por ejemplo, el rendimiento de las DNN, que inicialmente presentaban altas tasas de detección, se redujo en más del 40% en ciertos casos adversarios, lo cual sugiere una vulnerabilidad crítica en entornos donde los atacantes tienen la capacidad de alterar mínimamente los datos de entrada (Peng et al., 2019).

Esta investigación resalta la urgencia de incorporar mecanismos de defensa robustos en los IDS modernos, tales como técnicas de entrenamiento adversario, defensas por distorsión, y validaciones cruzadas con tráfico cifrado y legítimo. Asimismo, plantea la necesidad de utilizar evaluaciones más realistas que contemplen no solo ataques directos, sino también la manipulación sutil del entorno de red para evadir la detección. En este contexto, los sistemas que se entrenan y validan únicamente en entornos limpios o estáticos podrían generar una falsa percepción de seguridad al no considerar el espectro completo de amenazas adaptativas.

El estudio dice que mezclar métodos tradicionales con redes neuronales profundas puede ser una buena estrategia. Si se ajustan bien a diferentes situaciones, estos enfoques híbridos parecen ser más fuertes y resistentes ante cambios.

Esto evidencia que la seguridad basada en DL no debe depender exclusivamente de la precisión bajo condiciones ideales, sino también de su capacidad de adaptación y robustez frente a ataques que buscan intencionalmente degradar el rendimiento del sistema.

2.3 Preservación de la privacidad en IDS

Proteger la privacidad de los usuarios es muy importante cuando se trata de sistemas que detectan intrusiones, especialmente en áreas como la banca, la salud y el gobierno.

En este sentido, el estudio de (Lu et al., 2021) examina qué tan bien funcionan diferentes clasificadores en conjuntos de datos que han sido anonimizados. Muestra que se puede detectar amenazas con precisión bastante alta sin sacrificar la privacidad de las personas.

Se usa IBM SPSS Modeler para analizar un conjunto de datos de tráfico de red que ya había sido anonimizado. Se aplican técnicas como árboles de decisión, redes neuronales, SVM y Naive Bayes para examinar la información. Se analizan algunas métricas de rendimiento como la precisión, el recall, el puntaje F1 y también cuántos falsos positivos. Por ejemplo quitar el nombre a los atributos no hace que los modelos tengan más problemas para detectar patrones peligrosos. Ese es uno de los puntos más importantes del estudio.

Los clasificadores de aprendizaje automático funcionan bien es diferentes condiciones, lo que muestra que, si se hace bien, las técnicas de anonimización no arruinan la información clave que se necesita para detectar algo de manera efectiva. Esto afecta directamente cómo se usan los sistemas de detección de intrusiones en la vida real, especialmente en lugares donde hay que seguir reglas de privacidad como el RGPD o la HIPAA.

En este contexto, lo que tendría sentido sería empezar a usar sistemas de detección que funcionen bien con técnicas de privacidad diferencial o aprendizaje federado.

Estas formas de entrenamiento hacen que los modelos detecten cosas en diferentes lugares, sin tener que juntar todos los datos sensibles en un solo sitio.

Esto hace que sea menos probable que se dañen y también ayuda a seguir las reglas de protección de datos.

También, usar técnicas de anonimización sintética, como las GANs para crear datos falsos que parecen reales, parece ser una opción muy interesante para proteger la privacidad. Esto es especialmente útil en situaciones donde diferentes organizaciones necesitan compartir datos para trabajar juntas en análisis de ciberseguridad.

2.4 IDS en redes 4G/5G y amenazas emergentes

La llegada rápida de las redes móviles 4G y 5G ha traído varios retos para la seguridad en línea. Estas tecnologías no solo hacen que transferir datos sea mucho más rápido y que puedan conectarse más dispositivos, sino que también abren más puntos por donde los hackers pueden atacar. Esto hace que las redes sean más vulnerables a nuevos tipos de ataques, incluyendo intrusiones distribuidas y amenazas que persisten por mucho tiempo (Bodnar et al., 2013; Eyeleko & Feng, 2023; Ott & Sethmann, 2010). (Cheminod et al., 2013) destacaron que las redes de estas redes necesitan reglas más claras y medidas de seguridad más completas, especialmente porque están conectadas con sistemas industriales, autos autónomos y dispositivos IoT. Asimismo, (Sheatsley et al., 2022) advierte advierte que están aumentando los ataques de denegación de servicio (DoS), el suplantamiento de identidad y los escaneos automáticos. Estos métodos aprovechan la complejidad y variedad del entorno 5G para pasar desapercibidos de las soluciones clásicas de detección.

Con todo esto en cuenta, los sistemas para detectar intrusiones necesitan ponerse al día y usar métodos más avanzados, como el aprendizaje profundo y el aprendizaje automático.

Las máquinas de vectores de soporte (SVM) han mostrado que son muy buenas para distinguir entre tráfico normal y raro, incluso en lugares donde los datos cambian mucho (Xia & Ouyang, 2025; W. L. Zhao et al., 2025). Por otro lado, las redes neuronales convolucionales (CNN) ayudan a detectar patrones en los datos de tráfico, sin necesidad de crear reglas o características específicas a mano (L. Y. Chen et al., 2025; Ferreira et al., 2025; Kuang et al., 2025; Sahnoun et al., 2025; X. P. Wang et al., 2025; Zeng et al., 2025).

Un avance nuevo es la creación de datos falsos usando redes generativas adversarias (GAN). Esto ayuda a entrenar sistemas de detección de intrusiones (IDS) en situaciones simuladas, incluso si esos ataques nunca han ocurrido antes (Gangadharan et al., 2025; Kumar et al., 2025; Vobugari et al., 2022).

Esto hace que el sistema sea mejor en detectar nuevas amenazas, en comparación con los métodos solo supervisados que usan muestras que ya están etiquetadas.

En realidad, están probando combinaciones de diferentes tipos de modelos, como autoencoders, GAN y árboles de decisión, para mejorar la precisión y la estabilidad en la detección (Lim et al., 2024b).

En este contexto, los sistemas IDS suelen dividirse en dos tipos: los que detectan usando firmas (Signature-based IDS o DIDS) y los que buscan anomalías (Anomaly-based IDS o AIDS).

Los DIDS se destacan por su baja tasa de falsos positivos y alta precisión frente a amenazas conocidas, ya que comparan el tráfico con patrones previamente almacenados (Amjad et al., 2025; An & Zhang, 2024; Kokoç et al., 2021; G. Q. Liu et al., 2025; Morís et al., 2025; Mtebe & Kondoro, 2019; Q. Wang et al., 2025; J. Y. Zhao et al., 2025).

Pero todavía no son muy buenos para detectar ataques nuevos o raros (M. J. Chen et al., 2025; Cui et al., 2025; Jiang et al., 2025; Yuan et al., 2025; Zheng et al., 2025; Zhou et al., 2025). En cambio, los IDS buscan patrones de comportamiento que no son comunes, lo que los hace útiles para identificar amenazas que aún no se conocen bien, aunque eso también significa que usan más recursos y pueden generar más alertas falsas (Suresh et al., 2024).

Para resumir, pasar a redes 4G y 5G significa que los sistemas de detección de intrusiones necesitan ajustarse. Esto incluye tener en cuenta los ambientes móviles, el cifrado de extremo a extremo, varios puntos de acceso y la capacidad de crecer y adaptarse rápidamente (Jamal et al., 2023b; R. Y. Liu et al., 2025; Zhang et al., 2025; D. W. Zhao et al., 2025).

Solo con modelos que mezclen inteligencia artificial y datos que se actualizan en tiempo real, podremos detectar y responder mejor a las amenazas en el mundo del 5G.

3. METODOLOGÍA

Esta investigación utiliza una metodología de investigación analítica descriptiva y un enfoque práctico, enfocado en identificar las vulnerabilidades, amenazas y riesgos que existen en una red financiera.

Estos tres conceptos están muy relacionados, pero tienen diferencias importantes.

Vulnerabilidades: son esas fallas o puntos débiles en sistemas, ya sea en el software, en la infraestructura física o en las personas (como falta de entrenamiento). Estas fallas pueden ser aprovechadas por amenazas para causar problemas.

Amenazas: Amenazas son cosas que ocurren o acciones que toman ventaja de puntos débiles para hacer daño.

Estas pueden ser cosas que hacemos a propósito, como ciberataques, o accidentes que ocurren sin querer, como desastres naturales.

Riesgos: Surgen de la combinación entre amenazas y vulnerabilidades. Indican qué tan probable es que pase algo malo y cuánto podría afectarlo.

Para bajar los riesgos, se recomiendan algunas medidas técnicas de seguridad.

- Antivirus, firewall, antimalware
- VPN y gestión de contraseñas
- Sistemas de detección de intrusos (como Suricata)
- Políticas de respaldo y actualización continua

Elegimos Suricata para la evaluación. Es un sistema de detección y prevención de intrusiones que es de código abierto. Puede revisar los datos que pasa por la red en detalle, relacionar eventos y analizar el tráfico en tiempo real.

Esta herramienta se implementó en una empresa financiera de mediano tamaño dedicada a servicios de crédito, con una red de aproximadamente 100 dispositivos, servidores internos y conexión a servicios en la nube.

La elección de este escenario se debe a que las instituciones financieras son uno de los blancos más frecuentes de ataques como phishing, escaneo de puertos, infección por malware y ex filtración de datos.

4. RESULTADOS

Para escribir este ensayo, primero se hace una simulación, y luego se instala la herramienta IDS en una organización del sector financiero que principalmente otorga créditos.

La organización tiene una red que incluye unos 100 dispositivos, servidores propios y un intercambio continuo con servicios en la nube. Todo eso hace que gestionar la seguridad informática sea un reto complicado y siempre cambiante (Gómez Castaño et al., 2023).

Este entorno se eligió por una razón: las instituciones financieras suelen ser un blanco principal para los ciberataques. Los hackers usan métodos como el phishing, el escaneo de puertos, el malware y la filtración de datos para atacarles.

En este contexto, detectar cosas en tiempo real es clave para asegurarse de que la información se mantenga segura y confiable.

Herramientas avanzadas como Suricata, que usan una arquitectura con inspección profunda de paquetes (Deep Packet Inspection), tienen un procesamiento muy rápido y mecanismos para relacionar eventos, las hacen ideales para entornos muy exigentes como el sector financiero (Nyasore et al., 2020).

Después de un tiempo probándolo, los resultados fueron bastante claros y mostraron que la organización mejoró mucho en detectar y enfrentar amenazas.

Antes Antes de poner en marcha una herramienta IDS, la empresa solía tener alrededor de 16 incidentes de seguridad cada año, según lo que reportan otras empresas del sector financiero. (Kaspersky, 2023). Con una herramienta IDS en funcionamiento como Suricata, esta cifra se redujo drásticamente en un 50%, situándose en 8 eventos por año. Esta disminución a la mitad no solo representa un número; representa una reducción considerable en la exposición al riesgo y en las potenciales interrupciones operativas.

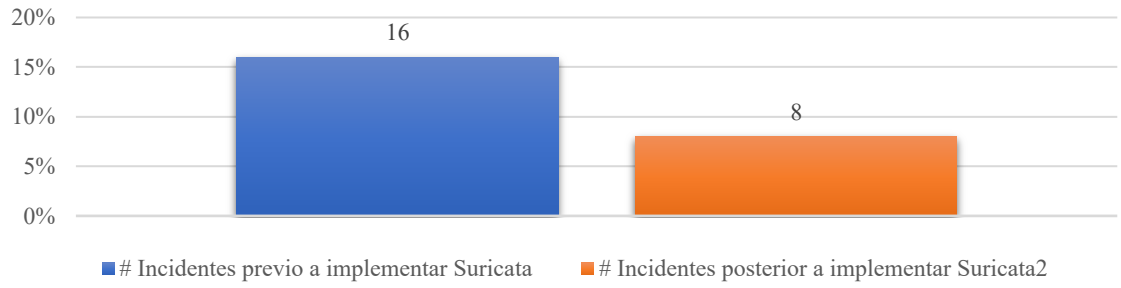


Figura 1 Reducción de Incidentes de Seguridad Anuales

Las métricas obtenidas durante la simulación de tráfico real, específicamente para el sector financiero, consolidaron la capacidad de Suricata como un IDS robusto:

Tasas de Detección (TPR): Una capacidad extremadamente alta para identificar amenazas. La detección de escaneos de puertos alcanzó un 99.3%, mientras que la identificación de ataques de Denegación de Servicio (DoS) y otras intrusiones superó el 94%. En promedio, la Tasa de Verdaderos Positivos (TPR) se mantuvo en un rango del 97% al 98%, un rendimiento que se alinea con los estándares observados en estudios comparativos de la industria. Esto significa que Suricata es excepcionalmente bueno para 'ver' lo que los atacantes intentan hacer.

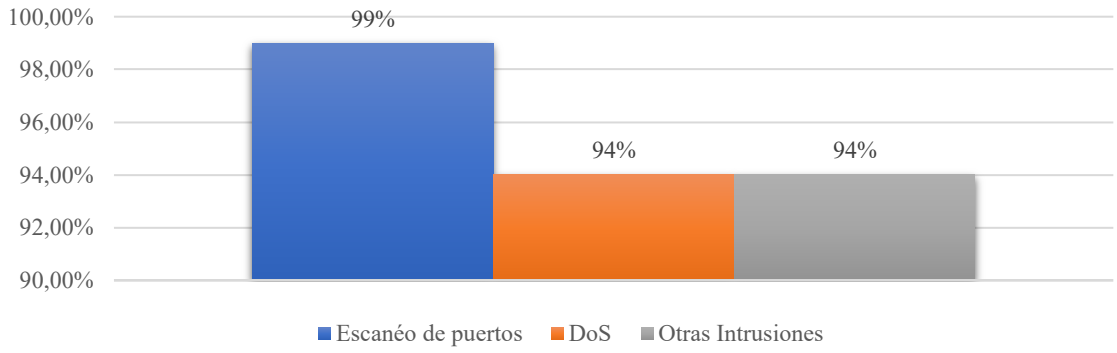


Figura 2 Tasa de Detección de Verdaderos Positivos (TPR) por Tipo de Amenaza

Tasa de Falsos Positivos (FPR): A pesar de la alta precisión, se evidenció una proporción notable de alertas incorrectas. La Tasa de Falsos Positivos (FPR) osciló entre el 15% y el 20% del volumen de tráfico analizado. Este hallazgo, consistente con investigaciones previas, subraya que, aunque Suricata detecta mucho, también genera cierto "ruido" que requiere atención manual. Es el costo de una vigilancia tan exhaustiva.

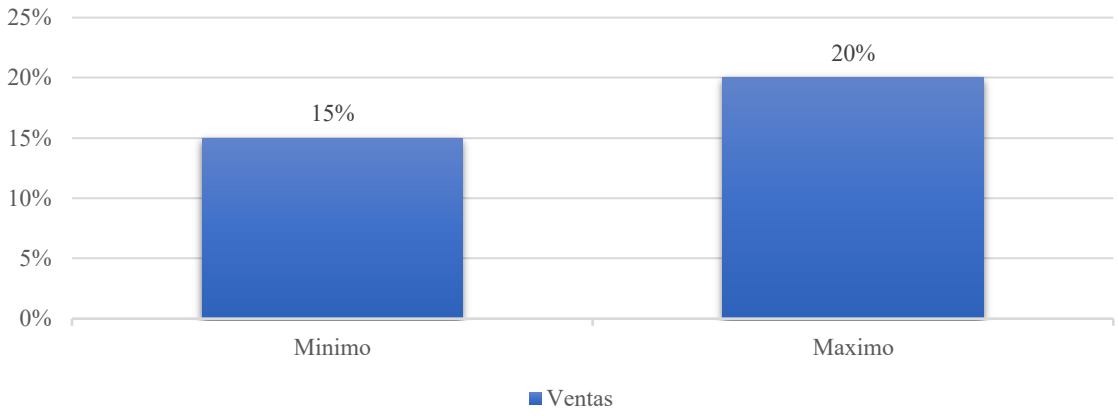


Figura 3 Tasa de Falsos Positivos (FPR)

Volumen de Tráfico Inspeccionado: Suricata demostró una resiliencia notable al procesar volúmenes significativos de tráfico simulado, incluyendo flujos simultáneos y datos cifrados, sin mostrar signos de sobrecarga. Su diseño con arquitectura multihilo le permitió gestionar eficientemente varios gigabits por segundo de tráfico, replicando condiciones reales y confirmando su capacidad para mantener un rendimiento consistente bajo alta demanda. Es decir, no se "ahoga" cuando el tráfico se intensifica.

Tipos de Amenazas Detectadas: Entre las amenazas exitosamente identificadas por Suricata se incluyen barridos de red, ataques de Denegación de Servicio (DoS), distribución de malware y simulaciones de intentos de phishing. En la mayoría de los casos, Suricata emitió alertas oportunas, especialmente en las fases iniciales de reconocimiento y explotación. Sin embargo, la mencionada proporción de falsos positivos implica que una revisión manual de algunas notificaciones, que resultan inofensivas, sigue siendo una parte esencial del proceso operativo.

Más allá de las métricas técnicas, la implementación de Suricata generó beneficios operativos y económicos directos:

Mejoras en el Tiempo de Respuesta del Equipo de TI: Se observó una mejora sustancial en la eficiencia del equipo de Tecnologías de la Información (TI). Antes de Suricata, los analistas

demoraban aproximadamente 50 minutos en detectar eventos críticos. Integrar las alertas en tiempo real y los logs detallados hizo que ese proceso bajara a 30 minutos, que es un 40% más rápido.

Esta rapidez no solo hace que todo sea más seguro, sino que también ayuda a que los técnicos trabajen más rápido y sean más efectivos.

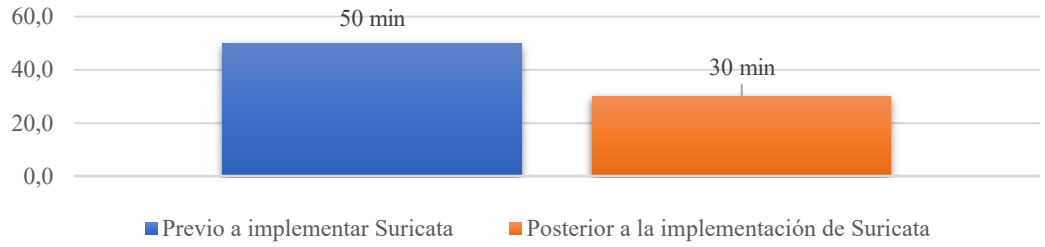


Figura 4 Mejora en el Tiempo de Respuesta del Equipo de TI

Ahorro en Pérdidas Operativas: Reduciendo la cantidad de incidentes y respondiendo más rápido, la entidad pudo evitar pérdidas económicas importantes.

Se calcula que bloquear al menos dos ataques graves al año, como los de phishing que roban credenciales o filtran datos, evita pérdidas de casi $100.000 en cada caso.

Este ahorro adicional de $200,000 al año viene de eventos que nunca llegaron a causar problemas operativos.

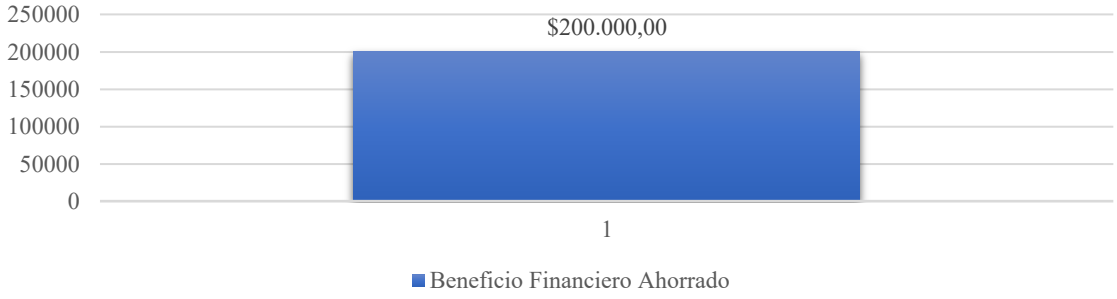


Figura 5 Ahorro Económico Anual Estimado

En resumen, al poner Suricata en esta empresa financiera, pudimos comprobar que funciona bien. Ayudó a reducir los problemas de seguridad a la mitad y detectó la mayoría de las amenazas, con una precisión promedio del 97%.

cibernética fuerte, sino que también vale la pena como inversión en ambientes financieros que son muy riesgosos.

Comparación de Suricata y OSSEC

Podemos decir que el IDS Suricata es esencial para el monitoreo de trafico de red en busca de patrones sospechoso, este detecta intrusos y los previene la cual tiene un alta capacidad en análisis y soporte. Mientras tanto OSSEC se centra en monitorear la actividad en los servidores y endpoint, revisando registros, realizando auditorias de archivos, detectando rootkits y otros comportamientos sospechosos en los sistemas, su funcionalidad es el monitoreo de logs es monitorear, la integridad de archivo el cual revisa si hay cambios en archivos críticos del sistema y posee respuesta automatizada.

Juntos puede proporcionar una defensa en profundidad: Suricata supervisando el trafico de red para detectar ataques externos y OSSEC monitoreando lo que sucede dentro de los servidores y sistemas, gestionando eventos y asegurando que no haya compromisos internos.

5. DISCUSIÓN

Este estudio está en línea con investigaciones previas, como la de (Javaid, 2016) esto significa que los sistemas de detección de intrusos que usan aprendizaje profundo realmente funcionan mejor contra amenazas complicadas, especialmente cuando hay muchos datos involucrados.

A pesar de eso, también hay algunos inconvenientes, como que estos sistemas pueden ser engañados o confundidos por ataques creados para arruinar su funcionamiento.

Aunque es bastante preciso, todavía a veces detecta cosas que parecen amenazas, pero en realidad no lo son. Esto muestra lo importante que es juntar métodos diferentes, mezclando el aprendizaje supervisado con entender cómo se comporta el sistema.

Por otro lado, como Suricata es una herramienta abierta, es mucho más fácil adaptarla a las necesidades específicas de la empresa y ajustarla a lo que realmente importa en ese contexto.

Suricata offers some technical advantages over other intrusion detection systems like Snort and Zeek (which was previously called Bro).

Algunos estudios, como el de (Kumar Ahuja & Kumar, 2014). Suricata funciona mejor y es más preciso que Snort, especialmente cuando hay mucho tráfico en la red. Esto se debe a que está diseñado para manejar varias tareas a la vez de manera eficiente.

Zeek se centra en analizar el comportamiento y modelar eventos, por lo que resulta una herramienta útil para integrar con otros sistemas. Sin embargo, no detecta ataques activos de inmediato con la misma rapidez. Mientras tanto, investigaciones como las de Waleed y sus colegas (Waleed et al., 2022) destacan que es realmente bueno para realizar una verificación

profunda y consciente del contexto, lo que puede ayudar a reducir muchas falsas alarmas cuando lo usa junto con herramientas como Suricata.

Al comparar cómo funciona Suricata con otros sistemas que combinan detección por firmas y técnicas de aprendizaje profundo, se nota que mejora bastante tanto en precisión como en eficiencia.

Un estudio llevado a cabo por (Fotiadou et al., 2021), en 2021, un estudio centrado en detectar anomalías en redes definidas por software (SDN) encontró que los métodos híbridos que usan aprendizaje profundo superaron a Suricata. Estos enfoques lograron una tasa de detección del 99,2 % y redujeron los falsos positivos al 5,6 %.

Estos resultados muestran que, aunque Suricata es una herramienta fuerte y bastante conocida, su rendimiento puede mejorar mucho si se combina con técnicas modernas de análisis inteligente. Las estrategias recientes que usan aprendizaje por conjuntos y selección de características han demostrado ser bastante prometedoras para detectar intrusiones. (Espinosa Zúñiga, 2020), por ejemplo, aplicó algoritmos como Random Forest, CatBoost y XGBoost, junto con técnicas de selección de características, logrando desarrollar un modelo que no solo mejora la precisión, sino que también reduce significativamente el tiempo de procesamiento. Esto lo convierte en una solución viable para integrarse con sistemas IDS como Suricata. Esto enfoca a un diseño más eficiente, en el que el IDS funcione como uso de sensor principal fusionado por modelos analíticos en entornos dinámicos. En un mundo como el internet de las cosas, donde se producen diferentes tipos de tráfico en orden y en mayor cantidad.

Cada vez los IDS tradicionales son más evidentes. (Beatriz Parra de Gallo, 2022), después de hacer análisis exhaustivo sobre el uso de aprendizaje para la detección de intrusiones en redes del internet de las cosas. Se muestra que los modelos que están basados en aprendizaje automático muestran un resultado eficiente y que es adaptable frente a amenazas el cual son variables. Este resultado significa mucho para las próximas generaciones, y usar herramientas como Suricata sería de gran ayuda en esto.

Sobre todo, lo que es en entorno distribuidos y móviles. (Perdigón Llanes, 2022) se evalúa entorno con mayor cantidad en el tráfico de red, usando hardware especializados como los procesadores Kunpeng 920, dando a conocer que el sistema opera de manera eficiente a velocidades de hasta 20 Gbps. Su rendimiento realmente depende de cómo se ajusten las reglas, de escoger bien motores de búsqueda como Hyperscan y de manejar cuidadosamente la infraestructura que lo soporta. Estos resultados muestran que Suricata puede manejar más carga

sin problemas, siempre y cuando se configure y administre de manera adecuada. También es importante recordar que, aunque los modelos de inteligencia artificial son muy buenos en muchas cosas, necesitan seguir aprendiendo y actualizándose constantemente para poder hacer frente a nuevas amenazas.

6. CONCLUSIÓN

La era digital ha hecho que la informática sea clave para empresas y organizaciones públicas, y eso ha puesto la ciberseguridad en un lugar cada vez más importante.

Los Sistemas de Detección de Intrusos (IDS) se han convertido en herramientas muy importantes. Su tarea principal es detectar y bloquear accesos no autorizados antes de que puedan dañar o comprometer la información.

Pensando en las amenazas y problemas que enfrenta este sector, los datos muestran que contar con un sistema de detección de intrusiones sólido realmente marca la diferencia.

De hecho, los incidentes de seguridad que pasan cada año se reducen a la mitad. Diferentes formas de medir cómo detectamos amenazas muestran que somos bastante buenos. La tasa de verdaderos positivos (TPR) suele estar entre el 97% y el 98%, lo que significa que detectamos la mayoría de las amenazas reales. Además, escaneos de puertos alcanzan una efectividad del 93%, y en ataques de Denegación de Servicio (DoS), logramos detectar más del 94%. Todo esto demuestra que tenemos una capacidad sólida para identificar una variedad amplia de amenazas en línea.

La evaluación también mostró que hay algunos problemas importantes, sobre todo con la cantidad de falsos positivos, que están entre el 15 % y el 20 %. Esta situación puede cansar mucho a los equipos de seguridad, hacer que se satures con alertas y hacer que gasten tiempo y recursos en investigar cosas que en realidad son inofensivas.

La implementación efectiva de herramientas IDS no depende únicamente de la capacidad tecnológica, sino también de una inversión constante en personal cualificado y una infraestructura adaptable.

Este estudio ofrece información importante que ayuda a tomar mejores decisiones estratégicas. También ayuda a construir infraestructuras de ciberseguridad que sean más resistentes y flexibles, para mantenerse al día en un mundo digital que cambia constantemente.

7. REFERENCIAS

Alawida, M., Abu Shawar, B., Abiodun, O. I., Mehmood, A., Omolara, A. E., & Al Hwaitat, A. K. (2024). *Unveiling the Dark Side of ChatGPT: Exploring Cyberattacks and Enhancing User Awareness*. *15*(1). https://doi.org/10.3390/info15010027

Allahrakha, N. (2024). *Global perspectives on cybercrime legislation*. *8*(10). https://doi.org/10.24294/jipd.v8i10.6007

Amjad, A., Huroon, A. M., Chang, H. T., & Tai, L. C. (2025). Dynamic fire and smoke detection module with enhanced feature integration and attention mechanisms. *PATTERN ANALYSIS AND APPLICATIONS*, *28*(2). https://doi.org/10.1007/s10044-025-01461-6 WE - Science Citation Index Expanded (SCI-EXPANDED)

An, S., & Zhang, S. (2024). Effects of ability grouping on students' collaborative problem solving patterns: Evidence from lag sequence analysis and epistemic network analysis. *Thinking Skills and Creativity*, *51*. https://doi.org/10.1016/j.tsc.2023.101453

Aroca Cedeño, J. G. (2024). *Análisis técnico y ético del uso de arte generativo con redes generativas adversarias* [{B.S.} thesis].

Baidal Perero, M. V., & Quinde Cruz, P. A. (2024). *Revisión de literatura sobre el alcance tecnológico de MPLS y GPON en el contexto ecuatoriano* [{B.S.} thesis]. https://dspace.ups.edu.ec/handle/123456789/28120

Beatriz Parra de Gallo, H. (2022). Proposal for a Forensic Action Guide for Internet of Things (IoT) Environments. In *Computacion y Sistemas* (Vol. 26, Issue 1, pp. 441–460). Instituto Politecnico Nacional. https://doi.org/10.13053/CyS-26-1-3898

Bodnar, C., Schanck, J. F., Raghavan, K., Smith, N. G., Hess, K., Buirge, B. M., Melvin, R., & Hackett, B. (2013). Work in progress: Starfish schoolhouse: Development of a story based elearning module to teach regenerative medicine concepts to middle and high school students and teachers. *ASEE Annual Conference and Exposition, Conference Proceedings*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84884343188&partnerID=40&md5=ddbec47e02c5e32b30873a95e49348de

Castro Macías, B. A. (2022). *Modelos de seguridad, acciones y protocolos para la prevención de vulnerabilidades de la seguridad de la información mediante las tecnolog{\'\i}as IOT Y API RESTFUL* [{B.S.} thesis]. https://dspace.ups.edu.ec/handle/123456789/23329

Cheminod, M., Durante, L., & Valenzano, A. (2013). Review of security issues in industrial networks. *IEEE Transactions on Industrial Informatics*, *9*(1). https://doi.org/10.1109/TII.2012.2198666

Chen, L. Y., Cao, Z., Zhang, W. J., Tang, X., Zhao, D., Zhang, D. Q., Liao, H. E., & Chen, F. (2025). Thinking Like Sonographers: Human-Centered CNN Models for Gout Diagnosis From Musculoskeletal Ultrasound. *IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING*, *72*(4), 1508–1518. https://doi.org/10.1109/TBME.2024.3510275 WE - Science Citation Index Expanded (SCI-EXPANDED)

Chen, M. J., Xu, H., & Lv, P. (2025). Semantic-Aware Global and Local Fusion Model for Image Enhancement. In Z. Lin, M. M. Cheng, R. He, K. Ubul, W. Silamu, H. Zha, J. Zhou, & C. L. Liu (Eds.), *PATTERN RECOGNITION AND COMPUTER VISION, PT IX, PRCV 2024* (Vol. 15039, Issues 7th Chinese Conference on Pattern Recognition and Computer Vision, pp. 27–41). https://doi.org/10.1007/978-981-97-8692-3_3 WE - Conference Proceedings Citation Index - Science (CPCI-S)

Chen, Y. S., Huang, H. Z., Li, J., Zheng, Z. J., Gao, F. J., Han, X. G., & Gao, Y. L. (2025). Digital twin comprehensive models: a study of ancient tree ecological environment quality assessment based on a cyber-physical system. *ENVIRONMENTAL MONITORING AND ASSESSMENT*, *197*(4).

https://doi.org/10.1007/s10661-025-13923-9 WE - Science Citation Index Expanded (SCI-EXPANDED)

Chévez Morán, M. J. (2021). *Estudio de los patrones de seguridad para la atenuación de las irregularidades, las debilidades y amenazas en empresas de servicios de telecomunicaciones*. http://dspace.ups.edu.ec/handle/123456789/20568

Cui, J. R., Sun, H. S., Zhao, M., Kuang, C. W., & Xu, Y. (2025). A Faster Fire Detection Network with Global Information Awareness. In Z. Lin, M. M. Cheng, R. He, K. Ubul, W. Silamu, H. Zha, J. Zhou, & C. L. Liu (Eds.), *PATTERN RECOGNITION AND COMPUTER VISION, PRCV 2024, PT XII* (Vol. 15042, Issues 7th Chinese Conference on Pattern Recognition and Computer Vision, pp. 361–375). https://doi.org/10.1007/978-981-97-8858-3_25 WE - Conference Proceedings Citation Index - Science (CPCI-S)

Denham, A. R., Gonzalez-Sanchez, J., Chavez-Echeagaray, M.-E., & Atkinson, R. K. (2012). Mobile applications as tools to support embodied learning: Current practice and future directions. *International Journal of Cyber Behavior, Psychology and Learning*, *2*(4), 1 – 16. https://doi.org/10.4018/ijcbpl.2012100101

Espinosa Zúñiga, J. J. (2020). Aplicación de algoritmos Random Forest y XGBoost en una base de solicitudes de tarjetas de crédito. *Ingeniería Investigación y Tecnología*, *21*(3). https://doi.org/10.22201/fi.25940732e.2020.21.3.022

Eyeleko, A. H., & Feng, T. (2023). A Critical Overview of Industrial Internet of Things Security and Privacy Issues Using a Layer-Based Hacking Scenario. *IEEE Internet of Things Journal*, *10*(24), 21917–21941. https://doi.org/10.1109/JIOT.2023.3308195

Falowo, O. I., Edinam Botsyoe, L., Koshoedo, K., & Ozer, M. (2024). *Enhancing Cybersecurity With Artificial Immune Systems and General Intelligence: A New Frontier in Threat Detection and Response*. *12*, 123811–123822. https://doi.org/10.1109/ACCESS.2024.3454543

Ferreira, G. B., Silva, P., & Silva, R. (2025). Elevating Healthcare AI: Achieving Efficiency and Accuracy in Medical Applications with Surrogate-Based Multiobjective Compression of ResNet50 CNNs. In A. Paes & F. A. N. Verri (Eds.), *INTELLIGENT SYSTEMS, BRACIS 2024, PT IV* (Vol. 15415, Issue 34th Brazilian Conference on Intelligent Systems, pp. 137–151). https://doi.org/10.1007/978-3-031-79038-6_10 WE - Conference Proceedings Citation Index - Science (CPCI-S)

Fotiadou, K., Velivassaki, T. H., Voulkidis, A., Skias, D., Tsekeridou, S., & Zahariadis, T. (2021). Network traffic anomaly detection via deep learning. *Information (Switzerland)*, *12*(5). https://doi.org/10.3390/info12050215

Gallegos Manrique, L. A., & Lynch Escobar, C. D. (2024). *Revisión de literatura de la norma ISO/IEC 27001 en el sector de las telecomunicaciones de la ciudad de Guayaquil: Evaluación de la seguridad de las redes y sistemas informáticos* [{B.S.} thesis].

Gangadharan, K., Purandaran, A., Malathi, K., Subramanian, B., Jeyaraj, R., & Jung, S. K. (2025). From Data to Decisions: The Power of Machine Learning in Business Recommendations. *IEEE ACCESS*, *13*, 17354–17397. https://doi.org/10.1109/ACCESS.2025.3532697 WE - Science Citation Index Expanded (SCI-EXPANDED)

García Pérez, D. S. (2024). *Impacto de ataques ransomware en las empresas de salud y medidas de mitigación* [{B.S.} thesis]. https://dspace.ups.edu.ec/handle/123456789/28109

Gómez Castaño, J. C., Castaño Pérez, N. J., & Correa Ortiz, L. C. (2023). Sistemas de detección y prevención de intrusos. *Ciencia e Ingeniería Neogranadina*, *33*(1). https://doi.org/10.18359/rcin.6534

Holguín Mendoza, J. D. (2021). *Categorización de protocolos de seguridad en criptomonedas para mitigar ataques informáticos: una revisión sistemática* [{B.S.} thesis].

Huma, Z. E., Latif, S., Ahmad, J., Idrees, Z., Ibrar, A., Zou, Z., Alqahtani, F., & Baothman, F. (2021). A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things. *IEEE Access*, *9*, 55595–55605. https://doi.org/10.1109/ACCESS.2021.3071766

Jackson, J., Jackson, L. E., Ukwuoma, C. C., Kissi, M. D., Oluwasanmi, A., & Qin, Z. G. (2025). A patch-based deep learning framework with 5-B network for breast cancer multi-classification using histopathological images. *ENGINEERING APPLICATIONS OF ARTIFICIAL INTELLIGENCE*, *148*. https://doi.org/10.1016/j.engappai.2025.110439

Jamal, M. H., Khan, M. A., Ullah, S., Alshehri, M. S., Almakdi, S., Rashid, U., Alazeb, A., & Ahmad, J. (2023a). Multi-step attack detection in industrial networks using a hybrid deep learning architecture. *Mathematical Biosciences and Engineering : MBE*, *20*(8). https://doi.org/10.3934/mbe.2023615

Jamal, M. H., Khan, M. A., Ullah, S., Alshehri, M. S., Almakdi, S., Rashid, U., Alazeb, A., & Ahmad, J. (2023b). Multi-step attack detection in industrial networks using a hybrid deep learning architecture. *Mathematical Biosciences and Engineering : MBE*, *20*(8). https://doi.org/10.3934/mbe.2023615

Jia, H., Liu, J., Zhang, M., He, X., & Sun, W. (2021). Network intrusion detection based on IE-DBN model. *Computer Communications*, *178*. https://doi.org/10.1016/j.comcom.2021.07.016

Jiang, Y. H., Shi, X. L., Jiang, X. H., Feng, J., Lu, Y., & Xu, M. L. (2025). DiffuSaliency: Synthesizing Multi-object Images with Masks for Semantic Segmentation Using Diffusion and Saliency Detection. In Z. Lin, M. M. Cheng, R. He, K. Ubul, W. Silamu, H. Zha, J. Zhou, & C. L. Liu (Eds.), *PATTERN RECOGNITION AND COMPUTER VISION, PT III, PRCV 2024* (Vol. 15033, Issues 7th Chinese Conference on Pattern Recognition and Computer Vision, pp. 74–88). https://doi.org/10.1007/978-981-97-8502-5_6 WE - Conference Proceedings Citation Index - Science (CPCI-S)

Jin, X. B., Ma, H. J., Xie, J. Y., Kong, J. L., Deveci, M., & Kadry, S. (2025). Ada-STGMAT: An adaptive spatio-temporal graph multi-attention network for intelligent time series forecasting in smart cities. *EXPERT SYSTEMS WITH APPLICATIONS*, *269*. https://doi.org/10.1016/j.eswa.2025.126428

Kokoç, M., Akçapınar, G., Society, M. N. H.-E. T. &, & undefined 2021. (2021). Unfolding students' online assignment submission behavioral patterns using temporal learning analytics. *JSTORM Kokoç, G Akçapınar, MN HasnineEducational Technology & Society, 2021•JSTOR*. https://www.jstor.org/stable/26977869

Kovács, L., & Ghous, H. (2020). Efficiency comparison of Python and RapidMiner. *Multidiszciplináris Tudományok*, *10*(3). https://doi.org/10.35925/j.multi.2020.3.26

Kuang, H. L., Wang, Y. H., Tana, X., Yang, J. L., Sun, J. R., Liu, J., Qiu, W., Zhang, J. Y., Zhang, J. L., Yang, C. F., Wang, J. X., & Chen, Y. (2025). LW-CTrans: A lightweight hybrid network of CNN and Transformer for 3D medical image segmentation. *MEDICAL IMAGE ANALYSIS*, *102*. https://doi.org/10.1016/j.media.2025.103545 WE - Science Citation Index Expanded (SCI-EXPANDED)

Kumar, A., Singh, D., Jain, R., Jain, D. K., Gan, C. Q., & Zhao, X. D. (2025). Advances in DeepFake detection algorithms: Exploring fusion techniques in single and multi-modal approach. *INFORMATION FUSION*, *118*. https://doi.org/10.1016/j.inffus.2025.102993

Kumar Ahuja, G., & Kumar, G. (2014). Evaluation metrics for intrusion detection systems-a study. *Evaluation*, *2*(11).

Lara Bautista, J. de D. (2025). *Uso de AlexNet como red convolucional para la clasificación de imágenes médicas en el diagnóstico de cáncer de mama* [{B.S.} thesis]. https://dspace.ups.edu.ec/handle/123456789/29951

Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. In *Journal of Network and Computer Applications* (Vol. 36, Issue 1). https://doi.org/10.1016/j.jnca.2012.09.004

Liao, H. J., Richard Lin, C. H., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. In *Journal of Network and Computer Applications* (Vol. 36, Issue 1). https://doi.org/10.1016/j.jnca.2012.09.004

Lim, W., Yong, K. S. C., Lau, B. T., & Tan, C. C. L. (2024a). Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. In *Computers and Security* (Vol. 139). https://doi.org/10.1016/j.cose.2024.103733

Lim, W., Yong, K. S. C., Lau, B. T., & Tan, C. C. L. (2024b). Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. In *Computers and Security* (Vol. 139). https://doi.org/10.1016/j.cose.2024.103733

Liu, G. Q., Ge, H. W., Li, T., Su, S. Z., & Gao, P. L. (2025). Multi-view clustering via diversity induction and multi-layer concept factorization. *PATTERN ANALYSIS AND APPLICATIONS*, *28*(2). https://doi.org/10.1007/s10044-025-01455-4 WE - Science Citation Index Expanded (SCI-EXPANDED)

Liu, R. Y., Zhou, W., Zhang, J. H., Liu, X. Y., Si, P. Y., & Li, H. R. (2025). Model Inversion Attacks on Homogeneous and Heterogeneous Graph Neural Networks. In H. Duan, M. Debbabi, X. D. DeCarnavalet, X. Luo, X. Du, & M. H. A. Au (Eds.), *SECURITY AND PRIVACY IN COMMUNICATION NETWORKS, PT I, SECURECOMM 2023* (Vol. 567, Issues 19th International Conference on Security and Privacy in Communication Networks, pp. 125–144). https://doi.org/10.1007/978-3-031-64948-6_7 WE - Conference Proceedings Citation Index - Science (CPCI-S)

Lu, K. Di, Zeng, G. Q., Luo, X., Weng, J., Luo, W., & Wu, Y. (2021). Evolutionary Deep Belief Network for Cyber-Attack Detection in Industrial Automation and Control System. *IEEE Transactions on Industrial Informatics*, *17*(11). https://doi.org/10.1109/TII.2021.3053304

Maharani, L. (2022). Systematic Literature Review Method for Evaluation of User Experience on Ticket Booking Applications. *International Conference on Cyber and IT Service Management (CITSM)*, 1–7. https://doi.org/10.1109/CITSM52892.2021.9588807

Marsilio, L., Moglia, A., Manzotti, A., & Cerveri, P. (2025). Context-Aware Dual-Task Deep Network for Concurrent Bone Segmentation and Clinical Assessment to Enhance Shoulder Arthroplasty Preoperative planning. *IEEE OPEN JOURNAL OF ENGINEERING IN MEDICINE AND BIOLOGY*, *6*, 269–278. https://doi.org/10.1109/OJEMB.2025.3527877 WE - Emerging Sources Citation Index (ESCI)

Maseer, Z. K., Kadhim, Q. K., Al-Bander, B., Yusof, R., & Saif, A. (2024). Meta-analysis and systematic review for anomaly network intrusion detection systems: Detection methods, dataset, validation methodology, and challenges. In *IET Networks* (Vol. 13, Issues 5–6, pp. 339–376). John Wiley and Sons Inc. https://doi.org/10.1049/ntw2.12128

Medina Astudillo, I. D. (2024). *Prevención y resiliencia sobre infraestructuras críticas y su impacto en planificaciones I+ D+ i en ciberseguridad* [{B.S.} thesis]. https://dspace.ups.edu.ec/handle/123456789/26727

Mohammadian, H., Habibi Lashkari, A., & Ghorbani, A. A. (2022). Evaluating Deep Learning-based NIDS in Adversarial Settings. *International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0010867900003120

Molina Estupiñán, B. N. (2025). *Gestión y técnicas en la manipulación de datos para el área de seguridad de la información: una revisión sistemática* [{B.S.} thesis]. https://dspace.ups.edu.ec/handle/123456789/29946

Morís, D. I., de Moura, J., Carmona, E. J., Novo, J., & Ortega, M. (2025). Semantic-guided generative latent diffusion augmentation approaches for improving the neovascularization diagnosis in OCT-

A imaging. *PATTERN RECOGNITION LETTERS*, *189*, 31–37. https://doi.org/10.1016/j.patrec.2025.01.003

Mtebe, J. S., & Kondoro, A. W. (2019). Mining Students' Data to Analyse Usage Patterns in eLearning Systems of Secondary Schools in Tanzania. *Journal of Learning for Development*, *6*(3), 228 – 244. https://doi.org/10.56059/jl4d.v6i3.350

Mugoniwa, B., Ngassam, E. K., & Singh, S. (2023). Towards a Hybrid Federated Social Networking Architecture. A Case of Zimbabwe's Higher Education. *2023 IST-AFRICA CONFERENCE, IST-AFRICA*. https://doi.org/10.23919/IST-Africa60249.2023.10187749

Nazwita, & Ramadhani, S. (2017). Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata. *Seminar Nasional Teknologi Informasi, Komunikasi Dan Industri (SNTIKI)*.

Nevmerzhitskaya, J., Norvanto, E., & Virag, C. (2019). High Impact Cybersecurity Capacity Building. In I. Roceanu, C. Holotescu, L. Ciolan, A. C. Colibaba, & C. Radu (Eds.), *NEW TECHNOLOGIES AND REDESIGNING LEARNING SPACES, VOL II* (pp. 306–312). CAROL I NATL DEFENCE UNIV PUBLISHING HOUSE. https://doi.org/10.12753/2066-026X-19-113

Niyaz, Q., Sun, W., Javaid, A. Y., & Alam, M. (2015). A deep learning approach for network intrusion detection system. *EAI International Conference on Bio-Inspired Information and Communications Technologies (BICT)*. https://doi.org/10.4108/eai.3-12-2015.2262516

Nyasore, O. N., Zavarsky, P., Swar, B., Naiyeju, R., & Dabra, S. (2020). Deep Packet Inspection in Industrial Automation Control System to Mitigate Attacks Exploiting Modbus/TCP Vulnerabilities. *Proceedings - 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, IDS 2020*. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00051

Ott, A., & Sethmann, R. (2010). Hacking for fun and education: ELearning on network security. *9th European Conference on Information Warfare and Security 2010, ECIW 2010*, 229 – 232. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84873179262&partnerID=40&md5=42de851478b2c469a52d2b0ae4aec7cd

Peng, Y., Su, J., Shi, X., & Zhao, B. (2019). Evaluating deep learning based network intrusion detection system in adversarial environment. *ICEIEC 2019 - Proceedings of 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication*. https://doi.org/10.1109/ICEIEC.2019.8784514

Perdigón Llanes, R. (2022). Suricata como detector de intrusos para la seguridad en redes de datos empresariales. *CIENCIA UNEMI*, *15*(39). https://doi.org/10.29076/issn.2528-7737vol15iss39.2022pp44-53p

Pretolesi, D., Stanzani, I., Ravera, S., Vian, A., & Barla, A. (2025). Artificial intelligence and network science as tools to illustrate academic research evolution in interdisciplinary fields: The case of Italian design. *PLOS ONE*, *20*(1). https://doi.org/10.1371/journal.pone.0315216 WE - Science Citation Index Expanded (SCI-EXPANDED)

Rigchc Mero, A. (2022). *Determinación de los peligros en las redes sociales en entorno a niños y adolescentes para uso y prevención*. http://dspace.ups.edu.ec/handle/123456789/22843

Sahnoun, S., Mnif, M., Ghoul, B., Jemal, M., Fakhfakh, A., & Kanoun, O. (2025). Hybrid Solution Through Systematic Electrical Impedance Tomography Data Reduction and CNN Compression for Efficient Hand Gesture Recognition on Resource-Constrained IoT Devices. *FUTURE INTERNET*, *17*(2). https://doi.org/10.3390/fi17020089 WE - Emerging Sources Citation Index (ESCI)

Sekhar, J. C., Priyanka, R., Nanda, A. K., Josephson, P. J., Ebinezer, M. J. D., & Devi, T. K. (2025). Stochastic gradient boosted distributed decision trees security approach for detecting cyber

anomalies and classifying multiclass cyber-attacks. *COMPUTERS & SECURITY*, *151*. https://doi.org/10.1016/j.cose.2025.104320

Sheatsley, R., Papernot, N., Weisman, M. J., Verma, G., & McDaniel, P. (2022). Adversarial examples for network intrusion detection systems. *Journal of Computer Security*, *30*(5). https://doi.org/10.3233/JCS-210094

Suresh, A., Dwarakanath, B., Nanda, A. K., Santhosh Kumar, P., Sankar, S., & Cheerla, S. (2024). An Evolutionary Computation-Based Federated Learning for Host Intrusion Detection in Real-Time Traffic Analysis. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-023-10852-z

Teixeira, A., Bates, T., & Mota, J. (2019). What future(s) for distance education universities? Towards an open network-based approach. *RIED-REVISTA IBEROAMERICANA DE EDUCACION A DISTANCIA*, *22*(1), 107–126. https://doi.org/10.5944/ried.22.1.22288

Villamar Arellano, D. A. (2023). *Estrategias de prevención frente a los ciberataques en la Unidad Educativa Luis Alfredo Noboa Icaza* [{B.S.} thesis]. https://dspace.ups.edu.ec/handle/123456789/24173

Villao González, J. I., & López Zambrano, E. M. (2024). *Revisión de literatura sobre el uso de Machine Learning enfocados a la seguridad de la información para minimizar vulnerabilidades en el sector educativo* [{B.S.} thesis].

Vintimilla Murillo, K. A., & Sánchez Manzaba, A. D. (2024). *Diseño de un modelo de migración para redes de HFC mediante la tecnolog{\'\i}a GPON en el contexto ecuatoriano* [{B.S.} thesis].

Vobugari, N., Raja, V., Sethi, U., Gandhi, K., Raja, K., & Surani, S. R. (2022). *Advancements in Oncology with Artificial Intelligence— A Review Article*. *14*(5). https://doi.org/10.3390/cancers14051349

Waleed, A., Jamali, A. F., & Masood, A. (2022). Which open-source IDS? Snort, Suricata or Zeek. *Computer Networks*, *213*. https://doi.org/10.1016/j.comnet.2022.109116

Wang, Q., Liao, X., & Wu, H. (2025). Biased Block Term Tensor Decomposition for Temporal Pattern-aware QoS Prediction. *INTERNATIONAL JOURNAL OF PATTERN RECOGNITION AND ARTIFICIAL INTELLIGENCE*, *39*(02). https://doi.org/10.1142/S0218001425500016

Wang, X. P., Gong, D., Chen, Y., Zong, Z., Li, M., Fan, K., Jia, L. N., Cao, Q. Y., Liu, Q., & Yang, Q. (2025). Hybrid CNN-Mamba model for multi-scale fundus image enhancement. *BIOMEDICAL OPTICS EXPRESS*, *16*(3), 1104–1117. https://doi.org/10.1364/BOE.542471 WE - Science Citation Index Expanded (SCI-EXPANDED)

Xia, X. L., & Ouyang, M. X. (2025). A Recursive Learning Algorithm for the Least Squares SVM. In R. Hadfi, P. Anthony, A. Sharma, T. Ito, & Q. Bai (Eds.), *PRICAI 2024: TRENDS IN ARTIFICIAL INTELLIGENCE, PT I* (Vol. 15281, Issue 21st Pacific Rim International Conference on Artificial Intelligence, pp. 209–220). https://doi.org/10.1007/978-981-96-0116-5_17 WE - Conference Proceedings Citation Index - Science (CPCI-S)

Yuan, C. S., Qiu, W. Q., Zhou, Z. L., Li, X. T., & Chen, X. Y. (2025). FIL-FLD: Few-Shot Incremental Learning with EMD Metric for High Generalization Fingerprint Liveness Detection. In Z. Lin, M. M. Cheng, R. He, K. Ubul, W. Silamu, H. Zha, J. Zhou, & C. L. Liu (Eds.), *PATTERN RECOGNITION AND COMPUTER VISION, PRCV 2024, PT XV* (Vol. 15045, Issues 7th Chinese Conference on Pattern Recognition and Computer Vision, pp. 363–376). https://doi.org/10.1007/978-981-97-8499-8_25 WE - Conference Proceedings Citation Index - Science (CPCI-S)

Zeng, Y. H., Liu, Z. C., Liu, Z. Y., Peng, X. Y., Cui, H., Yan, J., Duan, S. K., Wang, L. D., & Chu, J. (2025). A lightweight gas classification and concentration prediction method based on PTQ-CNN by using an electronic nose system. *SENSORS AND ACTUATORS A-PHYSICAL*, *386*. https://doi.org/10.1016/j.sna.2025.116382

Zhang, Z. Y., Cao, Y. H., Zhou, N. R., Xu, X. Y., & Mou, J. (2025). Novel discrete initial-boosted Tabu learning neuron: dynamical analysis, DSP implementation, and batch medical image encryption. *APPLIED INTELLIGENCE*, *55*(1). https://doi.org/10.1007/s10489-024-05918-9 WE - Science Citation Index Expanded (SCI-EXPANDED)

Zhao, D. W., Yu, H., Chen, C., Li, L. X., & Mi, L. (2025). Speech Encryption Scheme Based on Chaotic Memristor Neural Network and S-Box. In D. F. Wong, Z. Wei, & M. Yang (Eds.), *NATURAL LANGUAGE PROCESSING AND CHINESE COMPUTING, PT IV, NLPCC 2024* (Vol. 15362, Issues 13th International Conference on Natural Language Processing and Chinese Computing, pp. 483–495). https://doi.org/10.1007/978-981-97-9440-9_37 WE - Conference Proceedings Citation Index - Science (CPCI-S) WE - Conference Proceedings Citation Index - Social Science & Humanities (CPCI-SSH)

Zhao, J. Y., Sun, L., Sun, Z., Fu, Y. L., Shao, W., Zhou, X., Si, H. P., & Zhang, D. Q. (2025). Edge-enhanced semi-supervised vertical convolutional neural network for tubular structure segmentation: Application to medical images. *PATTERN RECOGNITION*, *162*. https://doi.org/10.1016/j.patcog.2024.111302

Zhao, W. L., Xu, Y., & Wang, C. Z. (2025). A hybrid ABC-SVM approach for multi-dimensional data classification with synthetic data balancing. *INTERNATIONAL JOURNAL OF EMBEDDED SYSTEMS*, *18*(1). https://doi.org/10.1504/IJES.2025.144931 WE - Emerging Sources Citation Index (ESCI)

Zheng, Y., Wang, J. H., Jing, J. Y., & Peng, C. L. (2025). Face Anti-spoofing Based on Multi-view Anomaly Detection. In Z. Lin, M. M. Cheng, R. He, K. Ubul, W. Silamu, H. Zha, J. Zhou, & C. L. Liu (Eds.), *PATTERN RECOGNITION AND COMPUTER VISION, PRCV 2024, PT XV* (Vol. 15045, Issues 7th Chinese Conference on Pattern Recognition and Computer Vision, pp. 420–434). https://doi.org/10.1007/978-981-97-8499-8_29 WE - Conference Proceedings Citation Index - Science (CPCI-S)

Zhou, P., Chen, F., Li, B. W., Tang, Z., Liu, H., & Du, M. Y. (2025). Competing Dual-Network with Pseudo-Supervision Rectification for Semi-Supervised Medical Image Segmentation. In Z. Lin, M. M. Cheng, R. He, K. Ubul, W. Silamu, H. Zha, J. Zhou, & C. L. Liu (Eds.), *PATTERN RECOGNITION AND COMPUTER VISION, PRCV 2024, PT XIV* (Vol. 15044, Issues 7th Chinese Conference on Pattern Recognition and Computer Vision, pp. 545–559). https://doi.org/10.1007/978-981-97-8496-7_38 WE - Conference Proceedings Citation Index - Science (CPCI-S)