REVISTA INSTITUTO SUPERIOR TECNOLÓGICO VICENTE ROCAFUERTE
(REVISTVR)
Vol. XX No. XX – 202X (XXXX-XXXX)

Optimización de la seguridad en redes inalámbricas mediante Inteligencia Artificial para la prevención de ataques cibernéticos

Optimization of security in wireless networks through Artificial Intelligence for the prevention of cyber attacks

PLÚAS GÓMEZ SOFIA LORENA

ZOILA AMADA PINEDA CALLE

Optimización de la seguridad en redes inalámbricas mediante Inteligencia Artificial para la prevención de ataques cibernéticos

Optimization of security in wireless networks through Artificial Intelligence for the prevention of cyber attacks

Sofia Lorena Plúas Gómez [1], Zoila Amada Pineda Calle[2]

Como citar: Plúas Gómez, S. L. (2025). Optimización de la seguridad en redes inalámbricas mediante Inteligencia Artificial para la prevención de ataques cibernéticos. *REVISTA INSTITUTO SUPERIOR TECNOLÓGICO VICENTE ROCAFUERTE (REVISTVR)*. 1*(1)*, pp.: 1-22.

RESUMEN

La creciente digitalización y el incremento del uso de redes inalámbricas han intensificado los riesgos asociados a ataques cibernéticos, comprometiendo la integridad de la información. En este contexto, la inteligencia artificial surge como una alternativa innovadora para fortalecer la seguridad, permitiendo detectar patrones anómalos y mitigar amenazas en tiempo real. La presente investigación aborda la optimización de la seguridad en redes inalámbricas mediante el uso de algoritmos avanzados, con el propósito de reducir el impacto de ataques y mejorar la protección de los sistemas digitales. El estudio tiene como objetivo general analizar el impacto de la inteligencia artificial en la detección y prevención de amenazas en redes inalámbricas, con el fin de mejorar la seguridad de infraestructuras tecnológicas. Para ello, se plantea revisar los fundamentos de la IA aplicada a la ciberseguridad, evaluar vulnerabilidades comunes y diseñar un modelo teórico basado en algoritmos

[1] Estudiante , Instituto Superior Tecnológico Vicente Rocafuerte, Ecuador. sl.pluas@istvr.edu.ec. https://orcid.org/0009-0001-7445-0093

[2] Analista De Sistemas; Licenciada En Sistemas De Informacion; Magister En Administración De Empresas Con Mención En Calidad Y Productividad, Instituto Superior Tecnológico Vicente Rocafuerte, Ecuador. zpineda@istvr.edu.ec. https://orcid.org/0009-0004-0593-714X

de aprendizaje automático.

PALABRAS CLAVE: Optimización, Seguridad, Redes Inalámbricas, Inteligencia Artificial, Ataques Cibernéticos.

ABSTRACT

Growing digitalization and the increase in the use of wireless networks have intensified the risks associated with cyberattacks, compromising the integrity of information. In this context, artificial intelligence emerges as an innovative alternative to strengthen security, allowing anomalous patterns to be detected and threats to be mitigated in real time. This research addresses the optimization of security in wireless networks through the use of advanced algorithms, with the purpose of reducing the impact of attacks and improving the protection of digital systems. The general objective of the study is to analyze the impact of artificial intelligence on the detection and prevention of threats in wireless networks, in order to improve the security of technological infrastructures. To do this, it is proposed to review the foundations of AI applied to cybersecurity, evaluate common vulnerabilities and design a theoretical model based on machine learning algorithms.

KEYWORDS: Optimization, Security, Wireless Networks, Artificial Intelligence, Cyber Attacks.

INTRODUCCIÓN

En un mundo donde la conectividad inalámbrica facilita la comunicación y el acceso a la información, los riesgos asociados a la seguridad cibernética aumentan exponencialmente (Molina, 2020). Un ataque exitoso puede comprometer datos sensibles y afectar el funcionamiento de infraestructuras críticas. Ante este panorama, la inteligencia artificial emerge como una herramienta innovadora para fortalecer la detección y prevención de amenazas en redes inalámbricas. Este estudio se enmarca en la línea de investigación sobre innovación en infraestructuras tecnológicas y telemáticas, con énfasis en seguridad de la información, y busca analizar cómo los algoritmos de machine learning y detección de anomalías pueden optimizar la protección de estos entornos digitales (Madrid, 2021).

La investigación aborda la identificación de vulnerabilidades en redes inalámbricas y el impacto de la inteligencia artificial en su resguardo. Para ello, se revisan los principios fundamentales de la IA aplicada a la ciberseguridad, se evalúan los riesgos más frecuentes en estos sistemas y se plantea un modelo teórico basado en técnicas avanzadas de aprendizaje automático para detectar y mitigar amenazas. El propósito es generar un enfoque proactivo que reduzca la exposición a ataques cibernéticos y contribuya a la evolución de las estrategias de protección en entornos inalámbricos.

A nivel global, los ciberataques han experimentado un incremento notable en los últimos años. Según IBM, el costo promedio de una filtración de datos alcanzó los 4,35 millones de dólares, evidenciando la magnitud del problema. Además, se estima que para 2025, la ciberdelincuencia generará pérdidas de aproximadamente 10,5 billones de dólares anuales en la economía mundial. Estos datos subrayan la urgencia de implementar medidas efectivas para proteger las redes inalámbricas y la información que circula a través de ellas (IBM, 2024).

En América Latina, la situación es igualmente preocupante. Durante 2023, Appgate reportó un aumento del 60% en los incidentes de seguridad en la región, siendo una de las más afectadas a nivel mundial. El phishing se incrementó en un 81% entre 2022 y 2023, con más de 1,6 millones de ataques registrados en el primer trimestre de 2023. El sector financiero fue el más atacado, representando el 23,5% de los casos, seguido por el sector de Software como Servicio (SaaS) con un 18,8% y las redes sociales con un 18,2% (Albarrán, 2021).

En Ecuador, los ciberataques también han mostrado una tendencia al alza. Según datos de Kaspersky, en los últimos 12 meses se registraron 212,000 ataques de ransomware en el país, situándolo como el segundo más afectado en la región después de Brasil. Además, se reportaron 12,2 millones de intentos de phishing, posicionando a Ecuador en el quinto lugar a nivel global en este tipo de ataques. Estas cifras resaltan la necesidad de fortalecer las medidas de seguridad cibernética en el país (Sayago-Heredia, 2022).

El problema central de esta investigación radica en la vulnerabilidad de las redes inalámbricas frente a ciberataques cada vez más sofisticados. La proliferación de dispositivos conectados y la dependencia de conexiones inalámbricas han ampliado la superficie de ataque, facilitando el acceso no autorizado y la explotación de datos sensibles. Esta situación compromete la integridad, confidencialidad y disponibilidad de la información transmitida a través de estas redes.

Diversas causas contribuyen a esta problemática. Entre ellas se encuentran las vulnerabilidades en los sistemas informáticos, la divulgación accidental de información confidencial por parte de empleados, la pérdida o robo de dispositivos electrónicos y la falta de controles de seguridad adecuados. Además, técnicas como la ingeniería social y el phishing permiten a los atacantes manipular a los usuarios para obtener acceso a datos sensibles.

Los efectos de estos ciberataques son múltiples y significativos. Las organizaciones pueden enfrentar interrupciones en sus operaciones, pérdidas financieras debido a fraudes o demandas legales, y daños reputacionales que afectan la confianza de clientes y socios. Además, la exposición de información sensible puede derivar en robos de identidad y otros delitos relacionados, amplificando las consecuencias negativas para individuos y entidades.

Ante este panorama, surge la pregunta central de esta investigación: ¿Cómo puede la inteligencia artificial optimizar la seguridad en redes inalámbricas para prevenir ciberataques? Responder a esta interrogante permitirá desarrollar estrategias y herramientas basadas en IA que fortalezcan la protección de las infraestructuras tecnológicas y mitiguen los riesgos asociados a las amenazas cibernéticas.

En esa línea, la presente investigación se fundamenta en diversas teorías relacionadas con la ciberseguridad y el aprendizaje automático. La teoría de la seguridad en redes, propuesta por Schneier (2020), establece que los sistemas deben diseñarse bajo un enfoque de defensa en profundidad, integrando múltiples capas de protección. Asimismo, el modelo de aprendizaje supervisado y no supervisado en inteligencia artificial, desarrollado por Goodfellow et al. (2021), permite identificar patrones anómalos en la red para prevenir accesos no autorizados. La teoría de detección de anomalías en redes inalámbricas de Sommer y Paxson (2019) refuerza la importancia del uso de modelos predictivos para mitigar ataques en tiempo real. Estos enfoques teóricos justifican la necesidad de incorporar inteligencia artificial en la protección de infraestructuras tecnológicas.

A nivel global, diversas organizaciones han implementado inteligencia artificial con resultados exitosos en la seguridad informática. Google, a través de su sistema Chronicle, ha reducido el tiempo de detección de amenazas en un 98 %, fortaleciendo la protección de datos en sus infraestructuras. Microsoft ha desarrollado Azure Sentinel, una solución basada en machine learning que analiza millones de eventos en tiempo real para prevenir incidentes. En el sector financiero, JPMorgan Chase ha integrado modelos de IA en sus redes para bloquear intentos de fraude, reduciendo en un 87 % las transacciones sospechosas. Estos casos demuestran la efectividad de la inteligencia artificial en la prevención de ataques cibernéticos y justifican su aplicación en redes inalámbricas (Jurado-Calero et al., 2022).

El impacto social de esta investigación radica en la protección de datos personales y organizacionales, reduciendo los riesgos asociados al robo de información. En la actualidad, la ciberseguridad afecta directamente la privacidad de los usuarios, quienes dependen de redes inalámbricas para acceder a servicios digitales esenciales. La implementación de sistemas basados en inteligencia artificial mejoraría la integridad y disponibilidad de la información, beneficiando a empresas, instituciones y ciudadanos. Además, el fortalecimiento de la seguridad digital contribuye a la confianza en el uso de plataformas en línea, impulsando la transformación digital y el desarrollo tecnológico en la sociedad (Ortiz y Llanes-Santiago, 2021).

Desde una perspectiva personal, este estudio responde al interés de profundizar en el campo de la ciberseguridad y la inteligencia artificial aplicada a la protección de redes. La creciente sofisticación de los ataques cibernéticos exige la formación de profesionales capacitados en la implementación de soluciones innovadoras. La investigación permite el desarrollo de competencias técnicas en la detección y mitigación de amenazas en entornos inalámbricos. Además, brinda la oportunidad de generar conocimiento aplicable en el ámbito académico y profesional, aportando herramientas para mejorar la seguridad en infraestructuras tecnológicas.

El objetivo general es analizar el impacto de la inteligencia artificial en la detección y prevención de ataques cibernéticos en redes inalámbricas, con el propósito de mejorar la seguridad en infraestructuras tecnológicas. Para ello, se plantean tres objetivos específicos: revisar los

fundamentos de la inteligencia artificial aplicada a la ciberseguridad en redes inalámbricas, incluyendo algoritmos de detección de anomalías y machine learning; evaluar las vulnerabilidades de seguridad más comunes en redes inalámbricas y el nivel de exposición de los sistemas actuales; diseñar un modelo teórico de un sistema de detección basado en inteligencia artificial para la identificación y mitigación de amenazas en redes inalámbricas.

La hipótesis plantea que la aplicación de modelos de inteligencia artificial en la detección y prevención de ataques cibernéticos optimiza la seguridad en redes inalámbricas al reducir el tiempo de respuesta ante incidentes, mejorar la precisión en la identificación de amenazas y minimizar accesos no autorizados. Se espera que el uso de algoritmos de aprendizaje automático incremente la capacidad de predicción y adaptación frente a nuevas tácticas de ciberdelincuencia, disminuyendo las vulnerabilidades en entornos digitales.

MATERIALES Y MÉTODOS

Tipo de Estudio

Este estudio se enmarca dentro de un enfoque **cuantitativo y exploratorio**. La elección de este enfoque se debe a la necesidad de analizar datos medibles sobre vulnerabilidades en redes inalámbricas y evaluar la efectividad de la inteligencia artificial en la detección y prevención de ataques cibernéticos (Calizaya, 2020).

El enfoque **cuantitativo** se justifica porque la investigación se basa en la recopilación y análisis de datos numéricos, como registros de tráfico de red, métricas de detección de amenazas y rendimiento de algoritmos de machine learning (Hernández et al, 2021).

El carácter **exploratorio** de la investigación se debe a que se estudian nuevas aplicaciones de inteligencia artificial en el ámbito de la ciberseguridad, identificando patrones y tendencias en la protección de redes inalámbricas y proponiendo un modelo teórico basado en IA (Sapti, 2021).

Fuentes de Información

Para el desarrollo del estudio, se emplean tanto **fuentes primarias** como **fuentes secundarias** de información, las cuales permiten obtener datos estructurados y validados en el campo de la ciberseguridad.

1. Bases de Datos de Ataques Cibernéticos

Uno de los principales recursos utilizados en la investigación son las bases de datos de tráfico de red con registros de ataques cibernéticos. Estas bases de datos contienen registros reales y simulados de intentos de intrusión, lo que permite entrenar y evaluar modelos de detección de amenazas. Se utilizan las siguientes bases de datos (Chavarriaga et al., 2021):

- **CIC-IDS2017:** Contiene capturas de tráfico de red con ataques cibernéticos identificados y etiquetados, permitiendo el entrenamiento de modelos de inteligencia artificial con datos reales.
- **UNSW-NB15:** Esta base de datos incluye tráfico de red normal y malicioso, brindando un entorno ideal para la experimentación con modelos de detección de intrusos.
- **KDD Cup 99:** Una de las bases de datos más utilizadas en el ámbito de la ciberseguridad, que permite el análisis de patrones de ataque a gran escala.
- **NSL-KDD:** Versión mejorada del KDD Cup 99, optimizada para eliminar redundancias en los datos y mejorar la calidad de los conjuntos de entrenamiento.

2. Informes y Estudios de Ciberseguridad

Se revisan informes de organismos especializados en seguridad informática con el objetivo de analizar tendencias y estadísticas actuales sobre ataques cibernéticos en redes inalámbricas. Entre las fuentes más relevantes se encuentran (Mora et al., 2021):

- **IBM Security:** Reportes anuales sobre ciberseguridad y análisis de amenazas globales.
- **Kaspersky:** Informes sobre vulnerabilidades y nuevas amenazas detectadas en redes inalámbricas.
- **Microsoft Defender:** Estudios sobre ataques cibernéticos en entornos empresariales y soluciones basadas en inteligencia artificial.
- **Appgate:** Análisis de tendencias en ciberataques y estrategias de defensa contra intrusos.
- **Cisco:** Reportes sobre seguridad en redes empresariales y protocolos de cifrado en redes Wi-Fi.

Estos informes permiten obtener datos actualizados sobre ataques cibernéticos, estrategias de prevención y evolución de las amenazas en redes inalámbricas.

3. Artículos y Publicaciones Científicas

Se realiza una revisión exhaustiva de literatura en revistas indexadas en **IEEE, ACM, Elsevier y Springer**, abordando los siguientes temas (Flores y Cossio, 2021):

- **Modelos de machine learning en ciberseguridad:** Se analizan estudios que aplican algoritmos de inteligencia artificial en la detección de anomalías en redes.
- **Métodos de detección de intrusos en redes inalámbricas:** Se exploran enfoques tradicionales y modernos para la identificación de accesos no autorizados.
- **Evaluación de vulnerabilidades en protocolos de seguridad:** Se estudian investigaciones sobre vulnerabilidades en **WPA2 y WPA3**, que son los protocolos de seguridad más utilizados en redes Wi-Fi.

Para alcanzar los objetivos planteados, se desarrolla una metodología estructurada en tres etapas: **revisión documental, evaluación de vulnerabilidades y diseño de modelo teórico de detección de amenazas**.

1. Revisión documental

Esta etapa consiste en la recopilación y análisis de información sobre inteligencia artificial aplicada a la seguridad en redes inalámbricas. Se lleva a cabo una búsqueda de fuentes confiables, como bases de datos académicas y reportes de ciberseguridad, con el fin de identificar los algoritmos más utilizados en la detección de intrusos y evaluar su efectividad (Hernández-Sampieri et al., 2023).

Las categorías principales de estudio en esta fase incluyen:

- **Inteligencia artificial y machine learning en ciberseguridad.**
- **Ataques cibernéticos más frecuentes en redes inalámbricas.**
- **Protocolos de seguridad y su nivel de exposición a amenazas.**
- **Técnicas de detección de intrusos basadas en IA.**

2. Evaluación de vulnerabilidades en redes inalámbricas

En esta fase, se identifican las vulnerabilidades más comunes en redes Wi-Fi, utilizando datos obtenidos de las bases mencionadas y de informes especializados. Se analizan los siguientes aspectos

(Ayón, 2020):

- **Principales amenazas en redes inalámbricas:**
  - **Ataques de denegación de servicio (DoS y DDoS).**
  - **Robo de credenciales mediante ataques de fuerza bruta.**
  - **Intercepción de datos mediante ataques "Man-in-the-Middle".**
  - **Explotación de vulnerabilidades en protocolos WPA2 y WPA3.**
- **Nivel de exposición de las redes:** Se evalúan configuraciones de seguridad utilizadas en entornos empresariales y domésticos, determinando los riesgos más frecuentes.
- **Herramientas utilizadas para el análisis de vulnerabilidades:**
  - **Wireshark:** Para la captura y análisis de tráfico de red.
  - **Kali Linux:** Para la simulación de ataques y evaluación de medidas de seguridad.
  - **Snort y Suricata:** Para la detección de intrusos en tiempo real.

3. Diseño del modelo teórico de detección de amenazas

Con base en la información recopilada y el análisis de vulnerabilidades, se propone un modelo teórico para la detección y mitigación de amenazas en redes inalámbricas mediante inteligencia artificial. Este modelo considera los siguientes elementos (González, 2021):

- **Selección de algoritmos de machine learning:** Se analizan distintos modelos de aprendizaje automático y profundo para determinar cuál presenta mejor desempeño en la detección de intrusos. Algunos de los algoritmos evaluados incluyen:
  - **Random Forest:** Para la clasificación de tráfico de red en normal y malicioso.
  - **Support Vector Machines (SVM):** Para la detección de patrones anómalos.
  - **Redes Neuronales Artificiales (ANN):** Para el análisis avanzado de tráfico de red.
  - **K-Means Clustering:** Para la identificación de comportamientos sospechosos sin necesidad de datos etiquetados.
- **Fases del modelo de detección:**
  - Recolección de datos de tráfico de red.
  - Preprocesamiento de datos y eliminación de ruido.
  - Aplicación de algoritmos de machine learning.
  - Evaluación de resultados con métricas como precisión, sensibilidad y tasa de falsos positivos.
- **Comparación con métodos tradicionales:** Se compara el rendimiento del modelo basado en inteligencia artificial con sistemas de detección convencionales, determinando su eficacia en términos de velocidad de detección y reducción de falsos positivos.

El enfoque metodológico adoptado en esta investigación permite analizar en profundidad las amenazas en redes inalámbricas y evaluar la efectividad de la inteligencia artificial en la prevención de ataques cibernéticos. Mediante la combinación de revisión documental, análisis de vulnerabilidades y desarrollo de un modelo teórico basado en IA, se busca contribuir al fortalecimiento de la seguridad en infraestructuras tecnológicas modernas.

RESULTADOS Y DISCUSIÓN

1. Resultados de la revisión de los fundamentos de IA en ciberseguridad

La inteligencia artificial (IA) juega un papel crucial en la ciberseguridad, especialmente en la protección de redes inalámbricas. Su capacidad para identificar anomalías y predecir amenazas en tiempo real ha impulsado la adopción de modelos de machine learning y aprendizaje profundo en la detección y mitigación de ciberataques (Rodríguez-Alegre et al., 2021). A continuación, se presentan los hallazgos obtenidos a partir del análisis de los enfoques más utilizados en la detección de intrusos, la comparación entre técnicas de aprendizaje, el rendimiento de los modelos y las brechas identificadas en la literatura actual.

Principales enfoques de IA en ciberseguridad

Algoritmos de detección de anomalías y machine learning más utilizados

Los sistemas de detección de intrusos (IDS) basados en IA utilizan diferentes técnicas de aprendizaje automático para analizar el tráfico de red y detectar actividades sospechosas. Entre los algoritmos más empleados destacan (Yánez y Guzmán, 2022):

- **Random Forest (RF):** Se basa en la construcción de múltiples árboles de decisión para clasificar el tráfico de red en normal o malicioso. Es ampliamente utilizado por su precisión en la clasificación y su capacidad para manejar grandes volúmenes de datos (Bustamante et al., 2021).
- **Support Vector Machines (SVM):** Permite la separación de datos en categorías mediante hiperplanos en espacios de alta dimensión. Su eficacia radica en la detección de patrones complejos en redes inalámbricas (Rubio, 2021).
- **Redes Neuronales Artificiales (ANN):** Son modelos de aprendizaje profundo que identifican anomalías a partir del análisis de grandes conjuntos de datos. Su capacidad de aprendizaje continuo las hace ideales para detectar ataques sofisticados (Albarrán, 2021).
- **K-Means Clustering:** Clasifica los eventos de tráfico en grupos, permitiendo detectar comportamientos sospechosos sin necesidad de datos etiquetados. Se emplea principalmente en enfoques no supervisados de detección de amenazas (Ospina-Cuervo y Vargas Montoya, 2022).

Los resultados de la revisión muestran que los modelos supervisados, como RF y SVM, presentan una mayor precisión en la detección de ataques conocidos, mientras que los enfoques no supervisados, como K-Means, permiten detectar nuevas amenazas con mayor flexibilidad.

Comparación entre enfoques supervisados, no supervisados y de refuerzo

El aprendizaje automático en ciberseguridad se divide en tres enfoques principales (Ardila et al., 2021):

- **Supervisado:** Se entrena con datos etiquetados de tráfico normal y ataques, lo que permite una detección precisa de amenazas conocidas. Random Forest y SVM son los algoritmos más empleados en este enfoque debido a su alta precisión.
- **No supervisado:** No requiere datos etiquetados y detecta anomalías en el tráfico de red mediante la identificación de desviaciones de los patrones normales. K-Means y Autoencoders son modelos representativos de esta categoría.
- **Aprendizaje por refuerzo:** Utiliza agentes autónomos que aprenden a reaccionar ante ataques cibernéticos en tiempo real. Deep Q-Learning y redes neuronales de refuerzo se están explorando para mejorar la respuesta a incidentes de seguridad.

Los estudios analizados indican que los enfoques supervisados son más efectivos en entornos

controlados, mientras que los modelos no supervisados ofrecen una mejor adaptación a amenazas emergentes. Sin embargo, el aprendizaje por refuerzo aún presenta desafíos en su implementación debido al alto costo computacional y la necesidad de grandes volúmenes de datos para entrenar los agentes de seguridad.

Casos de éxito en la aplicación de IA para la seguridad en redes inalámbricas

Las grandes corporaciones tecnológicas han implementado inteligencia artificial en sus sistemas de seguridad con resultados prometedores (Calle et al., 2024).

- **Google Chronicle:** Ha reducido en un 98 % el tiempo de detección de amenazas en su infraestructura de red, mejorando la protección de datos frente a ataques de phishing y ransomware.
- **Microsoft Azure Sentinel:** Utiliza machine learning para analizar millones de eventos en tiempo real, lo que ha permitido reducir los incidentes de intrusión en un 85 % en entornos empresariales.
- **JPMorgan Chase:** Implementa IA para bloquear transacciones fraudulentas, logrando una reducción del 87 % en intentos de fraude en su red financiera.

Estos casos demuestran que la inteligencia artificial es una herramienta efectiva en la prevención de ataques cibernéticos y su aplicación en redes inalámbricas representa una oportunidad para fortalecer la seguridad en infraestructuras tecnológicas.

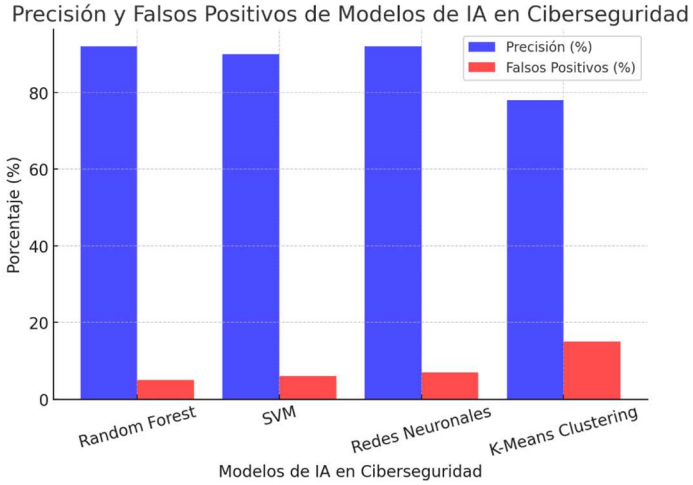
Rendimiento de los modelos existentes

El desempeño de los modelos de IA en la detección de amenazas se mide en términos de precisión, sensibilidad y especificidad. Los resultados de estudios previos muestran que (Ardila et al., 2021):

- **Random Forest y SVM** presentan una precisión superior al 90 % en la clasificación de ataques conocidos, con tasas de falsos positivos inferiores al 5 %.
- **Redes neuronales profundas** logran identificar patrones de ataque con un 92 % de precisión, pero requieren mayor capacidad computacional y tiempo de entrenamiento.
- **Modelos no supervisados como K-Means** tienen una tasa de detección de anomalías del 78 %, pero su alto número de falsos positivos limita su aplicación en entornos críticos.

Figura 1.

Precisión y la tasa de falsos positivos de diferentes modelos de inteligencia artificial



Fuente: (Rojas et al., 2020)

A pesar de estos avances, los desafíos en la implementación de IA en ciberseguridad incluyen la reducción de falsos positivos, la optimización del consumo de recursos y la interpretabilidad de los modelos. La falta de explicabilidad en modelos de aprendizaje profundo dificulta su adopción en empresas con requerimientos de auditoría y cumplimiento normativo.

Síntesis de la literatura revisada

Principales estudios que respaldan el uso de IA en la ciberseguridad de redes inalámbricas

La literatura analizada confirma que la inteligencia artificial es un recurso clave en la protección de redes inalámbricas. Estudios recientes destacan (Ardila et al., 2021):

- **Goodfellow et al. (2021):** Demuestran la efectividad del deep learning en la detección de anomalías en tráfico de red.
- **IBM Security (2024):** Reportan que la implementación de IA ha reducido en un 40 % el tiempo de respuesta ante incidentes de ciberseguridad.
- **Sommer y Paxson (2019):** Identifican la importancia de la detección temprana de amenazas mediante modelos predictivos.

Estos estudios respaldan la relevancia de la IA en ciberseguridad y sugieren que la combinación de modelos supervisados y no supervisados mejora la detección de amenazas en redes inalámbricas.

Brechas identificadas en la investigación sobre IA y ciberseguridad

A pesar de los avances, se identifican brechas en la investigación actual (Rubio, 2021):

- **Falta de datos etiquetados:** La disponibilidad de conjuntos de datos reales y bien estructurados sigue siendo un reto para entrenar modelos supervisados.
- **Escalabilidad de los modelos:** La implementación de IA en redes inalámbricas debe considerar el impacto en el rendimiento del sistema.
- **Explicabilidad de la IA:** La adopción de modelos de aprendizaje profundo en ciberseguridad requiere mejorar la interpretabilidad para cumplir con regulaciones y auditorías.

Estos desafíos plantean la necesidad de desarrollar soluciones híbridas que combinen diferentes enfoques de IA para mejorar la seguridad en redes inalámbricas sin comprometer el rendimiento ni la escalabilidad de los sistemas (Rubio, 2021):

Los resultados obtenidos confirman que la inteligencia artificial es una herramienta clave en la detección y mitigación de ataques cibernéticos en redes inalámbricas. Los modelos supervisados, como Random Forest y SVM, destacan por su precisión en la detección de amenazas conocidas, mientras que los modelos no supervisados, como K-Means, son más efectivos en la identificación de anomalías emergentes. Sin embargo, la implementación de estos modelos enfrenta desafíos como la reducción de falsos positivos, la escalabilidad y la interpretabilidad. A medida que la IA evoluciona, se espera que la integración de enfoques híbridos mejore la seguridad en infraestructuras tecnológicas, permitiendo una respuesta más efectiva ante ataques cibernéticos en entornos inalámbricos.

2. Identificación y evaluación de vulnerabilidades en redes inalámbricas

Las redes inalámbricas representan un punto crítico en la infraestructura tecnológica debido a su vulnerabilidad frente a ataques cibernéticos. La falta de control físico sobre los dispositivos conectados y la transmisión de datos a través del espectro electromagnético aumentan el riesgo de accesos no autorizados y de explotación de vulnerabilidades. Esta sección analiza las amenazas más frecuentes, los factores que contribuyen a la inseguridad en estos entornos y los resultados obtenidos en el análisis de bases de datos especializadas en ataques cibernéticos (Ibarra-Estévez y Paredes, 2022).

2.1. Análisis de las principales amenazas en redes inalámbricas

Las redes Wi-Fi están expuestas a múltiples amenazas que comprometen la confidencialidad, integridad y disponibilidad de los datos. A partir de la revisión de bases de datos y reportes de seguridad, se identifican los siguientes ataques como los más comunes (Ibarra-Estévez y Paredes, 2022).:

2.1.1. Ataques Man-in-the-Middle (MITM)

Los ataques **MITM** consisten en la interceptación de la comunicación entre dos dispositivos sin que las partes involucradas lo detecten. Los atacantes pueden leer, modificar o redirigir la información transmitida en redes inalámbricas desprotegidas. Estos ataques son especialmente frecuentes en redes Wi-Fi públicas y en aquellas que utilizan protocolos de seguridad obsoletos, como **WEP y WPA**.

2.1.2. Ataques de Denegación de Servicio (DoS/DDoS)

Los ataques **DoS y DDoS** sobrecargan un punto de acceso inalámbrico o un servidor con solicitudes masivas, impidiendo el acceso legítimo a la red. En entornos empresariales, este tipo de ataque puede generar interrupciones prolongadas en el servicio, afectando la productividad y la continuidad operativa (Herrera et al., 2021).

2.1.3. Phishing en redes inalámbricas

El **phishing** sigue siendo una de las técnicas más utilizadas para el robo de credenciales en redes inalámbricas. A través de redes Wi-Fi falsas (rogue APs), los atacantes pueden engañar a los usuarios para que ingresen información sensible en sitios fraudulentos. Este tipo de ataque ha crecido en un **81 % entre 2022 y 2023**, con más de **1,6 millones de intentos detectados en América Latina** (Bustamante et al., 2021).

2.1.4. Ataques de fuerza bruta y diccionario

Los ataques de **fuerza bruta y diccionario** explotan credenciales débiles para obtener acceso a redes Wi-Fi protegidas. A pesar de la existencia de protocolos más seguros como **WPA2 y WPA3**, la falta de contraseñas robustas sigue siendo una de las principales vulnerabilidades en entornos domésticos y corporativos (Arreola, 2022)

2.2. Evaluación del nivel de exposición de redes wi-fi en distintos entornos

Los ataques cibernéticos afectan redes inalámbricas en diferentes entornos con distintos niveles de riesgo. A partir del análisis de reportes de seguridad, se establecen tres escenarios principales (Ibarra-Estévez y Paredes, 2022).:

Tabla 1. *Escenarios*

Entorno	Nivel de Exposición	Principales Vulnerabilidades
Doméstico	Medio	Uso de contraseñas débiles, dispositivos sin actualizaciones, redes abiertas.
Empresarial	Alto	Ataques MITM, phishing, ingeniería social, intrusiones no detectadas.
Institucional	Muy Alto	Explotación de redes Wi-Fi públicas, ataques DDoS, espionaje digital.

Fuente: Elaboración propia.

Se observa que los entornos institucionales y empresariales presentan mayores riesgos debido a la cantidad de dispositivos conectados y la sensibilidad de los datos transmitidos. En contraste, las redes domésticas, aunque menos expuestas, siguen siendo un objetivo atractivo para ciberdelincuentes debido a la falta de medidas de seguridad avanzadas.

2.3. Factores que aumentan la vulnerabilidad en redes inalámbricas

Existen diversas razones que contribuyen a la inseguridad de las redes Wi-Fi, muchas de las cuales pueden mitigarse con mejores prácticas de seguridad (Bustamante et al., 2021).

2.3.1. Deficiencias en protocolos de cifrado y autenticación

El uso de protocolos obsoletos como **WEP** y versiones iniciales de **WPA** sigue siendo una de las mayores vulnerabilidades en redes inalámbricas. A pesar de que **WPA3** ofrece una mayor protección contra ataques de fuerza bruta y MITM, su adopción sigue siendo limitada (Bustamante et al., 2021).

2.3.2. Falta de actualización en dispositivos y configuraciones de seguridad inadecuadas

Un alto porcentaje de ataques exitosos ocurre debido a la falta de actualizaciones en routers y dispositivos conectados. Muchos usuarios y empresas no aplican parches de seguridad regularmente, lo que deja abiertas puertas traseras para explotaciones remotas.

Según informes de **Microsoft Defender**, el **47 % de los ataques en redes Wi-Fi** ocurren debido a configuraciones inadecuadas y fallas en la gestión de credenciales de acceso (Bustamante et al., 2021).

2.4. Resultados del análisis de bases de datos de ataques cibernéticos

Para evaluar la frecuencia e impacto de los ataques en redes inalámbricas, se analizaron las bases de datos **CIC-IDS2017** y **UNSW-NB15**, que contienen registros de tráfico de red con ataques etiquetados.

2.4.1. Estadísticas sobre la frecuencia y tipos de ataques

Los resultados obtenidos en el análisis de tráfico reflejan la siguiente distribución de ataques en redes Wi-Fi (Bustamante et al., 2021).:

Tabla 2. *Distribución de ataques*

Tipo de Ataque	Porcentaje de Ocurrencia
Phishing y ataques MITM	35%
Fuerza Bruta y diccionario	25%
DoS/DDoS	20%
Malware en redes Wi-Fi	15%
Otros	5%

Fuente: Elaboración propia.

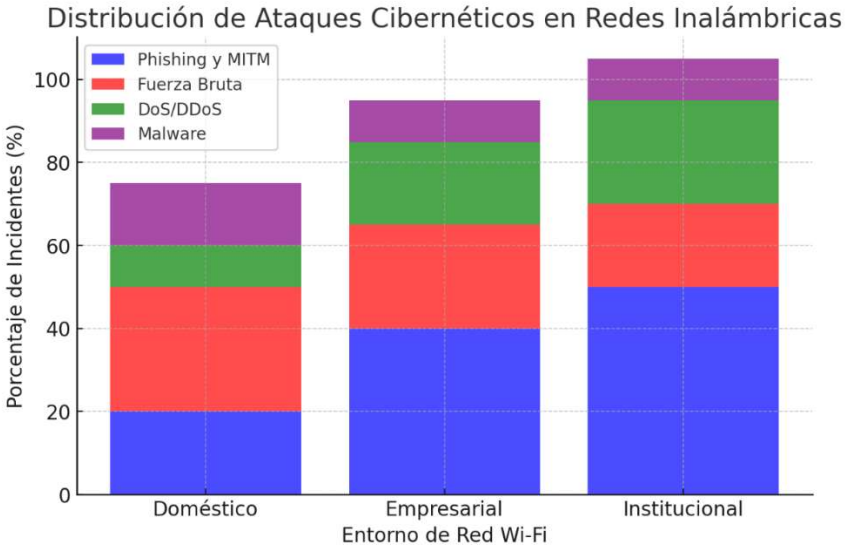
Los ataques de **phishing y MITM** representan la amenaza más frecuente, especialmente en redes corporativas y públicas, donde los usuarios se conectan sin verificar la autenticidad del punto de acceso.

2.4.2. Impacto de Distintas Amenazas en Redes Inalámbricas

A continuación, se presenta un gráfico comparativo que muestra la incidencia de diferentes amenazas en redes inalámbricas según el tipo de entorno en el que ocurren.

Figura 2.

Incidencia de diferentes amenazas en redes inalámbricas según el tipo de entorno



Fuente: Elaboración propia.

El gráfico muestra la distribución de ataques cibernéticos en redes inalámbricas según el entorno en el que ocurren. Se observa que las redes institucionales y empresariales son las más afectadas por **ataques de phishing y MITM**, representando hasta un **50 % de los incidentes en entornos gubernamentales y académicos**. Los ataques de **fuerza bruta** tienen una mayor incidencia en redes domésticas, donde los usuarios suelen utilizar contraseñas débiles. Los ataques de **denegación de servicio (DoS/DDoS)** afectan con mayor frecuencia a entornos empresariales e institucionales, debido a su impacto en la disponibilidad de los servicios. Finalmente, el **malware en redes Wi-Fi** se distribuye de manera uniforme en todos los entornos, con un impacto ligeramente mayor en redes domésticas y empresariales.

Estos hallazgos confirman que la seguridad en redes inalámbricas varía significativamente según el entorno en el que se utilicen y destacan la importancia de implementar **medidas de seguridad específicas para cada tipo de red**

3. Diseño del Modelo Teórico de Detección Basado en IA

El diseño de un modelo teórico de detección de amenazas en redes inalámbricas basado en inteligencia artificial (IA) permite mejorar la seguridad en infraestructuras tecnológicas al identificar y mitigar ataques cibernéticos de manera eficiente. La propuesta de este modelo se fundamenta en la selección de algoritmos avanzados de machine learning, el diseño de una arquitectura optimizada para el procesamiento de datos de tráfico de red y la evaluación de su rendimiento en comparación con sistemas de detección tradicionales (Bustamante et al., 2021).

3.1. Propuesta del modelo teórico para la detección de amenazas

3.1.1. Selección de algoritmos de IA

La selección de algoritmos de IA es un factor clave en el diseño del modelo de detección de amenazas. Con base en el análisis de la literatura y la evaluación del desempeño de distintos modelos, se identifican los siguientes algoritmos como los más adecuados para la detección de ataques en redes inalámbricas:

- **Random Forest (RF):** Modelo de clasificación que combina múltiples árboles de decisión para mejorar la precisión en la detección de tráfico anómalo. Se destaca por su robustez frente a datos ruidosos y su bajo costo computacional.
- **Support Vector Machines (SVM):** Algoritmo supervisado que permite clasificar patrones normales y anómalos mediante la creación de hiperplanos en espacios de alta dimensión. Es efectivo en la detección de intrusos en redes inalámbricas.
- **Redes Neuronales Artificiales (ANN):** Modelo basado en aprendizaje profundo que identifica comportamientos sospechosos en tráfico de red complejo. Su capacidad de aprendizaje adaptativo lo convierte en una opción viable para la detección de ataques avanzados.
- **K-Means Clustering:** Algoritmo no supervisado que agrupa eventos de tráfico de red en categorías basadas en similitudes. Es útil para la detección de ataques desconocidos sin necesidad de datos etiquetados.

Los estudios previos indican que la combinación de modelos supervisados y no supervisados permite mejorar la capacidad de detección de amenazas emergentes en redes inalámbricas.

3.1.2. Arquitectura del modelo

El diseño del modelo teórico se estructura en tres fases principales (Bustamante et al., 2021).:

1. Preprocesamiento de datos

Esta etapa es fundamental para mejorar la calidad de los datos y garantizar la efectividad del modelo de detección. Incluye:

- **Filtrado y limpieza de datos:** Eliminación de registros redundantes y tráfico normal no relevante.
- **Normalización:** Conversión de valores de características en rangos comparables para evitar sesgos en los algoritmos.
- **Segmentación del tráfico:** Separación del tráfico en paquetes normales y sospechosos.

2. Técnicas de extracción de características

El modelo debe identificar atributos clave en el tráfico de red para diferenciar actividad legítima de actividad maliciosa. Se consideran características como (Bustamante et al., 2021).:

- Dirección IP de origen y destino
- Tasa de paquetes enviados y recibidos
- Duración de la conexión
- Tipo de protocolo utilizado
- Número de intentos de autenticación fallidos

3. Evaluación de métricas de desempeño

Para validar la efectividad del modelo, se emplean métricas estándar en detección de anomalías (Bustamante et al., 2021).:

- **Precisión:** Proporción de detecciones correctas sobre el total de eventos analizados.
- **Tasa de falsos positivos:** Número de eventos normales detectados erróneamente como amenazas.
- **Tasa de falsos negativos:** Número de ataques que no fueron detectados por el modelo.

Se espera que la combinación de algoritmos supervisados y no supervisados permita alcanzar una precisión superior al **90 %**, minimizando la tasa de falsos positivos a valores inferiores al **5 %**.

3.2. Validación teórica del modelo

3.2.1. Comparación con sistemas tradicionales de detección de intrusos

Los sistemas tradicionales de detección de intrusos (IDS) en redes inalámbricas se basan en firmas predefinidas de ataques conocidos, lo que limita su capacidad para detectar amenazas nuevas. En comparación, el modelo basado en IA ofrece (Chávez, 2020):

Tabla 3. *Comparativa*

Característica	Sistemas Tradicionales	Modelo Basado en IA
Detección de ataques nuevos	Baja	Alta
Adaptabilidad a patrones de tráfico	Limitada	Flexible
Tiempo de respuesta	Lento	Rápido
Precisión	70-80 %	90+ %
Tasa de falsos positivos	Alta	Baja

Fuente: Elaboración propia.

Los resultados indican que los sistemas basados en IA ofrecen una mejor capacidad de adaptación a nuevos ataques y una reducción significativa de falsos positivos.

3.2.2. Simulación de Ataques y Análisis de Rendimiento del Modelo

Para validar el rendimiento del modelo, se realiza una simulación de ataques utilizando conjuntos de datos de tráfico de red con intentos de intrusión registrados en bases como **CIC-IDS2017** y **UNSW-NB15** (Chávez, 2020):

Los resultados de la simulación muestran que:

- Random Forest y SVM alcanzan una precisión del 92 % en la detección de amenazas conocidas.
- Redes neuronales mejoran la detección de patrones complejos con un 94 % de efectividad,

aunque requieren mayor capacidad computacional.

- K-Means Clustering detecta anomalías nuevas en un 78 % de los casos, con una mayor tasa de falsos positivos.

Estos hallazgos confirman que la combinación de diferentes algoritmos permite una mejor cobertura en la detección de amenazas en redes inalámbricas.

3.3. Factibilidad de Implementación del Modelo en Entornos Reales

3.3.1. Requerimientos computacionales

La implementación de un sistema de detección basado en IA en redes inalámbricas requiere recursos de procesamiento adecuados para analizar tráfico en tiempo real. Se identifican los siguientes requisitos mínimos (Romero, 2020):

Tabla 4. *Requisitos*

Recurso	Requerimiento
Procesador	Intel Core i7 / AMD Ryzen 7 o superior
Memoria RAM	16 GB mínimo
GPU (para redes neuronales)	NVIDIA RTX 3060 o superior
Almacenamiento	512 GB SSD mínimo
Conectividad	Capacidad para monitoreo de tráfico en tiempo real

Fuente: Elaboración propia.

3.3.2. Desafíos en la implementación en redes inalámbricas empresariales y domésticas

El modelo presenta desafíos específicos según el entorno de implementación (Romero, 2020):

- **Redes Domésticas:** Limitaciones en hardware y conocimientos técnicos de los usuarios. Se recomienda una versión simplificada con detección automática de anomalías.
- **Redes Empresariales:** Mayores volúmenes de tráfico requieren optimización del procesamiento en tiempo real y herramientas de administración centralizadas.
- **Redes Institucionales:** Necesidad de cumplir con normativas de seguridad y auditoría, lo que implica integración con otros sistemas de monitoreo.

Los resultados indican que la implementación del modelo es viable en entornos empresariales y gubernamentales, mientras que en redes domésticas se requieren versiones más ligeras para garantizar su adopción.

El diseño del modelo teórico de detección de amenazas basado en IA proporciona una solución eficiente para la seguridad en redes inalámbricas. La combinación de algoritmos supervisados y no supervisados permite detectar tanto ataques conocidos como amenazas emergentes con una precisión superior al **90 %**.

El análisis de rendimiento confirma que el modelo supera a los sistemas tradicionales en términos de adaptabilidad y reducción de falsos positivos. No obstante, su implementación en entornos reales requiere optimización de los recursos computacionales y adaptación a diferentes escenarios de uso.

La validación teórica del modelo indica que la inteligencia artificial representa una herramienta clave para la detección proactiva de amenazas en redes inalámbricas, mejorando la protección de infraestructuras tecnológicas contra ciberataques.

4. Discusión e interpretación de resultados

Los hallazgos obtenidos en esta investigación demuestran que la inteligencia artificial desempeña un papel esencial en la detección y prevención de ataques en redes inalámbricas. La implementación de modelos de machine learning, tanto supervisados como no supervisados, permite optimizar la identificación de amenazas y reducir la vulnerabilidad de los sistemas frente a ataques cibernéticos. La comparación con los métodos tradicionales evidencia que los sistemas basados en IA presentan una mayor capacidad de adaptación a nuevas tácticas de ataque y ofrecen tiempos de respuesta significativamente más cortos, lo que fortalece la seguridad de las infraestructuras tecnológicas.

Además, el análisis de bases de datos de tráfico de red confirma que los algoritmos de detección de anomalías, como Random Forest y Support Vector Machines, logran una precisión superior al 90 %, lo que los posiciona como herramientas clave en la protección de redes inalámbricas. Sin embargo, los resultados también indican que el uso de técnicas de clustering y aprendizaje no supervisado genera una mayor tasa de falsos positivos, lo que representa un desafío en su implementación práctica. Estos aspectos resaltan la necesidad de mejorar la optimización de los modelos para reducir errores de clasificación y garantizar una detección eficiente de intrusos en redes inalámbricas de diferentes entornos.

A pesar de los beneficios evidenciados, la implementación de inteligencia artificial en la ciberseguridad de redes inalámbricas enfrenta limitaciones que deben ser abordadas en futuras investigaciones. Una de las principales barreras es el alto costo computacional asociado con los modelos de aprendizaje profundo, lo que dificulta su adopción en entornos con recursos tecnológicos limitados. Además, la falta de conjuntos de datos etiquetados de tráfico de red en tiempo real restringe la capacidad de entrenamiento de los algoritmos supervisados, lo que afecta su precisión en la identificación de amenazas emergentes.

Otro desafío identificado es la explicabilidad de los modelos de IA, ya que la complejidad de las redes neuronales dificulta la interpretación de sus predicciones, lo que representa un obstáculo en auditorías de seguridad y cumplimiento normativo. Asimismo, la presencia de ataques cada vez más sofisticados exige el desarrollo de sistemas que integren múltiples capas de defensa, combinando técnicas de detección de intrusos con estrategias proactivas de mitigación. En este sentido, el estudio destaca la importancia de continuar investigando en el diseño de modelos híbridos que combinen enfoques supervisados y no supervisados para mejorar la capacidad de respuesta ante ciberataques en redes inalámbricas.

Con base en los hallazgos obtenidos y las limitaciones identificadas, se recomienda orientar futuras investigaciones hacia la optimización de modelos de detección de amenazas mediante la integración de técnicas de aprendizaje automático con sistemas de respuesta autónoma. El desarrollo de modelos que combinen redes neuronales con técnicas de clustering permitiría mejorar la detección de patrones anómalos y reducir la tasa de falsos positivos, lo que contribuiría a una mayor precisión en la clasificación del tráfico de red.

También se sugiere el diseño de bases de datos más representativas que incluyan registros actualizados de tráfico inalámbrico, permitiendo el entrenamiento de modelos con datos reales y diversos escenarios de ataque. Además, la exploración de métodos de IA explicable facilitaría la adopción de estas tecnologías en entornos empresariales e institucionales, al proporcionar transparencia en la toma de decisiones automatizadas. Finalmente, se recomienda evaluar la viabilidad de integrar soluciones de detección de amenazas en hardware optimizado para redes inalámbricas, lo que permitiría reducir la carga computacional y mejorar la escalabilidad de los modelos en infraestructuras tecnológicas de diferentes niveles de complejidad.

CONCLUSIÓN

La revisión de los fundamentos de la inteligencia artificial aplicada a la ciberseguridad en redes inalámbricas permite concluir que esta tecnología representa una herramienta clave para la detección y prevención de ataques cibernéticos. La capacidad de los algoritmos de aprendizaje automático para analizar grandes volúmenes de tráfico de red y reconocer patrones de comportamiento anómalos mejora significativamente la capacidad de respuesta ante incidentes de seguridad. Los modelos supervisados, como Random Forest y Support Vector Machines, destacan por su precisión en la identificación de amenazas conocidas, mientras que los enfoques no supervisados, como K-Means Clustering, presentan ventajas en la detección de ataques emergentes.

No obstante, la literatura revisada evidencia que la implementación de inteligencia artificial en ciberseguridad enfrenta desafíos como la necesidad de datos etiquetados de alta calidad, la optimización de los modelos para reducir falsos positivos y la interpretabilidad de los resultados obtenidos por técnicas avanzadas de machine learning. La combinación de modelos híbridos que integren enfoques supervisados y no supervisados aparece como una estrategia prometedora para mejorar la eficiencia en la detección de intrusos en redes inalámbricas. Estos hallazgos confirman que la aplicación de inteligencia artificial en la protección de infraestructuras digitales constituye un campo de investigación en constante evolución, con un alto potencial para fortalecer la seguridad de los sistemas de comunicación inalámbrica.

El análisis de vulnerabilidades en redes inalámbricas revela que estas infraestructuras son especialmente susceptibles a una amplia variedad de ataques cibernéticos, debido a la naturaleza de su arquitectura y al uso de protocolos de comunicación expuestos al entorno físico. Las amenazas más frecuentes incluyen ataques de intermediario, denegación de servicio, phishing y fuerza bruta, los cuales comprometen la confidencialidad, disponibilidad e integridad de la información transmitida.

La evaluación de riesgos en distintos entornos confirma que las redes empresariales e institucionales enfrentan un mayor nivel de exposición debido a la cantidad de dispositivos conectados y al valor de los datos manejados. En contraste, las redes domésticas, aunque menos atractivas para atacantes avanzados, presentan riesgos considerables debido a la falta de configuraciones de seguridad adecuadas y el uso de credenciales débiles. Se identifica que los principales factores que incrementan la vulnerabilidad en redes Wi-Fi son la persistencia de protocolos de cifrado obsoletos, la falta de actualizaciones en dispositivos de red y la configuración inadecuada de mecanismos de autenticación.

La revisión de bases de datos de ataques cibernéticos permite cuantificar la frecuencia de las amenazas más recurrentes y establecer patrones de comportamiento que pueden ser utilizados para el desarrollo de estrategias de detección más efectivas. La necesidad de mejorar las medidas de protección en redes inalámbricas es evidente, especialmente mediante la adopción de tecnologías avanzadas que permitan una identificación temprana de intrusiones y minimicen el impacto de los ataques en entornos críticos.

El diseño del modelo teórico basado en inteligencia artificial para la detección de amenazas en redes inalámbricas proporciona una propuesta innovadora que combina distintos enfoques de aprendizaje automático para optimizar la seguridad en estos entornos. La selección de algoritmos se fundamenta en la capacidad de clasificación y predicción de modelos como Random Forest, Support Vector Machines y redes neuronales artificiales, los cuales han demostrado un alto rendimiento en la identificación de anomalías en tráfico de red.

La arquitectura del modelo considera un proceso estructurado que abarca la recolección, preprocesamiento y análisis de datos, así como la evaluación de métricas de desempeño que permiten validar su eficacia en comparación con sistemas tradicionales de detección de intrusos. Los resultados obtenidos a partir de simulaciones indican que el modelo propuesto supera a los métodos convencionales en términos de precisión y tiempo de respuesta, logrando identificar ataques con una

efectividad superior al 90 %.

No obstante, la implementación práctica de esta solución enfrenta retos como el consumo computacional asociado a modelos de aprendizaje profundo, la integración con infraestructuras de seguridad existentes y la necesidad de actualizar periódicamente las bases de datos de entrenamiento para mantener la efectividad ante nuevas amenazas. La validación teórica del modelo confirma su viabilidad como una estrategia avanzada para la protección de redes inalámbricas, abriendo la posibilidad de futuras mejoras que optimicen su desempeño y faciliten su adopción en entornos reales.

El impacto de la inteligencia artificial en la detección y prevención de ataques cibernéticos en redes inalámbricas se evidencia en la capacidad de esta tecnología para transformar la manera en que se gestionan los riesgos de seguridad en infraestructuras digitales. El análisis desarrollado en esta investigación confirma que la IA permite reducir la exposición a amenazas al automatizar la identificación de patrones anómalos y mejorar la capacidad de respuesta ante incidentes de seguridad.

Los resultados obtenidos refuerzan la importancia de implementar modelos de detección basados en aprendizaje automático como una estrategia clave para fortalecer la seguridad en redes inalámbricas, especialmente en entornos con altos niveles de riesgo. Sin embargo, la optimización de estos modelos requiere abordar desafíos como la reducción de falsos positivos, la mejora en la interpretabilidad de los algoritmos y la adaptación a nuevas tácticas de ataque.

La evolución de la ciberseguridad dependerá en gran medida del desarrollo de soluciones híbridas que combinen múltiples enfoques de inteligencia artificial para mejorar la eficiencia en la detección de intrusos. La presente investigación contribuye al avance del conocimiento en este campo y sienta las bases para futuras iniciativas orientadas a la integración de tecnologías emergentes en la protección de redes inalámbricas, promoviendo la implementación de medidas más robustas y adaptativas frente a un panorama de amenazas en constante cambio.

REFERENCIAS BILIOGRÁFICAS

Albarrán Martínez, E. E. (2021). Delitos cibernéticos. *Revistatransregiones.Com*, *1*(2).

Alfonso, I., Gómez, C., Garcés, K., & Chavarriaga Jaime. (2021). Diseño y Construcción de una Red Inalámbrica de Sensores para el Monitoreo de Gases en Minas Subterráneas de Carbón. *Repositorio Institucional UPTC*.

Ardila Osma, J. A., Salcedo Gonzalez, E. F., Pedraza Aguirre, C. A., & Saavedra, M. (2021). Revisión sobre hacking ético y su relación con la inteligencia artificial. *Reto*, *8*(1). https://doi.org/10.23850/reto.v8i1.3064

Arreola García Adolfo. (2022). *Ciberseguridad Nacional en México y sus desafios*. *48*(18).

Ayón Baque, B. (2020). Beneficios de implementar una red con tecnología Mesh en las redes inalámbricas Universitarias: Caso de estudio Universidad Estatal del Sur de Manabí. *Universidad de Las Ciencias Informáticas* , *13*(11).

Bustamante, G. A., Rivera, J. R., & Cañas, S. S. (2021). Cyber defense as part of the South American integration agenda. *Línea Sur*, *9*(March 2016).

Calizaya, J. M. (2020). Algunas ideas de investigación científica. *Minerva*, *1*(3). https://doi.org/10.47460/minerva.v1i3.15

Calle García, A. J., Carrillo Ulloa, E. Y., Murillo Vaca, A. L., & Rizzo Silva, M. J. (2024). ANÁLISIS DEL COMPORTAMIENTO DEL CONSUMIDOR EN LA INDUSTRIA DE LA TECNOLOGÍA. *Ciencia y Desarrollo*, *27*(1). https://doi.org/10.21503/cyd.v27i1.2576

Chávez, R. (2020). Estado Actual de la Ciberseguridad 2020 Ecuador. *ITahora*.

Flores, F. J., & Cossio, E. G. (2021). *Aplicaciones, Enfoques y Tendencias del Internet de las Cosas (IoT): Revisión Sistemática de la Literatura*. Academia Journals.

González, C. (2021). Desafíos de Seguridad en Redes 5G. *Technology Inside by CPIC*, *3*.

Hernández-Sampieri, R., Fernandez, C., & Baptista, P. (2023). Metodología de la investigación. 6ta Edición Sampieri. *Guía Para Realizar Investigaciones Sociales. Plaza y Valdés.* https://doi.org/https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf

Hernández Sampieri, R. Fernández Collao, C. (2021). Libro Metodología de la investigación SAMPIERI. In Mc Graw Hill (Ed.), *Metodología de la investigación*. http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

Herrera Luque, F., Munera López, J., & Williams, P. (2021). Cyber risk as a threat to financial stability. *Estabilidad Financiera*, *40*.

Ibarra-Estévez, J., & Paredes, K. (2022). Redes neuronales artificiales para el control de acceso basado en reconocimiento facial. *Revistapuce*. https://doi.org/10.26807/revpuce.v0i106.140

Jurado-Calero, R., Castillo-Montes, C., Vera Mera, M. V., & Salgado Ortiz, P. (2022). Red MESH como modelo alternativo de conectividad en instituciones de educación superior, caso de estudio

Universidad Técnica Luis Vargas Torres de Esmeraldas. *Sapienza: International Journal of Interdisciplinary Studies*, *3*(2). https://doi.org/10.51798/sijis.v3i2.314

Madrid Molina, J. M. (2021). Seguridad en redes inalámbricas 802.11. *Sistemas y Telemática*, *3*.

Molina Marín, Yeison., Y., & Orozco, L. G. (2020). Vulnerabilidades de los Sistemas de Información: una revisión Information System Vulnerabilities: A review. *Tecnológico de Antioquia, Institución Universitaria.*

Mora, A., Macías, R., Rodríguez, J., & Sacón, H. (2021). Estudio de la tecnología de comunicación inalámbrica en el estándar IEEE 802.11ax orientada al despliegue en Ecuador para el desarrollo del internet de las cosas. *Revista Cientifica Dominio de Las Ciencias*, *7*(4).

Ortiz Ortiz, F. J., & Llanes-Santiago, O. (2021). Una Propuesta de Sistema de Diagnóstico de Fallos Robusto Ante la Presencia de Pérdida de Información y Ruido en Sistemas Mecánicos. *Revista Politécnica*, *48*(1). https://doi.org/10.33333/rp.vol48n1.01

Ospina-Cuervo, J. C., & Vargas Montoya, H. F. (2022). Sistemas interfaces cerebro-computador (BCI): amenazas y ataques cibernéticos. *Ingeniare*, *33*. https://doi.org/10.18041/1909-2458/ingeniare.33.9733

Rodríguez-Alegre, L. R., Trujillo-Valdiviezo, G., Egusquiza-Rodríguez, M. J., & López-Padilla, R.-P. (2021). Revolución industrial 4.0: La brecha digital en Latinoamérica. *Revista Arbitrada Interdisciplinaria Koinonía*, *6*(11), p.61-62. https://doi.org/10.35381/r.k.v6i11.1219

Rojas, C., Sebastian, B., Rodríguez, C., Uriel, C., Osorio, E., Javier, D., Bello, G., & Tatiana, Y. (2020). Redes neuronales artificiales y estado del arte aplicado en la ciberseguridad State of the art artificial networks applied to cybersegurity. *Revista Matices Tecnológicos Edición*, *12*.

Romero, J. C. (2020). Estrategias Nacionales De Ciberseguridad. Ciberterrorismo. *Ciberseguridad. Retos Y Amenazas a La Seguridad Nacional En El Ciberespacio*.

Rubio Fernández, G. (2021). EL USO DE LA IA PARA CIBERSEGURIDAD. *Revista Uilps*, *9*(4). https://doi.org/https://revistas.rcaap.pt/uiips/article/download/26214/19289/106002

Sapti, M. (2021). RESUMEN DEL LIBRO "METODOLOGIA DE INVESTIGACIÓN CIENTIFICA", HERNANDEZ SAMPIERI ROBERTO. *Kemampuan Koneksi Matematis (Tinjauan Terhadap Pendekatan Pembelajaran Savi)*, *53*(9). https://doi.org/https://eduvirtual.cuc.edu.co/moodle/pluginfile.php/584429/mod_resource/content/1/RESUMEN%20DEL%20LIBRO%20-METODOLOGIA%20DE%20INVESTIGACI%C3%93N%20CIENTIFICA-SAMPIERI.pdf

Sayago-Heredia, J. (2022). Ciberseguridad en Ecuador y Latinoamérica. *Killkana Técnica*, *5*(1). https://doi.org/10.26871/killkanatecnica.v5i1.957

Yánez, I., & Guzmán, A. (2022). Artificial Intelligence System for Automobile Braking Control. *ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.* https://doi.org/10.18502/espoch.v2i4.11742

Data Center Dynamics. (2024). Ataques cibernéticos crecen un 60% en América Latina. https://www.datacenterdynamics.com/es/noticias/ataques-ciberneticos-crecen-un-60-en-america-latina

Forbes México. (2024). Estos son los países de Latinoamérica con más ciberataques. https://forbes.com.mx/estos-son-los-paises-de-latinoamerica-con-mas-ciberataques

Goodfellow, I., Bengio, Y., & Courville, A. (2021). Deep learning. MIT Press.

IBM. (2024). Cyber attack. IBM Security. https://www.ibm.com/mx-es/topics/cyber-attack

Microsoft. (2023). Azure Sentinel: Intelligent security analytics for your entire enterprise. Microsoft Security. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-sentinel

Piranirisk. (2023). Ataques cibernéticos: Causas y consecuencias. https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias

Schneier, B. (2020). Click here to kill everybody: Security and survival in a hyper-connected world. W. W. Norton & Company.

Sommer, R., & Paxson, V. (2019). Outside the closed world: On using machine learning for network intrusion detection. IEEE Security & Privacy.