Revista Multidisciplinaria Perspectivas Investigativas
Multidisciplinary Journal Investigative Perspectives
Vol. 5(especial tecnología), 23-34, 2025
https://doi.org/10.62574/rmpi.v5iTecnologia.276

Algoritmos de Machine Learning e inteligencia artificial en la detección de patrones de ciberataques
Machine Learning and artificial intelligence algorithms in the detection of cyber-attack patterns

Wendy Viviana Obregón-Martínez
wendy.obregon@gmail.com
Red de Investigación Koinonia, Portoviejo, Manabí, Ecuador
https://orcid.org/0000-0003-2402-6670

Gabriel Eduardo Morejón-López
gabriel.morejon@utm.edu.ec
Universidad Técnica de Manabí, Portoviejo, Manabí, Ecuador
https://orcid.org/0000-0001-8902-4583

César Armando Moreira-Zambrano
cmoreira@espam.edu.ec
Escuela Superior Politécnica Agropecuaria de Manabí, "Manuel Félix López", Calceta, Manabí, Ecuador
https://orcid.org/0000-0002-0781-0757

Luis Nibaldo Oyarzún-Álava
luis.oyarzun@utm.edu.ec
Universidad Técnica de Manabí, Portoviejo, Manabí, Ecuador
https://orcid.org/0000-0002-5264-6810

RESUMEN

El presente artículo tiene como objetivo evaluar el desempeño de diversos algoritmos de machine learning en la detección de ciberataques en la mitigación de amenazas dentro de redes y sistemas informáticos. La metodología fue de validación experimental y la ejecución se realizó mediante el método informático ciclo en V. Se evidenció la efectividad de los algoritmos de *Machine Learning* (ML) en la detección y mitigación de ciberataques, destacándose su capacidad para identificar patrones maliciosos en el tráfico de red. Los resultados obtenidos validan la aplicabilidad de modelos como *Support Vector Machines* (SVM) y *Naive Bayes* (NB), los cuales han demostrado un desempeño significativo en la clasificación de amenazas, siendo SVM más eficiente en la detección de ataques complejos y NB más rápido y con menor costo computacional. En términos prácticos, la implementación de estos modelos en entornos empresariales y gubernamentales podría mejorar significativamente la capacidad de respuesta ante ciberataques.

Descriptores: elección de tecnología; evaluación de la tecnología; aplicación informática. (Fuente: Tesauro UNESCO).

ABSTRACT

This article aims to evaluate the performance of various machine learning algorithms in the detection of cyber-attacks in the mitigation of threats within networks and computer systems. The methodology was experimental validation and the execution was carried out using the V-cycle computing method. The effectiveness of *Machine Learning* (ML) algorithms in the detection and mitigation of cyber-attacks was demonstrated, highlighting their ability to identify malicious patterns in network traffic. The results obtained validate the applicability of models such as *Support Vector Machines* (SVM) and *Naive Bayes* (NB), which have demonstrated significant performance in threat classification, with SVM being more efficient in detecting complex attacks and NB faster and with lower computational cost. In practical terms, implementing these models in enterprise and government environments could significantly improve cyberattack response capabilities.

Descriptors: choice of technology; technology assessment; computer applications. (Source: UNESCO Thesaurus).

Recibido: 29/01/2025. Revisado: 12/02/2025. Aprobado: 25/02/2025. Publicado: 26/02/2025.
Sección artículos de Tecnología

INTRODUCCIÓN

En un mundo digitalizado, la seguridad de la información, ampliamente conocida como ciberseguridad, se ha convertido en un aspecto fundamental para la protección de datos y sistemas. Por lo tanto; la evolución de las amenazas cibernéticas ha pasado de ataques convencionales, como el malware y el phishing, a estrategias más sofisticadas como la denegación de servicio distribuida (DDoS) y las amenazas persistentes avanzadas (APT). En este escenario, la necesidad de mejorar los mecanismos de detección y respuesta ante incidentes es más apremiante que nunca (Flores, 2020). Asimismo, ante esta creciente complejidad, la inteligencia artificial (IA), y en particular el machine learning (aprendizaje automático), ha emergido como una herramienta para fortalecer la defensa cibernética, por cuanto permiten procesar grandes volúmenes de datos en tiempo casi real, dotando a los sistemas de una capacidad de adaptación superior, logrando una detección de anomalías mucho más precisa que los métodos tradicionales basados en firmas (León, 2022).

En este orden, la adopción de la IA en seguridad informática impulsa la automatización y optimización de procesos críticos, como el filtrado de intrusiones, la clasificación de incidentes, así como la toma de decisiones de mitigación. Por consiguiente, estos avances resultan fundamentales para organizaciones que enfrentan un número creciente de alertas, así como eventos de seguridad, desafiando su capacidad de respuesta y gestión eficiente de riesgos (Zhang et al., 2021). Para ello, se examinan algoritmos ampliamente utilizados en el campo de la ciberseguridad, tales como Naive Bayes, Support Vector Machines (SVM), redes neuronales y aprendizaje, proporcionando una visión integral de su aplicación en entornos reales y proponiendo lineamientos estratégicos para su implementación efectiva (Obregón-Martínez, et al 2024).

En este escenario, el presente artículo tiene como objetivo evaluar el desempeño de diversos algoritmos de machine learning en la detección de ciberataques en la mitigación de amenazas dentro de redes y sistemas informáticos.

MÉTODO

La investigación se realizó en la empresa proveedores de internet ISP MASNET de Manabí.

Los materiales utilizados fueron:

a) La Infraestructura como servicio
b) El sistema de virtualización
c) Sistemas de almacenamiento masivo y sistemas operativos tradicionales con la finalidad de proveer una alta disponibilidad, así como confiabilidad de operatividad de los servicios que ofrece MASNET.

La metodología utilizada fue de validación experimental y la ejecución se realizó mediante el método informático ciclo en V. Se contemplaron las fases de:

a) Especificaciones
b) Diseño de alto nivel y de detalle
c) Implementación
d) Test unitario, de integración y operacional

Fase de Especificaciones

Para esta fase fue fundamental la utilización de equipos tecnológicos ya desplegados en un proveedor de internet, dentro de los cuales se definen router, switch, servidores físicos, los mismos que tiene información de los registros log, tráfico generado de la red de datos, los mismos que permiten albergar las diferentes anomalías que se generan desde la WAN hacia la red la LAN lo que en ocasiones permite la inhibición de los sistemas imagen 1.

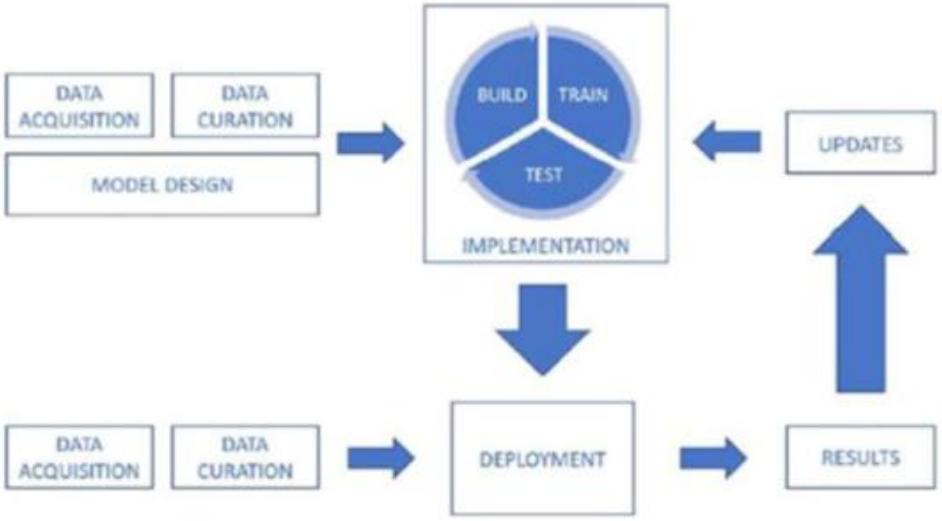

Figura 1. *Adquisición de datos y entrenamiento del modelo.* Elaborado por autores.

Dentro de esta fase se realiza la detección de ataques no registrados, dirigidos a vulnerabilidades aún no identificadas en el sistema operativo o software (conocidos como Zero Day), presenta un desafío tecnológico significativo. Aquellos que desarrollan malware están familiarizados con las debilidades de los sistemas de seguridad y se esfuerzan por superar las defensas del mercado. Con el propósito de evitar e identificar posibles ataques, se utilizan sistemas asociación o correlación que integran métodos de Inteligencia Artificial, especialmente Machine Learning (ML). No obstante, si el malware logra eludir las defensas perimetrales, firewalls, filtros como de aplicaciones web y las políticas Zero Trust, la última barrera de protección se encuentra en el agente protector integrado al sistema operativo del dispositivo. (Portela, 2022, p. 5).

Fase de diseño de alto nivel y de detalle

En diseño de alto nivel de un sistema de detección de ciberataques basado en algoritmos de Machine Learning, se han definido seis fases clave en el proceso de diseño, abarcando desde la infraestructura de red hasta la mitigación de amenazas ver tabla 1.

Tabla 1. *Detección y mitigación de ciberataques.*

Fase	Descripción
Infraestructura de Red	Routers, Switches, Servidores, Firewalls. Captura de tráfico y logs de eventos sospechosos.
Recolección de Datos	Fuentes: Tráfico de red, logs de servidores, eventos de seguridad. Métodos: Wireshark, Tcpdump, Splunk, ELK Stack.
Preprocesamiento de Datos	Limpieza de datos, eliminación de redundancias y valores nulos. Extracción de características clave (Feature Engineering).
Modelo de Machine Learning	Uso de algoritmos como SVM, Naive Bayes y Redes Neuronales. Entrenamiento y evaluación con métricas de rendimiento.
Detección de Ciberataques	Clasificación de tráfico (Malicioso vs. Legítimo). Identificación de patrones de ataques en tiempo real.
Respuesta y Mitigación	Bloqueo automático de amenazas. Aplicación de reglas en Firewalls e IDS/IPS. Implementación de Zero Trust y segmentación de red.

Elaborado por autores.

Fase de implementación

Dentro de esta fase se explican las herramientas existentes para detección, prevención de intrusiones y de administración de eventos y de la seguridad de la información se pueden fácilmente adaptar a la propuesta de modelos de aprendizaje automático y ejecución de procesos sobre mitigación de la ciberseguridad, a razón de buscar generar más confianza en el uso de las tecnologías, disminuir el impacto de las pérdidas e incrementar la transparencia en los procesos de gestión. Los algoritmos de machine learning en la IA pueden desempeñar un papel crucial en la detección de patrones de ciberataques y la mitigación de su impacto. Aquí hay algunas maneras en que estos algoritmos son útiles en este contexto:

Detección de anomalías: utilizan modelos de aprendizaje no supervisado para identificar comportamientos inusuales en los datos de red. Esto permite detectar actividades sospechosas que podrían indicar un ciberataque en curso como el análisis de comportamiento los mismo que permiten que los algoritmos de aprendizaje automático pueden analizar el comportamiento normal de usuarios y sistemas para identificar desviaciones significativas. Esto facilita la detección de actividades maliciosas que podrían pasar desapercibidas mediante métodos tradicionales (Aljamal et al., 2019).

Mediante el uso de algoritmos predictivos, la IA puede anticipar posibles amenazas al analizar patrones históricos y tendencias, esto ayuda en la identificación temprana de posibles ciberataques y permite la toma de medidas preventivas, detección de Amenazas Avanzadas Persistentes (ATP): Los algoritmos de inteligencia artificial son eficaces para identificar patrones asociados con amenazas avanzadas persistentes, estas amenazas suelen ser más complejas y persistentes, y los modelos de IA pueden ser entrenados para reconocer sus características distintivas (Obregón-Martínez, et al 2024).

Los algoritmos de IA pueden automatizar la respuesta a incidentes de seguridad, permitiendo respuestas más rápidas y precisas ante amenazas, esto implica la habilidad de separar sistemas comprometidos, impedir el acceso de direcciones IP perjudiciales y emprender acciones correctivas de forma autónoma. Identificando firmas maliciosas, los algoritmos pueden analizar patrones de código malicioso para identificar firmas específicas de malware, esto facilita la detección de amenazas conocidas y la aplicación de medidas de seguridad específicas (Flores, 2020).

Los modelos de machine learning pueden actualizarse con nuevos datos para mantenerse al día con las tácticas cambiantes de los ciberdelincuentes. Técnicas, es un trabajo de investigación de tecnología aplicada; combinando técnicas de análisis documental y de contenido sobre algoritmos de IA y su comportamiento en la ciberseguridad. La utilización del conjunto de datos representativos es utilizados y representativos que contengan ejemplos de amenazas y comportamientos normales. Estos conjuntos deben abarcar diversas tácticas de ciberataques y reflejar la complejidad del entorno de seguridad. Validación Cruzada: aplican técnicas de validación cruzada para evaluar la generalización del algoritmo, esto implica fragmentar el conjunto de datos en varias secciones y entrenar/probar el modelo en diversas combinaciones, lo que ayuda a evaluar su rendimiento en diversas condiciones (Obregón-Martínez, et al 2024).

Por otra parte, las matrices de confusión se utilizan para evaluar la capacidad del algoritmo para clasificar correctamente las instancias, esto incluye la identificación de verdaderos positivos, verdaderos negativos, falsos positivos y falsos negativos, proporcionando una visión detallada del rendimiento. Curvas ROC (Receiver Operating Characteristic), analizan las curvas ROC y calculan el área bajo la curva (AUC) para medir la capacidad de discriminación del modelo entre las clases de interés. (Obregón-Martínez, et al 2024).

Fase de test unitario

El concepto de ciberseguridad incorpora un conjunto de estrategias, técnicas y medidas diseñadas para resguardar los sistemas de información, redes, dispositivos electrónicos y datos digitales de posibles incidentes maliciosos, accesos no autorizados, robo de información, daños entre otras vulnerabilidades (Hirare, 2017). El objetivo principal es asegurar la privacidad, autenticidad y accesibilidad de los activos digitales y protegerlos de amenazas cibernéticas, esto también implica la adopción de acciones preventivas, identificación temprana de intrusiones y reacción rápida ante tales incidentes. Con base en esto se busca analizar herramientas que utilicen algoritmos de machine learning con IA para potenciar la capacidad de reconocimiento de ciberataques.

Los algoritmos de machine learning pueden desempeñar un papel importante en búsqueda de patrones de seguridad para poder mitigar el impacto de los ciberataques, puesto que ayudarían en procesos de detección de anomalías como son los comportamientos normales de los sistemas y redes para identificar patrones extraños que podrían significar ataques en curso, siendo importante detectar desviaciones inusuales en el tráfico de la red, el uso de los recursos entre otros indicadores claves (Flores, 2020).

Estos algoritmos pueden ser entrenados con un conjunto de datos etiquetados que contienen ejemplos de ciberataques y actividades legítimas, a medida que se alimenta al algoritmo con más datos, pueden aprender a reconocer patrones y características específicas asociadas con diferentes tipos de ataques. También se pueden utilizar redes neuronales profundas y otros enfoques de aprendizaje profundo que son efectivos para analizar datos no estructurados y extraer características complejas, estos consiguen detectar amenazas incipientes al procesar grandes cantidades de registros de actividades y tráfico de red (Castellanos et al., 2020).

Poder analizar modelos de comportamiento para usuarios, dispositivos o sistemas; Identificado patrones típicos y alertar cuando se desvían de ellos, y de esta manera detectar actividades sospechosas y no autorizadas.

RESULTADOS

SVM un algoritmo de aprendizaje supervisado, se emplea en la clasificación y regresión, siendo particularmente relevante en el ámbito de la detección de malware, SVM busca encontrar un hiperplano óptimo que pueda separar de manera eficiente las instancias de malware de las instancias no maliciosas en un espacio multidimensional. Ayuda a encontrar un conjunto reducido de patrones comunes entre los dispositivos, el tráfico de red generado y acumulado en los registros a través de los cuales se determinó la ocurrencia de los ataques.

Kernel Trick: SVM utiliza a menudo el "kernel trick" para mapear los elementos a un espacio de atributos de mayor dimensión, facilitando la identificación de un hiperplano que pueda separar las clases de manera más efectiva. Se empleó el algoritmo de clasificación probabilística basado en el teorema de Bayes, se lo utilizó para calcular las probabilidades condicionales de pertenencia a una clase dada con los campos seleccionados.

/

	id.resp_h	id.resp_p	proto	service	duration	orig_bytes	...	\
0	47.114.46.156	23.0	tcp	NaN	2.998793	0	...	
1	178.0.255.246	29619.0	udp	NaN	<NA>	<NA>	...	
2	63.54.63.20	23.0	tcp	NaN	<NA>	<NA>	...	
3	145.92.75.64	40632.0	udp	NaN	<NA>	<NA>	...	
4	86.198.71.53	8080.0	tcp	NaN	<NA>	<NA>	...	
...	...	...	...	...	...	...	...	
39995	176.64.18.6	23978.0	udp	NaN	<NA>	<NA>	...	
39996	73.190.94.184	19537.0	udp	NaN	<NA>	<NA>	...	
39997	27.199.8.223	23.0	tcp	NaN	2.998542	0	...	
39998	236.83.107.101	54946.0	udp	NaN	<NA>	<NA>	...	
39999	205.236.111.104	8385.0	tcp	NaN	2.998547	0	...	

	local_resp	missed_bytes	history	orig_pkts	orig_ip_bytes	resp_pkts	\
0	NaN	0.0	S	3.0	180.0	0.0	
1	NaN	0.0	D	1.0	40.0	0.0	
2	NaN	0.0	S	1.0	60.0	0.0	
3	NaN	0.0	D	1.0	40.0	0.0	
4	NaN	0.0	S	1.0	60.0	0.0	
...	...	...	...	...	...	...	
39995	NaN	0.0	D	1.0	40.0	0.0	
39996	NaN	0.0	D	1.0	40.0	0.0	
39997	NaN	0.0	S	3.0	180.0	0.0	
39998	NaN	0.0	D	1.0	40.0	0.0	
39999	NaN	0.0	S	3.0	180.0	0.0	

Figura 2. *Clasificación de puertos y protocolos precedencia del ataque*. Elaborado por autores

En el caso de la detección de malware se buscó en que intervalo de tiempo han ocurrido esas amenazas y se evalúan las probabilidades que ciertas características del tráfico de red indiquen la presencia de malware, dentro de sus características es fácil de implementar y funciona bien incluso con conjuntos de datos de dimensiones considerables, como se puede observar en la figura 3.

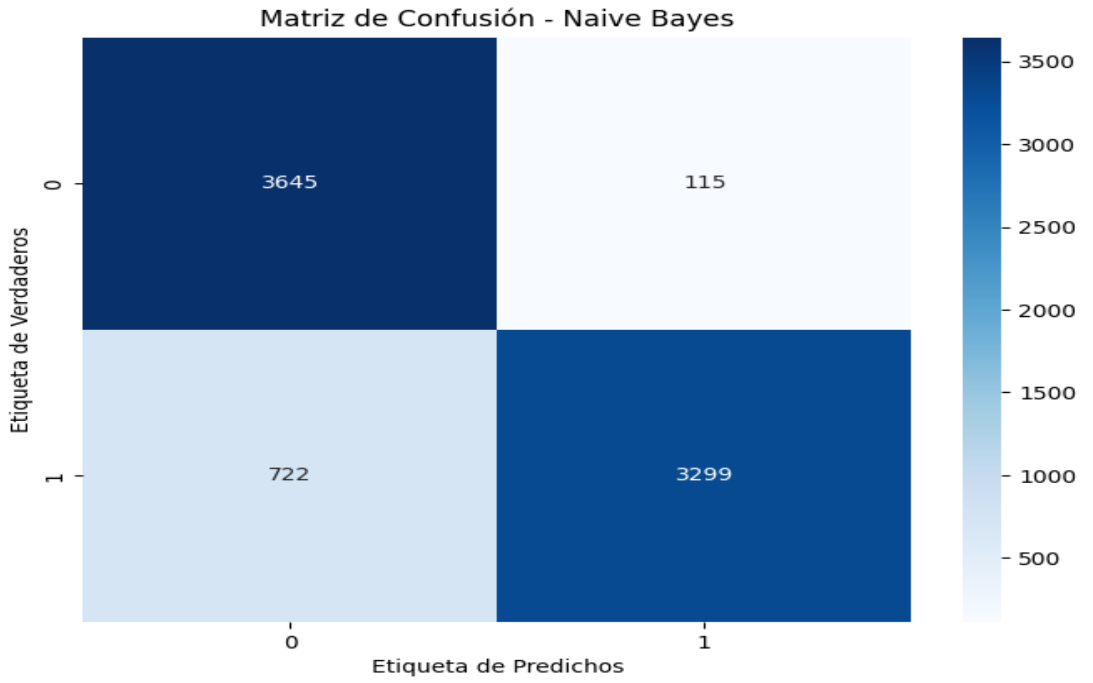

Figura 3. *Resultado de Matriz de confusión Naive Bayes*. Elaborado por autores.

Con los resultados derivados de la implementación de este algoritmo se ha empleado herramientas de visualización como el mapa de calor que se pueden revisar en las figuras, 4, 5, 6 y el código de barras en la figura 7, para representación visual de los datos, para evidenciar y resaltar los patrones y tendencias de datos obtenidos y de la manera que están relacionadas las diferentes variables para tener un mejor entendimiento y evaluación de la información referente a su funcionamiento y eficacia con respecto a la detección de patrones de amenazas cibernéticas.

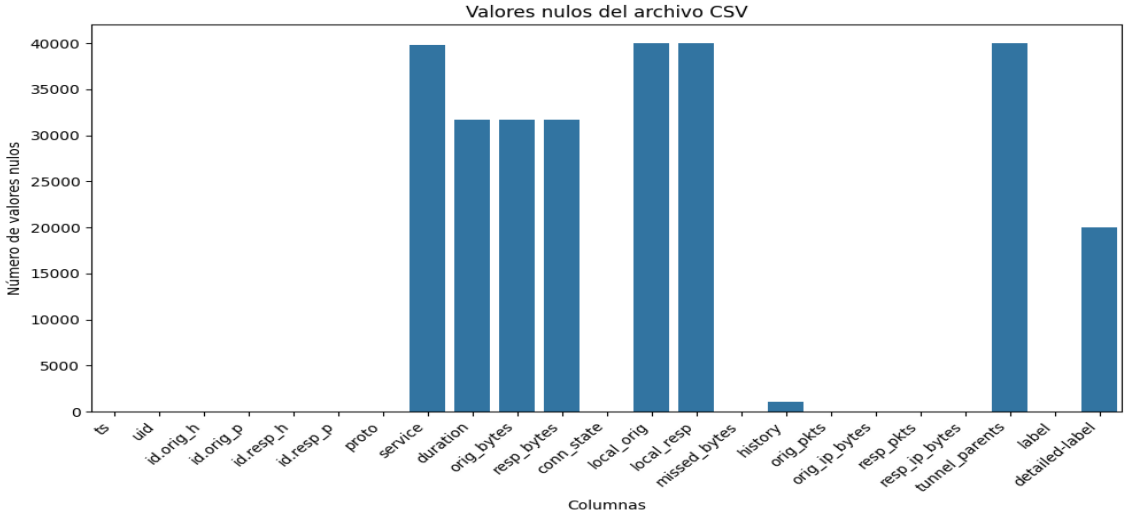

Figura 4. *Resultado en un gráfico de barras de búsqueda de valores nulos*. Elaborado por autores.

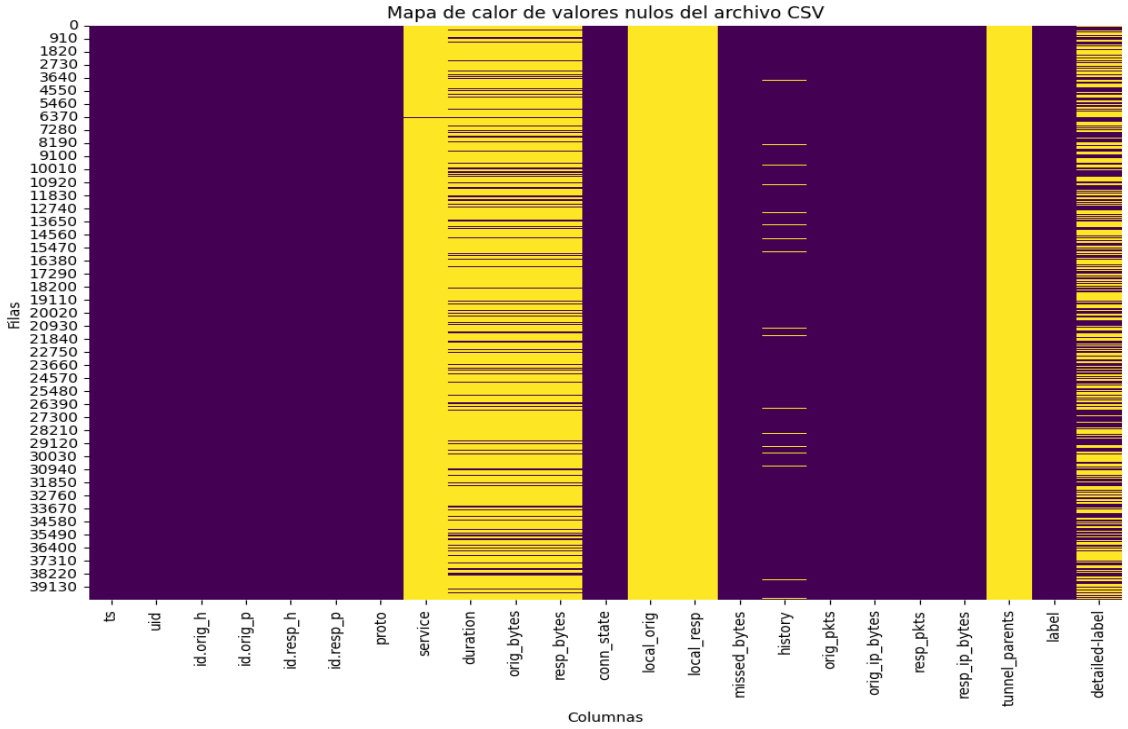

Figura 5. *Resultado en un mapa de calor de búsqueda de valores nulos.* Elaborado por autores.

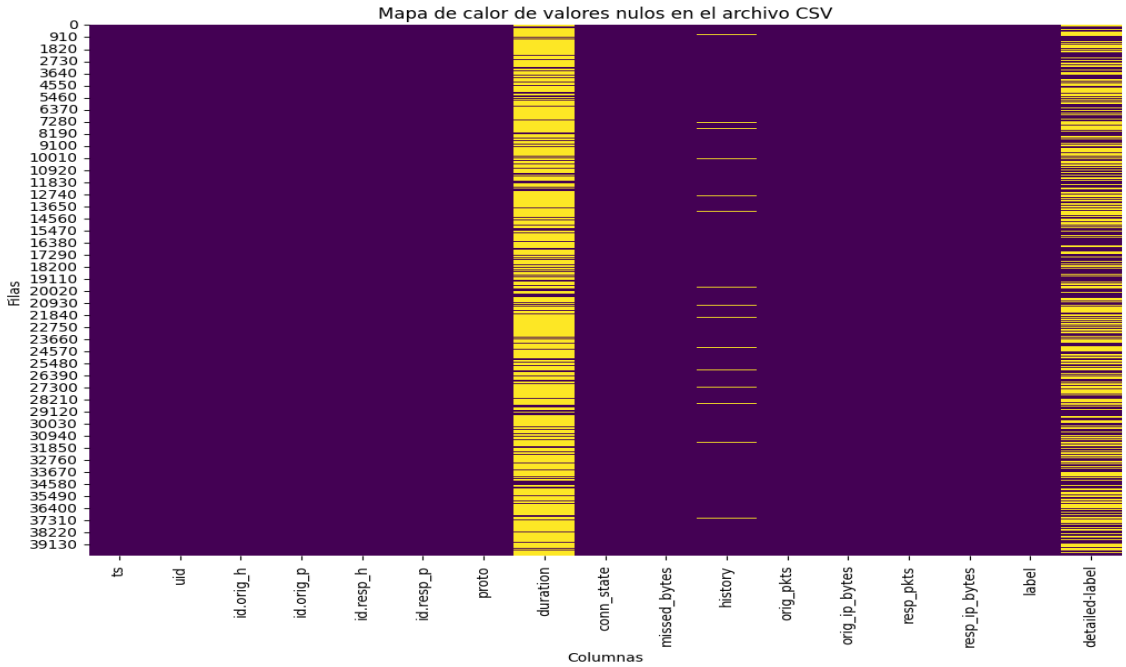

Figura 6. *Resultado en un mapa de calor de búsqueda de valores nulos.* Elaborado por autores.

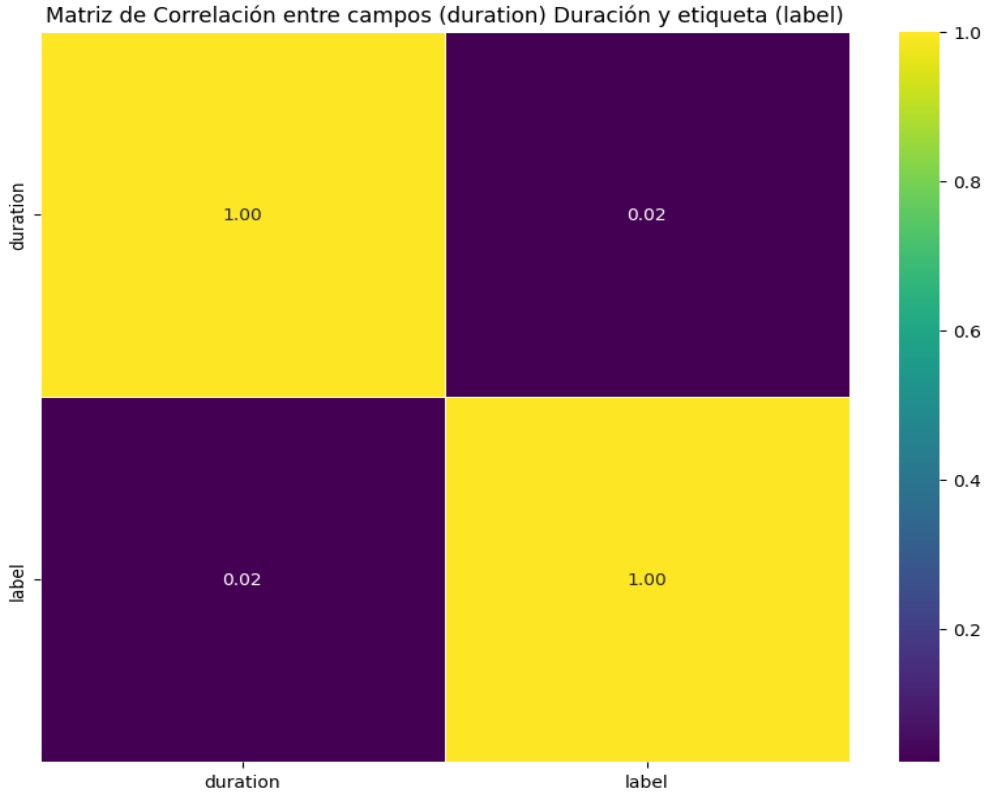

Figura 7. *Resultado de Matriz de Correlación entre campos duración y etiqueta*. Elaborado por autores.

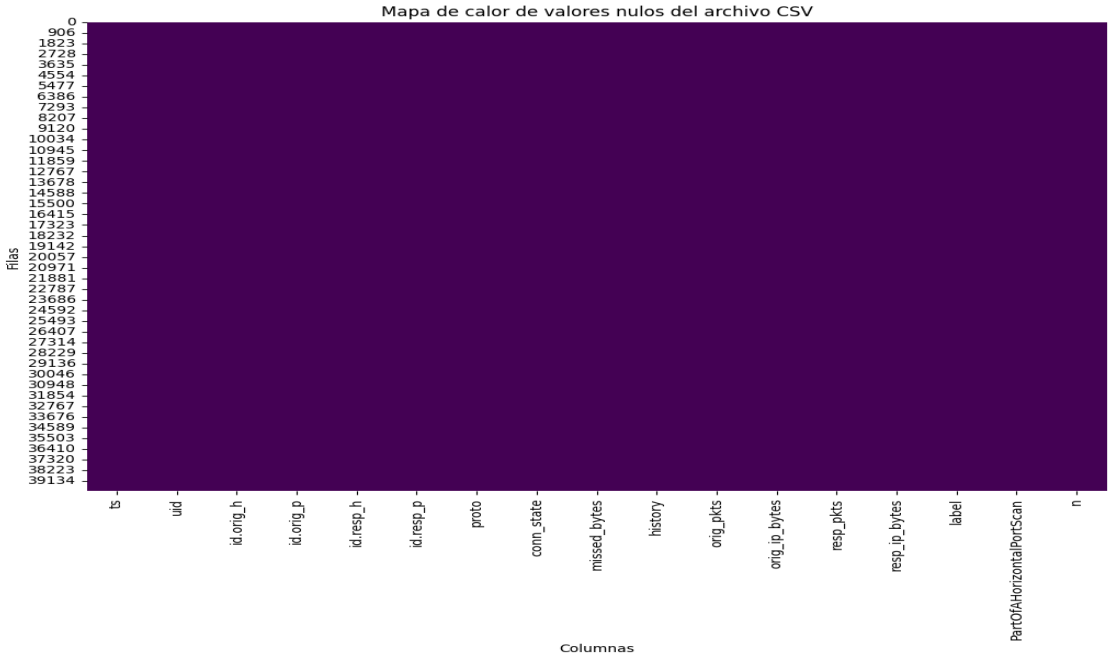

Figura 8. *Resultado de mapa de calor de valores nulos CSV*. Elaborado por autores.

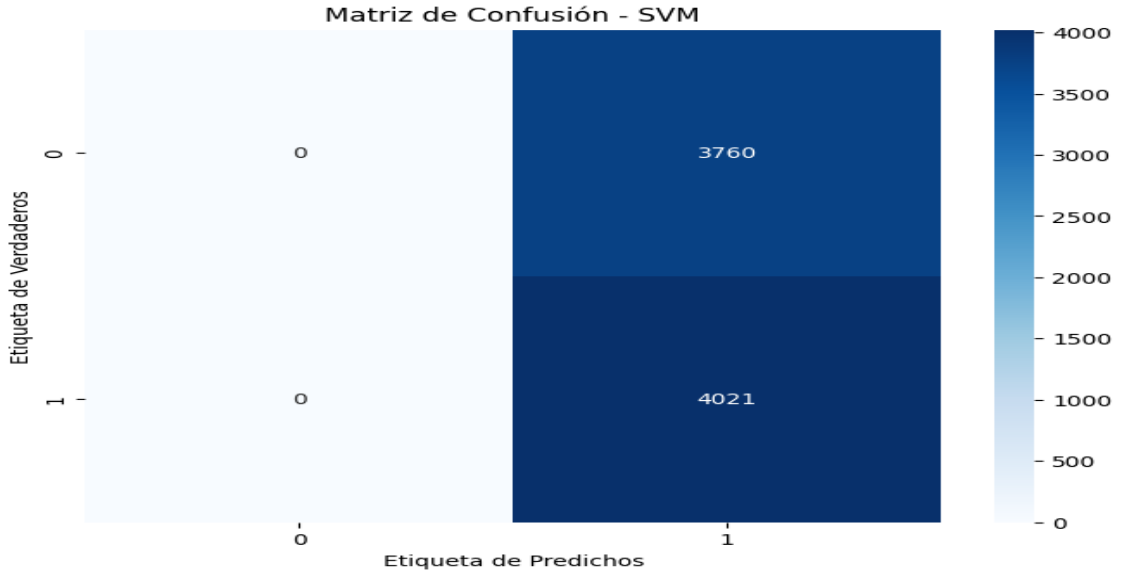

Figura 9. *Resultado Matriz de confusión SVM*. Elaborado por autores.

DISCUSIÓN

Los resultados obtenidos en esta investigación confirman la efectividad de los algoritmos de machine learning (ML) en la detección de ciberataques, validando su aplicabilidad en entornos de seguridad informática, en particular, el desempeño de Support Vector Machines (SVM) y Naive Bayes (NB) indica que el uso de modelos de clasificación probabilística y supervisada es altamente eficiente para identificar patrones maliciosos en tráfico de red (Castellanos et al., 2020). No obstante, para lograr un desempeño óptimo, se recomienda el desarrollo de modelos híbridos, la mejora en procesos de entrenamiento de algoritmos y la integración con herramientas avanzadas como sistemas de correlación de eventos (SIEM) y redes neuronales profundas (Aljamal et al., 2019).

Por otro lado, la detección de amenazas mediante ML, supera los enfoques tradicionales basados en firmas, por cuanto permite identificar ataques novedosos y variantes de malware sin depender exclusivamente de bases de datos de amenazas conocidas (Flores, 2020). Este resultado es consistente con estudios previos que han señalado la necesidad de incorporar modelos predictivos que aprendan de patrones anómalos y evolucionen con nuevas amenazas (Zhang et al., 2021). Por otro lado; a pesar del éxito de los modelos utilizados, se identificaron algunos desafíos en la implementación de IA en ciberseguridad; en primer lugar, se evidenció la necesidad de optimizar el consumo computacional de los algoritmos, especialmente en entornos donde los datos procesados son extensos y en tiempo real (Portela, 2022), aunque los modelos de ML pueden reducir los falsos negativos, es fundamental minimizar los falsos positivos, por cuanto una detección errónea podría impactar en la operatividad de los sistemas protegidos (León, 2022).

Otro aspecto relevante es la comparación de los diferentes algoritmos evaluados, SVM demostró una mejor capacidad para detectar ataques complejos y multivariables, mientras que Naive Bayes destacó por su rapidez y bajo costo computacional, estas diferencias resaltan la importancia de seleccionar el algoritmo adecuado según el contexto de aplicación y las necesidades del sistema de seguridad (Ayerbe, 2020). En términos prácticos, la integración de estos algoritmos en sistemas de seguridad podría mejorar significativamente la detección de intrusos en redes empresariales y gubernamentales, permitiendo respuestas automatizadas y mitigaciones más efectivas (Dueñas, 2020). No obstante, la adaptabilidad y actualización continua de los modelos sigue siendo un reto importante, lo que sugiere la necesidad de

enfoques híbridos que combinen múltiples técnicas de ML y correlación de eventos en tiempo real (Quirumbay et al., 2022).

CONCLUSIONES

El estudio evidenció la efectividad de los algoritmos de *Machine Learning* (ML) en la detección y mitigación de ciberataques, destacándose su capacidad para identificar patrones maliciosos en el tráfico de red y superar los enfoques tradicionales basados en firmas. Los resultados obtenidos validan la aplicabilidad de modelos como *Support Vector Machines* (SVM) y *Naive Bayes* (NB), los cuales han demostrado un desempeño significativo en la clasificación de amenazas, siendo SVM más eficiente en la detección de ataques complejos y NB más rápido y con menor costo computacional.

La investigación resalta la relevancia de integrar estos algoritmos en sistemas de seguridad informática, por cuanto permiten la detección de amenazas avanzadas y variantes de malware sin depender exclusivamente de bases de datos de firmas conocidas. Sin embargo, se identifican desafíos como la necesidad de optimizar el consumo computacional, reducir los falsos positivos y garantizar la actualización continua de los modelos para adaptarse a las tácticas cambiantes de los ciberdelincuentes. En términos prácticos, la implementación de estos modelos en entornos empresariales y gubernamentales podría mejorar significativamente la capacidad de respuesta ante ciberataques, permitiendo una mitigación más efectiva y automatizada.

Se determinaron modelos basados en aprendizaje de máquina en los cuales se recurre a diferentes algoritmos para el análisis de información y previo entrenamiento de los mismos, lo que permitió obtener patrones típicos de los ciberataques y determinar la prevalencia y probabilidad de ocurrencia de los mismos. En base a las simulaciones realizadas se encontraron un conjunto reducido de patrones comunes entre los dispositivos, el tráfico de red generado y acumulado en los registros a través de los cuales se determinó la ocurrencia de los ataques.

FINANCIAMIENTO

No monetario

CONFLICTO DE INTERÉS

No existe conflicto de interés con personas o instituciones ligadas a la investigación.

AGRADECIMIENTOS

A la Universidad Católica de Cuenca.

REFERENCIAS

Aljamal, I., Tekeoglu, A., Bekirog, K., & Sengupta, S. (2019). *Hybrid intrusion detection system using machine learning techniques in cloud computing environments*. IEEE Computer Society. https://ieeexplore.ieee.org/document/8886794

Cabanillas, H. A., & Nizama, J. J. (2019). *Análisis de algoritmos de encriptación de datos de texto, una revisión de la literatura científica* [*Analysis of text data encryption algorithms - a review of the scientific literature*]. [Trabajo de investigación, Universidad Privada del Norte]. Repositorio de la Universidad Privada del Norte. https://hdl.handle.net/11537/31391

Castellanos-Rojas, B. S., Cortés-Rodríguez, C. U., Espitia-Osorio, D. J., & Garzón-Bello, Y. T. (2020). Redes neuronales artificiales y estado del arte aplicado en la ciberseguridad [Redes neuronales artificiales y estado del arte aplicado en la ciberseguridad]. *Revista Matices Tecnológicos,* UNISANGIL, *12*. 58-63.

Dueñas, J. (2020). *Aplicación de técnicas de machine learning a la ciberseguridad: Aprendizaje supervisado para la detección de amenazas web mediante clasificación basada en árboles de decisión [Application of machine learning techniques to cybersecurity:*

Supervised learning for web threat detection using decision tree-based classification]. Universidad Oberta de Catalunya. http://hdl.handle.net/10609/118166

Flores, C. (2020). Inteligencia artificial, machine learning, deep learning aplicados a la ciberseguridad. *INF-FCPN-PGI Revista PGI*, (7), 11–13.

Hirare, Carolina. (2017). Ciberseguridad. Presentación del dossier [Cybersecurity. Introductionto Dossier]. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (20), 8-15. https://doi.org/10.17141/urvio.20.2017.2859

Jiménez, C., & Ramírez, O. (2022). *Propuesta de buenas prácticas de ciberseguridad para el uso de chatbots en el sector privado costarricense [Cybersecurity best practices proposal for the use of chatbots in the Costa Rican private sector]*. Universidad Cenfotec. https://repositorio.ucenfotec.ac.cr/handle/123456789/xmlui/handle/123456789/349

León, D. A., Martínezq, J. G., Ardila, I. A., & Mosquera, D. J. (2022). Inteligencia artificial para el control de tráfico en redes de datos: Una Revisión [Artificial intelligence for traffic control in data networks: A Review]. *Entre Ciencia e Ingeniería*, *16*(31), 17-24. Epub July 15, 2023.https://doi.org/10.31908/19098367.2655

Obregón-Martínez, W. V., & Morejón–López, G. E. (2024). *Evaluación del desempeño de algoritmos de machine learning dentro de la IA para uso en la búsqueda de patrones de ciberataques y mitigación de su impacto [Performance evaluation of machine learning algorithms within AI for use in finding patterns of cyber-attacks and mitigating their impact].* Universidad Tecnológica de Israel. Tesis de maestría.

Portela, M. (2022). Panorama de la inteligencia artificial en el dominio de la ciberseguridad [Overview of artificial intelligence in the cybersecurity domain]. *RUIDERAe: Revista de Unidades de Información, 19.*

Quirumbay, D., Castillo-Yagual, C., & Coronel-Suárez, I. (2022). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad [A review of Deep Learning applied to cybersecurity]. *Revista Científica Y Tecnológica UPSE*, *9*(1), 57-65. https://doi.org/10.26423/rctu.v9i1.671

Zhang, Z., Ning, H., Shi, F., & et al. (2022). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review, 55*(2), 1029–1053. https://doi.org/10.1007/s10462-021-09976-0