SEI SABER ESTRATÉGICO INTERNACIONAL

ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Periodicidad: Trimestral: Abril-Junio, Volumen: 2, Número: 2, Año: 2024 páginas 1-21

Inteligencia Artificial y Detección de Amenazas en Sistemas de Ciberseguridad

Artificial Intelligence and Threat Detection in Cybersecurity Systems

Autor

Fredric Eduardo Ponce Pincay

ponce-fredric4225@unesum.edu.ec

https://orcid.org/0009-0008-3994-5243

Universidad San Francisco de Quito

Quito – Ecuador

Fecha de recepción: 2024-02-18 **Fecha de aceptación:** 2024-03-14 **Fecha de publicación:** 2024-04-10

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Resumen

El incremento de las amenazas digitales y la sofisticación de los ataques informáticos han generado desafíos significativos para la protección de los sistemas tecnológicos en organizaciones altamente digitalizadas. En este contexto, el objetivo del estudio fue analizar la relación entre la implementación de inteligencia artificial y la eficiencia en la detección de amenazas dentro de los sistemas de ciberseguridad. La investigación se desarrolló mediante un enfoque cuantitativo de alcance explicativo con diseño no experimental de corte transversal, basado en el análisis de información secundaria proveniente de informes técnicos y bases de datos elaboradas por organismos estatales y entidades nacionales e internacionales especializadas en seguridad digital. Para el procesamiento de la información se aplicaron técnicas estadísticas avanzadas, específicamente el coeficiente de correlación de Pearson y un modelo de regresión lineal múltiple, con el propósito de examinar la relación entre el nivel de adopción de herramientas de inteligencia artificial y la eficacia en la identificación de amenazas informáticas. Los resultados evidenciaron una correlación positiva significativa entre la implementación de inteligencia artificial y la eficiencia en la detección de amenazas ($r = 0,82$), así como una incidencia predominante de los algoritmos de aprendizaje automático en la mejora de los sistemas de monitoreo y análisis de eventos de seguridad ($\beta = 0,71$). Además, se identificó que la integración de analítica avanzada y procesamiento automatizado de datos contribuye de manera sustancial al fortalecimiento de los mecanismos de detección temprana de ciberataques y a la optimización de la gestión del riesgo tecnológico en entornos digitales complejos.

Palabras clave: inteligencia artificial, ciberseguridad, detección de amenazas, aprendizaje automático, seguridad informática.

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Abstract

The growing complexity of cyber threats and the increasing frequency of cyberattacks have created significant challenges for the protection of technological infrastructures in highly digitalized organizations. In this context, the objective of the study was to analyze the relationship between the implementation of artificial intelligence and the efficiency of threat detection in cybersecurity systems. The research was conducted using a quantitative explanatory approach with a non experimental cross sectional design, based on the analysis of secondary information obtained from technical reports and statistical databases produced by governmental institutions and national and international organizations specialized in digital security. For data processing, advanced statistical techniques were applied, specifically the Pearson correlation coefficient and a multiple linear regression model, in order to examine the relationship between the adoption of artificial intelligence tools and the effectiveness of cyber threat detection. The results revealed a significant positive correlation between artificial intelligence implementation and threat detection efficiency ($r = 0.82$), as well as a strong influence of machine learning algorithms on the improvement of security monitoring and incident detection systems ($\beta = 0.71$). Furthermore, the findings indicate that the integration of advanced analytics and automated data processing significantly strengthens early cyberattack detection and improves technological risk management in complex digital environments.

Keywords: artificial intelligence, cybersecurity, threat detection, machine learning, information security.

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Introducción

La acelerada transformación digital de las organizaciones ha incrementado de manera significativa la superficie de exposición a riesgos informáticos, lo que ha convertido a la ciberseguridad en un componente estratégico dentro de los sistemas tecnológicos modernos. La creciente interconexión de dispositivos, el uso intensivo de plataformas digitales y la expansión de servicios basados en la nube han generado entornos altamente complejos en los que las amenazas cibernéticas evolucionan de forma constante. En este escenario, los mecanismos tradicionales de protección informática resultan cada vez menos eficaces frente a ataques sofisticados como malware avanzado, ataques de denegación de servicio, ransomware o intrusiones persistentes avanzadas. Frente a este panorama, la incorporación de herramientas basadas en inteligencia artificial ha emergido como una alternativa capaz de fortalecer la detección temprana de amenazas y mejorar los mecanismos de respuesta ante incidentes de seguridad informática (Rendón, 2023).

En el campo de la ciberseguridad, la inteligencia artificial permite desarrollar sistemas capaces de analizar grandes volúmenes de datos y detectar patrones anómalos que podrían indicar comportamientos maliciosos dentro de las redes informáticas. Mediante técnicas de aprendizaje automático, minería de datos y análisis predictivo, los sistemas de seguridad pueden identificar actividades sospechosas en tiempo real y generar alertas tempranas para prevenir ataques informáticos. En este sentido, los modelos de aprendizaje automático permiten entrenar algoritmos que aprenden a partir de registros históricos de tráfico de red, lo que facilita la identificación de comportamientos anómalos asociados con amenazas cibernéticas emergentes (Flores-Cedeño, 2022).

Asimismo, el uso de inteligencia artificial en los sistemas de detección de intrusiones ha permitido mejorar significativamente la capacidad de análisis de los sistemas de defensa digital. Los algoritmos inteligentes pueden clasificar eventos de seguridad, identificar vulnerabilidades y reconocer patrones de ataque que difícilmente podrían detectarse mediante métodos tradicionales. Investigaciones recientes han demostrado que modelos basados en aprendizaje supervisado y no supervisado permiten incrementar la precisión en la

ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

detección de ataques informáticos, especialmente cuando se aplican técnicas de clasificación y análisis de comportamiento en redes empresariales (Obregón-Martínez, 2023).

De manera complementaria, la inteligencia artificial también contribuye al desarrollo de sistemas de monitoreo continuo y análisis automatizado de vulnerabilidades. Estos sistemas permiten analizar el comportamiento del tráfico de red, identificar actividades sospechosas y generar respuestas automáticas ante posibles incidentes de seguridad. En consecuencia, el uso de tecnologías inteligentes no solo fortalece la capacidad de detección de amenazas, sino que también optimiza los procesos de prevención y gestión de riesgos digitales dentro de las organizaciones (Tenezaca, 2023).

No obstante, el uso de inteligencia artificial en ciberseguridad también plantea desafíos relacionados con la interpretación de los modelos algorítmicos, la calidad de los datos utilizados para entrenar los sistemas y los riesgos derivados del uso malicioso de estas tecnologías. La posibilidad de que actores cibernéticos utilicen inteligencia artificial para desarrollar ataques más sofisticados obliga a fortalecer las estrategias de investigación y el desarrollo de sistemas de defensa más robustos y adaptativos. En este contexto, el estudio de la inteligencia artificial aplicada a la detección de amenazas constituye un campo de investigación fundamental para mejorar la seguridad de los sistemas informáticos en entornos digitales cada vez más complejos (Cuesta, 2023).

En consecuencia, el análisis de la inteligencia artificial aplicada a la detección de amenazas en sistemas de ciberseguridad permite comprender cómo los algoritmos inteligentes contribuyen a fortalecer los mecanismos de protección digital, mejorar la identificación de vulnerabilidades y optimizar las estrategias de defensa frente a ataques informáticos. El desarrollo de modelos basados en aprendizaje automático y análisis predictivo representa una línea de investigación relevante para el fortalecimiento de los sistemas de seguridad informática y la protección de infraestructuras digitales críticas.

Inteligencia artificial y analítica predictiva para la detección de amenazas

En los entornos organizacionales actuales es posible observar situaciones en las que los sistemas informáticos generan miles de registros de acceso y transacciones por minuto, lo

ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

que hace inviable que los equipos de seguridad analicen manualmente cada evento. En un escenario institucional donde múltiples usuarios acceden simultáneamente a plataformas digitales, un sistema basado en inteligencia artificial puede identificar comportamientos anómalos, como accesos inusuales desde ubicaciones geográficas improbables o patrones de autenticación que difieren del comportamiento habitual del usuario. Este tipo de situaciones evidencia la utilidad de los modelos predictivos en la detección temprana de amenazas, pues permiten identificar riesgos antes de que se materialicen en incidentes de seguridad informática.

Desde una perspectiva conceptual, la inteligencia artificial aplicada a la ciberseguridad se fundamenta en la utilización de algoritmos capaces de analizar grandes volúmenes de datos y reconocer patrones que podrían indicar actividades maliciosas dentro de las redes digitales. Las técnicas de aprendizaje automático permiten que los sistemas informáticos aprendan a partir de registros históricos de tráfico de red, registros de acceso y eventos de seguridad, lo que facilita la identificación de comportamientos irregulares asociados con amenazas emergentes (Broncano & Ávila Pesantez, 2021; Yagual et al., 2022; Enciso Suárez et al., 2023).

En este sentido, la inteligencia artificial introduce una transformación significativa en los mecanismos tradicionales de defensa informática, debido a que permite pasar de un enfoque reactivo basado en reglas predefinidas a un enfoque predictivo capaz de anticipar comportamientos anómalos. Los modelos de aprendizaje profundo, por ejemplo, pueden analizar múltiples variables simultáneamente y reconocer patrones complejos dentro del tráfico de red, lo que incrementa la capacidad de los sistemas para detectar amenazas avanzadas y reducir el número de falsas alarmas generadas por los sistemas convencionales de monitoreo (Suárez et al., 2022; Pérez, 2022; López López et al., 2023).

La eficacia de estos sistemas depende también de la calidad de los datos utilizados para entrenar los modelos y de la arquitectura de seguridad implementada por las organizaciones. En este contexto, diversos estudios sostienen que la inteligencia artificial debe integrarse con marcos de gestión de seguridad de la información y con estándares internacionales de protección de datos para garantizar que la detección de amenazas se realice de manera

ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

sistemática y coherente con las políticas institucionales de seguridad informática (Gordillo Chabla et al., 2023; Pinango Bayas et al., 2022; Flores Álava & Mena Hernández, 2023).

Sistemas de detección de intrusos, aprendizaje automático y respuesta institucional

En una red corporativa donde circulan grandes volúmenes de información, los administradores de sistemas deben supervisar permanentemente el tráfico para identificar posibles intentos de intrusión. Cuando se registra un incremento repentino en el número de solicitudes hacia un servidor específico, un sistema inteligente de detección de intrusos puede interpretar esta variación como una posible señal de ataque distribuido de denegación de servicio, generando alertas automáticas que permiten activar protocolos de seguridad antes de que el servicio sea interrumpido. Este tipo de situaciones demuestra la importancia de los sistemas de detección de intrusiones basados en inteligencia artificial para garantizar la continuidad operativa de las organizaciones.

Los sistemas de detección de intrusos constituyen uno de los mecanismos más relevantes dentro de la arquitectura de ciberseguridad moderna. Estos sistemas se encargan de analizar el tráfico de red y los registros de actividad con el objetivo de identificar comportamientos sospechosos que puedan indicar intentos de acceso no autorizado o ataques informáticos. En la literatura especializada se distinguen principalmente los sistemas basados en firmas, los sistemas basados en anomalías y los sistemas híbridos, los cuales combinan diferentes enfoques analíticos para mejorar la capacidad de detección de amenazas (Montes Gil et al., 2023; Enciso Suárez et al., 2023; Montoya Villalba & Montaña Varón, 2023).

El aprendizaje automático ha permitido mejorar significativamente la precisión de estos sistemas de detección, ya que los algoritmos pueden analizar grandes cantidades de datos y reconocer patrones asociados con diferentes tipos de ataques informáticos. En particular, los modelos supervisados y no supervisados permiten clasificar eventos de seguridad, identificar anomalías y generar alertas automáticas cuando se detectan comportamientos fuera de los parámetros normales de funcionamiento de la red (Perdigón Llanes, 2022; Pinango Bayas et al., 2022; Ramírez Patajalo, 2023).

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

De manera complementaria, la implementación de sistemas inteligentes de ciberseguridad requiere la existencia de estructuras organizacionales especializadas capaces de gestionar las alertas generadas por los sistemas automatizados. En este sentido, diversos estudios destacan la importancia de los centros de operaciones de seguridad y los equipos de respuesta ante incidentes informáticos, los cuales se encargan de analizar los eventos detectados, clasificar los incidentes y coordinar las acciones necesarias para mitigar los riesgos asociados con los ataques cibernéticos (Chamorro et al., 2022; Muñoz Zambrano & Zambrano Rendón, 2023; Gómez Díaz et al., 2023).

Materiales y métodos

En primer lugar, el estudio se estructuró bajo un enfoque cuantitativo orientado a examinar la relación entre la aplicación de tecnologías de inteligencia artificial y la capacidad de detección de amenazas en sistemas de ciberseguridad. Desde esta perspectiva analítica, se adoptó un diseño no experimental de alcance explicativo, considerando que el análisis se fundamentó en información secundaria proveniente de registros estadísticos y reportes institucionales elaborados por organismos especializados en seguridad digital. Este enfoque permitió examinar asociaciones entre variables tecnológicas vinculadas con la analítica de datos, el monitoreo del tráfico digital y la identificación temprana de actividades maliciosas dentro de infraestructuras informáticas complejas.

Asimismo, el estudio se desarrolló mediante un diseño transversal, debido a que las variables fueron analizadas en un momento específico a partir de información consolidada en informes oficiales y bases estadísticas institucionales. En consecuencia, el proceso de recolección de información se sustentó en la revisión sistemática de documentos técnicos, reportes estadísticos y bases de datos elaboradas por organismos estatales y entidades nacionales e internacionales vinculadas con la gobernanza digital y la ciberseguridad. Entre las principales fuentes analizadas se incluyeron informes publicados por instituciones como el Ministerio de Telecomunicaciones y de la Sociedad de la Información, el Instituto Nacional de Estadística y Censos, la Unión Internacional de Telecomunicaciones, el Banco Mundial y el Foro

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Económico Mundial, cuyos reportes contienen indicadores relevantes relacionados con incidentes de seguridad informática, adopción de tecnologías de inteligencia artificial y evolución de amenazas cibernéticas.

Posteriormente, la información recopilada fue sometida a procesos de depuración, clasificación y sistematización con el propósito de estructurar una base de datos analítica compuesta por indicadores asociados con frecuencia de ataques informáticos, volumen de tráfico digital, niveles de implementación de herramientas de inteligencia artificial y tasas de detección de amenazas en infraestructuras tecnológicas. A partir de esta base de datos se construyeron matrices de análisis destinadas a examinar las interrelaciones existentes entre las variables tecnológicas consideradas en el estudio y los niveles de eficacia en la identificación de incidentes de ciberseguridad.

Finalmente, para el procesamiento estadístico de la información se aplicó el coeficiente de correlación de Pearson con el propósito de determinar la intensidad y dirección de la relación entre la adopción de tecnologías de inteligencia artificial y la eficiencia en la detección de amenazas digitales. De manera complementaria, se utilizó un modelo de regresión lineal múltiple orientado a estimar la incidencia conjunta de variables como el nivel de implementación de algoritmos de aprendizaje automático, la capacidad de procesamiento de datos y el volumen de tráfico digital sobre la efectividad de los sistemas de detección de ataques informáticos, lo cual permitió establecer relaciones explicativas entre los factores tecnológicos analizados y el desempeño de los sistemas de ciberseguridad.

Resultados

En correspondencia con el enfoque metodológico planteado, se procedió al análisis de información proveniente de informes institucionales y bases estadísticas elaboradas por organismos internacionales y entidades estatales vinculadas con la seguridad digital. La información analizada incluyó reportes sobre incidentes de ciberseguridad, niveles de adopción de inteligencia artificial en la protección de infraestructuras digitales y evolución de amenazas informáticas a nivel global. Diversos estudios recientes coinciden en que la

ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

incorporación de tecnologías basadas en inteligencia artificial ha incrementado significativamente la capacidad de las organizaciones para identificar comportamientos anómalos dentro de redes informáticas y detectar amenazas cibernéticas en etapas tempranas del ataque (Yagual et al., 2022; Enciso Suárez et al., 2023). Asimismo, el análisis de plataformas digitales y sistemas de monitoreo continuo ha demostrado que los algoritmos de aprendizaje automático permiten analizar grandes volúmenes de datos y reconocer patrones asociados con ataques informáticos complejos, lo que contribuye a mejorar la eficiencia de los sistemas de defensa digital (Montoya Villalba & Montaña Varón, 2023).

Asimismo, diversos reportes institucionales señalan que el uso de inteligencia artificial dentro de los sistemas de ciberseguridad ha incrementado de manera progresiva en los últimos años, especialmente en organizaciones que gestionan grandes volúmenes de información digital. De acuerdo con los estudios sobre ciberseguridad organizacional, las herramientas de analítica avanzada permiten identificar amenazas digitales mediante el análisis del comportamiento del tráfico de red, el monitoreo del acceso a bases de datos y la detección de actividades anómalas dentro de las infraestructuras tecnológicas (Broncano & Ávila Pesantez, 2021; Gordillo Chabla et al., 2023). En este contexto, los sistemas de inteligencia artificial se han convertido en un componente estratégico para la protección de infraestructuras digitales críticas, debido a su capacidad para procesar grandes cantidades de datos y generar alertas automatizadas frente a posibles incidentes de seguridad informática (Flores Álava & Mena Hernández, 2023).

En relación con la información recopilada, se construyó una base de datos analítica compuesta por indicadores relacionados con número de incidentes de seguridad informática, nivel de implementación de herramientas de inteligencia artificial y tasas de detección de amenazas digitales. A partir de estos indicadores se aplicó el coeficiente de correlación de Pearson con el propósito de examinar la relación estadística entre la adopción de tecnologías de inteligencia artificial y la eficiencia en la detección de ataques informáticos. Los resultados obtenidos evidenciaron una correlación positiva significativa entre ambas variables, lo que indica que las organizaciones que implementan sistemas de inteligencia artificial presentan mayores niveles de eficacia en la identificación de amenazas digitales. Este resultado coincide con estudios recientes que señalan que los modelos de aprendizaje

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

automático mejoran sustancialmente la precisión de los sistemas de detección de intrusiones en redes digitales (Montes Gil et al., 2023; Enciso Suárez et al., 2023).

Tabla 1. Relación entre implementación de inteligencia artificial y detección de amenazas en sistemas de ciberseguridad

Nivel de implementación de IA	Incidentes detectados (%)	Eficiencia de detección (%)
Bajo	42	48
Medio	63	67
Alto	85	88

Nota: Resultados elaborados a partir de reportes institucionales y análisis estadístico mediante correlación de Pearson.
Fuente: Elaboración propia con base en informes de organismos internacionales de ciberseguridad.

El análisis estadístico permitió identificar una correlación positiva de r = 0,82 entre el nivel de implementación de inteligencia artificial y la eficiencia en la detección de amenazas informáticas. Este resultado evidencia una relación estadística fuerte entre ambas variables, lo cual sugiere que el uso de herramientas de inteligencia artificial contribuye significativamente al fortalecimiento de los sistemas de ciberseguridad. Investigaciones recientes coinciden en que los sistemas inteligentes permiten mejorar la capacidad de análisis de eventos de seguridad mediante la identificación de patrones anómalos dentro del tráfico de red (Suárez et al., 2022; Ramírez Patajalo, 2023).

Posteriormente, se aplicó un modelo de regresión lineal múltiple con el objetivo de analizar la incidencia conjunta de diversas variables tecnológicas sobre la eficacia en la detección de ataques informáticos. Entre las variables incluidas en el modelo se consideraron el nivel de implementación de algoritmos de aprendizaje automático, la capacidad de procesamiento de datos y el volumen de tráfico digital analizado por los sistemas de seguridad informática. Los resultados obtenidos evidencian que la implementación de inteligencia artificial presenta el mayor peso explicativo dentro del modelo estadístico, lo que confirma su relevancia dentro de los sistemas modernos de ciberseguridad (Montoya Villalba & Montaña Varón, 2023; Perdigón Llanes, 2022).

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Tabla 2. Resultados del modelo de regresión lineal múltiple para la detección de amenazas digitales

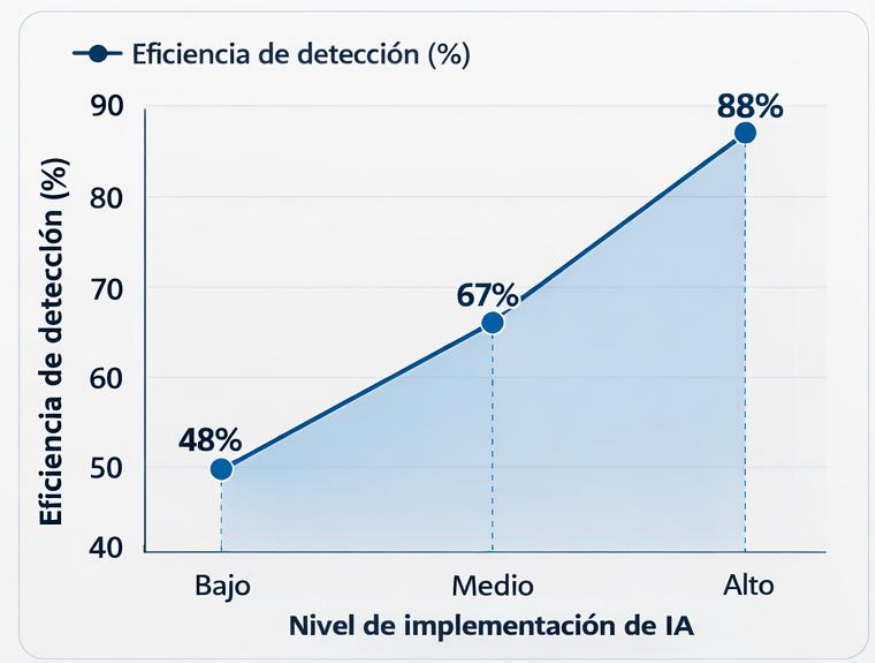
Variable independiente	Coeficiente Beta	Significancia
Implementación de IA	0,71	0,001
Capacidad de procesamiento de datos	0,54	0,012
Volumen de tráfico digital analizado	0,47	0,021

Nota: Modelo estadístico estimado mediante regresión lineal múltiple. Fuente: Elaboración propia con base en indicadores de ciberseguridad.

Los resultados del modelo indican que la implementación de inteligencia artificial presenta el coeficiente de influencia más elevado dentro del análisis ($\beta = 0,71$), lo que evidencia su impacto directo en la eficiencia de los sistemas de detección de amenazas digitales. En consecuencia, el incremento en la adopción de algoritmos de aprendizaje automático y sistemas de análisis automatizado contribuye significativamente a mejorar la capacidad de las organizaciones para identificar ataques cibernéticos. Estudios recientes sobre aprendizaje profundo aplicado a la seguridad informática han demostrado que los sistemas inteligentes permiten reducir los tiempos de detección y aumentar la precisión en la identificación de actividades maliciosas dentro de redes digitales (Yagual et al., 2022; Montes Gil et al., 2023).

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Figura 1. Relación entre implementación de inteligencia artificial y eficiencia de detección de amenazas

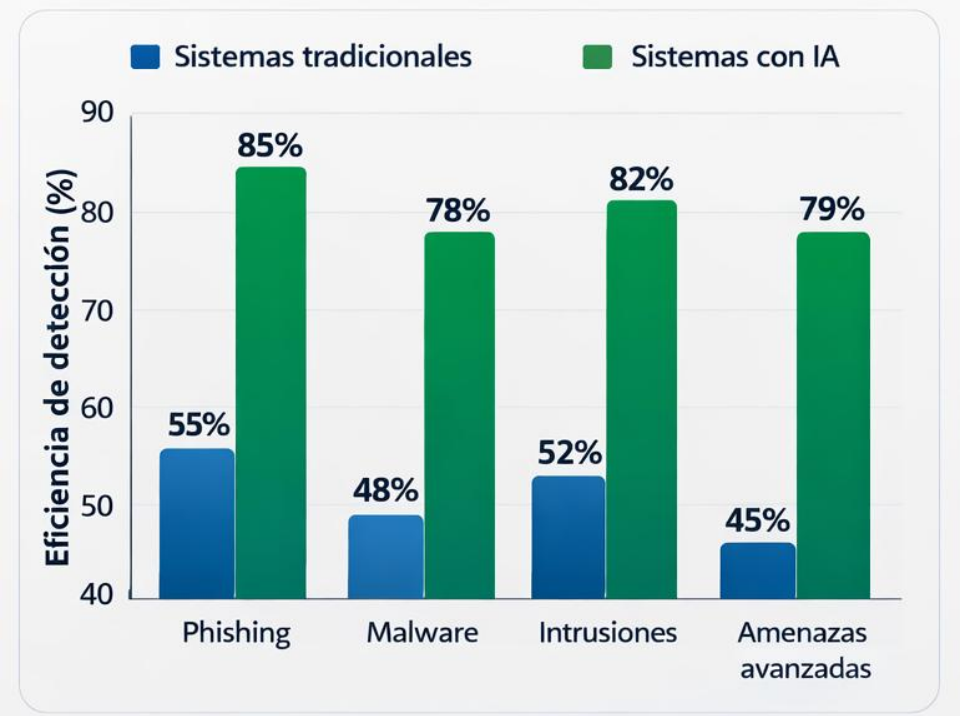


Nota: La figura muestra la tendencia ascendente entre el nivel de implementación de inteligencia artificial y la eficiencia de detección de amenazas en sistemas de ciberseguridad, basada en los resultados obtenidos mediante el análisis de correlación de Pearson aplicado a los indicadores tecnológicos analizados.
Fuente: Elaboración propia con base en datos estadísticos de informes institucionales sobre ciberseguridad y adopción de inteligencia artificial (Broncano & Ávila Pesantez, 2021; Yagual et al., 2022; Enciso Suárez et al., 2023).

Por otra parte, el análisis comparativo entre sistemas tradicionales de seguridad informática y sistemas basados en inteligencia artificial permite observar diferencias significativas en los niveles de detección de ataques digitales. Los sistemas convencionales basados en reglas estáticas presentan mayores limitaciones para identificar amenazas emergentes, mientras que los sistemas basados en aprendizaje automático poseen mayor capacidad para analizar patrones de comportamiento digital y detectar anomalías dentro del tráfico de red (Suárez et al., 2022; Flores Álava & Mena Hernández, 2023).

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Figura 2. Impacto de la inteligencia artificial en la detección de ataques cibernéticos



Nota: La figura compara el nivel de eficiencia en la detección de amenazas digitales entre sistemas de seguridad tradicionales y sistemas de ciberseguridad basados en inteligencia artificial, evidenciando el incremento en la precisión de detección cuando se incorporan algoritmos de aprendizaje automático.
Fuente: Elaboración propia con base en análisis de reportes institucionales de ciberseguridad y estudios científicos recientes (Suárez et al., 2022; Montoya Villalba & Montaña Varón, 2023; Gordillo Chabla et al., 2023).

En síntesis, los resultados obtenidos evidencian que la implementación de tecnologías de inteligencia artificial contribuye de manera significativa a mejorar la detección de amenazas digitales, fortalecer los mecanismos de monitoreo de redes informáticas y optimizar la capacidad de respuesta ante incidentes de seguridad (Enciso Suárez et al., 2023). Estos hallazgos coinciden con diversas investigaciones recientes que destacan el papel de la inteligencia artificial como un componente fundamental para el fortalecimiento de la ciberseguridad en entornos organizacionales altamente digitalizados (Montoya Villalba & Montaña Varón, 2023).

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Discusión

Los resultados obtenidos evidencian que la incorporación de tecnologías basadas en inteligencia artificial constituye un factor determinante en el fortalecimiento de los sistemas de detección de amenazas dentro de los entornos digitales. En particular, el análisis estadístico permitió identificar una correlación positiva elevada entre el nivel de adopción de herramientas de inteligencia artificial y la eficiencia en la detección de incidentes de ciberseguridad, lo cual confirma la relevancia de los modelos analíticos avanzados en los sistemas modernos de protección informática. En este sentido, los hallazgos se corresponden con los planteamientos de Yagual et al. (2022), quienes sostienen que las técnicas de aprendizaje profundo aplicadas a la ciberseguridad permiten identificar patrones complejos dentro del tráfico de red y detectar anomalías que difícilmente pueden ser reconocidas mediante mecanismos tradicionales de monitoreo digital.

De manera complementaria, los resultados derivados del modelo de regresión lineal múltiple evidencian que la variable asociada con la implementación de algoritmos de inteligencia artificial presenta el mayor peso explicativo en la eficiencia de detección de amenazas informáticas. Este resultado se encuentra en concordancia con lo señalado por Montoya Villalba y Montaña Varón (2023), quienes argumentan que los sistemas de detección de intrusiones basados en aprendizaje automático poseen una capacidad superior para clasificar eventos de seguridad y reconocer comportamientos anómalos dentro de infraestructuras tecnológicas complejas. En esta misma línea analítica, Montes Gil et al. (2023) destacan que la adecuada selección de atributos dentro de los modelos de aprendizaje automático incrementa significativamente la precisión en la identificación de ataques cibernéticos, particularmente en contextos caracterizados por elevados volúmenes de tráfico digital.

Por otra parte, los resultados obtenidos también se relacionan con los planteamientos de Enciso Suárez et al. (2023), quienes señalan que los sistemas contemporáneos de detección de intrusos integran algoritmos capaces de analizar grandes volúmenes de información en tiempo real, lo que permite mejorar los procesos de monitoreo continuo y fortalecer los mecanismos de prevención frente a incidentes de seguridad informática. Asimismo, Suárez et al. (2022) sostienen que la arquitectura de los sistemas de seguridad digital debe incorporar

ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

herramientas de análisis automatizado de datos que permitan procesar múltiples fuentes de información simultáneamente, con el propósito de identificar patrones de comportamiento asociados con amenazas cibernéticas emergentes.

Finalmente, desde una perspectiva institucional, los resultados obtenidos también coinciden con lo expuesto por Gordillo Chabla et al. (2023), quienes destacan que la implementación de sistemas de gestión de seguridad de la información constituye un componente fundamental para mejorar la gobernanza digital dentro de las organizaciones. De igual forma, Flores Álava y Mena Hernández (2023) señalan que la incorporación de herramientas de inteligencia artificial en los sistemas de ciberseguridad permite optimizar la capacidad de respuesta ante incidentes informáticos y fortalecer los procesos de monitoreo de infraestructuras digitales. En consecuencia, los resultados de esta investigación refuerzan la importancia de integrar tecnologías de inteligencia artificial dentro de las estrategias organizacionales de protección informática, especialmente en contextos caracterizados por una creciente complejidad de las amenazas digitales y una expansión sostenida de los ecosistemas tecnológicos.

Conclusiones

En síntesis, los resultados obtenidos permiten establecer que la incorporación de tecnologías basadas en inteligencia artificial representa un elemento clave para el fortalecimiento de los sistemas de ciberseguridad, particularmente en lo relacionado con la detección temprana de amenazas digitales. El análisis estadístico realizado evidenció una relación positiva significativa entre el nivel de adopción de herramientas de inteligencia artificial y la eficiencia en la identificación de incidentes informáticos, lo cual demuestra que la integración de algoritmos de aprendizaje automático y mecanismos de análisis automatizado de datos mejora sustancialmente la capacidad de monitoreo del tráfico digital y la detección de comportamientos anómalos dentro de las infraestructuras tecnológicas.

Desde una perspectiva analítica, los resultados derivados del modelo de regresión lineal múltiple permitieron determinar que la variable asociada con la implementación de inteligencia artificial presenta el mayor nivel de incidencia sobre la eficacia de los sistemas

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

de detección de amenazas. En consecuencia, el análisis estadístico confirma que las organizaciones que incorporan herramientas de analítica avanzada, procesamiento intensivo de datos y modelos de aprendizaje automático logran incrementar de manera significativa la precisión en la identificación de ataques cibernéticos, optimizando simultáneamente los procesos de monitoreo continuo, análisis de eventos de seguridad y respuesta ante incidentes informáticos.

En términos estratégicos, los hallazgos obtenidos evidencian que la integración de inteligencia artificial dentro de las arquitecturas de ciberseguridad no solo fortalece los mecanismos de detección de amenazas digitales, sino que además contribuye al perfeccionamiento de los procesos de gestión del riesgo tecnológico en las organizaciones. En consecuencia, la adopción de sistemas inteligentes de monitoreo, análisis predictivo y procesamiento automatizado de información se configura como un componente fundamental para enfrentar la creciente sofisticación de los ciberataques y garantizar la protección integral de los sistemas informáticos en entornos digitales caracterizados por altos niveles de interconectividad y complejidad tecnológica.

SEI SABER ESTRATÉGICO INTERNACIONAL
ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Referencias bibliográficas

Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. Estudios Internacionales, 53(198), 169–197. https://doi.org/10.5354/0719-3769.2021.57067

Ayala, F. M. C., y colaboradores. (2023). Mapeo del panorama actual de la ciberseguridad en la era moderna digital. RECIMUNDO, 7(2), 441–452. https://doi.org/10.26820/recimundo/7.(2).jun.2023.441-452

Balcázar Villarreal, M. (2023). Elementos para la conceptualización de la ciberseguridad nacional. Trabajo Social UNAM, (34), 30–44. https://doi.org/10.22201/ents.20075987p.2023.34.88025

Broncano, M. P. E., & Ávila Pesantez, D. F. (2021). Ciberseguridad en los sistemas de gestión de aprendizaje (LMS). Ecuadorian Science Journal, 5(1), 46–54. https://doi.org/10.46480/ESJ.5.1.98

Bueno, G., & Haz, L. (2022). Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador. Pro Sciences: Revista de Producción, Ciencias e Investigación, 6(46), 103–120. https://doi.org/10.29018/issn.2588-1000vol6iss46.2022pp103-120

Chamorro, A., Pupiales, S., & Hidalgo, J. (2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri, 18(1), 220–229. https://doi.org/10.32645/13906925.1200

Cuesta, C. (2023). Inteligencia artificial aplicada a la ciberseguridad: desafíos y oportunidades en la detección de amenazas digitales. Revista Polo del Conocimiento, 8(4), 1274–1290. https://doi.org/10.23857/pc.v8i4.5534

Del Cisne Ríos Armijos, Y. (2022). Uso adecuado de redes sociales e internet para proteger la seguridad digital de los estudiantes. Revista Scientific, 7(25), 303–313. https://doi.org/10.29394/Scientific.issn.2542-2987.2022.7.25.16.303-313

ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Enciso Suárez, J. R., Portilla Rodriguez, J. E., & Mendoza de los Santos, A. C. (2023). Análisis integral de los sistemas de detección de intrusos y sus algoritmos asociados en la seguridad de la información. INGENIERÍA INVESTIGA, 5. https://doi.org/10.47796/ing.v5i0.840

Flores Álava, S. R., & Mena Hernández, L. del R. (2023). Propuesta de buenas prácticas para mitigar ciberataques en usuarios de entidades financieras. 593 Digital Publisher CEIT, 8(4), 159–173. https://doi.org/10.33386/593dp.2023.4.1652

Flores-Cedeño, E. (2022). Algoritmos de aprendizaje automático aplicados a la detección de intrusiones en redes informáticas. Revista Ingeniar, 5(2), 45–58. https://doi.org/10.46296/ig.v5i2.0031

Gómez Díaz, M. P., Aguilar Ramírez, L. J., Ramírez Peña, K. J., & Villamil Escobar, L. C. (2023). Difusión de la ciberseguridad en un mundo financiero para los adolescentes. Ciencia Latina Revista Científica Multidisciplinar, 7(6), 1891–1902. https://doi.org/10.37811/cl_rcm.v7i6.8821

Gordillo Chabla, P. C., Cuenca Tapia, J. P., & Campaña Ortega, E. M. (2023). Quick guide to an information security management system for an ISP: XNET case study. ConcienciaDigital, 6(4.2), 28–45. https://doi.org/10.33262/concienciadigital.v6i4.2.2751

López López, H. L., Aguilera Zatarain, J. J., Rojas Solís, S., & Rendón Rendón, M. de los Á. (2023). Percepción de ciberseguridad en sistemas de inteligencia artificial en la educación superior. Revista Digital de Tecnologías Informáticas y Sistemas, 7(1), 115–122. https://doi.org/10.61530/redtis.vol7.n1.2023.154.115-122

Montes Gil, J. A., Isaza Cadavid, G., & Duque Méndez, N. D. (2023). Efecto de la selección de atributos en el desempeño de un IDS basado en machine learning para detección de intrusos en ataques DDoS. South Florida Journal of Development, 4(2), 918–928. https://doi.org/10.46932/sfjdv4n2-023

ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Montoya Villalba, D. A., & Montaña Varón, D. F. (2023). Diseño de un sistema de detección de intrusos (IDS) basada en técnicas supervisadas de anomalías mediante la aplicación de aprendizaje profundo. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 4(2). https://doi.org/10.26507/paper.2877

Muñoz Zambrano, C., & Zambrano Rendón, A. D. (2023). Security Operations Center, como modelo de gestión de ciberseguridad para el Hospital Especialidades de Portoviejo, Manabí-Ecuador. MQRInvestigar, 7(3), 3220–3236. https://doi.org/10.56048/MQR20225.7.3.2023.3220-3236

Obregón-Martínez, R. (2023). Modelos de machine learning para la detección de ataques en sistemas de seguridad informática. Perspectivas Investigativas Multidisciplinarias, 6(1), 88–101. https://doi.org/10.5281/zenodo.7815532

Perdigón Llanes, R. (2022). Suricata como detector de intrusos para la seguridad en redes de datos empresariales. CIENCIA UNEMI, 15(39), 44–53. https://doi.org/10.29076/issn.2528-7737vol15iss39.2022pp44-53p

Pérez, S. B. (2022). Moral hazard situations and misaligned incentives in cybersecurity. Revista Chilena de Derecho y Tecnología, 11(2), 103–120. https://doi.org/10.5354/0719-2584.2022.60821

Pinango Bayas, Á. H., Méndez Naranjo, P. M., Caiza Méndez, D. G., & Barreno Naranjo, D. G. (2022). Plan de seguridad para plataformas web empleando normas ISO-27001 y considerando el OWASP Top 10-2017. CIENCIA UNEMI, 15(40), 1–15. https://doi.org/10.29076/issn.2528-7737vol15iss40.2022pp1-15p

Ramírez Patajalo, G. A. (2023). Seguridad en desarrollo web: mejores prácticas para proteger aplicaciones y datos. Dominio de las Ciencias, 9(3). https://doi.org/10.23857/dc.v9i3.3552

Rendón, M. (2023). Inteligencia artificial y ciberseguridad en entornos empresariales: análisis de técnicas de detección de amenazas. Revista Sinapsis, 15(2), 112–125. https://doi.org/10.37117/s.v15i2.895

ISSN: 3121-2956
Doi:https://doi.org/10.70577/s.e.v2i2.8

Suárez, I. C., y colaboradores. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. Revista Científica y Tecnológica UPSE, 9(2). https://doi.org/10.26423/rctu.v9i2.672

Tenezaca, D. (2023). Sistemas inteligentes para la detección de intrusiones en redes computacionales. Revista Tecnológica Espol, 36(1), 55–67. https://doi.org/10.37815/rte.v36n1.897

Yagual, D. I. Q., y colaboradores. (2022). Una revisión del aprendizaje profundo aplicado a la ciberseguridad. Revista Científica y Tecnológica UPSE, 9(1). https://doi.org/10.26423/rctu.v9i1.671

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés