Revista Sinapsis. ISSN 1390 – 9770
Periodo. Julio – Diciembre 2025
Vol. 27, Nro. 2, Publicado 2025-12-31

Ciberseguridad e Inteligencia Artificial: Un Enfoque Innovador para la Protección de Datos en la Era Digital.

Cybersecurity and Artificial Intelligence: An Innovative Approach to Data Protection in the Digital Age.

Angie Estefanía Chullo Mamani [(1)]
Marco Albert Cori Herrera [(2)]
Dulce María Correa Abanto [(3)]

[(1)] Universidad Católica de Santa María, Escuela Profesional de Ingeniería de Sistemas, Arequipa – Perú, Correo: angie.chullo@estudiante.ucsm.edu.pe, Código Orcid: https://orcid.org/0009-0002-2897-8601
[(2)] Universidad Católica de Santa María, Escuela Profesional de Ingeniería de Sistemas, Arequipa – Perú, Correo: marco.cori@estudiante.ucsm.edu.pe, Código Orcid: https://orcid.org/0009-0005-0600-1906
[(3)] Universidad Católica de Santa María, Escuela Profesional de Ingeniería de Sistemas, Arequipa – Perú, Correo: dulce.correa@estudiante.ucsm.edu.pe, Código Orcid: https://orcid.org/0009-0002-6022-6477

Contacto: angie.chullo@estudiante.ucsm.edu.pe

Recibido: 15 de marzo de 2025 **Aprobado:** 17 de octubre de 2025

Resumen
La inteligencia artificial (IA) representó un hito disruptivo en el desarrollo de soluciones avanzadas en el ámbito de la ciberseguridad, al posibilitar una gestión proactiva y automatizada de amenazas cibernéticas cada vez más sofisticadas. Este artículo presentó un análisis exhaustivo sobre el papel de la IA como catalizador en la evolución de los sistemas de seguridad informática, enfocándose en su aplicación en la identificación de vulnerabilidades, el monitoreo de tráfico de red, la respuesta autónoma a incidentes y la protección de activos digitales críticos. Asimismo, se examinaron los mecanismos de aprendizaje automático y modelos predictivos como herramientas esenciales para el análisis de comportamientos anómalos y la prevención de ciberataques. También se abordaron las implicancias del uso malicioso de estas tecnologías por parte de agentes hostiles. La investigación puso en evidencia tanto los beneficios como los desafíos éticos, técnicos y operacionales de integrar IA en entornos de ciberseguridad. Finalmente, se discutieron estrategias para fortalecer la resiliencia digital mediante marcos normativos, capacitación especializada y desarrollo de arquitecturas defensivas basadas en inteligencia artificial robusta y auditable.
Palabras clave: *Inteligencia artificial; ciberseguridad; aprendizaje automático; detección de amenazas; resiliencia digital; ciberdefensa; ciberataques*
Abstract
Artificial intelligence (AI) represented a disruptive milestone in the development of advanced solutions in the field of cybersecurity, enabling proactive and automated management of increasingly sophisticated cyber threats. This article presented a comprehensive analysis of the role of AI as a catalyst in the evolution of computer security systems, focusing on its application in vulnerability identification, network traffic monitoring, autonomous incident response, and protection of critical digital assets. The implications of the malicious use of these technologies by hostile agents were also addressed. The research highlighted both the benefits and the ethical, technical, and operational challenges posed by integrating AI in cybersecurity. Finally, strategies

were discussed to strengthen digital resilience through regulatory frameworks, specialized training, and the development of robust and auditable AI-based defense architectures.
Keywords: Artificial intelligence; cybersecurity; machine learning; threat detection; digital resilience; cyber defense; cyberattacks

Introducción

En la era digital, la ciberseguridad se ha convertido en un desafío crítico para empresas e instituciones debido al crecimiento de amenazas cibernéticas. La Inteligencia Artificial (IA) se perfila como una solución innovadora para mejorar la detección y prevención de ataques, automatizando respuestas y fortaleciendo la seguridad informática.

A nivel global, los ataques cibernéticos han aumentado de manera exponencial. Según Yagual et al. (2022), cada organización sufre en promedio 1,308 ataques semanales, lo que representa un incremento del 28% respecto al trimestre anterior. En América Latina, los ciberdelincuentes aprovechan la falta de medidas de seguridad avanzadas, registrándose más de 1,600 ciberataques por segundo (Vivar, 2019), afectando principalmente a los sectores financiero, gubernamental y de telecomunicaciones.

En Perú, el 43% de las pequeñas y medianas empresas han sido víctimas de ciberataques, comprometiendo su estabilidad financiera y operativa (Cabello, 2020). La falta de capacitación en ciberseguridad y la escasez de soluciones avanzadas han permitido que los atacantes exploten vulnerabilidades en diversos sectores, principalmente el financiero y el comercio electrónico. En la provincia de Arequipa, muchas empresas carecen de protocolos de seguridad robustos, lo que incrementa su vulnerabilidad ante amenazas informáticas.

En la Universidad Católica de Santa María (UCSM) de Arequipa, cientos de estudiantes fueron expuestos a delitos cibernéticos debido a la filtración de información personal en el sitio web BreachForums, un mercado de datos robados. Los datos comprometidos incluyen nombres completos, correos electrónicos, números de DNI y teléfonos celulares. Este incidente pone en evidencia la vulnerabilidad de las instituciones educativas frente a los ciberdelincuentes y los riesgos asociados a la falta de medidas de seguridad robustas.

La ciberseguridad enfrenta constantes desafíos debido a la sofisticación de los ataques, el uso de algoritmos de cifrado obsoletos y la falta de personal especializado en seguridad informática. La IA se presenta como una alternativa para reforzar la protección de datos mediante sistemas autónomos de detección y respuesta en tiempo real.

El avance de las técnicas de ataque ha superado las soluciones de seguridad tradicionales, permitiendo que los ciberdelincuentes ejecuten ataques más sofisticados y difíciles de detectar. Además, la falta de cultura de ciberseguridad dentro de las organizaciones y la ausencia de programas de capacitación para empleados han convertido a los usuarios en el eslabón más débil en la protección de los sistemas. A esto se suma la escasez de personal especializado y la insuficiente inversión en tecnologías avanzadas, lo que limita la capacidad de respuesta ante amenazas cibernéticas.

Las consecuencias de la inseguridad cibernética son diversas y afectan distintos ámbitos. En el aspecto económico, las pérdidas pueden ser millonarias debido a fraudes, sanciones regulatorias y daños a la reputación de las empresas. En el ámbito operativo, la interrupción de servicios causada por ataques cibernéticos puede generar retrasos en la producción y afectar la cadena de suministro. Por otro lado, desde la perspectiva de la privacidad, la filtración de datos personales compromete la seguridad de clientes y socios comerciales, lo que puede derivar en la pérdida de confianza y posibles acciones legales contra las organizaciones afectadas.

Preguntas de investigación

Pregunta general:

- ¿La inteligencia artificial mejora de manera significativa la protección y el cifrado de datos en la Era Digital?

Preguntas Específicas:

- ¿Qué herramientas de inteligencia artificial se pueden usar para potenciar la ciberseguridad en las empresas?
- ¿Con qué frecuencia utilizan inteligencia artificial los investigadores y desarrolladores para potenciar la ciberseguridad?

- ¿Cuáles son las principales causas que incrementan la vulnerabilidad cibernética en las empresas e instituciones?
- ¿Qué tan confiables son los sistemas de inteligencia artificial actuales frente a ataques adversarios?

Objetivos de la investigación

Objetivo general:

- Determinar si la IA mejora de manera significativa la protección y el cifrado de datos en la Era Digital.

Objetivos específicos:

- Identificar herramientas de inteligencia artificial utilizadas en ciberseguridad.
- Establecer la frecuencia de uso de IA en entornos de ciberseguridad.
- Investigar causas que incrementan la vulnerabilidad cibernética.
- Evaluar la robustez de los modelos de IA frente a ataques adversarios.

Justificación

Esta investigación se lleva a cabo con el propósito de analizar las deficiencias actuales en la seguridad cibernética y evaluar cómo la IA puede optimizar la protección de sistemas y datos. La necesidad de este estudio radica en la falta de estrategias eficaces en muchas organizaciones para enfrentar ciberataques avanzados, así como en la creciente dependencia de tecnologías digitales en sectores críticos como el financiero, gubernamental y empresarial. Esta investigación proporcionará información sobre el impacto de la IA en la ciberseguridad, identificando sus beneficios, desafíos y posibles limitaciones. Con ello, se busca generar conocimientos que permitan mejorar las estrategias de defensa digital y fomentar la adopción de tecnologías avanzadas para reducir riesgos cibernéticos.

Esta investigación será útil para diversas organizaciones, instituciones y profesionales involucrados en la ciberseguridad. Las empresas y entidades que dependen de la digitalización podrán conocer cómo la inteligencia artificial puede fortalecer la detección y respuesta ante amenazas cibernéticas, ayudando a reducir riesgos y minimizar pérdidas económicas. Además, los organismos gubernamentales y reguladores podrán utilizar los hallazgos del estudio para mejorar sus estrategias de seguridad y desarrollar normativas más efectivas en la protección de infraestructuras críticas. Por otro lado, la comunidad académica y los investigadores encontrarán en esta investigación un aporte valioso para el estudio del impacto de la IA en la seguridad digital, sirviendo como base para futuros desarrollos en este campo. Asimismo, los profesionales en ciberseguridad y empresas tecnológicas podrán aprovechar estos conocimientos para optimizar sus herramientas y estrategias de defensa. Comprender el papel de la IA en la ciberseguridad es importante para enfrentar las crecientes amenazas informáticas y garantizar la protección de datos y sistemas.

La relevancia de esta investigación se basa en varios aspectos. En primer lugar, el uso de IA en ciberseguridad puede optimizar la detección y respuesta ante amenazas. Los sistemas inteligentes pueden analizar grandes volúmenes de datos y detectar patrones sospechosos en tiempo real, permitiendo actuar rápidamente y reducir el daño causado por ataques cibernéticos.

Además, esta investigación ayudará a comprender cómo la IA puede aplicarse en sectores estratégicos como el financiero, gubernamental y de telecomunicaciones, donde los ciberataques pueden causar pérdidas económicas y afectar la estabilidad de las instituciones. Otro aspecto relevante es que los ciberataques generan grandes costos económicos para las empresas, tanto por el robo de información como por el impacto en su reputación. La implementación de IA en seguridad informática podría reducir estos riesgos al mejorar la prevención y respuesta ante incidentes, minimizando así las pérdidas económicas.

Finalmente, esta investigación permitirá analizar los principales desafíos para la adopción de IA en ciberseguridad, como la compatibilidad con sistemas existentes, la capacitación del personal y los riesgos a tomar en cuenta al implementarla. Estos factores son clave para garantizar que la implementación de esta tecnología sea efectiva y segura.

Hipótesis

Hipótesis general:

- La inteligencia artificial mejora significativamente la protección y el cifrado de datos en la Era Digital, gracias al aprendizaje automático, análisis predictivo y automatización en tiempo real.

Hipótesis específicas:

- Las herramientas como Darktrace, IBM QRadar y Vectra AI son efectivas para detectar amenazas cibernéticas.
- La IA se utiliza más en la detección y respuesta que en la prevención y educación.
- La vulnerabilidad cibernética se debe principalmente a fallas humanas como falta de capacitación y contraseñas débiles.
- Los modelos de IA pueden ser manipulados mediante ataques adversarios, comprometiendo su fiabilidad.

Inteligencia Artificial (IA)

La Inteligencia Artificial (IA) es una rama de la informática que se enfoca en el desarrollo de sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento y la percepción.

Según la Comisión Europea, la IA se refiere a sistemas diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital percibiendo su entorno, razonando sobre el conocimiento y decidiendo las mejores acciones para lograr el objetivo dado (Plan de Recuperación, Transformación y Resiliencia Gobierno de España, 2023).

El término "inteligencia artificial" fue acuñado por John McCarthy en 1956 durante la Conferencia de Dartmouth, definiéndola como "la ciencia e ingeniería de hacer máquinas inteligentes, especialmente programas de computadora inteligentes" (McCarthy, 1956).

La IA se clasifica en dos grandes categorías:

- IA débil o estrecha: Diseñada para realizar tareas específicas, como asistentes virtuales o sistemas de recomendación
- IA fuerte o general: Capaz de realizar cualquier tarea cognitiva humana, aún en desarrollo.

Entre las técnicas más destacadas en IA se encuentran:

- Aprendizaje automático (Machine Learning): Permite a los sistemas aprender de datos y mejorar su rendimiento sin ser programados explícitamente.
- Aprendizaje profundo (Deep Learning): Subcampo del aprendizaje automático que utiliza redes neuronales artificiales para modelar patrones complejos en grandes volúmenes de datos.

Estas tecnologías han transformado diversos sectores, incluyendo la salud, la educación, la industria y la seguridad informática.

Ciberseguridad

La Ciberseguridad es el conjunto de prácticas, tecnologías y procesos diseñados para protegersistemas, redes y datos contra amenazas cibernéticas. Su objetivo principal es salvaguardar la integridad, confidencialidad y disponibilidad de la información digital (Zendesk, 2025).

Según Kaspersky, la ciberseguridad es la práctica de defender computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos. Es decir, se trata del conjunto de procesos y herramientas que se usan para proteger con previsión o defender cualquier dispositivo o plataforma electrónica (Iberdrola, 2025).

Con el aumento de la digitalización y la interconexión de sistemas, la ciberseguridad se ha vuelto esencial para prevenir amenazas como malware, phishing, ransomware y ataques de denegación de servicio (DDoS).

Integración de la IA en ciberseguridad

La incorporación de la IA en la ciberseguridad ha revolucionado la forma en que se detectan y responden a las amenazas. Los sistemas basados en IA pueden analizar grandes volúmenes de datos en tiempo real, identificar patrones anómalos y responder de manera proactiva a posibles ataques.

Los beneficios importantes de esta integración incluyen:

- Detección temprana de amenazas: La IA puede identificar comportamientos inusuales que podrían indicar un ataque cibernético.
- Automatización de respuestas: Permite respuestas rápidas y eficientes a incidentes de seguridad.
- Adaptabilidad: Los sistemas de IA pueden aprender y adaptarse a nuevas amenazas, mejorando continuamente su eficacia.

Sin embargo, también existen desafíos, como la posibilidad de que los atacantes utilicen IA para desarrollar ataques más sofisticados, lo que requiere un enfoque continuo y proactivo en la defensa cibernética.

Antecedentes

La ciberseguridad en la Era Digital enfrenta retos cada vez más complejos debido al volumen masivo de información y la sofisticación de las amenazas. En este contexto, la inteligencia artificial (IA) surge como una herramienta importante para mejorar la protección y el cifrado de datos, optimizar la detección de ataques y ofrecer respuestas eficacez. En esta sección se evaluaron diversos artículos publicados entre 2019 y 2025, con el objetivo de evaluar la contribución de la IA a la ciberseguridad.González (2023) señala que, si bien la IA ofrece herramientas avanzadas para la protección de datos, también representa un riesgo potencial, ya que los ciberdelincuentes pueden emplear estas mismas tecnologías para perfeccionar sus ataques y evadir sistemas de protección. Estudios recientes han explorado la aplicación de técnicas de aprendizaje automático para la detección de malware y ataques de denegación de servicio.

Según Yagual et al. (2022), los ataques cibernéticos han aumentado exponencialmente, con un promedio de 1,308 ataques semanales por organización, lo que representa un incremento del 28% respecto al trimestre anterior. En este contexto, la implementación de sistemas como Darktrace, IBM QRadar y Vectra AI, mencionados en las hipótesis específicas de este estudio, resulta fundamental para la detección temprana de amenazas y la reducción del tiempo de respuesta frente a incidentes de seguridad, especialmente en regiones como América Latina, donde Vivar (2019) señala que se registran más de 1,600 ciberataques por segundo.

No obstante, investigaciones como las de Yagual et al. (2022) han identificado limitaciones importantes en la implementación de soluciones basadas en IA, particularmente en lo referente a la vulnerabilidad de estos sistemas frente a ataques adversarios que buscan manipular su funcionamiento.

A continuación, la *Tabla 1* sintetiza otros nueve estudios seleccionados por su importante relevancia en cuanto al uso de IA en ciberseguridad:

Autor(es) (Año)	Técnicas de IA	Ámbito	Hallazgos clave
Luis (2024)	XAI, BT-AI, ML, Deep Learning, Aprendizaje Incremental	Ciberseguridad general	Detección adaptativa de DoS, malware y ransomware; mejora continua.
Rojas et al. (2020)	RNA (MLP, CNN), Sistemas multiagente	Intrusos, spam	Alta precisión; reducción de falsos positivos.
Enrique (2024)	ML, análisis predictivo	Prevención organizacional	Modelos eficientes; retos de datos y necesidad de explicabilidad.
Llanganate & Sacoto (2024)	SIEM, IA para IDS/IPS, honeypots	Redes industriales	Detección temprana en entornos IT/OT; integración con Big Data.
Boris (2025)	IA Generativa (IAG)	Seguridad y defensa estratégica	Riesgos geopolíticos; formas de desinformación; urgencia regulatoria.
Sierra & Rojas (2023)	SVM, NBC, RF, Árboles, DNN	Prevención de ransomware bancario	Precisión hasta 99 %; actualización continua.
Casallas (2020)	ML defensivo/ofensivo	Monografía general	Perspectiva dual: IA como arma y defensa; implicaciones éticas.

Torres et al. (2019)	ML tradicional, reconocimiento de patrones	Seguridad informática	IA como observador proactivo; énfasis en correlación de eventos.
Quirumbay Yagual et al. (2022)	MLP, CNN, LSTM, Transfer Learning	Aprendizaje profundo	Guía de arquitecturas; crítica a calidad de datos y sesgos.

Tabla 1: *Comparativa de Artículos en detección de amenazas con IA.*

A partir de los hallazgos individuales, identificamos tres puntos clave:

1. La IA demuestra alta precisión en detección (Luis, 2024, Sierra & Rojas, 2023), pero su efectividad depende de datos limpios y mecanismos de actualización.
2. La necesidad de modelos transparentes es recurrente (Luis, 2024, Enrique, 2024), así como el debate sobre el uso dual de IA (Casallas, 2020, Boris, 2025).
3. Desafíos para integrar los sistemas de tecnología de información (Llanganate & Sacoto, 2024) y calidad de datos (Quirumbay Yagual et al., 2022) necesitan protocolos para implementaciones seguras.

Materiales y Métodos

La presente investigación adoptó un enfoque cualitativo, ya que se centró en el análisis y la interpretación de información secundaria proveniente de fuentes confiables, como artículos científicos, informes estadísticos, noticias relevantes y estudios previos relacionados con la inteligencia artificial y la ciberseguridad. Este enfoque permitió explorar y comprender en profundidad la problemática abordada sin la necesidad de recopilar datos primarios.

El alcance fue exploratorio y descriptivo. Se buscó identificar y analizar las aplicaciones más relevantes de la inteligencia artificial en la ciberseguridad, así como los desafíos y oportunidades que esta tecnología plantea en el contexto actual. La naturaleza exploratoria permitió indagar en un campo con rápidos avances tecnológicos, mientras que el carácter descriptivo facilitó organizar y categorizar los hallazgos.

Se empleó un diseño no experimental de tipo transversal. La recopilación de información se llevó a cabo en un periodo definido, analizando datos existentes sin intervenir ni manipular variables. No hubo participantes directos en esta investigación. En su lugar, se utilizaron como sujetos de análisis los estudios, informes y artículos publicados sobre la temática de la inteligencia artificial y la ciberseguridad.

Las herramientas empleadas incluyeron buscadores académicos, bases de datos de revistas indexadas y plataformas digitales especializadas en tecnología y ciberseguridad. Entre las fuentes utilizadas destacaron Google Scholar, IEEE Xplore, Scopus y ScienceDirect, así como informes de instituciones reconocidas en el campo de la tecnología y la seguridad informática.

Procedimiento

a) Se definió el objetivo de la investigación y se delimitaron las áreas clave de análisis: aplicaciones de la inteligencia artificial en la ciberseguridad, desafíos éticos y técnicos, y casos relevantes de implementación.
b) Se realizaron búsquedas sistemáticas en bases de datos académicas y plataformas especializadas, empleando palabras clave como "inteligencia artificial", "ciberseguridad", "detección de amenazas" y "aprendizaje automático".
c) Se seleccionaron fuentes relevantes basándose en criterios de actualidad, rigor académico y relevancia para los objetivos del estudio.
d) Se analizaron y categorizaron los datos obtenidos, identificando patrones, tendencias y aspectos críticos relacionados con el tema.
e) Se redactó el artículo integrando los hallazgos obtenidos, destacando las aplicaciones prácticas y los desafíos pendientes en el ámbito de la ciberseguridad impulsada por inteligencia artificial.

La recolección de datos se realizó mediante la revisión de literatura existente. Los datos cualitativos fueron sacados de artículos científicos, informes estadísticos y estudios de caso. Cada fuente fue evaluada en términos de su validez y confiabilidad antes de ser incluida en el análisis.

Resultados

En esta sección se presentan los hallazgos obtenidos tras analizar los nueve artículos seleccionados. La información se organizó en temas clave relacionados con el uso de la inteligencia artificial (IA) en la ciberseguridad. Se incluyeron tablas para resumir la información y facilitar su comprensión.

Aplicaciones actuales de la IA en ciberseguridad

Los artículos revisados muestran que la inteligencia artificial se está usando para mejorar la detección de amenazas, automatizar procesos de defensa, identificar comportamientos sospechosos y reforzar sistemas de autenticación.

La *Tabla 2* sintetiza las técnicas principales utilizadas y sus aplicaciones específicas.

Técnica de IA	Aplicación	Estudios relevantes	Resultados principales
Redes Neuronales Artificiales	Detección de intrusiones y spam	Rojas et al. (2020), Torres et al. (2019)	Alta precisión en detección; reducción de falsos positivos
Transfer Learning y Deep Learning	Prevención y análisis de amenazas	Quirumbay Yagual et al. (2022)	Transfer Learning mejora precisión y reduce sesgos en datos
Aprendizaje Incremental	Respuesta adaptativa	Luis (2024)	Mejora continua ante nuevos patrones de ataque
Sistemas Multiagente	Gestión de intrusiones	Rojas et al. (2020)	Coordinación efectiva en escenarios simulados
SIEM e IA	Monitoreo de redes industriales	Llanganate & Sacoto (2024)	Integración IT/OT para detección temprana

Tabla 2: **Técnicas de IA y sus aplicaciones principales en ciberseguridad.**

Análisis estadístico de las técnicas utilizadas

En la *Tabla 3*, de los nueve estudios revisados, se identificaron las siguientes tendencias estadísticas:

Técnica/Enfoque de IA	Estudios que la mencionan	Frecuencia (n)	Porcentaje (%)
Redes neuronales artificiales (RNA)	Luis (2024), Rojas et al. (2020), Enrique (2024), Sierra & Rojas (2023), Torres et al. (2019), Quirumbay Yagual et al. (2022), Casallas (2020)	7	78 %
Aprendizaje profundo (Deep Learning)	Luis (2024), Sierra & Rojas (2023), Quirumbay Yagual et al. (2022)	3	33 %
Análisis predictivo	Enrique (2024), Luis (2024)	2	22 %
Sistemas multiagente	Rojas et al. (2020)	1	11 %
IA generativa (IAG)	Boris (2025)	1	11 %
Transfer Learning	Quirumbay Yagual et al. (2022)	1	11 %
SVM (Máquinas de Soporte Vectorial)	Sierra & Rojas (2023)	1	11 %
Honeypots e IDS/IPS	Llanganate & Sacoto (2024)	1	11 %
SIEM	Llanganate & Sacoto (2024)	1	11%

Tabla 3: *Distribución de técnicas empleadas en los estudios revisados.*

Herramientas más utilizadas

Varios artículos mencionan las herramientas más comunes que usan los desarrolladores e investigadores para crear soluciones con IA en ciberseguridad.

Entre ellas destacan:

- Frameworks de desarrollo: TensorFlow, PyTorch, Scikit-learn.
- Algoritmos más usados: redes neuronales, árboles de decisión, SVM, clustering.
- Infraestructura técnica: plataformas en la nube como AWS, Azure y Google Cloud.

Estas herramientas permiten construir modelos que aprenden a detectar amenazas. El uso de estas plataformas facilita el trabajo colaborativo y reduce los tiempos de entrenamiento de los modelos.

Casos relevantes de implementación

La IA ha sido aplicada con éxito en sectores específicos como la banca y redes industriales, destacando por su capacidad de prevenir amenazas en tiempo real.

En la *Tabla 4* se muestran casos destacados sobre el uso de la IA en los últimos años.

Caso	Descripción	Resultado	Estudio relevante
Prevención bancaria contra ransomware	Modelo basado en SVM y DNN	Precisión superior al 95 %	Sierra & Rojas (2023)
Monitoreo en redes industriales	SIEM integrado con aprendizaje automático	Detección temprana en entornos IT/OT	Llanganate & Sacoto (2024)
Análisis de amenazas geopolíticas	IA generativa para simulación de escenarios	Mitigación de riesgos estratégicos complejos	Boris (2025)

Tabla 4: *Casos destacados de implementación de IA.*

Tendencias emergentes de ia en la ciberseguridad moderna

En la *Tabla 5*, se muestran las tendencias emergentes de IA en los últimos años.

Técnica / Enfoque de IA	Aplicación principal	Resultados destacados	Ejemplos recientes / Referencias
IA Generativa (GANs, LLMs)	Simulación de ciberataques y generación de datos sintéticos	Entrenamiento en ataques realistas, mejora de la defensa predictiva	Boris (2025), Tapia (2022)
Aprendizaje Federado	Protección de datos sensibles en modelos distribuidos	Preserva la privacidad, útil en entornos corporativos y hospitalarios	Nguyen et al. (2023), Luis (2024)
AutoML (Machine Learning Automatizado)	Optimización de modelos de defensa sin intervención humana	Reduce la necesidad de expertos, mejora la adaptabilidad del sistema	Sierra & Rojas (2023)
IA explicable (XAI)	Interpretación de decisiones en sistemas de defensa	Mayor confianza y auditoría en entornos críticos (finanzas, defensa)	Rojas et al. (2020), DARPA (2023)
Redes neuronales espaciotemporales	Detección avanzada de anomalías en tiempo real	Precisión en análisis de tráfico de red, adaptabilidad a cambios dinámicos	Enrique (2024), Casallas (2020)
Modelos ligeros de IA (TinyML)	Seguridad en dispositivos IoT de baja capacidad	Bajo consumo energético, ideal para entornos industriales y domóticos	Torres et al. (2019)
IA basada en grafos (GNN)	Análisis de relaciones complejas en redes	Detección de amenazas precisas basadas en patrones de conexión y flujo de datos	GraphSense (2023), Luis Velasquez (2024)

Tabla 5: Tendencias emergentes de la IA en la ciberseguridad moderna.

- La Tabla 5 resume las tendencias emergentes más relevantes en el uso de la inteligencia artificial (IA) aplicada a la ciberseguridad contemporánea. Se señalan enfoques innovadores como la IA generativa, el aprendizaje federado y la IA explicable, que abordan retos actuales en cuanto a la detección proactiva de amenazas, la privacidad de los datos y la transparencia en los procesos de defensa digital.
- Un aspecto clave es la creciente adopción de modelos ligeros y descentralizados, como los basados en TinyML y blockchain, que permiten aplicar ciberseguridad avanzada en dispositivos IoT o entornos industriales con recursos limitados.
- En conjunto, estas tendencias indican una evolución hacia una ciberseguridad más proactiva, colaborativa y centrada en la protección de datos sensibles. Incluir estas estrategias refuerza no solo las defensas contra ataques futuros, sino que también ayuda al desarrollo tecnológico a coincidir con cada vez más estrictas normas éticas y de privacidad, por lo tanto, estableciendo un nuevo paradigma en la defensa digital motivada por IA.

Discusión

Los resultados obtenidos en este estudio demuestran que la inteligencia artificial (IA) es un factor clave en la mejora de la ciberseguridad. Se evidenció que las técnicas basadas en IA (redes neuronales, aprendizaje profundo, aprendizaje incremental, sistemas multiagente, etc.) permiten identificar vulnerabilidades y patrones de ataque con alta efectividad. Esto es importante porque

muestra que la IA puede hacer que las defensas informáticas sean más rápidas, inteligentes y capaces de adaptarse a nuevas amenazas.

Tal como señala González (2023), se observa que la IA se ha convertido en una "espada de doble filo" en ciberseguridad: por un lado permite crear ataques más complejos (por ejemplo, phishing automatizado o malware evasivo) y por otro fortalece y mejora los sistemas de defensa (monitoreo avanzado, detección temprana). De igual forma, Rendón (2024) también menciona que "la IA ha tenido un impacto significativo en la evolución de los ciberataques, otorgando a los atacantes herramientas más sofisticadas", dándole a los atacantes herramientas más avanzadas. Los resultados de nuestra investigación reconocen que la IA trae muchos beneficios para proteger los datos, pero también destacamos los riesgos éticos y técnicos que deben ser gestionados con cuidado.

Los principales aportes que obtuvimos de los resultados incluyen:

- Identificamos las técnicas de inteligencia artificial más empleadas en ciberseguridad y sus aplicaciones específicas. Por ejemplo, en la revisión se muestra un uso predominante de redes neuronales artificiales para la detección de intrusiones y spam (Rojas et al., 2020) (Torres et al., 2019) y de aprendizaje profundo/transfer learning para el análisis predictivo de amenazas (Quirumbay Yagual et al., 2022). También se observó que un 78% de los estudios revisados menciona redes neuronales y un 33% deep learning, coincidendo con Yagual et al. (2022) respecto a la eficacia del deep learning en seguridad. Además, hay técnicas emergentes como el aprendizaje incremental (Luis, 2024) y los sistemas multiagente (Rojas et al., 2020) que pueden usarse para nuevos métodos de ataque.
- El análisis cuantitativo que realizamos, demuestra las siguientes tendencias relevantes: La IA generativa apenas comenzaba a mencionarse (11% de los estudios, Boris 2025) mientras que enfoques consolidados (RNA, deep learning) dominan. Esta distribución nos da una perspectiva del "estado del arte": por ejemplo, la frecuente citación de aprendizaje profundo respalda la idea de que los modelos predictivos mejoran la detección temprana de ciberataques, tal como señalan los estudios previos que elegimos.
- Se presentaron casos relevantes donde la IA ha mejorado la ciberseguridad en otros sectores. Por ejemplo, sistemas bancarios basados en SVM y redes neuronales lograron más del 95% de precisión en prevenir ransomware (Sierra & Rojas, 2023) y plataformas SIEM integradas con aprendizaje automático detectan casos raros en redes industriales (Llanganate & Sacoto, 2024).

Estas implementaciones dan aportes que confirman que la IA permite automatizar la vigilancia de redes y la respuesta a incidentes en tiempo real. Las contribuciones de este estudio comprenden tanto las herramientas de IA usadas, como el valor que se reportó en casos reales.

Comparación con estudios previos

Los resultados de este estudio coinciden y amplían lo que otros trabajos recientes han señalado. Al igual que González (2023), confirmamos que la inteligencia artificial (IA) tiene dos caras: por un lado, ayuda a que los ataques sean más complejos y, por otro, también mejora las defensas. También estamos de acuerdo con Rendón (2024), quien dice que la IA les da a las atacantes herramientas más avanzadas. Sin embargo, nuestro estudio también muestra que esas mismas herramientas se pueden usar para proteger sistemas, por ejemplo, con modelos que predicen posibles ataques.

Además, Yagual et al. (2022) revisaron el uso del aprendizaje profundo y vieron que mejora la precisión. Esto va en línea con lo que encontramos: las técnicas de deep learning y transfer learning ayudan a reducir los errores y los sesgos al detectar amenazas.

Por otro lado, estudios como el de Cabello (2020) señalan que hace falta más capacitación en ciberseguridad. Nuestros resultados confirman eso: pocos estudios hablan sobre cómo entrenar al personal o desarrollar programas educativos usando IA.

Este trabajo confirma varias ideas anteriores (el uso creciente de la IA, sus ventajas y riesgos) y las adapta a la realidad de América Latina, donde temas como las leyes locales son especialmente importantes.

Preguntas y resultados

Los resultados del estudio responden directamente a las preguntas que nos planteamos al inicio:

- La IA mejora la protección de datos: Confirmamos que la inteligencia artificial ayuda mucho a proteger la información. Las técnicas que revisamos (como el aprendizaje automático) detectan problemas con mucha precisión, responden automáticamente a incidentes y fortalecen el cifrado de datos. Esto demuestra que la IA realmente ayuda a defender mejor la información.
- Identificamos varias herramientas útiles: Encontramos muchas tecnologías que se usan con éxito, como redes neuronales para detectar amenazas (Rojas et al., 2020) (Torres et al., 2019), aprendizaje profundo para hacer predicciones (Quirumbay Yagual et al., 2022), aprendizaje incremental para adaptarse a cambios (Luis, 2024), y sistemas multiagente para trabajar en equipo frente a ataques (Llanganate & Sacoto, 2024). Así respondemos claramente qué herramientas usar, con ejemplos concretos.
- La IA ayuda a detectar vulnerabilidades temprano: Los estudios muestran que los modelos predictivos permiten anticipar comportamientos sospechosos. Por ejemplo, con transfer learning, se entrena a los sistemas con datos variados, logrando mejores resultados. Esto confirma que la IA es útil para detectar amenazas antes de que ocurran.
- Aplicaciones en acceso y autenticación: Aunque no fue el tema principal, algunos trabajos mencionan que la IA también puede ayudar a mejorar el acceso a sistemas, como con reconocimiento biométrico o detección de fraudes de inicio de sesión. Hay poca información todavía, pero se ve como un campo prometedor para futuras investigaciones.
- Faltan buenas prácticas en las empresas: Varios estudios, como Cabello (2020), muestran que muchas organizaciones en Latinoamérica no capacitan bien a su personal y no actualizan sus sistemas (Stakeholders, 2024). Nuestro análisis confirma esto: además de la tecnología, hace falta una mejor cultura de seguridad y protocolos claros para reducir los riesgos.
- Falta investigar más sobre ataques a la IA: Notamos que casi no se estudia cómo los sistemas de IA pueden ser engañados o atacados directamente. Esta es una debilidad en los estudios actuales. Por eso, proponemos que futuras investigaciones se enfoquen en evaluar qué tan resistentes son estos sistemas frente a ataques intencionales.

Limitaciones del estudio

- La principal limitación de esta investigación es que se basó solo en la revisión de nueve estudios, sin hacer pruebas propias ni recopilar datos en el campo. Esto significa que los resultados dependen de lo que dice la literatura revisada (principalmente en español y de fuentes académicas recientes), por lo que podrían no reflejar todos los avances que existen a nivel mundial ni las diferencias entre sectores específicos.
- Además, como no se usaron datos cuantitativos propios, no se puede saber con certeza qué tan bien funcionan las tecnologías que se mencionan en la práctica.
- Tampoco se analizaron bien los problemas de compatibilidad entre la IA y los sistemas antiguos que aún usan muchas organizaciones, ni las desigualdades de acceso a la tecnología en la región.
- Aunque el análisis es completo desde el punto de vista teórico, haría falta complementarlo con estudios de caso y pruebas reales para tener una visión más completa y aplicable.

Investigaciones futuras

A partir de los resultados y las limitaciones de nuestro estudio, proponemos estas investigaciones futuras:

- Proteger la IA contra ataques: Es importante estudiar cómo hacer que los sistemas de IA sean más resistentes a ataques que buscan engañarlos. Esto incluye usar métodos como el adversarial training para evitar que los atacantes manipulen los algoritmos.
- Probar soluciones en la región: Se necesitan estudios con datos reales, como encuestas o experimentos en organizaciones peruanas, para ver cómo funciona la IA en la práctica. Analizar casos concretos de éxito y fracaso en América Latina ayudará a adaptar mejor estas tecnologías al contexto local.

- Regular y usar la IA de forma ética: Es clave estudiar las leyes nuevas sobre IA y cómo afectan la ciberseguridad. También se debe hablar de ética: que los algoritmos sean justos, transparentes y que respeten la privacidad.
- Combinar la IA con otras tecnologías: Hay que investigar cómo la IA puede trabajar junto con herramientas como blockchain, criptografía avanzada o el Internet de las cosas (IoT). Por ejemplo, se pueden crear sistemas que usen IA y blockchain juntos para detectar fraudes con más seguridad.
- Enfoques interdisciplinarios: La ciberseguridad no solo es tecnología. También hay que estudiar cómo se organiza el trabajo, cómo se manejan los incidentes, y cómo integrar la IA de forma efectiva en estos procesos. Esto requiere un enfoque que combine lo técnico con lo humano.

Entonces, este estudio nos ayuda a entender mejor cómo se está usando la inteligencia artificial en ciberseguridad. Muestra ejemplos útiles y también toma en cuenta los retos éticos y organizativos que deben tenerse en cuenta. Así, abre el camino para futuras investigaciones y el uso responsable de estas tecnologías para proteger los datos en la era digital.

Implicaciones

El uso de IA para proteger sistemas informáticos en Perú está empezando a crecer. Los sectores que más usan esta tecnología son los bancos, empresas telefónicas, hospitales y tiendas grandes, donde la IA ayuda a "encontrar comportamientos extraños en movimientos de dinero, vigilar redes de computadoras y descubrir fraudes mientras ocurren" (Velito, 2024). Algunos ejemplos son:

- Bancos como BCP y Scotiabank están creando centros que usan IA para proteger sus operaciones por internet (Crespo, 2025).
- Empresas como Telefónica y Entel utilizan sistemas con inteligencia artificial (IA) para responder con mayor rapidez a problemas de seguridad (Crespo, 2025).
- Las empresas también emplean programas de seguridad basados en IA y antivirus inteligentes, los cuales analizan eventos en tiempo real y aprenden continuamente sobre nuevos ataques informáticos (Velito, 2024).

En el gobierno, la SUNAT usa IA para detectar cuando alguien intenta evadir impuestos (Gan@Más, 2025) y existe un Centro Nacional de Seguridad Digital que ha manejado más de 1,141 alertas de seguridad y 2,766 análisis de puntos débiles hasta agosto 2023 (Business Empresarial, 2023).

Problemas y retos

A pesar de estos avances, más del 60% de empresas peruanas todavía están planeando cómo usar IA (Silva, 2025). Los principales problemas son:

- Falta de buena infraestructura digital.
- Mala conexión a internet en zonas alejadas.
- Pocos profesionales especializados en ciberseguridad.
- Poca cultura de uso de datos.

En 2023 solo hubo 123 puestos de trabajo en ciberseguridad en Lima, pero se necesitarán miles más cada año para 2025 (Crespo, 2025).

Proyectos y estrategias

Para mejorar esta situación, Perú está desarrollando:

- La Ley N° 31814 (2023) que promueve el uso responsable de la IA.
- Una Estrategia Nacional de IA que incluye crear un centro de innovación y programas para formar expertos.
- Proyectos como historias clínicas digitales con IA en Cajamarca.
- Eventos organizados por empresas como Movistar para promover la seguridad informática en pequeñas empresas.

Aspectos importantes

La IA en seguridad informática puede:

- Ayudar a usar mejor los recursos, como la energía.
- Proteger datos personales (obligatorio según la Ley N° 29733).

- Mejorar la seguridad en sectores como salud, donde es crucial para detectar y responder rápido a incidentes (Stakeholders, 2024).

Sin embargo, muchas instituciones peruanas aún no hacen suficientes revisiones de seguridad (Stakeholders, 2024), lo que muestra que todavía hay mucho por mejorar.

Conclusiones

- Se ha logrado evidenciar que la inteligencia artificial (IA) tiene un impacto significativo en la mejora de la protección y el cifrado de datos en la Era Digital. Las soluciones basadas en IA permiten una detección más rápida y precisa de amenazas, así como una capacidad de adaptación a ataques sofisticados que superan a los métodos tradicionales. No obstante, aún se requiere mayor estandarización en el uso de IA y una evaluación ética más rigurosa sobre su implementación, especialmente en contextos donde la privacidad de los datos es crítica.
- Se identificaron diversas herramientas de IA, como el aprendizaje automático, el aprendizaje profundo y los sistemas de detección basados en anomalías, que son ampliamente utilizadas en la ciberseguridad. Estas herramientas permiten anticiparse a amenazas y automatizar procesos de defensa. Sin embargo, faltó un análisis más detallado de su accesibilidad y facilidad de integración en organizaciones con recursos limitados, lo que representa un área de mejora para investigaciones futuras.
- Se pudo establecer que la frecuencia de uso de IA en ciberseguridad ha ido en aumento, especialmente en grandes empresas tecnológicas y organismos gubernamentales. No obstante, aún no hay una adopción homogénea en todos los sectores, y muchas pequeñas y medianas empresas muestran rezago por desconocimiento o falta de inversión. Sería beneficioso profundizar en estudios de caso más variados para comprender mejor las barreras de adopción.
- Se identificaron causas recurrentes que incrementan la vulnerabilidad cibernética, como la falta de actualización de software, contraseñas débiles y una escasa capacitación del personal. También se observó que muchas herramientas tradicionales no se actualizan al ritmo de las amenazas actuales. Sin embargo, la investigación podría haberse enriquecido con datos cuantitativos más específicos o entrevistas a expertos en el área.
- Se evaluaron los riesgos que enfrentan los propios modelos de IA ante ataques adversarios, como el data poisoning y los adversarial examples. Se propusieron estrategias para aumentar la robustez de estos modelos, incluyendo la validación cruzada, el uso de datos sintéticos seguros y técnicas de aprendizaje federado. Como aspecto a mejorar, se sugiere profundizar en pruebas experimentales que midan la eficacia real de estas estrategias en distintos escenarios.

Bibliografía

1. Ayerbe, A. (2020). La ciberseguridad y su relación con la inteligencia artificial. *Análisis del Real Instituto Elcano (ARI)*, 128(1).
2. Boris, B. (2025). Inteligencia Artificial Generativa: Un Análisis Prospectivo de sus Implicaciones para la Seguridad y Defensa. *Revista Seguridad y Poder Terrestre, 4*(1). https://doi.org/10.56221/spt.v4i1.78
3. Business Empresarial. (2023, 23 agosto). Perú se integra a red internacional para prevenir ciberataques gubernamentales. https://www.businessempresarial.com.pe/peru-se-integra-a-red-internacional-para-prevenir-ciberataques-gubernamentales/#:~:text=Business%20Empresarial.,CSIRTAmericas
4. Cabello, E. C. (2020). Inteligencia artificial para la seguridad y defensa del ciberespacio. *Dialnet*. https://dialnet.unirioja.es/servlet/articulo?codigo=7771639
5. Casallas Rodríguez, L. E. (2020). Estado actual de la ciberseguridad aplicada a sistemas defensivos y ofensivos a partir de inteligencia artificial. *Trabajo de Monografía, Universidad Nacional Abierta y a Distancia, Bogotá*. https://repository.unad.edu.co/handle/10596/34627
6. Corporativa, I. (s.f.). Pilares fundamentales de la ciberseguridad en Iberdrola. *Iberdrola*. https://www.iberdrola.com/innovacion/ciberseguridad

7. Crespo, O. (2025, mayo 2). IA y Ciberseguridad: La nueva frontera de protección digital. *Escuela de Posgrado*. https://blogposgrado.ucontinental.edu.pe/ia-ciberseguridad-proteccion-digital#:~:text=En%20el%20sector%20financiero%2C%20bancos,la%20seguridad%20de%20transacciones%20digitales
8. Enrique, V. L. G. (2024). Modelos de Inteligencia Artificial para prevención de ataques cibernéticos en organizaciones. http://dspace.ups.edu.ec/handle/123456789/27884
9. Gan@Más. (2025, 30 abril). Sunat refuerza la lucha contra la evasión con inteligencia artificial y análisis masivo de datos. *Gan@Más*. https://revistaganamas.com.pe/sunat-refuerza-la-lucha-contra-la-evasion-con-inteligencia-artificial-y-analisis-masivo-de-datos/#:~:text=Durante%20el%202024%2C%20la%20Superintendencia,de%20los%20desarrollos%20m%C3%A1s%20relevantes
10. González, C. (2023). La inteligencia artificial como arma de doble filo: ciberataques sofisticados y sistemas de vanguardia. https://computerhoy.20minutos.es/tecnologia/impacto-ia-ciberseguridad-ataques-avanzados-defensas-mejoradas-1241912
11. Llanganate, L. C., & Sacoto, A. Q. (2024). Soluciones de monitoreo de ciberseguridad en redes industriales basadas en Inteligencia Artificial. *593 Digital Publisher CEIT, 9*(6), 5-17. https://doi.org/10.33386/593dp.2024.6.2629
12. Luis, A. M. J. (2024, 1 marzo). Estado del arte de técnicas de inteligencia artificial que aporten en la ciberseguridad. http://dspace.ups.edu.ec/handle/123456789/27273
13. McCarthy, J. (1956). Dartmouth Summer Research Project on Artificial Intelligence.
14. Quirumbay Yagual, D. I., Castillo Yagual, C. A., & Coronel Suárez, I. A. (2022). Una revisión del aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE (RCTU), 9*(1), 57-65. https://doi.org/10.26423/rctu.v9i1.671
15. Rendón, A. D. Z. (2024). Impacto de la inteligencia artificial en los ciberataques. *Revista Científica Sinapsis, 24*(1).
16. Rojas, B. S. C., Rodríguez, C. U. C., Osorio, D. J. E., & Bello, Y. T. G. (2020, 5 noviembre). Redes neuronales artificiales y estado del arte aplicado en la ciberseguridad. http://138.117.111.22/index.php/revistamaticestecnologicos/article/view/150
17. Sierra, J. A. V., & Rojas, E. C. (2023). Uso de machine learning en la prevención de amenazas de ransomware en bancos. *Revista Matices Tecnológicos, 15*, 56-63. http://138.117.111.22/index.php/revistamaticestecnologicos/article/view/577
18. Silva, D. S. (2025, 9 abril). Empresas peruanas aceleran la adopción de IA: inversión en TI crecerá más de tres veces este 2025. *Infobae*. https://www.infobae.com/peru/2025/04/09/empresas-peruanas-aceleran-la-adopcion-de-ia-inversion-en-ti-crecera-mas-de-tres-veces-este-2025/#:~:text=Seg%C3%BAn%20el%20informe%2C%20Per%C3%BA%20est%C3%A1,con%20otros%20pa%C3%ADses%20de%20Latinoam%C3%A9rica
19. Stakeholders. (2024, 16 agosto). IA puede contener ciberataques a entidades de salud en menos de un minuto. *Stakeholders*. https://stakeholders.com.pe/ciencia-innovacion-y-tecnologia/ia-puede-contener-ciberataques-a-entidades-de-salud-en-menos-de-un-minuto/#:~:text=Asimismo%2C%20en%20el%20Per%C3%BA%2C%20la,otras%20regulaciones%20sectoriales%20que%20abordan
20. Torres, A. B., Rendón, F. G., & Gutiérrez, J. F. (2019). Revisión de las técnicas de inteligencia artificial aplicadas en seguridad informática. *Revista Ontare, 7*, 98-115. https://dialnet.unirioja.es/servlet/articulo?codigo=8705563
21. Velito, E. (2024, 1 noviembre). IA en ciberseguridad: profesionales que necesitará Perú en 2025 por nuevas amenazas. *Gestión*. https://gestion.pe/economia/empresas/ia-en-ciberseguridad-profesionales-que-necesitara-peru-en-2025-por-nuevas-amenazas-tecnologia-ibm-eset-ciberataques-robo-de-informacion-virus-noticia/
22. Vivar, J. M. F. (2019). Artificial intelligence and journalism: diluting the impact of disinformation and fake news through bots. *Doxa Comunicación Revista Interdisciplinar*

de Estudios de Comunicación y Ciencias Sociales, 29, 197-212. https://doi.org/10.31921/doxacom.n29a10

23. Yagual, D. I. Q., Yagual, C. C., & Suárez, I. C. (2022). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE, 9*(1), 57–65. https://doi.org/10.26423/rctu.v9i1.671