9 No.1 (2025): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.9.1.2025.e62

Opportunities and challenges in cyber threat detection with artificial intelligence

Oportunidades y retos en la detección de amenazas cibernéticas con inteligencia artificial

Autores:

Bermeo-Aucay, Freddy Rafael
UNIVERSIDAD CATÓLICA DE CUENCA
Ingeniero de Sistemas, Estudiante
Cuenca-Ecuador
freddy.bermeo1@est.ucacue.edu.ec
https://orcid.org/0000-0002-4868-7185

Barriga-Andrade, Jhonattan Javier
UNIVERSIDAD CATÓLICA DE CUENCA
Docente de la Unidad Académica de Posgrados
Cuenca- Ecuador
jhonattan.barriga@ucacue.edu.ec
https://orcid.org/0000-0001-7334-9113

Cuenca-Tapia, Juan Pablo
UNIVERSIDAD CATÓLICA DE CUENCA
Magíster en Sistemas de Información Gerencial, Docente de la Unidad Académica de Tecnologías de la Información y Comunicación (TIC), Unidad Académica de Posgrados
Cuenca-Ecuador
jcuenca@ucacue.edu.ec
https://orcid.org/0000-0001-5982-634X

Fechas de recepción: 20-DIC-2024 aceptación: 20-ENE-2025 publicación: 15-MAR-2025
https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

Este artículo basado en un análisis documental y estudios recientes, explora las oportunidades y desafíos de la integración de la Inteligencia Artificial (IA) en la ciberseguridad del sector financiero. Se destaca cómo la IA supera las limitaciones de las soluciones tradicionales al detectar amenazas desconocidas en tiempo real, analizar patrones anómalos y automatizar respuestas. A pesar de su potencial, la adopción de IA enfrenta retos como la necesidad de infraestructuras robustas, personal especializado y altos costos, además de riesgos éticos relacionados con la privacidad y los sesgos algorítmicos. Sin embargo, sus beneficios incluyen la optimización de recursos, mayor resiliencia operativa y fortalecimiento de la confianza del cliente. Este estudio concluye que la implementación de la IA, basada en estrategias éticas y bien planificadas, puede transformar la seguridad financiera al mitigar amenazas y optimizar procesos, así también revela que, a pesar de los desafíos asociados a la implementación de la IA, su uso puede incrementar significativamente la resiliencia operativa y la confianza de los clientes en el sector financiero. Los resultados muestran que la IA puede reducir incidentes cibernéticos en un 40 % y optimizar recursos operativos, destacando su potencial transformador en el sector financiero.

Palabras clave: Amenazas; Inteligencia Artificial; ciberseguridad; vulnerabilidades; detección

Abstract

This article explores the opportunities and challenges of integrating Artificial Intelligence (AI) into financial sector cybersecurity. It highlights how AI overcomes the limitations of traditional solutions by detecting unknown threats in real time, analyzing anomalous patterns, and automating responses. Despite its potential, AI adoption faces challenges such as the need for robust infrastructures, specialized personnel, and high costs, as well as ethical risks related to privacy and algorithmic biases. However, its benefits include resource optimization, greater operational resilience, and strengthening customer trust. This study concludes that the implementation of AI, based on well-planned and ethical strategies, can transform financial security by mitigating threats and optimizing processes, and also reveals that, despite the challenges associated with implementing AI, its use can significantly increase operational resilience and customer trust in the financial sector. The results show that AI can reduce cyber incidents by 40% and optimize operational resources, highlighting its transformative potential in the financial sector.

Keywords: Threats; Artificial Intelligence; cybersecurity; vulnerabilities; detection

Introducción

En la era digital, las amenazas cibernéticas han evolucionado hasta convertirse en uno de los principales desafíos para la seguridad de los sistemas críticos, especialmente en sectores sensibles como el financiero. Estas amenazas, impulsadas por técnicas avanzadas como el phishing, el malware y otros ataques emergentes, han puesto de manifiesto las limitaciones de las soluciones tradicionales de ciberseguridad. Según (Meena, 2024), el phishing por sí solo puede generar pérdidas millonarias a nivel mundial, destacando la necesidad de desarrollar enfoques innovadores para mitigar los riesgos asociados.

La Inteligencia Artificial (IA) ha emergido como una herramienta innovadora para enfrentar los retos de la ciberseguridad, proporcionando capacidades superiores de detección y prevención. Tecnologías tales como el aprendizaje profundo han evidenciado su eficacia en la identificación de patrones anómalos en información compleja (Meena, 2024). Por ejemplo, los modelos CNN y LSTM han conseguido una precisión del 97 % en la detección de sitios web malintencionados y del 88 % en la detección de comportamientos malintencionado (Olafuyi, 2023), lo cual evidencia el potencial de la Inteligencia Artificial para enfrentar desafíos complejos en el ámbito de la ciberseguridad.

Estas limitaciones, combinadas con la creciente sofisticación de las amenazas, refuerzan la necesidad de adoptar tecnologías disruptivas como el aprendizaje profundo y el procesamiento de lenguaje natural, capaces de transformar los paradigmas actuales de ciberseguridad.

En este escenario, resulta pertinente plantear ¿cómo la inteligencia artificial puede superar las limitaciones actuales en la detección de amenazas cibernéticas, maximizando su impacto positivo mientras mitiga los riesgos asociados?, particularmente en el contexto de las entidades financieras. Este enfoque busca responder a una necesidad imperiosa de avanzar hacia soluciones más robustas que fortalezcan la ciberseguridad en un sector esencial para la estabilidad económica y social (Guillermo, 2021).

En Ecuador y América Latina, el sector financiero constituye uno de los pilares esenciales de la economía mundial. Las vulnerabilidades no solo comprometen la seguridad de los sistemas, sino

que también afectan la confianza de los usuarios y pueden desencadenar repercusiones económicas de gran envergadura (Márquez Díaz, 2017).

Las soluciones de ciberseguridad que se fundamentan en firmas y normativas preestablecidas han demostrado ser insuficientes para la detección y mitigación de ataques de mayor complejidad, exponiendo a las instituciones a vulnerabilidades ante brechas de seguridad de creciente sofisticación (Guillermo, 2021).

A diferencia de las soluciones basadas en firmas, que dependen de bases de datos previamente conocidas, la IA identifica anomalías en tiempo real, incluso frente a ataques inéditos. Esto la posiciona como una herramienta clave en la evolución de la ciberseguridad.

En la actualidad, la creciente complejidad y sofisticación de las amenazas cibernéticas requiere la implementación de tecnologías avanzadas para garantizar la salvaguarda de los sistemas informáticos. Tanto el Machine Learning (ML) como el Deep Learning (DL) ofrecen capacidades avanzadas para la detección de amenazas cibernéticas, utilizando técnicas como el aprendizaje supervisado y las redes neuronales profundas para identificar patrones anómalos y predecir comportamientos maliciosos.

Por ejemplo, el Procesamiento de Lenguaje Natural (NLP) puede aplicarse para analizar logs de auditoría en tiempo real, identificando patrones sospechosos que permitan detectar brechas de seguridad. Asimismo, el Deep Learning (DL) ha demostrado ser eficaz en predecir patrones de fraude financiero mediante el análisis de grandes volúmenes de transacciones históricas, mejorando la precisión en la toma de decisiones.

En este contexto, tecnologías como Machine Learning y Deep Learning permiten una detección más precisa y en tiempo real de amenazas avanzadas, superando las limitaciones de las herramientas tradicionales al adaptarse dinámicamente a nuevos patrones de ataque.

La integración de Machine Learning (ML) e Inteligencia Artificial (IA) en la inteligencia de negocios está redefiniendo cómo las empresas analizan datos y toman decisiones estratégicas (Bharadiya, 2023). Estas tecnologías permiten detectar patrones complejos en grandes volúmenes de información, lo que habilita aplicaciones como la analítica predictiva, utilizada para prever demandas, optimizar inventarios y mejorar la gestión de recursos. Además, el uso de chatbots y

asistentes virtuales basados en IA automatiza interacciones rutinarias con los clientes, incrementando la eficiencia operativa y personalizando experiencias, lo que refuerza la relación con los consumidores (Bharadiya, 2023). La automatización del análisis de datos y la detección de anomalías también facilitan la identificación de irregularidades y áreas de mejora, mejorando la precisión en la toma de decisiones.

(Bharadiya, 2023) destaca cómo ML e IA no solo transforman la inteligencia de negocios, sino que también plantean la necesidad de un enfoque ético y transparente en su implementación para garantizar un impacto positivo y sostenible.

Frente a este panorama, resulta fundamental explorar tecnologías disruptivas que puedan abordar estas limitaciones y garantizar una protección más robusta. La inteligencia artificial ofrece una vía prometedora para superar estos desafíos, pero su adopción plantea interrogantes sobre su capacidad para enfrentar las amenazas actuales mientras se gestionan adecuadamente los riesgos técnicos y éticos asociados.

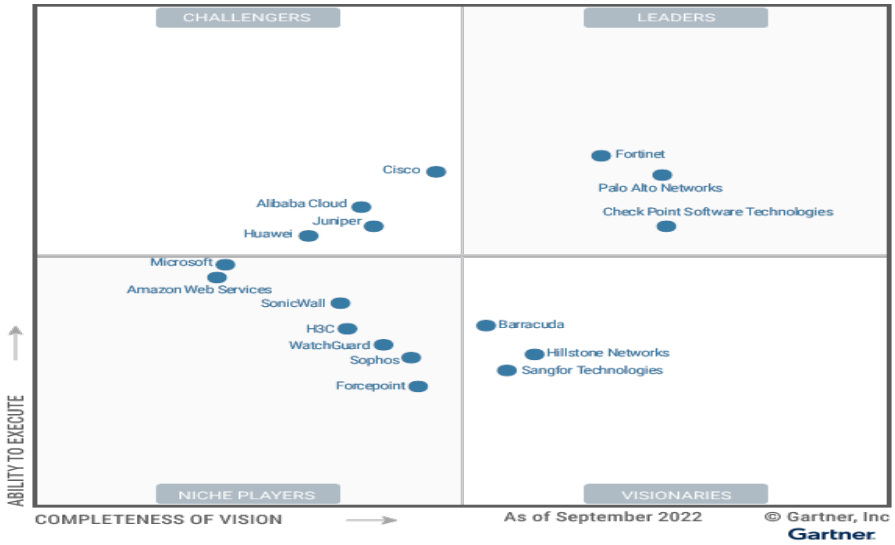
La implementación de inteligencia artificial (IA) en el sector financiero enfrenta desafíos significativos que requieren una gestión cuidadosa para maximizar sus beneficios. Así también, Según (Organización de los Estados Americanos, 2018), la inteligencia artificial (IA) presenta una serie de oportunidades significativas para el fortalecimiento de la ciberseguridad en el sector financiero, convirtiéndose en una herramienta clave para abordar las complejidades de las amenazas actuales.

De acuerdo con un estudio realizado por (Fortiguard, 2024), se prevé que los criminales cibernéticos seguirán utilizando tácticas específicas que les han permitido lograr sus objetivos de forma constante. Sin embargo, en la época actual, los perpetradores tienen a su disposición una amplia variedad de recursos, que abarcan una creciente diversidad de alternativas disponibles.

Conforme los firewalls de red se convierten en firewalls de malla híbridos (firewall en la nube y firewall como servicio), la integración de Inteligencia Artificial se torna indispensable en las propuestas de los proveedores, lo que representa un desafío en la elección del proveedor más adecuado.

Figura 1

Cuadrante mágico para firewalls de red.



Nota: Evaluación de 17 proveedores con el propósito de asistir a los líderes en seguridad y gestión de riesgos en la toma de decisiones pertinentes para su entidad (Gartner, 2022b).

En base a la Figura 1, empresas como Check Point Software Technologies, Palo Alto Networks y Fortinet se destacan por ser pioneras en la detección de amenazas a través de la Inteligencia Artificial. Palo Alto Networks proporciona una mejora en el filtrado de URL, seguridad DNS, protección de IoT y prevención de amenazas, además de funciones avanzadas de DLP. Por ejemplo, el uso de IA en las soluciones de Palo Alto Networks permitió a una entidad financiera reducir en un 40 % los incidentes relacionados con malware en un período de seis meses, lo que destaca la eficacia de estas tecnologías en entornos críticos. Fortinet se posiciona como líder en la implementación de redes distribuidas con barreras de seguridad integradas y en la creación de redes de área amplia en dispositivos compactos.

Las innovaciones implementadas por FortiNAC, tales como ZTNA, un sandbox y SOC, optimizan la seguridad proactiva y la administración de acceso. Check Point Software Technologies incorpora la gestión centralizada en la nube mediante soluciones como Quantum Lightspeed y FWaaS, las cuales son compatibles con entornos contemporáneos como OpenShift y Docker. Asimismo, se emplea micro segmentación para un control granular (Gartner, 2022a).

Aunque la implementación de IA requiere recursos significativos, los beneficios a largo plazo, como la reducción de riesgos operativos y la mejora en la confianza del cliente, justifican su adopción estratégica en el sector financiero.

Material y métodos

La metodología empleada en este artículo consistió en una revisión documental exhaustiva de publicaciones académicas, informes técnicos y artículos de revistas indexadas entre los años 2018 y 2024. Los criterios de inclusión fueron: estudios relacionados con el uso de IA en ciberseguridad, investigaciones sobre el sector financiero, reportes anuales de amenazas por entidades de firewalls y documentos que incluyeran análisis empíricos sobre detección de amenazas.

El objetivo de este trabajo es examinar de manera integral las oportunidades y desafíos que plantea la implementación de la Inteligencia Artificial en el sector financiero, con el propósito de mostrar un panorama claro que facilite su adopción de manera ética y efectiva.

Esta perspectiva no solo busca abordar los desafíos inmediatos, sino también sentar las bases para una evolución sostenida de la seguridad en el sector financiero, integrando tecnologías avanzadas con prácticas responsables y estratégicas.

Este análisis permitirá identificar áreas clave de oportunidad y formular recomendaciones prácticas para facilitar la adopción ética y efectiva de IA en el sector financiero.

Resultados y Discusión

La investigación evidenció que la integración de la Inteligencia Artificial (IA) en el sector financiero presenta tanto desafíos significativos como oportunidades transformadoras. Desde el punto de vista de la detección de amenazas, se identificaron limitaciones inherentes a las herramientas tradicionales, incapaces de abordar ataques inéditos o variantes avanzadas. Sin embargo, la IA demostró su capacidad para detectar amenazas desconocidas en tiempo real, analizando patrones anómalos y respondiendo de manera proactiva, lo que mejora significativamente la contención de incidentes.

Tabla 1.

Crecimiento en la Adopción de Inteligencia Artificial por Industria (2023 vs. 2024)

Industria	Adopcion IA en 2023	Adopcion IA en 2024
Sector Publico	Proyectos iniciales en gobernanza de datos.	Incremento en automatización y eficiencia.
Sector Privado - Finanzas	79% reportó transformaciones significativas.	Mayor enfoque en atención al cliente y logística.
	Detección de fraudes y personalización básica.	Análisis predictivo y ciberseguridad avanzada.
Salud	Diagnósticos y análisis básicos.	Tratamientos personalizados y optimización.
Educación	Proyectos piloto limitados.	Ampliación de plataformas de aprendizaje.
Manufactura	Mantenimiento predictivo en pruebas.	Automatización avanzada y mejora de productividad.
Agricultura	Fase inicial de agricultura de precisión.	Optimización de recursos y gestión de cultivos.
Multiples Funciones	<33% integraron IA en varias funciones.	50% usan IA en marketing, TI y desarrollo.
General	50% de empresas adoptaron IA.	72% implementaron IA, impulsada por IA generativa.

Nota: Elaboración propia.

La Tabla 1 presenta un análisis del crecimiento en la adopción de inteligencia artificial por diferentes industrias entre 2023 y 2024, destacando el sector financiero como líder en avances tecnológicos para ciberseguridad. Este crecimiento refleja la necesidad de implementar tecnologías avanzadas para enfrentar amenazas cibernéticas cada vez más sofisticadas.

El aumento en la adopción de IA, impulsado por la implementación de modelos predictivos y generativos, resalta la importancia de inversiones estratégicas en infraestructura tecnológica. Por ejemplo, el sector privado mostró una transformación significativa en áreas como logística y atención al cliente, mientras que el sector público avanzó hacia la automatización para mejorar la eficiencia administrativa.

El sector financiero avanzó de la detección básica de fraudes a análisis predictivo y ciberseguridad avanzada. En manufactura, la IA pasó del mantenimiento predictivo inicial a la automatización

avanzada, mejorando la productividad. Finalmente, en agricultura, se observó un salto de la agricultura de precisión en fase inicial a tecnologías que optimizan recursos hídricos y gestionan cultivos de manera más eficiente. Este progreso refleja una integración más profunda y práctica de la IA en cada industria.

En sectores como salud, educación y manufactura, la IA ha evolucionado de aplicaciones básicas, como diagnósticos y mantenimiento predictivo, a soluciones más avanzadas, incluyendo tratamientos personalizados y automatización industrial. En agricultura y finanzas, el uso de IA pasó de fases experimentales a optimizaciones tangibles, mejorando tanto la gestión de cultivos como la ciberseguridad en operaciones financieras. Este progreso refleja una integración más profunda de la IA en los procesos operativos de la región.

Tabla 2.

Desafíos y oportunidades con la integración de IA en el sector Financiero.

.	Desafíos	Oportunidades
Detección de amenazas	➢ Limitación de herramientas tradicionales frente a ataques inéditos. ➢ Riesgo de brechas de seguridad con impacto económico y reputacional.	➢ Detección en tiempo real de amenazas desconocidas. ➢ Identificación de patrones anómalos para respuestas más efectivas ante incidentes
Infraestructura y recursos técnicos	➢ Requiere infraestructura robusta y capacidades avanzadas para procesar grandes volúmenes de datos. ➢ Dependencia de personal especializado, escaso en algunos contextos.	➢ Aprendizaje continuo que mejora los modelos con nuevos datos. ➢ Adaptación dinámica frente a la evolución de las tácticas de los atacantes.
Implicaciones éticas y legales	➢ Riesgo de privacidad en el manejo de datos sensibles. ➢ Posibles sesgos en algoritmos que afectan decisiones y cumplimiento normativo.	➢ Mejora en la toma de decisiones estratégicas. ➢ Evaluación más precisa de riesgos y desarrollo de estrategias efectivas para la gestión de incidentes.

Costos asociados	➢ Altas inversiones en tecnología, capacitación y mantenimiento. ➢ Barrera económica significativa para entidades pequeñas	➢ Automatización de tareas complejas, optimizando recursos. ➢ Reducción de tiempos de respuesta y mejora en la contención de ataques
Confianza del cliente	➢ Impacto en la confianza ante fallas de seguridad. ➢ Desafíos para garantizar la percepción positiva de las instituciones	➢ Protección sólida de datos y transacciones que fortalece la confianza del cliente. ➢ Posicionamiento como líderes en innovación y confiabilidad

Nota: Elaboración propia.

En la Tabla 2, se identifican desafíos como la necesidad de infraestructuras robustas y personal especializado. Sin embargo, las oportunidades son igualmente significativas, incluyendo la detección en tiempo real de amenazas desconocidas y la automatización de tareas complejas. Este balance de desafíos y oportunidades resalta la importancia de enfoques estratégicos que combinen inversión tecnológica con capacitación continua.

En términos de infraestructura, la implementación de IA requiere sistemas robustos y capacidades computacionales avanzadas, lo que puede ser una barrera para entidades con recursos limitados. No obstante, el aprendizaje continuo que caracteriza a estos sistemas permite su adaptación dinámica frente a tácticas emergentes de los atacantes, fortaleciendo la resiliencia operativa. Desde una perspectiva ética y legal, se destacaron preocupaciones relacionadas con la privacidad de los datos y posibles sesgos en los algoritmos. A pesar de ello, la IA puede facilitar la toma de decisiones estratégicas mediante análisis precisos de riesgos y el desarrollo de estrategias efectivas para la gestión de incidentes.

Finalmente, aunque los costos de adopción representan un desafío significativo, especialmente para instituciones pequeñas, la automatización de procesos complejos optimiza recursos y reduce tiempos de respuesta, consolidando la confianza del cliente al garantizar una protección más sólida de sus datos y transacciones.

Estos hallazgos respaldan la necesidad de una estrategia combinada que priorice tanto la inversión tecnológica como la formación continua del personal, para garantizar una adopción efectiva de las tecnologías de IA en el sector financiero.

Tabla 3

Ciberataques Relacionados con IA en América Latina (Datos del 2023)

Aspecto Analizado	Descripción	Porcentaje/Impacto
Incremento en Ciberataques	Aumento de ataques a sistemas basados en IA en comparación con 2022.	Incremento del 38%.
Sectores Más Afectados	Finanzas y gobierno son los sectores principales blanco de ciberataques.	52% de los ataques dirigidos a estos sectores.
Tipos de Ataques Comunes	Robo de datos sensibles y manipulación de algoritmos en sistemas automatizados (Ransomware)	65% relacionados con robo de datos.
Impacto Regional	Infraestructuras críticas como energía y telecomunicaciones enfrentaron riesgos significativos.	No cuantificado, pero categorizado como crítico.
Principales Vulnerabilidades	Uso inadecuado de algoritmos de IA y falta de mecanismos avanzados de ciberseguridad.	Alta incidencia en entornos con infraestructura limitada.

Nota: Elaboración propia.

Adicional, los datos de la Tabla 3 confirman un incremento del 38 % en los ciberataques dirigidos a sistemas basados en IA en América Latina, con un impacto crítico en sectores como finanzas y gobierno, concentrando el 52% de los ataques, principalmente relacionados con el robo de datos sensibles y la manipulación de algoritmos, que representaron el 65% de los incidentes, este

panorama subraya la necesidad de fortalecer los mecanismos de defensa cibernética mediante la adopción de tecnologías de IA más robustas y escalables.

La inteligencia artificial representa un motor clave para el desarrollo de la región, ofreciendo amplias oportunidades. La optimización de procesos es uno de los mayores beneficios, permitiendo mejoras en sectores como salud, con diagnósticos y tratamientos personalizados, y manufactura, con automatización avanzada (Foces-Vivancos et al., 2023).

Además, países como Brasil y Chile lideran con estrategias nacionales de IA, promoviendo la ética y la regulación responsable. Esto fortalece la confianza y el desarrollo sostenible, posicionando a la región como un referente en la adopción de tecnologías emergentes (Foces-Vivancos et al., 2023).

La capacidad de la IA para identificar y responder a amenazas avanzadas en tiempo real representa un cambio paradigmático en la manera de abordar la seguridad en este sector crítico. Sin embargo, la implementación de estas tecnologías plantea desafíos técnicos, económicos y éticos que requieren una gestión cuidadosa.

La integración de la Inteligencia Artificial en el sector financiero se presenta como una solución efectiva para superar las limitaciones de las herramientas tradicionales de ciberseguridad, especialmente en un contexto donde las amenazas cibernéticas son cada vez más sofisticadas.

Desde una perspectiva técnica, aunque las capacidades avanzadas de detección y aprendizaje continuo son un diferenciador clave, la necesidad de infraestructuras robustas y recursos especializados subraya la importancia de una planificación estratégica en su adopción. Las entidades financieras con recursos limitados podrían beneficiarse de soluciones escalables y colaborativas que reduzcan los costos iniciales de implementación, como servicios en la nube optimizados con IA.

En términos éticos y legales, el manejo responsable de datos sensibles es crucial para mitigar riesgos relacionados con la privacidad y garantizar la confianza del cliente. Asimismo, la eliminación de sesgos en los algoritmos debe ser una prioridad para evitar decisiones injustas o inexactas que puedan tener consecuencias negativas en la percepción pública y el cumplimiento normativo.

Los resultados también resaltan la importancia de posicionar a la IA como una herramienta estratégica para mejorar la competitividad en el sector financiero. Al automatizar procesos complejos, reducir tiempos de respuesta y fortalecer la protección de los datos, las instituciones pueden no solo garantizar la seguridad de sus sistemas, sino también consolidar su reputación como líderes en innovación.

Por tanto, las instituciones financieras deben adoptar un enfoque proactivo que no solo considere los beneficios operativos, sino también los riesgos éticos y técnicos, promoviendo un marco regulatorio que fomente la innovación responsable.

En concreto, aunque los retos técnicos, éticos y económicos son significativos, las oportunidades que ofrece la IA justifican plenamente su adopción. Un enfoque balanceado, que contemple tanto los beneficios como las limitaciones, permitirá a las instituciones financieras maximizar el impacto positivo de esta tecnología disruptiva, transformando los desafíos actuales en catalizadores de innovación y resiliencia.

Estos hallazgos destacan cómo la IA se ha consolidado como una herramienta transformadora en el sector financiero, capaz de mejorar la detección de amenazas y optimizar la ciberseguridad. No obstante, la adopción requiere superar desafíos técnicos, económicos y éticos identificados en esta investigación.

Conclusiones

La implementación de la Inteligencia Artificial (IA) en el sector financiero representa una oportunidad crucial para transformar la manera en que se aborda la ciberseguridad, especialmente frente al incremento en la sofisticación de las amenazas cibernéticas. A lo largo de este trabajo, se ha analizado cómo la IA puede superar las limitaciones de las soluciones tradicionales, destacando sus capacidades para detectar y prevenir amenazas en tiempo real mediante el análisis de patrones anómalos y la automatización de respuestas a incidentes. Este enfoque proactivo refuerza la seguridad de las entidades financieras, minimizando el impacto económico y reputacional de los ataques.

Se sugiere que las instituciones financieras adopten un enfoque por fases en la implementación de IA, comenzando con pilotos en áreas clave como detección de fraudes, seguido de un escalamiento gradual respaldado por políticas éticas claras.

No obstante, su adopción conlleva desafíos significativos. Las instituciones deben contar con infraestructuras robustas y capacidades computacionales avanzadas para procesar grandes volúmenes de datos, lo que puede ser un obstáculo para entidades con recursos limitados. Además, se evidenció la necesidad de personal especializado para el entrenamiento y mantenimiento de los modelos de IA, lo que incrementa la dependencia de talento técnico en un contexto donde su disponibilidad es escasa.

Desde una perspectiva ética y legal, el manejo de datos sensibles y la eliminación de sesgos en los algoritmos son aspectos fundamentales para garantizar que las decisiones basadas en IA sean justas, precisas y respetuosas de la privacidad (Organización de los Estados Americanos, 2018). El cumplimiento normativo en estos aspectos no solo es esencial para mitigar riesgos legales, sino también para mantener la confianza del cliente, un elemento clave en el sector financiero.

Por otro lado, los costos asociados con la implementación de IA, si bien significativos, pueden ser amortiguados mediante la automatización de procesos complejos que optimizan los recursos y reducen los tiempos de respuesta (Fortiguard, 2024). Este factor contribuye a una mayor eficiencia operativa y al fortalecimiento de la resiliencia organizacional.

En síntesis, mientras que la adopción de IA en el sector financiero presenta retos técnicos, económicos y éticos, los beneficios superan ampliamente estas barreras cuando se gestionan adecuadamente. La IA no solo tiene el potencial de abordar las complejidades actuales de la ciberseguridad, sino también de posicionar a las instituciones financieras como líderes en innovación y confiabilidad. Tal como lo señala (Gartner, 2022a), las tecnologías basadas en IA están transformando las herramientas de ciberseguridad en plataformas más robustas e integrales, esenciales para proteger activos críticos y garantizar la continuidad del negocio en un entorno digital en constante evolución.

De cara al futuro, es fundamental que las instituciones adopten un enfoque estratégico que equilibre los beneficios y riesgos de la IA, integrando prácticas éticas y sostenibles que maximicen su impacto positivo (Organización de los Estados Americanos, 2018). Este enfoque permitirá no

solo superar los desafíos actuales, sino también sentar las bases para una evolución continua en la seguridad del sector financiero, consolidando su papel como un pilar esencial de la estabilidad económica global.

Se recomienda que las instituciones financieras inicien con pilotos controlados en áreas específicas, como la detección de fraudes, para evaluar la efectividad de los modelos de IA en un entorno seguro. Esta fase inicial debe incluir la capacitación de personal y la implementación de mecanismos de monitoreo continuo para garantizar una mejora constante en los sistemas de ciberseguridad.

Para mitigar los desafíos identificados, se recomienda que las instituciones financieras adopten un enfoque escalonado, iniciando con pilotos en áreas críticas como la detección de fraudes. Asimismo, es esencial fomentar alianzas estratégicas con proveedores de IA para compartir conocimientos y reducir los costos iniciales.

Futuras investigaciones podrían explorar cómo diseñar algoritmos éticos que minimicen sesgos, así como evaluar el impacto de regulaciones específicas en la adopción de IA en el sector financiero.

Referencias bibliográficas

Atencio-Gonzáles, R. E. (2023). Inteligencia artificial en Educación. *Cienciamatria*, *9*(17), 2–3. https://doi.org/10.35381/cm.v9i17.1150

Bharadiya, J. P. (2023). *Machine Learning and AI in Business Intelligence : Trends and Opportunities Machine Learning and AI in Business Intelligence : Trends and Opportunities*. *June*.

Calle García, J. S., Sotaminga Andi, A. S., Garay Arias, G. N., & Villavicencio Tuares, R. R. (2024). Inteligencia Artificial Y Su Contribución a La Innovación En Las Empresas. *Ciencia y Desarrollo*, *27*(2), 245. https://doi.org/10.21503/cyd.v27i2.2618

Chen Cheng, C., Chung, E., & Correa, N. (2023). inteligencia Artificial y su Impacto en la Industria de la Ingeniería. *Reicit*, *3*(1), 26–40. https://doi.org/10.48204/reict.v3n1.3948

Foces-Vivancos, M., Esquer-Portillo, A., García, X., Crespo, J., & Gutierrez, E. (2023). La Inteligencia Artificial en América Latina. *MIT Technology Review En Español*.

Fortiguard. (2024). *Cyberthreat Predictions for 2024 An Annual Perspective from FortiGuard Labs*.

Gartner. (2022a). *Magic Quadrant for Network Firewalls*. https://www.gartner.com/doc/reprints?id=1-2C2JDRLU&ct=221221&st=sb

Gartner. (2022b). *Magic Quadrant for Network Firewalls*. 2022.

Guillermo, R. (2021). El uso de la IA para ciberseguridad. *Rev UI_IPSantarém*, *9*(4), 1–7.

Márquez Díaz, J. E. (2017). Armas cibernéticas. Malware inteligente para ataques dirigidos. *Ingenierías USBMed*, *8*(2), 48–57. https://doi.org/10.21500/20275846.2955

McKinsey & Company. (2024). El estado de la IA a principios de 2024: la adopción de la IA generativa aumenta y comienza a generar valor. *McKinsey & Company*. https://www.mckinsey.com/locations/south-america/latam/hispanoamerica-en-potencia/el-estado-de-la-ia-a-principios-de-2024-la-adopcion-de-la-ia-generativa-aumenta-y-comienza-a-generar-valor/es-CL

Meena, S. R. (2024). Sparseness Controlled Proportionate RLS Algorithm for Sparse and Non-Sparse Systems. *The International Journal of Advanced Networking and Applications*, *15*(05), 6101–6108. https://doi.org/10.35444/ijana.2024.15404

Olafuyi, B. A. (2023). Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Mitigation. *International Journal of Scientific and Research Publications*, *13*(12), 194–200. https://doi.org/10.29322/ijsrp.13.12.2023.p14419

Organización de los Estados Americanos. (2018). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe*. *1*, 1–182. http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Valeria, A., & Tipan, T. (2024). *Artículo de investigación La gestión administrativa : el cambio de estrategias gracias a la incursión de la inteligencia artificial intelligence*. *4*(5), 1–13. https://doi.org/10.59814/resofro.2024.4(5)e424

zscaler. (2024). *Perspectivas del sector público : Informe sobre seguridad de la IA de ThreatLabz 2024 Resumen ejecutivo del sector público*.

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.