HORIZON NEXUS JOURNAL
ISSN: 3073-1275

DOSO EDITORIAL CIENTÍFICA

Desarrollo y eficacia de los sistemas de ciberseguridad basados en inteligencia artificial en sectores financieros

Development and effectiveness of artificial intelligence-based cybersecurity systems in financial sectors

Boné-Andrade, Miguel Fabricio [1*]

[1] Universidad Politécnica Salesiana, Ecuador, Cuenca; https://orcid.org/0000-0002-8635-1869, mbonea@est.ups.edu.ec

* Autor Correspondencia

https://doi.org/10.70881/hnj/v2/n2/38

Cita: Boné-Andrade, M. F. (2024). Desarrollo y eficacia de los sistemas de ciberseguridad basados en inteligencia artificial en sectores financieros. *Horizon Nexus Journal*, *2*(2), 43-56. https://doi.org/10.70881/hnj/v2/n2/38.

Recibido: 08/03/2024
Revisado: 15/03/2024
Aceptado: 20/03/2024
Publicado: 30/04/2024

Resumen: El estudio explora el papel de la inteligencia artificial (IA) en fortalecer la ciberseguridad del sector financiero, un ámbito cada vez más expuesto a ciberataques sofisticados, como fraudes y phishing. Mediante una revisión de estudios recientes, se concluye que la IA permite una detección rápida y precisa de patrones anómalos, lo que mejora la respuesta ante incidentes y disminuye la carga en los equipos humanos de seguridad. La IA logra esto al analizar grandes volúmenes de datos y adaptar sus algoritmos, minimizando los falsos positivos y optimizando la protección de los sistemas financieros. No obstante, se identifican desafíos críticos para su implementación, como la gestión de datos sensibles y la ausencia de regulaciones éticas específicas, que son esenciales para garantizar la transparencia y confianza en estos sistemas. En conclusión, con un marco regulatorio adecuado, la IA es una herramienta indispensable para enfrentar las amenazas cibernéticas en el sector financiero de forma proactiva y eficaz.

Palabras clave: ciberseguridad; inteligencia artificial; sector financiero; fraude; amenazas cibernéticas.

Abstract: The study explores the role of artificial intelligence (AI) in strengthening cybersecurity in the financial sector, an area increasingly exposed to sophisticated cyberattacks such as fraud and phishing. A review of recent studies concludes that AI enables fast and accurate detection of anomalous patterns, improving incident response and reducing the burden on human security teams. AI achieves this by analyzing large volumes of data and adapting its algorithms, minimizing false positives and optimizing the protection of financial systems. However, critical challenges to its implementation are identified, such as the management of sensitive data and the absence of specific ethical regulations, which are essential to ensure transparency and trust in these systems. In conclusion, with an adequate regulatory framework, AI is an indispensable tool to address cyber threats in the financial sector proactively and effectively.

Keywords: cybersecurity; artificial intelligence; financial sector; fraud; cyber threats.

1. Introducción

El desarrollo de los sistemas de ciberseguridad basados en inteligencia artificial (IA) representa una innovación crucial para enfrentar las amenazas crecientes en el sector financiero. En un contexto caracterizado por una acelerada digitalización y un aumento en la sofisticación de los ciberataques, los sistemas tradicionales de seguridad muestran limitaciones en su capacidad de respuesta y adaptación a los ataques más avanzados (Crowe LLP, 2023). La IA se ha posicionado como una herramienta estratégica para mejorar la detección y mitigación de amenazas, especialmente en el ámbito financiero, donde la seguridad y la confiabilidad de los datos son esenciales para mantener la estabilidad y la confianza de los clientes en las instituciones financieras (IEEE, 2024).

El sector financiero ha sido un objetivo prioritario para los cibercriminales debido al valor de la información manejada y al potencial de generar beneficios económicos mediante el acceso no autorizado a sistemas financieros. Además, los atacantes emplean cada vez más la IA y el aprendizaje automático para diseñar ataques que evadan las defensas convencionales, lo cual incrementa la vulnerabilidad de los sistemas tradicionales de ciberseguridad. Estos sistemas, basados en reglas y configuraciones preestablecidas, no pueden adaptarse rápidamente a nuevas tácticas y patrones de comportamiento maliciosos, lo que limita su efectividad (McKinsey & Company, 2022). Por ello, la introducción de la IA en ciberseguridad no solo es una tendencia tecnológica, sino una necesidad para fortalecer los sistemas de defensa en el sector financiero.

Los ciberataques en el sector financiero pueden provocar desde pérdidas económicas significativas hasta daños en la reputación de las instituciones afectadas. Además, comprometen la privacidad y seguridad de los datos sensibles de los clientes, como información de cuentas, transacciones y datos personales, lo cual podría derivar en casos de fraude e impacto negativo en la confianza pública (Capgemini, 2019). En particular, la creciente complejidad de los ataques basados en IA, como el phishing automatizado y el uso de malware adaptativo, plantea retos significativos para las instituciones financieras que no cuentan con sistemas avanzados de detección y respuesta.

El aumento en la frecuencia y sofisticación de los ataques cibernéticos en el sector financiero ha generado un incremento en los costos asociados a la protección y mitigación de riesgos. Las inversiones en ciberseguridad ahora representan una proporción considerable del presupuesto de TI en muchas instituciones financieras, lo cual puede desviar recursos de otras áreas estratégicas (Crowe LLP, 2023). Sin embargo, los sistemas de IA ofrecen una solución potencialmente más rentable al permitir una detección más rápida y precisa de amenazas, reduciendo el tiempo y costo de respuesta (Juniper Research, 2022).

La implementación de sistemas de ciberseguridad basados en IA en el sector financiero es viable gracias a los avances recientes en aprendizaje automático y análisis de datos, que permiten desarrollar algoritmos capaces de identificar patrones inusuales en el comportamiento de transacciones en tiempo real. Estos sistemas aprenden de cada ataque, ajustando y mejorando continuamente sus capacidades de detección y respuesta, lo que reduce la dependencia de los equipos humanos y permite una respuesta más oportuna y eficaz frente a las amenazas emergentes (Crowe LLP, 2023).

Además, las instituciones financieras cuentan con una gran cantidad de datos históricos sobre transacciones y patrones de fraude, lo cual proporciona una base sólida para entrenar los algoritmos de IA y mejorar su precisión. La justificación de estos sistemas radica no solo en la capacidad de prevenir ataques, sino en la reducción del costo a largo plazo asociado con las violaciones de seguridad, la recuperación de datos y el daño reputacional (IEEE, 2022).

El presente artículo tiene como objetivo realizar una revisión exhaustiva de la literatura disponible sobre el desarrollo y la eficacia de los sistemas de ciberseguridad basados en IA en el sector financiero. Para ello, se analizarán los enfoques y metodologías más comunes en la implementación de estos sistemas, así como los principales desafíos y limitaciones reportados en estudios recientes. Asimismo, se pretende evaluar el impacto de la IA en la capacidad de las instituciones financieras para anticipar, detectar y mitigar ciberataques de forma proactiva y adaptativa. De esta manera, el artículo contribuirá a una comprensión integral de cómo la IA puede fortalecer la ciberseguridad en el sector financiero y de qué manera se pueden superar las barreras actuales para su implementación efectiva (MDPI, 2023).

La revisión de los sistemas de ciberseguridad basados en IA en el sector financiero no solo es relevante desde el punto de vista tecnológico, sino que también es una cuestión estratégica para la protección de la información y la estabilidad financiera global. Ante el avance continuo de los ciberataques, es fundamental que las instituciones financieras adopten tecnologías avanzadas que les permitan mantenerse un paso adelante en la identificación y prevención de riesgos. Por lo tanto, este estudio contribuirá a la literatura existente proporcionando una visión detallada de los beneficios, desafíos y mejores prácticas en el uso de IA para la ciberseguridad en el sector financiero.

2. Materiales y Métodos

La metodología empleada en este estudio se basa en un enfoque exploratorio de revisión bibliográfica, orientado a recopilar, analizar y sintetizar la información existente sobre la eficacia de los sistemas de ciberseguridad basados en inteligencia artificial (IA) en el sector financiero. Dada la naturaleza evolutiva de las amenazas cibernéticas y la constante innovación en soluciones de IA, este enfoque permite una visión amplia y contextual de los avances y desafíos reportados en estudios recientes.

Para la selección de fuentes, se aplicaron criterios de inclusión específicos, enfocándose en artículos científicos publicados en revistas indexadas y en informes de organismos especializados en tecnología y ciberseguridad financiera. Se estableció un rango temporal de los últimos diez años, con énfasis en estudios publicados en los últimos cinco años, lo que permitió capturar las tendencias y desarrollos más actuales. Asimismo, se priorizaron investigaciones que abordaran tanto la implementación como los impactos y limitaciones de los sistemas de IA en ciberseguridad.

El proceso de búsqueda y selección de información se llevó a cabo en bases de datos académicas como Scopus, Web of Science y IEEE Xplore, mediante el uso de palabras clave y términos de búsqueda relevantes, tales como "inteligencia artificial en ciberseguridad", "sectores financieros y amenazas cibernéticas" y "detección de fraude con IA". Este proceso incluyó una revisión inicial de títulos y resúmenes, con el objetivo

de identificar los estudios más pertinentes para el tema de investigación. Posteriormente, los artículos seleccionados fueron analizados en profundidad para extraer datos relevantes sobre los enfoques metodológicos, hallazgos principales, aplicaciones y limitaciones de los sistemas de IA en ciberseguridad.

El análisis de la información recopilada se realizó mediante una categorización de los estudios en función de su enfoque específico dentro del ámbito de la ciberseguridad y la IA. Esto incluyó la identificación de los métodos más comunes de implementación de IA en sistemas de defensa cibernética, los algoritmos empleados y las métricas utilizadas para evaluar su efectividad. Asimismo, se analizaron los desafíos reportados en la literatura, como las limitaciones de los algoritmos en escenarios complejos, las barreras de privacidad y las implicaciones éticas asociadas con el uso de IA en el sector financiero.

Finalmente, la síntesis de los resultados permitió estructurar los hallazgos en torno a temas clave que abordan los beneficios potenciales y las limitaciones de los sistemas de ciberseguridad basados en IA. Este enfoque de revisión bibliográfica facilita la identificación de áreas de oportunidad para futuras investigaciones y el establecimiento de recomendaciones para el fortalecimiento de la ciberseguridad en el sector financiero mediante IA, aportando una visión integral y actualizada sobre el estado y la efectividad de estas tecnologías.

3. Resultados

3.1. Avances en detección de amenazas

3.1.1. Identificación de patrones anómalos en tiempo real

La detección de patrones anómalos en tiempo real es fundamental en la ciberseguridad financiera, y los sistemas de IA ofrecen una ventaja significativa frente a los métodos tradicionales. La IA permite analizar flujos de datos complejos y establecer patrones de comportamiento normales, lo cual facilita la identificación de actividades inusuales que podrían indicar fraudes o accesos no autorizados (Elhassan et al., 2022). Este enfoque ayuda a reducir tiempos de respuesta, permitiendo que las instituciones financieras tomen medidas antes de que los ciberataques causen daños importantes.

Además, el análisis en tiempo real de grandes cantidades de datos permite detectar desviaciones en comportamientos históricos, como transacciones inusuales o intentos de acceso desde ubicaciones no reconocidas, lo cual incrementa la precisión y eficacia en la prevención de fraudes. La capacidad de estos sistemas para adaptarse y actualizar sus patrones de detección contribuye significativamente a la resiliencia en la ciberseguridad del sector financiero (Hanna, Burns & Presslar, 2022).

3.1.2. Mejora de la precisión mediante análisis de grandes volúmenes de datos

El aprendizaje automático en IA permite a los sistemas analizar grandes volúmenes de datos financieros, lo cual mejora notablemente la precisión en la detección de actividades fraudulentas. Al analizar datos históricos y actuales, estos sistemas logran distinguir entre actividades legítimas e ilegítimas, reduciendo así los falsos positivos que dificultan la eficiencia operativa de los equipos de seguridad (Elhassan et al., 2022).

Según estudios recientes, el uso de IA en el análisis de datos financieros ha permitido reducir en un 20% la incidencia de errores en la detección de fraudes, lo que representa una mejora considerable en la protección contra el fraude financiero (West, 2021).

Esta capacidad de análisis masivo también ha demostrado ser esencial para la detección de fraudes sofisticados, como el fraude escalonado, donde pequeñas transacciones realizadas en un corto periodo de tiempo intentan evadir la detección. La IA puede identificar estas actividades sospechosas al agrupar y analizar patrones de comportamiento, lo cual reduce el riesgo de pérdidas significativas para las instituciones (Van Vlasselaer et al., 2017).

3.1.3. Detección específica de fraude y phishing en el sector financiero

La IA ha permitido avances notables en la detección de fraudes y ataques de phishing, dos amenazas comunes en el sector financiero. Con el uso de técnicas avanzadas de reconocimiento de patrones, los sistemas de IA identifican rápidamente transacciones fraudulentas que intentan pasar desapercibidas, como transferencias bancarias pequeñas pero repetitivas. Esta capacidad de detección específica es clave para proteger la información sensible de los clientes y evitar pérdidas económicas (Elhassan et al., 2022; Hanna et al., 2022).

Además, la IA se utiliza en la identificación de ataques de phishing mediante el análisis del contenido de mensajes y correos electrónicos sospechosos. Mediante el procesamiento de lenguaje natural (NLP), estos sistemas analizan la semántica y el tono de las comunicaciones para detectar patrones de engaño que suelen estar presentes en correos de phishing. Esta capacidad para reconocer señales en los mensajes reduce significativamente la probabilidad de que empleados o clientes sean víctimas de ataques de ingeniería social (West, 2021).

3.1.4. Aplicación de procesamiento de lenguaje natural (nlp) en la detección de amenazas

El uso de procesamiento de lenguaje natural (NLP) en ciberseguridad permite a los sistemas de IA analizar el contenido textual de comunicaciones en busca de signos de amenazas. Esta tecnología es especialmente útil en el sector financiero, donde los atacantes emplean tácticas avanzadas para engañar a los usuarios. A través del NLP, los sistemas pueden detectar mensajes que contienen lenguaje sospechoso, enlaces maliciosos o patrones de comunicación engañosos, que son características comunes en ataques de phishing (Hanna et al., 2022).

La combinación de IA y NLP permite a las instituciones financieras proteger proactivamente a sus clientes, generando alertas y bloqueando comunicaciones potencialmente peligrosas antes de que el usuario interactúe con ellas. Esto representa una medida preventiva significativa en la mitigación de amenazas cibernéticas y demuestra la efectividad de la IA para enfrentar desafíos emergentes en ciberseguridad (Van Vlasselaer et al., 2017).

3.2. Desafíos en la Implementación de IA

La implementación de inteligencia artificial en el sector financiero ofrece beneficios sustanciales, pero enfrenta una serie de desafíos complejos que pueden limitar su efectividad y sostenibilidad a largo plazo. Estos retos incluyen la dificultad de trabajar con datos limitados, problemas de privacidad, costos de infraestructura y la falta de regulaciones y estándares éticos.

3.2.1. Limitada eficacia con datos escasos

La efectividad de los modelos de IA depende en gran medida de la cantidad y calidad de los datos disponibles. Sin embargo, en el sector financiero, la disponibilidad de datos puede ser limitada debido a la segmentación de bases de datos, restricciones legales y prácticas de privacidad que impiden compartir información sensible (Scalefocus, 2023). La calidad y accesibilidad de los datos son esenciales para el rendimiento de los modelos predictivos; datos incompletos o sesgados pueden llevar a resultados inexactos, lo cual es especialmente riesgoso en decisiones críticas, como la evaluación de créditos o la detección de fraudes (Ridzuan et al., 2024). En consecuencia, la falta de datos adecuados puede reducir la precisión de los modelos, limitando la capacidad de la IA para identificar patrones de fraude emergentes o cambios en el comportamiento del usuario.

3.2.2. Problemas de privacidad al manejar datos sensibles

El manejo de datos personales y financieros plantea un desafío importante en cuanto a privacidad y seguridad. La IA, al analizar grandes volúmenes de datos personales para generar predicciones, puede entrar en conflicto con las regulaciones de privacidad, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea y otras normativas locales. Este tipo de sistemas no solo depende de información financiera, sino que también integra datos sensibles de clientes, lo cual aumenta el riesgo de exposición a ciberataques y accesos no autorizados (FIS, 2024).

Además, la opacidad de algunos modelos de IA —también conocida como el problema de la "caja negra"— dificulta explicar cómo se usan y protegen los datos, lo cual compromete la transparencia y la confianza de los usuarios (Aldboush & Ferdous, 2023). En este contexto, la privacidad se convierte en un obstáculo fundamental, ya que los datos recopilados para un propósito específico podrían ser reutilizados sin el conocimiento o consentimiento explícito del usuario, lo cual plantea implicaciones éticas significativas.

3.2.3. Altos costos de infraestructura y mantenimiento

Implementar IA en el sector financiero requiere una infraestructura de TI robusta y costosa. Los modelos de IA necesitan hardware avanzado y capacidades de procesamiento de datos, lo cual implica inversiones significativas en centros de datos, almacenamiento y redes de alta velocidad (ICAEW, 2023). Además, el mantenimiento continuo de estos sistemas, que incluye actualizaciones de software, control de calidad y monitoreo de rendimiento, agrega costos operativos recurrentes. Estos gastos representan un desafío considerable, especialmente para instituciones más pequeñas o aquellas con presupuestos limitados.

Para hacer frente a estas barreras, muchas instituciones financieras recurren a proveedores externos de servicios de IA, lo cual introduce riesgos adicionales, como la dependencia de terceros y la posibilidad de vulneraciones de datos sensibles (Scalefocus, 2023). Por lo tanto, aunque la IA promete mejorar la eficiencia operativa y la precisión en las decisiones, los costos iniciales y de mantenimiento pueden ser prohibitivos para algunas organizaciones, limitando así su adopción.

3.2.4. Falta de regulación y estándares éticos

La rápida adopción de IA en el sector financiero ha superado el desarrollo de marcos regulatorios y estándares éticos adecuados, generando incertidumbre sobre cómo manejar cuestiones de transparencia, responsabilidad y equidad. A diferencia de otros sectores, la IA en finanzas debe lidiar con cuestiones éticas complejas, como el sesgo algorítmico y la justicia en la toma de decisiones. Por ejemplo, los sistemas de IA utilizados para la evaluación de créditos pueden basarse en datos que reflejan desigualdades sociales, perpetuando así patrones de discriminación que afectan desproporcionadamente a ciertos grupos (Ridzuan et al., 2024).

La regulación de la IA en el sector financiero también se enfrenta a desafíos debido a la diversidad de regulaciones internacionales. La ausencia de una normativa uniforme dificulta el establecimiento de estándares globales que garanticen la equidad y seguridad en el uso de IA. Los expertos destacan que, para mitigar estos riesgos, es fundamental desarrollar un marco ético que incluya transparencia en el procesamiento de datos y claridad en los mecanismos de toma de decisiones (ICAEW, 2023).

3.3. Eficiencia en respuesta ante incidentes

La incorporación de inteligencia artificial (IA) en la respuesta ante incidentes en el sector financiero no solo ha optimizado la capacidad de respuesta ante ciberamenazas, sino que también ha impulsado un marco de ciberseguridad más ágil, preciso y adaptable. Los beneficios clave incluyen la detección rápida y precisa de amenazas, la reducción de la carga de trabajo humano, el análisis en tiempo real y el aprendizaje continuo frente a nuevas tácticas de ataque. Estos aspectos consolidan la IA como una herramienta esencial para gestionar y mitigar incidentes de seguridad con eficiencia.

3.3.1. Respuesta más rápida y precisa ante amenazas

La capacidad de la IA para analizar grandes volúmenes de datos en tiempo real permite la detección y respuesta casi instantánea a amenazas potenciales. Este enfoque es crucial en el sector financiero, donde cada segundo cuenta para prevenir impactos financieros y daños reputacionales. Herramientas de IA, como los sistemas de Orquestación, Automatización y Respuesta de Seguridad (SOAR), permiten una contención automática de las amenazas, activando respuestas inmediatas que minimizan el impacto antes de que los incidentes puedan escalar (Squadcast, 2024). Estas plataformas utilizan algoritmos de aprendizaje automático que permiten identificar patrones anómalos de manera anticipada y ejecutar acciones automatizadas para contener incidentes con una precisión superior, optimizando así el tiempo de resolución (Cybermatters, 2024).

La investigación de Galaz et al. (2021) resalta cómo los sistemas de IA en incidentes de ciberseguridad han mejorado significativamente la continuidad del negocio en el sector

financiero. Este estudio confirma que los modelos de IA, al integrar datos históricos y análisis predictivos, pueden adaptar sus respuestas en función de la evolución de la amenaza, optimizando así la resiliencia operativa de las organizaciones.

3.3.2. Reducción de la carga en equipos humanos

La automatización de tareas básicas en la respuesta ante incidentes es otro de los beneficios clave de la IA, ya que permite delegar en estos sistemas procesos repetitivos y de clasificación de alertas, aliviando la carga en los equipos de seguridad. Esto permite a los expertos humanos concentrarse en tareas más complejas y de mayor relevancia estratégica, lo que mejora la eficiencia general del equipo de respuesta (LeewayHertz, 2024). Además, la IA es capaz de gestionar grandes volúmenes de alertas simultáneas, priorizando automáticamente aquellas con mayor riesgo potencial, lo cual evita que el equipo humano se vea abrumado por incidentes de bajo impacto (ZIF, 2024).

Según el estudio de Charles et al. (2023), los sistemas de IA en incidentes de seguridad han logrado una reducción notable en el tiempo medio de resolución (MTTR), al delegar tareas rutinarias de detección y triage. Esto no solo optimiza los recursos humanos, sino que también disminuye los costos asociados a las operaciones de seguridad, una ventaja relevante en el contexto de recursos limitados en el sector financiero.

3.3.3. Análisis en tiempo real para respuestas inmediatas

El análisis en tiempo real es fundamental en el manejo de incidentes en el sector financiero. La capacidad de la IA para monitorear continuamente redes y sistemas transaccionales permite identificar rápidamente anomalías que podrían indicar actividades maliciosas. Por ejemplo, plataformas como ZIF™ utilizan algoritmos avanzados para detectar y responder de inmediato ante patrones inusuales, lo que facilita intervenciones preventivas antes de que un incidente se convierta en una amenaza mayor (Blinkops, 2024).

La agilidad y precisión de estas plataformas de IA permite una respuesta inmediata, algo crítico en entornos financieros donde una pequeña demora puede traducirse en pérdidas financieras significativas. Según Cybermatters (2024), este enfoque de vigilancia proactiva en tiempo real también reduce la posibilidad de interrupciones operativas, mejorando la continuidad del negocio y fortaleciendo la infraestructura de seguridad de la organización.

3.3.4. Aprendizaje continuo frente a nuevas tácticas de ataque

Uno de los aspectos más destacados de los sistemas de IA en la respuesta ante incidentes es su capacidad de aprendizaje continuo, lo cual es esencial en un entorno de amenazas cibernéticas en constante evolución. Estos sistemas registran y analizan incidentes pasados, adaptando sus algoritmos para mejorar en la detección y contención de nuevas tácticas de ataque. Este aprendizaje adaptativo fortalece la capacidad de defensa de los sistemas de IA, permitiéndoles anticiparse a patrones de ataque emergentes y reforzar la seguridad organizacional (SoftwareMind, 2023).

La investigación de Tan et al. (2022) subraya la importancia del aprendizaje adaptativo en incidentes de seguridad, indicando que los sistemas que integran capacidades de aprendizaje automático y continuo pueden ofrecer una mejor respuesta a amenazas nuevas y complejas, mejorando así la preparación organizacional frente a ataques

avanzados. A través de este proceso de mejora constante, la IA no solo incrementa su precisión en la detección de amenazas, sino que también optimiza sus protocolos de respuesta ante incidentes recurrentes o variaciones en las tácticas de los atacantes.

4. Discusión

La adopción de la inteligencia artificial (IA) en la ciberseguridad financiera ha revolucionado la manera en que las instituciones abordan la detección y respuesta ante amenazas, mostrando un progreso significativo en eficiencia y resiliencia organizacional. Los resultados analizados destacan cómo la IA contribuye no solo a optimizar la respuesta ante incidentes, sino también a anticipar y mitigar riesgos emergentes mediante el aprendizaje continuo y el análisis de grandes volúmenes de datos en tiempo real. Este avance representa una transición de enfoques reactivos a sistemas predictivos, donde la IA juega un rol central en el fortalecimiento de las defensas cibernéticas y la continuidad operativa.

Uno de los aspectos más notables es la capacidad de la IA para mejorar la velocidad y precisión en la respuesta a amenazas, lo cual es particularmente crucial en el sector financiero. Las plataformas de IA, como los sistemas de Orquestación, Automatización y Respuesta de Seguridad (SOAR), han demostrado ser eficaces en la contención de amenazas, al automatizar procesos críticos y reducir el tiempo de detección y reacción (Blinkops, 2024). Este enfoque ha permitido que las instituciones financieras logren una reducción considerable en el tiempo medio de resolución de incidentes (MTTR), limitando así el alcance de los daños potenciales. Además, estos sistemas integran algoritmos de aprendizaje automático que analizan en tiempo real flujos de datos transaccionales, mejorando la precisión y disminuyendo la probabilidad de falsos positivos (ZIF, 2024). Esto no solo agiliza la respuesta a amenazas, sino que también permite concentrar recursos en incidentes de mayor criticidad, una ventaja indispensable en contextos de alta sensibilidad financiera.

La reducción de la carga en los equipos humanos representa otro beneficio sustancial de la IA en la gestión de incidentes. Al delegar tareas repetitivas y de clasificación a sistemas automatizados, los equipos de seguridad pueden enfocarse en el análisis y resolución de problemas complejos que requieren juicio y experiencia humana. Este enfoque optimiza los recursos disponibles y minimiza la carga cognitiva en los operadores, quienes pueden priorizar actividades estratégicas de alto valor (LeewayHertz, 2024). Además, estudios como el de Charles et al. (2023) subrayan que la automatización de respuestas iniciales mediante IA permite a las instituciones no solo reducir costos operativos, sino también asegurar una respuesta más uniforme y eficiente ante incidentes de ciberseguridad, fortaleciendo su infraestructura defensiva frente a un volumen creciente de amenazas.

El análisis en tiempo real es otro elemento diferenciador de la IA, ya que permite una detección temprana de patrones anómalos que podrían pasar desapercibidos en sistemas convencionales. Herramientas avanzadas como ZIF™ monitorean constantemente la infraestructura tecnológica de las organizaciones, detectando variaciones en los patrones de comportamiento de las transacciones y el tráfico de red que pudieran indicar un ataque inminente (ZIF, 2024). Esto es particularmente relevante

en el contexto financiero, donde una demora en la respuesta puede traducirse en pérdidas significativas y comprometer la confianza de los clientes. La capacidad de la IA para realizar este tipo de análisis inmediato minimiza las interrupciones operativas y asegura la continuidad del negocio, consolidando una infraestructura de ciberseguridad más robusta y resiliente (Cybermatters, 2024).

Sin embargo, uno de los elementos más transformadores de la IA en la respuesta ante incidentes es su capacidad de aprendizaje continuo. A medida que la IA analiza incidentes pasados, sus algoritmos se adaptan, mejorando su habilidad para detectar y responder a nuevas tácticas de ataque. Este aprendizaje adaptativo permite una evolución constante de las defensas cibernéticas, ajustándose a patrones emergentes y anticipando ataques potenciales basados en tácticas recientes (SoftwareMind, 2023). Estudios como los de Tan et al. (2022) y Galaz et al. (2021) confirman que los sistemas de IA con capacidad de aprendizaje continuo no solo mejoran en precisión, sino que también optimizan los protocolos de respuesta ante incidentes, contribuyendo así a una preparación organizacional avanzada ante amenazas en constante evolución.

No obstante, es importante señalar que, si bien la IA aporta grandes beneficios, su implementación no está exenta de desafíos. La opacidad de algunos modelos de IA, conocida como el problema de la "caja negra", plantea una dificultad significativa en la transparencia y explicabilidad de las decisiones automáticas. Esta falta de claridad en los procesos de toma de decisiones automatizadas puede generar desconfianza en los sistemas de IA, especialmente en el contexto financiero, donde la precisión y la justificación de las decisiones son esenciales (Squadcast, 2024). Además, la dependencia de grandes volúmenes de datos plantea desafíos en cuanto a la privacidad y el cumplimiento normativo, ya que el acceso y uso de datos sensibles debe ser gestionado bajo estrictas regulaciones de protección de datos, tales como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea.

Para concluir, la IA ha demostrado ser una herramienta fundamental en la modernización de la respuesta ante incidentes en el sector financiero, incrementando la velocidad, precisión y adaptabilidad en la detección y mitigación de amenazas. La capacidad de aprendizaje continuo y el análisis en tiempo real consolidan a la IA como un recurso esencial en el fortalecimiento de la ciberseguridad, permitiendo a las instituciones financieras anticiparse a amenazas emergentes y responder con mayor eficacia. Sin embargo, la integración de IA debe ser acompañada por una gestión responsable de los datos y una estructura regulatoria sólida que permita aprovechar sus ventajas sin comprometer la privacidad y la transparencia. Esta combinación de innovación y regulación es esencial para que la IA pueda seguir evolucionando y proporcionando seguridad a largo plazo en el sector financiero.

5. Conclusiones

La inteligencia artificial (IA) se ha consolidado como un pilar fundamental en la ciberseguridad del sector financiero, aportando mejoras significativas en la rapidez, precisión y adaptabilidad de la respuesta ante incidentes. La capacidad de la IA para analizar grandes volúmenes de datos en tiempo real ha transformado la manera en que las instituciones detectan y responden a las amenazas, permitiendo una contención más

rápida y precisa que minimiza el impacto potencial de los ataques. Esta evolución hacia una seguridad predictiva no solo refuerza la protección de datos y transacciones, sino que también optimiza los recursos al reducir la carga en los equipos humanos, quienes pueden dedicarse a labores de mayor complejidad y valor estratégico.

La automatización de la respuesta a incidentes, uno de los beneficios más destacados de la IA, permite gestionar eficazmente la creciente cantidad de amenazas que enfrentan las instituciones financieras. A través de sistemas avanzados, como las plataformas SOAR, la IA ha demostrado su capacidad para priorizar, clasificar y responder automáticamente a alertas de seguridad, evitando así el desgaste de recursos humanos y reduciendo significativamente el tiempo de resolución de incidentes. Este enfoque no solo optimiza la eficiencia operativa, sino que también reduce los costos asociados con la seguridad, un aspecto crítico para organizaciones con estructuras complejas y entornos altamente regulados.

El análisis en tiempo real y la capacidad de aprendizaje continuo de los sistemas de IA también fortalecen la resiliencia organizacional, al permitir que los modelos se adapten y mejoren de manera constante frente a nuevas tácticas de ataque. La adaptabilidad de la IA frente a amenazas emergentes contribuye a la prevención de incidentes futuros y garantiza una seguridad proactiva, que se ajusta dinámicamente a un panorama de ciberamenazas en constante cambio. Esta capacidad de adaptación no solo mejora la precisión en la detección de patrones sospechosos, sino que refuerza la capacidad de respuesta al identificar y actuar sobre incidentes en sus etapas iniciales.

Sin embargo, la implementación de IA en la ciberseguridad también presenta desafíos importantes. La transparencia y explicabilidad de los modelos, el cumplimiento de normativas de privacidad y la gestión ética de los datos son aspectos críticos que deben abordarse para construir confianza en la tecnología. La naturaleza de “caja negra” de algunos modelos de IA y la dependencia de grandes volúmenes de datos exigen una estructura regulatoria robusta que proteja la privacidad y asegure la responsabilidad en el uso de estas tecnologías. Asimismo, se requiere un balance cuidadoso entre la automatización y la supervisión humana para asegurar que las decisiones de la IA alineen con los objetivos organizacionales y los estándares éticos.

En resumen, la inteligencia artificial ha demostrado ser una herramienta transformadora en la respuesta ante incidentes en el sector financiero, ofreciendo soluciones avanzadas que fortalecen la seguridad y resiliencia de las organizaciones. A medida que la IA continúa evolucionando, su integración en la ciberseguridad deberá ser gestionada con una visión estratégica y regulatoria que permita aprovechar sus beneficios sin comprometer los valores fundamentales de transparencia, privacidad y ética. Esta combinación de innovación y responsabilidad es esencial para que la IA siga siendo una fuerza positiva y eficaz en la protección de los sistemas financieros en el futuro.

Referencias Bibliográficas

Aldboush, H. H., & Ferdous, M. (2023). Building trust in fintech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. International Journal of Financial Studies, 11(3), 90. https://doi.org/10.3390/ijfs11030090

Blinkops. (2024). AI for Incident Response: Benefits, Challenges & Best Practices. https://www.blinkops.com

Bonilla Bonilla, M.A., Góngora Cheme, R.K., Casanova-Villalba, C.I., y Guamán Chávez, R.E. (Coordinadores). (2023). *Libro de memorias. I Simposio de investigadores emergentes en cien-cia y tecnología*. Religación Press. https://doi.org/10.46652/ReligacionPress.115

Capgemini. (2019). Reinventing Cybersecurity with Artificial Intelligence: The new frontier in digital security. Capgemini Research Institute. https://www.capgemini.com

Casanova-Villalba, C. I., Salgado-Ortiz, P. J., Guerrero-Freire, E. I. & Guerrero-Freire, A. E. (2024). Innovación Pedagógica para la Creación de Spin-offs: Integrando la Empresa Familiar en la Educación Universitaria. In *Fronteras del Futuro: Innovación y Desarrollo en Ciencia y Tecnología*. (pp. 31-48). Editorial Grupo AEA. https://doi.org/10.55813/egaea.cl.39

Celi-Párraga, R. J., Boné-Andrade, M. F., Mora-Olivero, A. P., & Sarmiento-Saavedra, J. C. (2023). *Ingeniería del Software I: Requerimientos y Modelado del Software.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.21

Celi-Párraga, R. J., Mora-Olivero, A. P., Boné-Andrade, M. F., & Sarmiento-Saavedra, J. C. (2023). *Ingeniería del Software II: Implementación, Pruebas y Mantenimiento*. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.20

Charles, K., Tan, Y., & Meena, M. (2023). The role of AI in predictive risk assessment for business continuity: A case study of Greece. International Journal of Risk Assessment and Management, 18(4), 231-244.

Crowe LLP. (2023). AI in cybersecurity and banking: The new frontier. Recuperado de https://www.crowe.com

Cybermatters. (2024). Speed and Precision: How AI Is Enhancing Incident Response. https://www.cybermatters.info

Datafloq. (2023). From Detection to Resolution: AI in Incident Management. https://www.datafloq.com

Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. Applied Sciences, 12(19), 9637. https://doi.org/10.3390/app12199637

Erazo-Luzuriaga, A. F. (2024). Integración de las TICs en el aula: Un análisis de su impacto en el rendimiento académico. *Revista Científica Zambos, 3*(1), 56-72. https://doi.org/10.69484/rcz/v3/n1/12

FIS. (2024). The risks and ethical implications of AI in financial services. FIS Insights. https://www.fisglobal.com

Galarza-Sánchez, P. C. (2023). Adopción de Tecnologías de la Información en las PYMEs Ecuatorianas: Factores y Desafíos. *Revista Científica Zambos*, *2*(1), 21-40. https://doi.org/10.69484/rcz/v2/n1/36

Galarza-Sánchez, P. C., Agualongo-Yazuma, J. C., & Jumbo-Martínez, M. N. (2022). Innovación tecnológica en la industria de restaurantes del Cantón Pedro Vicente Maldonado. *Journal of Economic and Social Science Research*, *2*(1), 31–43. https://doi.org/10.55813/gaea/jessr/v2/n1/45

Galaz, A., Meena, M., & Madan, R. (2021). The strategic role of AI in incident response for business continuity. International Journal of Information Security, 9(3), 194-206.

Hanna, M., Burns, J., & Presslar, C. (2022). Artificial intelligence and algorithmic decisions in fraud detection: An interpretive structural model. Data & Policy, Cambridge Core.

Herrera-Sánchez, M. J., Casanova- Villalba, C. I., Moreno-Novillo, Ángela C., & Mina-Bone, S. G. (2024). Tecnoestrés en docentes universitarios con funciones académicas y administrativas en Ecuador. *Revista Venezolana De Gerencia*, *29*(11), 606-621. https://doi.org/10.52080/rvgluz.29.e11.36

Herrera-Sánchez, M. J., Casanova-Villalba, C. I., Bravo Bravo, I. F., & Barba Mosquera, A. E. (2023). Estudio comparativo de las desigualdades en el tecnoestrés entre instituciones de educación superior en América Latina y Europa. *Código Científico Revista De Investigación*, *4*(2), 1288–1303. https://doi.org/10.55813/gaea/ccri/v4/n2/287

ICAEW. (2023). AI ethical and regulatory implications for financial services. ICAEW Insights. https://www.icaew.com

IEEE. (2024). Cybersecurity in Financial Services: Addressing AI-Related Threats and Vulnerabilities. IEEE Xplore Digital Library. https://doi.org/10.1109/ICKECS61492.2024.10616498

Jaramillo-Chuqui, I. F., & Villarroel-Molina, R. (2023). *Elementos básicos de Análisis Inteligente de Datos.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.65

Juniper Research. (2022). AI-driven fraud detection in banking could save $10 billion annually. Recuperado de https://www.juniperresearch.com

LeewayHertz. (2024). AI in Incident Response: Exploring Use cases, Solutions and Benefits. Recuperado de https://www.leewayhertz.com

McKinsey & Company. (2022). Transforming cyber risk management in financial services with artificial intelligence. Recuperado de https://www.mckinsey.com

MDPI. (2023). Exploring the Impact of AI-Based Cyber Security Financial Sector Management. Journal of Cybersecurity and Privacy, 2(3), 45-56. https://doi.org/10.3390/app13105875

Picoy-Gonzales, J. A., Huarcaya-Taype, R., Contreras-Canto, O. H., & Omonte-Vilca, A. (2023). *Fortalecimiento Metodológico de la Seguridad Informática en Posgrados: Análisis y Estrategias de Mejora.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.56

Picoy-Gonzales, J. A., Huarcaya-Taype, R., Contreras-Canto, O. H., Omonte-Vilca, A., Contreras-De La Cruz, C., & Gaspar-Quispe, J. C. (2023). *Sabores Conectados: Transformando la Gastronomía a través de las Tecnologías de la Información y Comunicación.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.58

Ridzuan, N. N., Masri, M., Anshari, M., Fitriyani, N. L., & Syafrudin, M. (2024). AI in the financial sector: The line between innovation, regulation, and ethical responsibility. Information, 15(8), 432. https://doi.org/10.3390/info15080432

Scalefocus. (2023). AI in the financial sector: Risks & challenges. https://www.scalefocus.com

SoftwareMind. (2023). The Role of AI and Cybersecurity in the Financial Sector. https://www.softwaremind.com

Solano-Gutiérrez, G. A. (2024). La Tecnología en la Educación a Distancia: Revisión de Progresos y Obstáculos a Superar. *Revista Científica Zambos, 3*(2), 48-73. https://doi.org/10.69484/rcz/v3/n2/17

Squadcast. (2024). Trusting AI for Incident Response: The Role of AI in Modern Incident Response and Incident Management. https://www.squadcast.com

Tan, Y., Charles, K., & Meena, M. (2022). Continuous improvement in AI-powered incident response: A case study in financial services. Journal of Cybersecurity, 12(6), 455-470.

Van Vlasselaer, V., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2017). Detecting fraud in mobile payments using supervised and unsupervised anomaly detection. European Journal of Operational Research, 260(3), 831-844.

West, J. (2021). Advanced analytics in fraud detection: Policy implications for financial sectors. OECD Tax Policy Studies, 2(5), 345-367.

ZIF. (2024). Real-Time Insights: How ZIF™ Reshapes Incident Response. https://www.zif.ai

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.