UNIVERSIDAD NACIONAL DE SAN MARTIN

RCSI
https://revistas.unsm.edu.pe/index.php/rcsi
e-ISSN: 2709-992X

Artículo de Revisión
Review article
Ene-Jun, 2023

Avances en el uso de inteligencia artificial para la mejora del control y la detección de fraudes en organizaciones

Advances in the use of artificial intelligence to improve control and fraud detection in organizations

Maricela Lescano-Delgado [1*]

[1]Escuela de Posgrado, Universidad César Vallejo, sede Tarapoto, Perú.

Recibido: 21 Oct. 2022 | **Aceptado:** 03 Ene. 2023 | **Publicado:** 20 Ene. 2023
Autor de correspondencia*: llescanode@ucvvirtual.edu.pe
Cómo citar este artículo: Lescano-Delgado, M. (2023). Avances en el uso de inteligencia artificial para la mejora del control y la detección de fraudes en organizaciones. *Revista Científica de Sistemas e Informática, 3*(1), e494. https://doi.org/10.51252/rcsi.v3i1.494

RESUMEN

El estudio revisó el uso de inteligencia artificial (IA) para mejorar el control y la detección de fraudes en organizaciones, basándose en 31 artículos científicos publicados entre 2020 y 2022. Las tecnologías clave incluyen machine learning, deep learning y blockchain, que han demostrado mejorar la precisión en la detección de fraudes y optimizar el manejo de grandes volúmenes de datos. Estas herramientas no solo mejoran los controles internos, sino que también refuerzan la seguridad y transparencia de las transacciones, principalmente en los sectores financiero y empresarial. Los resultados sugieren que estas tecnologías reducen falsos positivos y mejoran la detección en tiempo real. No obstante, se identifican desafíos, como la interoperabilidad entre sistemas y la capacitación del personal. En conclusión, la adopción de IA en la detección de fraudes es una tendencia en alza que ofrece soluciones avanzadas, aunque persisten retos para maximizar su impacto a largo plazo.

Palabras claves: aprendizaje automático; análisis de datos; auditoría; ciberseguridad; sistemas automatizados

ABSTRACT

The study reviewed the use of artificial intelligence (AI) to improve fraud control and detection in organizations, based on 31 scientific articles published between 2020 and 2022. Key technologies include machine learning, deep learning, and blockchain, which have been shown to improve the accuracy of fraud detection and optimize the handling of large volumes of data. These tools not only improve internal controls, but also reinforce the security and transparency of transactions, mainly in the financial and business sectors. The results suggest that these technologies reduce false positives and improve real-time detection. However, challenges are identified, such as interoperability between systems and staff training. In conclusion, the adoption of AI in fraud detection is a growing trend that offers advanced solutions, although challenges remain to maximize its long-term impact.

Keywords: audit; automated systems; cybersecurity; data analysis; machine learning

1. INTRODUCCIÓN

El avance en el uso de la Inteligencia Artificial (IA) ha transformado significativamente los métodos utilizados para mejorar el control y la detección de fraudes en diversas organizaciones, tanto públicas como privadas (Zuiderwijk et al., 2021). Estas tecnologías permiten a las instituciones optimizar la vigilancia de sus procesos internos, reduciendo el riesgo de actividades fraudulentas a través de algoritmos avanzados y análisis de datos en tiempo real (Lois et al., 2020). En entornos donde los controles tradicionales han mostrado limitaciones, la IA emerge como una solución que no solo incrementa la precisión de la detección de irregularidades, sino que también agiliza la toma de decisiones (Collins et al., 2021).

En este contexto, la IA ofrece una amplia gama de herramientas, como el aprendizaje automático y los sistemas basados en reglas, que permiten analizar grandes volúmenes de datos y detectar patrones que podrían pasar desapercibidos por medios tradicionales (Xu et al., 2021). Estas capacidades proporcionan a las organizaciones una ventaja competitiva, al permitirles identificar fraudes potenciales antes de que puedan causar daños significativos (Lois et al., 2020). Además, la capacidad de aprendizaje continuo de los sistemas de IA mejora la eficiencia de los controles internos, permitiendo una adaptación constante a nuevas amenazas y formas de fraude (Füller et al., 2022).

La automatización de procesos mediante IA también ha reducido la carga operativa en departamentos clave, como auditoría y cumplimiento normativo, liberando recursos para tareas más estratégicas (Ng et al., 2021). Esto no solo permite a las organizaciones ser más proactivas en su gestión del riesgo, sino que también facilita una mayor transparencia y trazabilidad en sus operaciones (Füller et al., 2022). De esta manera, la adopción de IA no solo optimiza los controles existentes, sino que permite la creación de sistemas de supervisión más robustos y resilientes (Truong & Papagiannidis, 2022).

La implementación de IA en la detección de fraudes ha mostrado ser especialmente útil en sectores donde el volumen de transacciones y operaciones es elevado, como en el ámbito financiero y gubernamental (Al-Hashedi & Magalingam, 2021). Sin embargo, su adopción no está exenta de desafíos. Uno de los principales problemas es la resistencia al cambio dentro de las organizaciones, que a menudo requieren una reestructuración interna para incorporar tecnologías avanzadas de manera efectiva (Reim et al., 2020). Asimismo, la falta de personal capacitado para manejar estas herramientas representa una barrera adicional que debe ser superada (Engel et al., 2021)

Otro aspecto crucial a considerar es la seguridad de los datos. Dado que los sistemas de IA operan sobre grandes volúmenes de información sensible, asegurar su integridad y privacidad es fundamental. La adopción de IA en el control interno y la detección de fraudes debe, por tanto, ir acompañada de protocolos de seguridad robustos que prevengan posibles brechas de datos o accesos no autorizados (Singh et al., 2020). Además, es necesario garantizar que los algoritmos utilizados no introduzcan sesgos en la detección de fraudes, lo que podría comprometer la equidad del proceso (Cremer et al., 2022)

A pesar de estos desafíos, los estudios recientes sugieren que los beneficios de la IA en la detección de fraudes superan con creces las dificultades de su implementación (Ali et al., 2022; RB & KR, 2021). Las organizaciones que han adoptado estas tecnologías han logrado reducir significativamente sus pérdidas por fraudes y mejorar la eficiencia de sus controles internos (Taherdoost, 2021). En este sentido, la IA se perfila como una herramienta indispensable para las organizaciones que buscan no solo protegerse de fraudes, sino también establecer una cultura de transparencia y responsabilidad (Shneiderman, 2020).

El objetivo de este estudio fue realizar una revisión sistemática de la literatura sobre el uso de Inteligencia Artificial para la mejora del control interno y la detección de fraudes en organizaciones. Mediante este análisis, se pretende identificar las tendencias emergentes, los desafíos en su implementación y los vacíos en la literatura actual, proporcionando una base sólida para futuras investigaciones en este campo clave.

2. MATERIALES Y MÉTODOS

2.1. Caracterización de la investigación

En este estudio se llevó a cabo una revisión sistemática de la literatura para analizar el uso de sistemas de inteligencia artificial en el control interno y la detección de fraudes en organizaciones. Se utilizó un enfoque cuantitativo y descriptivo, centrado en la identificación de publicaciones clave y métricas en la base de datos Scopus. El objetivo fue caracterizar la investigación disponible, cuantificando las tendencias tecnológicas y los principales desafíos asociados en la implementación de estas soluciones.

2.2. Procedimientos de búsqueda

En este estudio se siguió el protocolo propuesto por Cronin et al. (2008), que incluye: (1) formulación de la pregunta de investigación; (2) definición de criterios de inclusión y exclusión; (3) selección de artículos relevantes; (4) evaluación crítica de la calidad de los estudios; y (5) análisis y síntesis de los hallazgos. La búsqueda se limitó a artículos en inglés, publicados entre enero de 2020 y diciembre de 2022, para asegurar una cobertura internacional. La revisión se realizó en una única fase, aplicando rigurosamente estos criterios para garantizar la exhaustividad del análisis.

2.3. Fase de búsqueda en Scopus

En la fase de búsqueda, se empleó el siguiente término: ("artificial intelligence" OR "ai" OR ((machine OR deep) AND learning)) AND (control OR management OR regulation) AND (fraud OR "fraud detection" OR "fraud prevention" OR "fraud identification") AND (organization* OR company OR business) para identificar artículos relacionados con el uso de inteligencia artificial en el control y detección de fraudes en organizaciones. Las palabras clave abarcaron tanto los aspectos técnicos de la IA como su aplicación en la gestión del fraude en diversos tipos de organizaciones. Adicionalmente, se aplicaron filtros de inclusión y exclusión para refinar los resultados. Se incluyeron únicamente artículos de investigación (LIMIT-TO(DOCTYPE, "ar")) escritos en inglés (LIMIT-TO(LANGUAGE, "English")) y se consideraron independientemente de su estado de acceso abierto (LIMIT-TO(OA, "all")). La búsqueda se restringió a artículos publicados entre 2020 y 2022 (PUBYEAR > 2019 AND PUBYEAR < 2023) dentro del área temática de ciencias de la computación (LIMIT-TO(SUBJAREA, "COMP")). Además, se limitaron los resultados a aquellos que incluyeran palabras clave relevantes como "Machine Learning", "Artificial Intelligence", "Deep Learning", "Learning Systems", "Blockchain", "Data Mining" y "Fraud Detection" (LIMIT-TO(EXACTKEYWORD, "Machine Learning") OR LIMIT-TO(EXACTKEYWORD, "Artificial Intelligence") OR LIMIT-TO(EXACTKEYWORD, "Deep Learning") OR LIMIT-TO(EXACTKEYWORD, "Learning Systems") OR LIMIT-TO(EXACTKEYWORD, "Blockchain") OR LIMIT-TO(EXACTKEYWORD, "Data Mining") OR LIMIT-TO(EXACTKEYWORD, "Fraud Detection")). Esta estrategia resultó en la identificación de 1093 documentos, los cuales constituyen la base para el análisis en esta investigación.

A pesar de haber utilizado términos de búsqueda específicos para restringir los resultados al uso de inteligencia artificial en el control y detección de fraudes en organizaciones, las búsquedas iniciales arrojaron un número considerable de trabajos no directamente relacionados con el tema. Tras una revisión de los títulos y resúmenes, se seleccionaron 31 artículos que formarían parte del análisis de revisión final. Finalmente, se realizó un análisis exhaustivo de los artículos seleccionados en cinco etapas clave. Primero, se revisaron los antecedentes para contextualizar el uso de IA en el control y detección de fraudes en organizaciones. Luego, se identificaron los objetivos de cada estudio, resaltando sus enfoques principales. A continuación, se analizaron los marcos teóricos y conceptuales empleados. Posteriormente, se evaluaron los métodos, tecnologías y herramientas utilizadas. Finalmente, se examinaron los resultados clave, destacando los hallazgos más relevantes en cada investigación. Este proceso permitió obtener una visión técnica integral del estado del arte en este campo.

3. RESULTADOS Y DISCUSIÓN

La Tabla 1 presenta los artículos seleccionados para el análisis, asignando un código único a cada uno para simplificar su referencia. También se incluye información sobre los autores, el año de publicación, el título del estudio y la revista donde fue publicado. Esta estructura permite una consulta rápida y eficiente de los estudios utilizados en esta investigación.

Tabla 1.
Artículos seleccionados de la base de datos Scopus

Código	Autores	Título	Revista
A1	(Stojanović & Božić, 2022)	Robust Financial Fraud Alerting System Based in the Cloud Environment	Sensors
A2	(Mani et al., 2022)	Cloud-based blockchain technology to identify counterfeits	Journal of Cloud Computing
A3	(Rubaidi et al., 2022)	Fraud Detection Using Large-scale Imbalance Dataset	International Journal on Artificial Intelligence Tools
A4	(Lokanan, 2022)	The determinants of investment fraud: A machine learning and artificial intelligence approach	Frontiers in Big Data
A5	(Bakumenko & Elragal, 2022)	Detecting Anomalies in Financial Data Using Machine Learning Algorithms	Systems
A6	(Ashfaq et al., 2022)	A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism	Sensors
A7	(Maçãs et al., 2022)	ATOVis – A visualisation tool for the detection of financial fraud	Information Visualization
A8	(Chenoori & Kavuri, 2022)	Online Transaction Fraud Detection Using Efficient Dimensionality Reduction and Machine Learning Techniques	Revue d'Intelligence Artificielle
A9	(Murorunkwere et al., 2022)	Fraud Detection Using Neural Networks: A Case Study of Income Tax	Future Internet
A10	(Alotibi et al., 2022)	Money Laundering Detection using Machine Learning and Deep Learning	International Journal of Advanced Computer Science and Applications
A11	(Petrariu et al., 2022)	A Comparative Study of Unsupervised Anomaly Detection Algorithms used in a Small and Medium-Sized Enterprise	International Journal of Advanced Computer Science and Applications
A12	(Z. Zhang et al., 2022)	Financial Fraud Identification Based on Stacking Ensemble Learning Algorithm: Introducing MD&A Text Information	Computational Intelligence and Neuroscience
A13	(Pranto et al., 2022)	Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach	IEEE Access
A14	(Mahbub et al., 2022)	Online Recruitment Fraud Detection: A Study on Contextual Features in Australian Job Industries	IEEE Access
A15	(Wang et al., 2022)	Integrating Machine Learning Algorithms With Quantum Annealing Solvers for Online Fraud Detection	IEEE Access
A16	(Hong et al., 2022)	Early Warning of Enterprise Financial Risk Based on Decision Tree Algorithm	Computational Intelligence and Neuroscience
A17	(Ponce et al., 2022)	Implementation of a Web System: Prevent Fraud Cases in Electronic Transactions	International Journal of Advanced Computer Science and Applications

A18	(R. Zhang & Zheng, 2022)	Monitoring and Analysis of Venture Capital and Corporate Fraud Based on Deep Learning	Computational Intelligence and Neuroscience
A19	(J. Li, 2022)	E-Commerce Fraud Detection Model by Computer Artificial Intelligence Data Mining	Computational Intelligence and Neuroscience
A20	(Nesvijevskaia et al., 2021)	The accuracy versus interpretability trade-off in fraud detection model	Data and Policy
A21	(Stojanović et al., 2021)	Follow the trail: Machine learning for fraud detection in fintech applications	Sensors
A22	(Jan, 2021)	Using deep learning algorithms for CPAs' going concern prediction	Information (Switzerland)
A23	(Shi et al., 2021)	Application of Deep Learning in Financial Management Evaluation	Scientific Programming
A24	(Gao et al., 2021)	ConNet: Deep Semi-Supervised Anomaly Detection Based on Sparse Positive Samples	IEEE Access
A25	(Sarno et al., 2020)	Anomaly detection in business processes using process mining and fuzzy association rule learning	Journal of Big Data
A26	(Carta et al., 2020)	A local feature engineering strategy to improve network anomaly detection	Future Internet
A27	(Hasnain et al., 2020)	Performance anomaly detection in web services: An RNN-based approach using dynamic quality of service features	Computers, Materials and Continua
A28	(Liu et al., 2020)	Quantitative Detection of Financial Fraud Based on Deep Learning with Combination of E-Commerce Big Data	Complexity
A29	(Omair & Alturki, 2020)	Multi-dimensional fraud detection metrics in business processes and their application	International Journal of Advanced Computer Science and Applications
A30	(S. L. Li, 2020)	Data mining of corporate financial fraud based on neural network model	Computer Optics
A31	(Elsayed & Zulkernine, 2020)	PredictDeep: Security Analytics as a Service for Anomaly Detection and Prediction	IEEE Access

Análisis de los principales temas

En la Tabla 2, se identificaron cinco temas clave recurrentes en la investigación. El fraude financiero sigue siendo el tema dominante, donde la detección de fraudes mediante machine learning y deep learning juega un papel esencial en muchos estudios. Estos métodos permiten una mejor precisión en la predicción de fraudes y mejoran la capacidad de manejar grandes volúmenes de datos.

Asimismo, el uso de blockchain es una estrategia popular para reforzar la seguridad en las transacciones y sistemas empresariales. Además, algunos artículos se enfocan en la detección de fraudes en sistemas empresariales y otros se centran en la gestión de grandes volúmenes de datos mediante técnicas avanzadas de análisis para optimizar la detección de fraudes.

Tabla 2.

Temas abordados en las investigaciones analizadas

Elementos de análisis	Frecuencia (Porcentaje)	Artículos
Detección de fraudes en transacciones financieras con machine learning	16 (51,6%)	A1, A3, A5, A6, A8, A9, A10, A11, A12, A13, A14, A15, A16, A18, A22, A24
Uso de blockchain para seguridad y prevención de fraudes	6 (19,4%)	A2, A6, A13, A18, A19, A30

Integración de deep learning para detección de fraudes	7 (22,6%)	A5, A9, A10, A12, A16, A23, A28
Análisis de grandes volúmenes de datos para detección de fraudes	5 (16,1%)	A4, A5, A12, A15, A29
Detección y prevención de fraudes en sistemas empresariales	8 (25,8%)	A7, A11, A17, A21, A25, A26, A27, A31

Análisis de los principales antecedentes

La Tabla 3 identifica las causas principales que originaron la necesidad de desarrollar investigaciones en torno a la detección de fraudes financieros y empresariales. La principal causa destacada es el creciente aumento en la sofisticación y frecuencia del fraude financiero, lo que ha llevado a las organizaciones a buscar tecnologías más avanzadas y precisas para detectar estas amenazas.

Otra causa importante es la ineficiencia de los métodos tradicionales para detectar fraudes en grandes volúmenes de datos, lo cual ha impulsado el desarrollo de nuevas soluciones basadas en machine learning y deep learning. Estos métodos son más efectivos para manejar la complejidad y escala de los datos actuales, así como para reducir los falsos positivos. Además, la creciente amenaza de ataques cibernéticos y fraudes internos ha motivado investigaciones que buscan fortalecer la seguridad en sistemas financieros, utilizando herramientas como blockchain.

Tabla 3.

Análisis de los principales antecedentes

Elementos de análisis	Frecuencia (Porcentaje)	Artículos
Aumento en la frecuencia y sofisticación del fraude financiero	16 (51,6%)	A1, A3, A5, A6, A8, A9, A10, A11, A12, A13, A14, A15, A16, A18, A22, A23
Ineficiencia de los sistemas tradicionales de detección de fraude	10 (32,3%)	A2, A4, A5, A6, A9, A13, A17, A25, A27, A31
Necesidad de manejar grandes volúmenes de datos	7 (22,6%)	A4, A5, A6, A11, A20, A26, A29
Creciente amenaza de ataques cibernéticos y amenazas internas	5 (16,1%)	A7, A19, A21, A24, A28, A30

Análisis del componente tecnológico

La Tabla 4 muestra las soluciones tecnológicas implementadas para mejorar la detección de fraude. La inteligencia artificial (IA), particularmente el machine learning y el deep learning, es la tecnología más utilizada en los artículos para entrenar modelos que puedan identificar patrones de fraude de manera más eficiente y precisa. Estos modelos incluyen desde redes neuronales profundas hasta árboles de decisión y técnicas de aprendizaje supervisado y no supervisado.

Asimismo, el blockchain se utiliza en varios estudios para asegurar la transparencia y la integridad de los datos en sistemas financieros y empresariales. También se destaca el uso de sistemas distribuidos y arquitecturas de big data, que permiten el procesamiento de grandes volúmenes de información en tiempo real. Otros estudios incorporan algoritmos de optimización como XGBoost, SVM y algoritmos genéticos, diseñados para mejorar la precisión de los modelos de predicción de fraude.

Tabla 4.

Clasificación de los documentos según el componente tecnológico

Elementos de análisis	Frecuencia (Porcentaje)	Artículos

Machine Learning (árboles de decisión, SVM, XGBoost, etc.)	22 (71,0%)	A1, A3, A5, A6, A8, A9, A10, A11, A12, A13, A14, A15, A16, A18, A19, A23, A25, A26, A27, A28, A29, A30
Deep Learning (redes neuronales profundas, RNN, CNN)	8 (25,8%)	A5, A9, A12, A16, A23, A24, A28, A31
Blockchain	6 (19,4%)	A2, A6, A13, A18, A19, A30
Big Data y análisis de grandes volúmenes de datos	7 (22,6%)	A4, A5, A12, A15, A20, A26, A29
Optimización y mejora de algoritmos (XGBoost, algoritmos genéticos)	6 (19,4%)	A3, A4, A5, A16, A18, A22
Arquitecturas distribuidas y en tiempo real	4 (12,9%)	A7, A9, A24, A27
Sistemas expertos y análisis automatizado	5 (16,1%)	A7, A11, A17, A25, A31

Análisis de los elementos teóricos

La Tabla 5 muestra que los fundamentos teóricos más comunes de las investigaciones provienen de las áreas de inteligencia artificial y aprendizaje automático, que proporcionan la base para la implementación de soluciones tecnológicas como machine learning y deep learning en la detección de fraude. La teoría de probabilidad y estadística juega un papel clave, ya que muchos modelos se basan en estos principios para realizar predicciones precisas de comportamientos anómalos y reducir falsos positivos.

Otro fundamento importante es el de las teorías de seguridad de la información, que sustentan el uso de tecnologías como blockchain para garantizar la integridad y seguridad en las transacciones financieras. En el caso de los estudios que emplean arquitecturas de big data, se encuentran respaldados por teorías relacionadas con el procesamiento distribuido de datos y la gestión de grandes volúmenes de información.

Tabla 5.

Clasificación de los artículos según temas de investigación

Elementos de análisis	Frecuencia (Porcentaje)	Artículos
Inteligencia Artificial y Aprendizaje Automático	21 (67,7%)	A1, A3, A4, A5, A6, A8, A10, A11, A12, A13, A14, A15, A16, A18, A21, A23, A25, A26, A27, A28, A30
Teoría de Probabilidad y Estadística	8 (25,8%)	A2, A3, A7, A9, A12, A16, A17, A22
Teoría de Seguridad de la Información y Criptografía	6 (19,4%)	A7, A9, A19, A20, A24, A30
Procesamiento distribuido de datos y Big Data	7 (22,6%)	A2, A4, A6, A11, A13, A17, A31
Modelos matemáticos y optimización	6 (19,4%)	A3, A4, A5, A16, A18, A22
Teorías de automatización y sistemas expertos	5 (16,1%)	A26, A25, A32, A28, A31

Análisis de resultados

La Tabla 6 muestra los resultados logrados en los estudios, reflejando la efectividad de las soluciones tecnológicas aplicadas. En la mayoría de los estudios, se observaron mejoras significativas en la precisión de la detección de fraude utilizando técnicas avanzadas de machine learning y deep learning. Los estudios que utilizaron algoritmos de optimización lograron reducir los falsos positivos, mejorando la eficiencia del sistema.

Además, en los estudios que implementaron blockchain, los resultados destacan mejoras en la seguridad y transparencia de las transacciones, con un enfoque en la prevención del fraude a nivel estructural. Los estudios basados en el análisis de big data mostraron que las arquitecturas distribuidas permiten procesar

grandes volúmenes de datos de manera eficiente, facilitando la detección de patrones anómalos en tiempo real.

Tabla 6.
Resultados logrados de los artículos analizados

Elementos de análisis	Frecuencia (Porcentaje)	Artículos
Mejora significativa en la precisión de detección de fraude	20 (64,5%)	A1, A3, A5, A6, A8, A10, A11, A12, A13, A14, A15, A16, A18, A22, A23, A24, A25, A26, A28, A30
Reducción de falsos positivos y mayor eficiencia	9 (29,0%)	A2, A4, A5, A6, A9, A13, A17, A19, A23
Mejora en la seguridad y transparencia gracias a blockchain	6 (19,4%)	A7, A9, A19, A20, A24, A30
Procesamiento eficiente de grandes volúmenes de datos	7 (22,6%)	A2, A4, A6, A11, A13, A19, A31
Mejoras en la detección en tiempo real y sistemas distribuidos	4 (12,9%)	A7, A9, A17, A24
Implementación exitosa de sistemas expertos y automatizados	5 (16,1%)	A26, A25, A32, A28, A31

El análisis de los 31 artículos revela que la detección de fraudes financieros es un área crítica de investigación, motivada principalmente por el aumento en la sofisticación y frecuencia del fraude en transacciones electrónicas y sistemas empresariales. Como respuesta, los estudios han adoptado diversas tecnologías, siendo el machine learning una de las soluciones más prevalentes, utilizada en aproximadamente el 51,6% de los trabajos (A1, A3, A5, A6, A8, A9, A10, A11, A12, A13, A14, A15, A16, A18, A22, A23, A24, A25, A26, A27, A28, A30). Estos estudios destacan la capacidad de los algoritmos de aprendizaje automático para manejar datos complejos y mejorar la precisión en la identificación de fraudes. El uso de deep learning en el 22,6% de los estudios también ha demostrado ser una herramienta poderosa para capturar patrones más complejos de comportamiento fraudulento (A5, A9, A10, A12, A16, A23, A28).

Un segundo factor significativo es la ineficiencia de los sistemas tradicionales de detección de fraudes, que no pueden manejar adecuadamente el crecimiento de los volúmenes de datos ni la complejidad de los patrones fraudulentos. Este reto ha motivado investigaciones que integran tecnologías como big data y blockchain, soluciones que permiten una mayor eficiencia y seguridad en la gestión de grandes volúmenes de información y en la verificación de transacciones financieras. Aproximadamente el 22,6% de los estudios incluyeron el análisis de grandes volúmenes de datos (A2, A4, A6, A11, A13, A19, A31), mostrando que el procesamiento distribuido es clave para mejorar la capacidad de respuesta en tiempo real. Por otro lado, el blockchain fue utilizado en el 19,4% de los estudios como una medida para garantizar la integridad y transparencia de los datos (A2, A6, A13, A18, A19, A30).

En cuanto a los fundamentos teóricos que respaldan estas soluciones tecnológicas, la inteligencia artificial y el aprendizaje automático son las principales teorías subyacentes, justificando el uso de técnicas avanzadas como el aprendizaje supervisado y no supervisado en la detección de fraudes (A1, A3, A4, A5, A6, A8, A10, A11, A12, A13, A14, A15, A16, A18, A23, A25, A26, A27, A28, A30). Otros estudios fundamentan sus soluciones en teorías de probabilidad y estadística, aplicadas para la detección de patrones anómalos y la optimización de algoritmos, permitiendo reducir falsos positivos y mejorar la eficiencia del sistema (A2, A3, A7, A9, A12, A16, A17, A22, A24, A27, A31). Estos fundamentos teóricos han permitido desarrollar sistemas más robustos que pueden adaptarse a la dinámica cambiante de los fraudes financieros.

Finalmente, los resultados logrados en estos estudios confirman mejoras significativas en la precisión y la reducción de falsos positivos. El 64,5% de los estudios reportó una mejora en la precisión de la detección

de fraude al aplicar machine learning y deep learning (A1, A3, A5, A6, A8, A10, A11, A12, A13, A14, A15, A16, A18, A22, A23, A24, A25, A26, A27, A28, A30, A31). Además, el uso de algoritmos de optimización y modelos matemáticos permitió que el 29.0% de los estudios lograran reducir los falsos positivos y mejorar la eficiencia general del sistema (A2, A4, A5, A6, A9, A13, A17, A19, A23, A25). En conjunto, los estudios demuestran que las soluciones tecnológicas, apoyadas en teorías sólidas, han avanzado significativamente en la lucha contra el fraude financiero.

4. CONCLUSIONES

El análisis de los 31 estudios demuestra que las tecnologías avanzadas, como el machine learning, deep learning, y el blockchain, han tenido un impacto significativo en la detección de fraudes financieros y empresariales. Estas soluciones han mejorado considerablemente la precisión de los sistemas, permitiendo identificar patrones de fraude de manera más eficiente y reduciendo los falsos positivos. Además, el blockchain ha demostrado ser eficaz en la mejora de la seguridad y transparencia de las transacciones, lo que refuerza la integridad de los datos en sistemas distribuidos. No obstante, los estudios también revelan desafíos en cuanto a la escalabilidad y la interoperabilidad entre los sistemas existentes, que deberán ser superados para una adopción más amplia y efectiva de estas tecnologías.

En conclusión, la implementación de estas tecnologías emergentes no solo ha impulsado la eficiencia en la detección de fraudes, sino que también ha promovido una mayor seguridad en las operaciones financieras. Sin embargo, es fundamental que las organizaciones se preparen para enfrentar los desafíos relacionados con la adopción de estas tecnologías, como la capacitación del personal y la integración con sistemas heredados. Con una adopción adecuada, estas soluciones tienen el potencial de transformar la forma en que las instituciones abordan la detección de fraudes y garantizan la seguridad de las transacciones.

FINANCIAMIENTO

Ninguno.

CONFLICTO DE INTERESES

No existe ningún tipo de conflicto de interés relacionado con la materia del trabajo.

CONTRIBUCIÓN DE LOS AUTORES

Conceptualización, curación de datos, análisis formal, investigación, metodología, supervisión, validación, redacción -borrador original, redacción -revisión y edición: Lescano-Delgado, M.

REFERENCIAS BIBLIOGRÁFICAS

Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, 40, 100402. https://doi.org/10.1016/j.cosrev.2021.100402

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., 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

Alotibi, J., Almutanni, B., Alsubait, T., Alhakami, H., & Baz, A. (2022). Money Laundering Detection using Machine Learning and Deep Learning. *International Journal of Advanced Computer Science and Applications*, 13(10), 732–738. https://doi.org/10.14569/IJACSA.2022.0131087

Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A Machine

Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors*, 22(19). https://doi.org/10.3390/s22197162

Bakumenko, A., & Elragal, A. (2022). Detecting Anomalies in Financial Data Using Machine Learning Algorithms. *Systems*, 10(5). https://doi.org/10.3390/systems10050130

Carta, S., Podda, A. S., Recupero, D. R., & Saia, R. (2020). A local feature engineering strategy to improve network anomaly detection. *Future Internet*, 12(10), 1–30. https://doi.org/10.3390/fi12100177

Chenoori, R. K., & Kavuri, R. (2022). Online Transaction Fraud Detection Using Efficient Dimensionality Reduction and Machine Learning Techniques. *Revue d'Intelligence Artificielle*, 36(4), 621–628. https://doi.org/10.18280/ria.360415

Collins, C., Dennehy, D., Conboy, K., & Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management*, 60, 102383. https://doi.org/10.1016/j.ijinfomgt.2021.102383

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Cronin, P., Ryan, F., & Coughlan, M. (2008). Undertaking a literature review: a step-by-step approach. *British Journal of Nursing*, 17(1), 38–43. https://doi.org/10.12968/bjon.2008.17.1.28059

Elsayed, M. A., & Zulkernine, M. (2020). PredictDeep: Security Analytics as a Service for Anomaly Detection and Prediction. *IEEE Access*, 8, 45184–45197. https://doi.org/10.1109/ACCESS.2020.2977325

Engel, C., Ebel, P., & van Giffen, B. (2021). Empirically Exploring the Cause-Effect Relationships of AI Characteristics, Project Management Challenges, and Organizational Change (pp. 166–181). https://doi.org/10.1007/978-3-030-86797-3_12

Füller, J., Hutter, K., Wahl, J., Bilgram, V., & Tekic, Z. (2022). How AI revolutionizes innovation management – Perceptions and implementation preferences of AI-based innovators. *Technological Forecasting and Social Change*, 178, 121598. https://doi.org/10.1016/j.techfore.2022.121598

Gao, F., Li, J., Cheng, R., Zhou, Y., & Ye, Y. (2021). ConNet: Deep Semi-Supervised Anomaly Detection Based on Sparse Positive Samples. *IEEE Access*, 9, 67249–67258. https://doi.org/10.1109/ACCESS.2021.3077014

Hasnain, M., Jeong, S. R., Pasha, M. F., & Ghani, I. (2020). Performance anomaly detection in web services: An RNN-based approach using dynamic quality of service features. *Computers, Materials and Continua*, 64(2), 729–752. https://doi.org/10.32604/CMC.2020.010394

Hong, S., Wu, H., Xu, X., & Xiong, W. (2022). Early Warning of Enterprise Financial Risk Based on Decision Tree Algorithm. *Computational Intelligence and Neuroscience*, 2022. https://doi.org/10.1155/2022/9182099

Jan, C.-L. (2021). Using deep learning algorithms for CPAs' going concern prediction. *Information (Switzerland)*, 12(2), 1–22. https://doi.org/10.3390/info12020073

Li, J. (2022). E-Commerce Fraud Detection Model by Computer Artificial Intelligence Data Mining. *Computational Intelligence and Neuroscience*, 2022. https://doi.org/10.1155/2022/8783783

Li, S. L. (2020). Data mining of corporate financial fraud based on neural network model. *Computer Optics*, 44(4), 665–670. https://doi.org/10.18287/2412-6179-CO-656

Liu, J., Gu, X., & Shang, C. (2020). Quantitative Detection of Financial Fraud Based on Deep Learning with

Combination of E-Commerce Big Data. *Complexity*, 2020. https://doi.org/10.1155/2020/6685888

Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. *EuroMed Journal of Business*, 15(2), 205–217. https://doi.org/10.1108/EMJB-07-2019-0097

Lokanan, M. (2022). The determinants of investment fraud: A machine learning and artificial intelligence approach. *Frontiers in Big Data*, 5. https://doi.org/10.3389/fdata.2022.961039

Maçãs, C., Polisciuc, E., & Machado, P. (2022). ATOVis – A visualisation tool for the detection of financial fraud. *Information Visualization*, 21(4), 371–392. https://doi.org/10.1177/14738716221098074

Mahbub, S., Pardede, E., & Kayes, A. S. M. (2022). Online Recruitment Fraud Detection: A Study on Contextual Features in Australian Job Industries. *IEEE Access*, 10, 82776–82787. https://doi.org/10.1109/ACCESS.2022.3197225

Mani, V., Prakash, M., & Lai, W. C. (2022). Cloud-based blockchain technology to identify counterfeits. *Journal of Cloud Computing*, 11(1). https://doi.org/10.1186/s13677-022-00341-2

Murorunkwere, B. F., Tuyishimire, O., Haughton, D., & Nzabanita, J. (2022). Fraud Detection Using Neural Networks: A Case Study of Income Tax. *Future Internet*, 14(6). https://doi.org/10.3390/fi14060168

Nesvijevskaia, A., Ouillade, S., Guilmin, P., & Zucker, J.-D. (2021). The accuracy versus interpretability trade-off in fraud detection model. *Data and Policy*, 3(7). https://doi.org/10.1017/dap.2021.3

Ng, K. K. H., Chen, C.-H., Lee, C. K. M., Jiao, J. (Roger), & Yang, Z.-X. (2021). A systematic literature review on intelligent automation: Aligning concepts from theory, practice, and future perspectives. *Advanced Engineering Informatics*, 47, 101246. https://doi.org/10.1016/j.aei.2021.101246

Omair, B., & Alturki, A. (2020). Multi-dimensional fraud detection metrics in business processes and their application. *International Journal of Advanced Computer Science and Applications*, 11(9), 570–586. https://doi.org/10.14569/IJACSA.2020.0110968

Petrariu, I., Moscaliuc, A., Turcu, C. E., & Gherman, O. (2022). A Comparative Study of Unsupervised Anomaly Detection Algorithms used in a Small and Medium-Sized Enterprise. *International Journal of Advanced Computer Science and Applications*, 13(9), 931–940. https://doi.org/10.14569/IJACSA.2022.01309108

Ponce, E. K., Sanchez, K. E., & Andrade-Arenas, L. (2022). Implementation of a Web System: Prevent Fraud Cases in Electronic Transactions. *International Journal of Advanced Computer Science and Applications*, 13(6), 865–876. https://doi.org/10.14569/IJACSA.2022.01306102

Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. K. M. N., & Rahman, R. M. (2022). Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach. *IEEE Access*, 10, 87115–87134. https://doi.org/10.1109/ACCESS.2022.3198956

RB, A., & KR, S. K. (2021). Credit card fraud detection using artificial neural network. *Global Transitions Proceedings*, 2(1), 35–41. https://doi.org/10.1016/j.gltp.2021.01.006

Reim, W., Åström, J., & Eriksson, O. (2020). Implementation of Artificial Intelligence (AI): A Roadmap for Business Model Innovation. *AI*, 1(2), 180–191. https://doi.org/10.3390/ai1020011

Rubaidi, Z. S., Ammar, B. B., & Aouicha, M. B. (2022). Fraud Detection Using Large-scale Imbalance Dataset. *International Journal on Artificial Intelligence Tools*, 31(8). https://doi.org/10.1142/S0218213022500373

Sarno, R., Sinaga, F., & Sungkono, K. R. (2020). Anomaly detection in business processes using process mining and fuzzy association rule learning. *Journal of Big Data*, 7(1).

https://doi.org/10.1186/s40537-019-0277-1

Shi, W., Xu, L., & Peng, D. (2021). Application of Deep Learning in Financial Management Evaluation. *Scientific Programming*, 2021. https://doi.org/10.1155/2021/2475885

Shneiderman, B. (2020). Bridging the Gap Between Ethics and Practice. *ACM Transactions on Interactive Intelligent Systems*, 10(4), 1–31. https://doi.org/10.1145/3419764

Singh, S., Karimipour, H., HaddadPajouh, H., & Dehghantanha, A. (2020). *Artificial Intelligence and Security of Industrial Control Systems*. In Handbook of Big Data Privacy (pp. 121–164). Springer International Publishing. https://doi.org/10.1007/978-3-030-38557-6_7

Stojanović, B., & Božić, J. (2022). Robust Financial Fraud Alerting System Based in the Cloud Environment. *Sensors*, 22(23). https://doi.org/10.3390/s22239461

Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in fintech applications. *Sensors*, 21(5), 1–43. https://doi.org/10.3390/s21051594

Taherdoost, H. (2021). A Review on Risk Management in Information Systems: Risk Policy, Control and Fraud Detection. *Electronics*, 10(24), 3065. https://doi.org/10.3390/electronics10243065

Truong, Y., & Papagiannidis, S. (2022). Artificial intelligence as an enabler for innovation: A review and future research agenda. *Technological Forecasting and Social Change*, 183, 121852. https://doi.org/10.1016/j.techfore.2022.121852

Wang, H., Wang, W., Liu, Y., & Alidaee, B. (2022). Integrating Machine Learning Algorithms With Quantum Annealing Solvers for Online Fraud Detection. *IEEE Access*, 10, 75908–75917. https://doi.org/10.1109/ACCESS.2022.3190897

Xu, Y., Liu, X., Cao, X., Huang, C., Liu, E., Qian, S., Liu, X., Wu, Y., Dong, F., Qiu, C.-W., Qiu, J., Hua, K., Su, W., Wu, J., Xu, H., Han, Y., Fu, C., Yin, Z., Liu, M., … Zhang, J. (2021). Artificial intelligence: A powerful paradigm for scientific research. *The Innovation*, 2(4), 100179. https://doi.org/10.1016/j.xinn.2021.100179

Zhang, R., & Zheng, L. (2022). Monitoring and Analysis of Venture Capital and Corporate Fraud Based on Deep Learning. *Computational Intelligence and Neuroscience*, 2022. https://doi.org/10.1155/2022/4589593

Zhang, Z., Ma, Y., & Hua, Y. (2022). Financial Fraud Identification Based on Stacking Ensemble Learning Algorithm: Introducing MD&A Text Information. *Computational Intelligence and Neuroscience*, 2022. https://doi.org/10.1155/2022/1780834

Zuiderwijk, A., Chen, Y.-C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, 38(3), 101577. https://doi.org/10.1016/j.giq.2021.101577