ISSN: 2806-5697
Vol. 7 – Núm. E2 / 2026

Inteligencia artificial y optimización de la detección de riesgos de fraude en comercio electrónico

Artificial Intelligence and Optimizing Fraud Risk Detection in E-Commerce

Inteligência artificial e otimização da deteção de riscos de fraude no comércio eletrónico

Guadalupe-Rodríguez, Wagner Rudy
Instituto Superior Tecnológico Vicente Rocafuerte
wguadalupe@istvr.edu.ec
https://orcid.org/0000-0002-6621-5413

López-Molina, Luis Andrés
Instituto Superior Tecnológico Vicente Rocafuerte
llopez@istvr.edu.ec
https://orcid.org/0000-0002-3088-1377

Pinela-Tigua, José Ottón
Instituto Superior Tecnológico Vicente Rocafuerte
jpinela@istvr.edu.ec
https://orcid.org/0000-0003-1713-8973

Cando-Cedeño, Jordan Lindon
Instituto Superior Tecnológico Vicente Rocafuerte
jcando@istvr.edu.ec
https://orcid.org/0009-0008-0632-8644

DOI / URL: https://doi.org/10.55813/gaea/ccri/v7/nE2/1713

Como citar:

Guadalupe-Rodríguez, W. R., López-Molina, L. A., Pinela-Tigua, J. O., & Cando-Cedeño, J. L. (2026). Inteligencia artificial y optimización de la detección de riesgos de fraude en comercio electrónico. *Código Científico Revista De Investigación*, *7*(E2), 828–854.

Recibido: 17/08/2026 **Aceptado**: 15/09/2026 **Publicado**: 30/09/2026

Resumen
El crecimiento del comercio electrónico ha incrementado la exposición de las plataformas digitales a distintas modalidades de fraude, evidenciando la necesidad de mecanismos de detección más ágiles, precisos y adaptables frente a riesgos cambiantes. En este contexto, la inteligencia artificial ha cobrado relevancia como alternativa para fortalecer los procesos de análisis y control en entornos transaccionales complejos. A partir de esta problemática, la presente investigación tuvo como objetivo analizar la incidencia del uso de inteligencia artificial en la optimización de la detección de riesgos de fraude en entornos de comercio electrónico. El estudio se desarrolló bajo un enfoque cuantitativo, con diseño no experimental, alcance correlacional y corte transversal. La muestra estuvo integrada por 54 estudiantes y profesionales vinculados a tecnología, análisis de datos, ciberseguridad, comercio electrónico y gestión de riesgos, seleccionados mediante muestreo no probabilístico por conveniencia. Para la recolección de datos se aplicó un cuestionario estructurado con escala Likert, cuya confiabilidad alcanzó un Alfa de Cronbach global de 0,855. Los resultados mostraron una correlación positiva alta y estadísticamente significativa entre el uso de inteligencia artificial y la optimización de la detección de riesgos de fraude (rho = 0,767; $p < 0,001$). Se concluye que ambas variables estuvieron significativamente asociadas en la muestra estudiada.

Palabras clave: inteligencia artificial, fraude digital, comercio electrónico, detección de riesgos, aprendizaje automático.

Abstract
The growth of e-commerce has increased the exposure of digital platforms to different forms of fraud, highlighting the need for more agile, accurate, and adaptable detection mechanisms to address changing risks. In this context, artificial intelligence has gained relevance as an alternative for strengthening analysis and control processes in complex transactional environments. Based on this issue, the objective of this study was to analyze the incidence of the use of artificial intelligence in optimizing fraud risk detection in e-commerce environments. The research was conducted under a quantitative approach, with a non-experimental design, correlational scope, and cross-sectional cut. The sample consisted of 54 students and professionals linked to technology, data analysis, cybersecurity, e-commerce, and risk management, selected through non-probabilistic convenience sampling. Data were collected through a structured Likert-scale questionnaire, whose reliability reached a global Cronbach's alpha of 0.855. The results showed a high and statistically significant positive correlation between the use of artificial intelligence and the optimization of fraud risk detection (rho = 0.767; $p < 0.001$). It is concluded that both variables were significantly associated within the sample studied
Keywords: artificial intelligence, digital fraud, e-commerce, risk detection, machine learning.

Resumo
O crescimento do comércio eletrónico aumentou a exposição das plataformas digitais a diferentes formas de fraude, destacando a necessidade de mecanismos de deteção mais ágeis, precisos e adaptáveis para fazer face aos riscos em constante evolução. Neste contexto, a inteligência artificial ganhou relevância como alternativa para reforçar os processos de análise e controlo em ambientes transacionais complexos. Com base nesta questão, o objetivo do presente estudo foi analisar a incidência da utilização da inteligência artificial na otimização da deteção do risco de fraude em ambientes de comércio eletrónico. A investigação foi realizada sob uma abordagem quantitativa, com um desenho não experimental, âmbito

correlacional e corte transversal. A amostra consistiu em 54 estudantes e profissionais ligados às áreas da tecnologia, análise de dados, cibersegurança, comércio eletrónico e gestão de risco, selecionados através de amostragem por conveniência não probabilística. Os dados foram recolhidos através de um questionário estruturado com escala de Likert, cuja fiabilidade atingiu um alfa de Cronbach global de 0,855. Os resultados revelaram uma correlação positiva elevada e estatisticamente significativa entre a utilização da inteligência artificial e a otimização da deteção do risco de fraude (rho = 0,767; p < 0,001). Conclui-se que ambas as variáveis se mostraram significativamente associadas na amostra estudada
Palavras-chave: inteligência artificial, fraude digital, comércio eletrónico, deteção de riscos, aprendizagem automática.

Introducción

El comercio electrónico se ha consolidado como uno de los espacios más dinámicos de la economía digital. Sin embargo, su expansión también ha incrementado la exposición a distintas formas de fraude. A medida que crecen las transacciones en línea, los medios de pago digitales y la interacción remota entre usuarios, comercios y plataformas, también se amplían las oportunidades para prácticas como el uso indebido de cuentas, los pagos fraudulentos y otras conductas que comprometen la seguridad operativa y la confianza del consumidor.

La literatura especializada reconoce que el fraude financiero y electrónico constituye un problema persistente y complejo, cuya detección exige mecanismos analíticos cada vez más precisos y adaptables (Ngai et al., 2011; Abdallah et al., 2016). A esta preocupación se han sumado revisiones más recientes que muestran cómo el fraude digital ha evolucionado junto con la sofisticación de los entornos transaccionales y el crecimiento del volumen de datos procesados por plataformas en línea (Ali et al., 2022; Sánchez-Aguayo et al., 2021).

Una de las principales limitaciones de los métodos tradicionales de detección es que suelen basarse en reglas estáticas o en revisiones posteriores a la transacción. Esa condición reduce su capacidad para responder a esquemas fraudulentos que cambian con rapidez. Abdallah et al. (2016) advierten que los sistemas de detección de fraude enfrentan obstáculos

como la transformación constante de los patrones delictivos, el desbalance de los datos y la necesidad de analizar grandes volúmenes de información en tiempo real.

Ngai et al. (2011) observaron que, aunque las técnicas de minería de datos han sido ampliamente utilizadas en la detección de fraude financiero, todavía persisten vacíos en la forma en que ciertos tipos de fraude son abordados desde la investigación y la práctica. Estudios más recientes han reforzado esta idea al señalar que la heterogeneidad de los datos, la presencia de clases desbalanceadas y la naturaleza dinámica del fraude continúan representando desafíos importantes para los sistemas de detección contemporáneos (Kanika et al., 2022; Tong & Shen, 2024).

La inteligencia artificial ha cobrado relevancia como una alternativa con mayor capacidad para procesar datos complejos, identificar relaciones no evidentes y reconocer comportamientos atípicos en escenarios digitales. En particular, la detección de anomalías basada en aprendizaje profundo se ha convertido en una línea de investigación significativa, precisamente porque permite descubrir patrones irregulares que no siempre resultan visibles mediante enfoques convencionales.

Pang et al. (2021) sostienen que este tipo de técnicas ofrece una base sólida para abordar problemas en los que los comportamientos anómalos son escasos, variables o difíciles de modelar mediante reglas fijas. En ese mismo sentido, diversos trabajos recientes han mostrado que los modelos basados en aprendizaje automático, aprendizaje profundo y estructuras gráficas amplían las posibilidades de identificar relaciones complejas en transacciones sospechosas y de mejorar la capacidad de detección en contextos digitales (Zhang et al., 2022; Chen et al., 2024; Compagnino et al., 2025).

En el contexto específico del comercio electrónico, esta discusión adquiere mayor relevancia porque las plataformas operan con datos heterogéneos, interacciones continuas y decisiones que deben tomarse con rapidez. La revisión sistemática de Mutemi y Bação (2024)

muestra que las técnicas de *machine learning* han ganado un papel cada vez más visible en la detección de fraude en *e-commerce*, al tiempo que evidencian oportunidades de mejora y vacíos de investigación en su aplicación dentro de mercados digitales.

Entonces Zhang et al. (2022) señalan que la detección de fraude en comercio electrónico demanda modelos capaces de captar relaciones estructurales más complejas entre usuarios, transacciones y comportamientos. A su vez, Li et al. (2021) muestran que parte del fraude en estos entornos no puede comprenderse únicamente desde eventos aislados, sino también desde patrones comunitarios y vínculos menos evidentes entre actores. En consecuencia, no basta con reconocer que el fraude representa un problema creciente. También resulta necesario analizar de qué manera el uso de inteligencia artificial contribuye a optimizar su detección en entornos de comercio electrónico, especialmente desde una perspectiva aplicada y orientada a la gestión del riesgo.

La presente investigación se justifica por la relevancia actual del fraude dentro de los entornos de comercio electrónico. El crecimiento de las transacciones digitales ha incrementado la necesidad de contar con mecanismos más precisos para identificar riesgos antes de que generen pérdidas económicas, afectaciones operativas o deterioro de la confianza del usuario. En este contexto, la literatura reciente ha mostrado que la detección de fraude en *e-commerce* sigue siendo un campo activo de estudio, precisamente porque las dinámicas fraudulentas evolucionan con rapidez y exigen respuestas analíticas más robustas que las aproximaciones convencionales (Mutemi & Bação, 2024; Almazroi & Ayub, 2023).

Aquí se vuelve necesario seguir generando evidencia sobre el valor de las tecnologías inteligentes en procesos de control y monitoreo. La pertinencia del estudio no radica únicamente en el interés académico por la inteligencia artificial, sino en su posible aporte frente a un problema que afecta de manera directa la estabilidad operativa y la confianza digital.

La investigación se justifica por su pertinencia tecnológica. La inteligencia artificial ha ampliado las posibilidades de análisis en escenarios donde el volumen de datos, la velocidad de las transacciones y la variabilidad de los patrones dificultan la detección mediante reglas fijas o revisiones manuales. Los enfoques basados en aprendizaje automático y detección de anomalías resultan especialmente valiosos, ya que permiten reconocer comportamientos atípicos y relaciones complejas entre variables que no siempre son visibles con métodos tradicionales (Pang et al., 2021).

Estudios recientes han mostrado que la integración de técnicas de aprendizaje supervisado, no supervisado y auto-supervisado puede fortalecer la precisión y la adaptabilidad de los sistemas de detección frente a escenarios cada vez más complejos (Chen et al., 2024; Wijaya et al., 2024). Por ello, estudiar su uso dentro del comercio electrónico no responde solo a una tendencia tecnológica, sino también a una necesidad operativa concreta.

La investigación posee valor académico porque contribuye a reducir la distancia entre el avance técnico de la inteligencia artificial y su comprensión aplicada en la detección de riesgos de fraude en *e-commerce*. Aunque ya existen revisiones y desarrollos orientados al uso de *machine learning* en este ámbito, todavía se identifican oportunidades para profundizar en cómo estas herramientas optimizan los procesos de detección dentro de contextos específicos de comercio digital, especialmente cuando se analizan desde una lógica de gestión de riesgos y no únicamente desde el rendimiento algorítmico (Mutemi & Bação, 2024).

Este estudio también dialoga con trabajos que han insistido en la necesidad de conectar el desarrollo técnico de los modelos con su interpretación práctica, su capacidad explicativa y su utilidad para la toma de decisiones en escenarios reales (Rao et al., 2022; Dichev et al., 2025). Esa articulación resulta importante porque permite que la discusión sobre inteligencia artificial no quede limitada al plano técnico, sino que se traslade a su utilidad en problemas concretos de seguridad digital.

Analizar el uso de inteligencia artificial en la optimización de la detección de riesgos de fraude puede aportar evidencia útil para fortalecer la toma de decisiones en plataformas digitales, mejorar criterios de prevención y orientar futuras implementaciones tecnológicas en organizaciones que operan en entornos de comercio electrónico. En ese sentido, el estudio no solo tiene valor teórico, sino también aplicación potencial en escenarios reales donde la seguridad transaccional y la confianza del usuario son factores decisivos para la sostenibilidad del negocio (Mutemi & Bação, 2024; Pang et al., 2021). Finalmente, la investigación se justifica por su utilidad práctica.

A ello se suma que investigaciones recientes continúan mostrando que la incorporación de modelos inteligentes en la detección de fraude ya no se percibe solo como una opción tecnológica avanzada, sino como un componente estratégico dentro de los sistemas contemporáneos de gestión del riesgo digital (Mytnyk et al., 2023; Odufisan et al., 2025).

Metodología

Una vez que el problema fue identificado se orientó la investigación a examinar de manera concreta la relación entre el uso de inteligencia artificial y la optimización de la detección de riesgos de fraude en entornos de comercio electrónico. El interés del estudio no se limitó a describir la importancia actual de estas herramientas dentro de los ecosistemas digitales, sino a analizarlas desde una perspectiva cuantitativa que permitiera trabajar con variables definidas, indicadores observables y datos susceptibles de tratamiento estadístico.

Se estableció como objetivo general analizar la incidencia del uso de inteligencia artificial en la optimización de la detección de riesgos de fraude en entornos de comercio electrónico. Este objetivo se formuló considerando que el crecimiento de las transacciones digitales ha hecho cada vez más necesario contar con mecanismos de detección más ágiles, precisos y consistentes frente a amenazas que evolucionan con rapidez.

A partir de este objetivo general se formularon objetivos específicos orientados a dar orden y profundidad al estudio. En primer lugar, se planteó identificar los principales riesgos de fraude presentes en entornos de comercio electrónico, ya que reconocer estas manifestaciones resultó indispensable para comprender la dimensión real del problema.

Luego se propuso determinar los elementos del uso de inteligencia artificial aplicables a la detección de riesgos de fraude en plataformas de comercio electrónico. Con ello se buscó delimitar con mayor claridad qué aspectos de esta tecnología podían ser observados dentro del estudio y cómo se vinculaban con los procesos de análisis y control.

Se estableció como objetivo específico evaluar la incidencia del uso de inteligencia artificial en la optimización de la detección de riesgos de fraude en entornos de comercio electrónico. Esta formulación respondió a la lógica del enfoque cuantitativo adoptado, pues permitió articular el problema, las variables y el análisis estadístico dentro de una misma línea de coherencia metodológica.

En correspondencia con estos objetivos, se planteó como hipótesis general que el uso de inteligencia artificial incide significativamente en la optimización de la detección de riesgos de fraude en entornos de comercio electrónico. Esta proposición partió de la idea de que herramientas capaces de procesar datos, reconocer patrones anómalos y apoyar la toma de decisiones pueden fortalecer de manera importante los procesos de prevención y detección dentro de plataformas digitales.

Complementariamente se formuló la hipótesis nula, según la cual el uso de inteligencia artificial no incide significativamente en la optimización de la detección de riesgos de fraude en entornos de comercio electrónico. La inclusión de ambas hipótesis permitió sostener el estudio dentro de un esquema cuantitativo claro, en el que la relación entre variables pudiera contrastarse de forma objetiva mediante procedimientos estadísticos.

La presente investigación se desarrolló bajo un enfoque cuantitativo, ya que se orientó al análisis de datos medibles relacionados con el uso de inteligencia artificial y su incidencia en la optimización de la detección de riesgos de fraude en entornos de comercio electrónico. Este enfoque permitió examinar la relación entre la variable independiente, correspondiente al uso de inteligencia artificial, y la variable dependiente, asociada a la optimización de la detección de riesgos de fraude, a partir de información obtenida mediante un instrumento estructurado.

Debido a que las variables no fueron manipuladas de manera deliberada, el estudio se enmarcó en un diseño no experimental, sino observadas y analizadas tal como se presentaron en el contexto de estudio. Asimismo, tuvo un alcance correlacional, puesto que buscó determinar la relación existente entre el uso de inteligencia artificial y la optimización de la detección de riesgos de fraude en entornos de comercio electrónico.

La investigación fue de corte transversal en su temporalidad dado que la recolección de la información se efectuó en un único momento. Esta decisión metodológica resultó coherente con el propósito del estudio, ya que permitió analizar el comportamiento de las variables en la muestra seleccionada sin intervenir sobre ellas.

La población objetivo estuvo conformada por estudiantes y profesionales vinculados a las áreas de tecnología, análisis de datos, ciberseguridad, comercio electrónico y gestión de riesgos, debido a que estos perfiles guardan relación directa con el objeto de estudio. No se trabajó con un marco poblacional cerrado ni con un registro único que permitiera establecer con precisión el número total de personas que integraban dicha población. Por esta razón, la selección de participantes se realizó mediante un muestreo no probabilístico por conveniencia.

La muestra quedó integrada por 54 participantes, elegidos con base en criterios de accesibilidad, disponibilidad y afinidad temática con la investigación. Esta cantidad se consideró suficiente para el análisis propuesto, dado que el estudio tuvo un alcance

correlacional y buscó examinar la relación entre variables dentro de un grupo pertinente al problema investigado. En este sentido, los resultados no se plantean en términos de representatividad estadística de una población total, sino como evidencia obtenida a partir de una muestra intencionalmente seleccionada por su vinculación con el tema.

Para la recolección de los datos se empleó la técnica de la encuesta y como instrumento se utilizó un cuestionario estructurado con escala tipo Likert. El instrumento fue diseñado con ítems cerrados orientados a medir las dimensiones e indicadores correspondientes a las dos variables del estudio: uso de inteligencia artificial, como variable independiente, y optimización de la detección de riesgos de fraude en entornos de comercio electrónico, como variable dependiente.

En relación con la variable uso de inteligencia artificial se consideraron aspectos como la frecuencia de uso, el apoyo en el análisis de datos, la identificación de patrones anómalos y la contribución al análisis de riesgos. Por su parte, para la variable optimización de la detección de riesgos de fraude, se contemplaron elementos como la precisión en la detección, la rapidez del análisis, la capacidad de anticipación y el apoyo en la toma de decisiones. Esta organización permitió que el cuestionario guardara coherencia con los objetivos del estudio y con la lógica del análisis cuantitativo planteado.

La validez del instrumento se determinó mediante juicio de expertos, con el propósito de evaluar la claridad, pertinencia y coherencia de los ítems en función de los objetivos planteados. Asimismo, la confiabilidad del cuestionario se estableció a través del coeficiente Alfa de Cronbach con un valor global de 0,855, con el fin de verificar la consistencia interna del instrumento y asegurar la estabilidad de las respuestas obtenidas.

Las variables consideradas en el estudio fueron el uso de inteligencia artificial, como variable independiente, y la optimización de la detección de riesgos de fraude en entornos de comercio electrónico, como variable dependiente. Ambas fueron operacionalizadas en

dimensiones e indicadores que orientaron la construcción del cuestionario aplicado a los participantes.

Tabla 1

Matriz de operacionalización de variables

Variable	Dimensiones	Indicadores	Técnica e instrumento	Escala
Uso de inteligencia artificial (Variable independiente)	Frecuencia y nivel de uso	Uso de herramientas de IA, familiaridad con IA, aplicación en análisis digital	Encuesta – Cuestionario estructurado	Likert de 5 puntos
	Capacidad analítica de la IA	Procesamiento de datos, identificación de patrones anómalos, detección de comportamientos sospechosos	Encuesta – Cuestionario estructurado	Likert de 5 puntos
	Utilidad en la gestión de riesgos	Identificación de riesgos, análisis preventivo, apoyo a la toma de decisiones	Encuesta – Cuestionario estructurado	Likert de 5 puntos
	Precisión en la detección	Exactitud en la identificación de riesgos, reducción de errores, diferenciación entre transacciones normales y sospechosas	Encuesta – Cuestionario estructurado	Likert de 5 puntos
Optimización de la detección de riesgos de fraude en entornos de comercio electrónico (Variable dependiente)	Rapidez del análisis	Disminución del tiempo de detección, agilidad en la revisión, respuesta oportuna	Encuesta – Cuestionario estructurado	Likert de 5 puntos
	Capacidad de anticipación	Identificación temprana de riesgos, reconocimiento preventivo de patrones fraudulentos, prevención de incidentes	Encuesta – Cuestionario estructurado	Likert de 5 puntos
	Apoyo a la toma de decisiones	Seguridad en la evaluación de casos, fortalecimiento del control, apoyo al monitoreo	Encuesta – Cuestionario estructurado	Likert de 5 puntos

Nota: (Autores, 2026).

El procedimiento metodológico se desarrolló en varias fases. En primer lugar, se realizó la revisión de literatura científica relacionada con inteligencia artificial, fraude digital, análisis de riesgos y comercio electrónico, lo que permitió sustentar teóricamente la investigación. Luego se diseñó el cuestionario en función de las variables, dimensiones e indicadores previamente definidos. Finalmente se aplicó el instrumento a los 54 participantes seleccionados. Finalmente, los datos recolectados fueron organizados, codificados y procesados para su respectivo análisis estadístico.

Para el análisis de la información se empleó estadística descriptiva e inferencial. En la fase descriptiva se utilizaron frecuencias y porcentajes para caracterizar las respuestas obtenidas en cada una de las variables. En la fase inferencial, se aplicó la correlación de

Spearman, debido a que el instrumento utilizó una escala ordinal tipo Likert y el estudio buscó determinar la relación entre las variables. Esta prueba permitió contrastar la hipótesis planteada y establecer si existió una relación significativa entre el uso de inteligencia artificial y la optimización de la detección de riesgos de fraude en entornos de comercio electrónico.

Resultados

La muestra estuvo conformada por 54 participantes. De ellos, 35 correspondieron a profesionales, lo que equivale al 64,8 %, mientras que 19 fueron estudiantes, representando el 35,2 %. Esta distribución muestra un predominio de participantes con perfil profesional, lo que aporta pertinencia a los resultados al tratarse de una población vinculada con contextos donde la inteligencia artificial, el análisis de datos y la gestión del riesgo tienen aplicación práctica.

En cuanto al área principal de vinculación el mayor porcentaje se concentró en tecnología, con 14 participantes (25,9 %). Le siguieron ciberseguridad y gestión de riesgos, con 10 participantes en cada caso (18,5 %), y comercio electrónico, con 8 participantes (14,8 %). Las áreas de análisis de datos y otras registraron 6 participantes cada una, equivalentes al 11,1 %. En conjunto, esta distribución muestra que la muestra estuvo integrada por perfiles diversos, pero cercanos al campo temático del estudio.

Respecto a la experiencia previa en el uso de herramientas de inteligencia artificial, 45 participantes indicaron que sí contaban con ella, lo que representa el 83,3 %, mientras que 9 señalaron no tenerla (16,7 %). Este dato sugiere que la mayoría de los encuestados tenía contacto previo con este tipo de tecnologías, lo que resulta relevante para la consistencia de las respuestas emitidas en el cuestionario.

En relación con el nivel de familiaridad con herramientas de inteligencia artificial, el grupo más numeroso reportó un nivel alto, con 20 participantes (37,0 %). A continuación, se ubicaron quienes señalaron un nivel medio, con 15 participantes (27,8 %), y muy alto, con 11

participantes (20,4 %). Los niveles bajo y muy bajo registraron 6 participantes (11,1 %) y 2 participantes (3,7 %), respectivamente. En términos generales, estos resultados muestran que la muestra no solo tenía experiencia previa, sino también un nivel de familiaridad predominantemente medio y alto con el uso de inteligencia artificial.

Se evidenció que 42 participantes manifestaron haber participado en actividades relacionadas con comercio electrónico, análisis de riesgos o fraude digital, lo que equivale al 77,8 %, mientras que 12 indicaron no haberlo hecho (22,2 %). Este comportamiento refuerza la pertinencia de la muestra para el desarrollo de la investigación, ya que una proporción importante de los encuestados presentaba cercanía con el problema analizado.

Tabla 2

Caracterización de la muestra

Variable	Categoría	Frecuencia	Porcentaje
Condición del participante	Estudiante	19	35,2 %
	Profesional	35	64,8 %
Área principal de vinculación	Tecnología	14	25,9 %
	Análisis de datos	6	11,1 %
	Ciberseguridad	10	18,5 %
	Comercio electrónico	8	14,8 %
	Gestión de riesgos	10	18,5 %
	Otra	6	11,1 %
Experiencia previa en IA	Sí	45	83,3 %
	No	9	16,7 %
Nivel de familiaridad con IA	Muy bajo	2	3,7 %
	Bajo	6	11,1 %
	Medio	15	27,8 %
	Alto	20	37,0 %
	Muy alto	11	20,4 %
Participación en temas relacionados	Sí	42	77,8 %
	No	12	22,2 %

Nota: La muestra estuvo conformada por 54 participantes entre estudiantes y profesionales vinculados a áreas relacionadas con tecnología, análisis de datos, ciberseguridad, comercio electrónico y gestión de riesgos (Autores, 2026).

Confiabilidad del instrumento

En relación con la confiabilidad del instrumento se pudo notar que el cuestionario aplicado estuvo integrado por 21 ítems distribuidos en dos variables. El análisis de consistencia interna mostró un Alfa de Cronbach global de 0,855, lo que indica un nivel adecuado de confiabilidad para el instrumento utilizado en el estudio. Este resultado permite sostener que,

en términos generales, los ítems mantuvieron una coherencia suficiente para la medición de las variables planteadas.

La variable uso de inteligencia artificial que estuvo compuesta por 9 ítems, alcanzó un Alfa de Cronbach de 0,770. Por su parte, la variable optimización de la detección de riesgos de fraude, integrada por 12 ítems, obtuvo un coeficiente de 0,718. Ambos resultados muestran niveles aceptables de consistencia interna, lo que respalda la estabilidad de las respuestas obtenidas y la pertinencia del cuestionario como instrumento de recolección de datos.

Metodológicamente podemos inferir que estos valores resultan favorables para el desarrollo del análisis estadístico posterior, ya que permiten trabajar con una base de datos cuya estructura interna presenta coherencia en la medición de los constructos evaluados. En consecuencia, la confiabilidad alcanzada por el instrumento constituyó un soporte importante para la fase descriptiva e inferencial del estudio.

Tabla 3

Confiabilidad del instrumento

Variable	Número de ítems	Alfa de Cronbach
Uso de inteligencia artificial	9	0,770
Optimización de la detección de riesgos de fraude	12	0,718
Instrumento total	21	0,855

Nota: El cuestionario aplicado estuvo conformado por 21 ítems distribuidos en dos variables. La confiabilidad del instrumento se evaluó mediante el coeficiente Alfa de Cronbach (Autores, 2026).

Estadísticos descriptivos por dimensiones

Los resultados descriptivos por dimensiones muestran que las puntuaciones obtenidas se ubicaron en niveles altos dentro de la escala aplicada. En la variable uso de inteligencia artificial, la dimensión con mayor media fue capacidad analítica de la IA, con 4,12, seguida de frecuencia y nivel de uso, con 4,08, y utilidad en la gestión de riesgos, con 4,05. Estas puntuaciones reflejan una valoración favorable del uso de la inteligencia artificial en procesos relacionados con el análisis de información y la gestión del riesgo.

En la variable optimización de la detección de riesgos de fraude, la dimensión con media más alta fue capacidad de anticipación, con 4,21. A continuación, se ubicaron rapidez

del análisis, con 4,18, apoyo a la toma de decisiones, con 4,10, y precisión en la detección, con 4,06. En conjunto, estas cifras muestran que las dimensiones asociadas a la detección de riesgos fueron valoradas de manera positiva por los participantes, con un comportamiento relativamente homogéneo entre ellas.

Al observar ambas variables en conjunto se puede apreciar que todas las dimensiones superaron la media de 4,00, lo que indica una tendencia general favorable en las respuestas obtenidas. Este comportamiento permite advertir que tanto el uso de inteligencia artificial como la optimización de la detección de riesgos de fraude fueron evaluados con puntuaciones altas dentro de la muestra estudiada.

Tabla 4

Estadísticos descriptivos por dimensiones

Variable	Dimensión	Media
Uso de inteligencia artificial	Frecuencia y nivel de uso	4,08
Uso de inteligencia artificial	Capacidad analítica de la IA	4,12
Uso de inteligencia artificial	Utilidad en la gestión de riesgos	4,05
Optimización de la detección de riesgos de fraude	Precisión en la detección	4,06
Optimización de la detección de riesgos de fraude	Rapidez del análisis	4,18
Optimización de la detección de riesgos de fraude	Capacidad de anticipación	4,21
Optimización de la detección de riesgos de fraude	Apoyo a la toma de decisiones	4,10

Nota: Las medias corresponden a las puntuaciones obtenidas en cada dimensión del cuestionario, calculadas a partir de una escala Likert de cinco puntos (Autores, 2026).

Prueba de hipótesis

Para contrastar la hipótesis del estudio se aplicó la correlación de Spearman entre la variable independiente total, correspondiente al uso de inteligencia artificial, y la variable dependiente total, relacionada con la optimización de la detección de riesgos de fraude en entornos de comercio electrónico. El análisis arrojó un coeficiente rho = 0,767, lo que muestra una relación positiva alta entre ambas variables.

En cuanto al nivel de significancia, se obtuvo un valor de $p < 0,001$, lo que indica que la relación identificada fue estadísticamente significativa. Este resultado permitió establecer que, dentro de la muestra analizada, el comportamiento de ambas variables presentó una asociación consistente en el sentido positivo.

A partir de estos datos, la prueba estadística mostró evidencia suficiente para rechazar la hipótesis nula y aceptar la hipótesis general planteada en la investigación. En términos de resultados, esto significa que el uso de inteligencia artificial se asoció de manera significativa con la optimización de la detección de riesgos de fraude en entornos de comercio electrónico.

Tabla 5

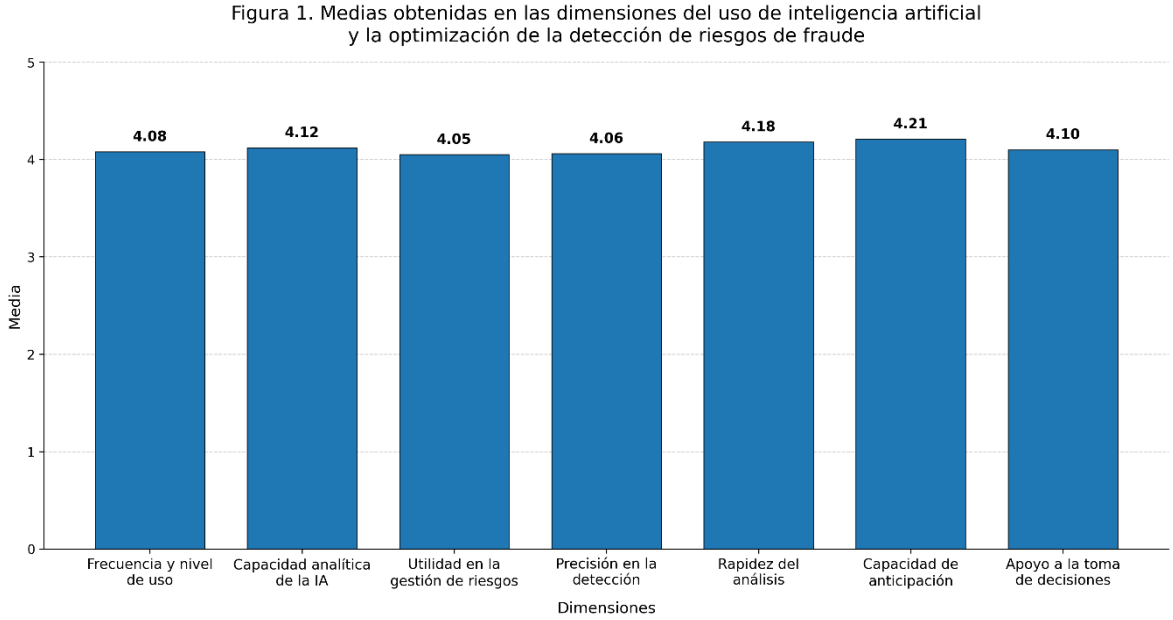
Prueba de hipótesis

Variables correlacionadas	Rho de Spearman	Significancia (bilateral)
Uso de inteligencia artificial / Optimización de la detección de riesgos de fraude	0,767	0,000

Nota: La correlación se calculó mediante el coeficiente Rho de Spearman. El valor de significancia fue menor a 0,001, por lo que se registró una relación estadísticamente significativa entre las variables analizadas (Autores, 2026).

Figura 1

Medias obtenidas en las dimensiones del uso de inteligencia artificial y la optimización de la detección de riesgos de fraude



Nota: (Autores, 2026).

Discusión

Los hallazgos del estudio permiten afirmar que el uso de inteligencia artificial ocupa un lugar relevante dentro de los procesos orientados a la detección de riesgos de fraude en entornos de comercio electrónico. Más allá de la confirmación estadística de la relación entre las variables, lo relevante es que esta asociación refuerza la pertinencia del problema planteado al

inicio de la investigación. En un contexto donde las transacciones digitales se desarrollan con rapidez y en volúmenes cada vez mayores, la identificación oportuna de riesgos deja de ser una ventaja secundaria y pasa a convertirse en una necesidad operativa. Desde esta perspectiva, los resultados sugieren que la inteligencia artificial no es percibida solo como una innovación tecnológica, sino como un recurso con potencial real para fortalecer procesos de control y monitoreo.

Al examinar el comportamiento general de las dimensiones evaluadas, se advierte una valoración favorable tanto del uso de inteligencia artificial como de su vínculo con la detección de riesgos de fraude. Este comportamiento permite inferir que, dentro de la muestra estudiada, la tecnología es reconocida como una herramienta con aplicación concreta en tareas de análisis, identificación de patrones y apoyo a la gestión del riesgo. La percepción positiva registrada en torno a estas funciones sugiere que la inteligencia artificial ya no es vista como un elemento accesorio. Más bien, aparece integrada a una lógica de trabajo orientada a mejorar la capacidad de respuesta frente a escenarios de fraude. En ese sentido, la optimización del proceso de detección no parece asociarse únicamente con una mejora técnica, sino también con una ventaja funcional dentro de dinámicas de prevención y control.

Otro aspecto relevante es que los resultados dirigen la atención hacia funciones especialmente sensibles dentro de los sistemas de detección: la capacidad de actuar con rapidez y la posibilidad de anticiparse a señales de riesgo. Esto sugiere que, desde la perspectiva de los participantes, una de las fortalezas más visibles de la inteligencia artificial radica en su potencial para ofrecer una lectura más dinámica del entorno transaccional. En escenarios de comercio electrónico, donde las amenazas pueden transformarse en intervalos muy breves, esta capacidad de respuesta adquiere un valor estratégico. Al mismo tiempo, el hecho de que otros aspectos vinculados con la gestión del riesgo y la toma de decisiones también hayan sido valorados de forma positiva indica que el aporte de estas herramientas no se limita al plano

operativo inmediato, sino que también puede proyectarse hacia procesos de análisis más amplios.

La composición de la muestra también ayuda a comprender el sentido de los hallazgos. El predominio de participantes con perfil profesional y con cercanía previa al uso de herramientas de inteligencia artificial sugiere que las valoraciones obtenidas no provinieron de una percepción distante del fenómeno estudiado. Por el contrario, las respuestas parecen apoyarse en experiencias o referencias relativamente próximas a contextos donde estas tecnologías ya tienen aplicaciones concretas. Esto aporta mayor pertinencia al análisis, ya que la valoración del papel de la inteligencia artificial se construyó desde perfiles vinculados con tecnología, análisis de datos, ciberseguridad, comercio electrónico y gestión de riesgos. En ese marco, la percepción favorable observada en el estudio puede entenderse no como una apreciación abstracta, sino como una lectura formada desde espacios donde estas herramientas tienen utilidad práctica.

Metodológicamente otro elemento que fortalece la discusión es la consistencia del instrumento utilizado. La confiabilidad alcanzada por el cuestionario permite sostener que la medición de las variables se realizó sobre una base estable, lo que reduce el riesgo de atribuir los hallazgos a respuestas desordenadas o a una estructura débil del instrumento. Esto resulta importante porque da mayor solidez a la interpretación de la relación observada entre el uso de inteligencia artificial y la detección de riesgos de fraude. En términos prácticos, significa que los ítems del cuestionario lograron captar de forma suficientemente coherente las percepciones de los participantes sobre ambos constructos. De este modo, la discusión no se apoya solo en una asociación estadística, sino también en una medición con consistencia interna adecuada.

Aunque los resultados fueron favorables su interpretación debe mantenerse dentro de los límites propios del diseño adoptado. Al tratarse de una investigación no experimental, correlacional y de corte transversal, los hallazgos permiten identificar asociación entre

variables, pero no establecer una relación causal en sentido estricto. Por ello, no sería metodológicamente correcto afirmar que la inteligencia artificial, por sí sola, produce mejoras automáticas en la detección del fraude. Lo que sí puede sostenerse es que, dentro de la muestra estudiada, ambas variables mostraron un comportamiento convergente y coherente con la lógica del modelo planteado. Del mismo modo, al haberse trabajado con una muestra seleccionada por conveniencia, la generalización de los hallazgos debe realizarse con prudencia, entendiendo que describen el comportamiento observado en este grupo específico.

La discusión permite afirmar que los resultados del estudio ofrecen una base empírica favorable para comprender el papel de la inteligencia artificial en los procesos de detección de riesgos de fraude dentro del comercio electrónico. Más allá del dato estadístico, lo que emerge del análisis es una percepción bastante clara: el uso de estas herramientas se asocia con mejoras en áreas clave del proceso de control, especialmente en la rapidez para analizar operaciones, en la capacidad de anticipar comportamientos sospechosos y en el fortalecimiento de decisiones orientadas a la prevención. Esto no significa que la inteligencia artificial deba asumirse como una solución absoluta o exenta de desafíos, pero sí que, dentro del marco de esta investigación, su incorporación aparece vinculada con una mejora percibida en funciones que son críticas para la seguridad y sostenibilidad de las plataformas digitales.

Comparación con otros estudios

Los resultados obtenidos en esta investigación guardan coherencia con diversos estudios que han señalado el papel cada vez más relevante de la inteligencia artificial en la detección de fraude dentro de entornos digitales. En este caso, la relación positiva y estadísticamente significativa entre el uso de inteligencia artificial y la optimización de la detección de riesgos de fraude sugiere que, para la muestra analizada, estas herramientas no solo se perciben como innovaciones tecnológicas, sino como recursos concretos para fortalecer procesos de análisis, anticipación y control. Esta tendencia coincide con lo reportado por

Mutemi y Bação (2024), quienes, a partir de una revisión sistemática sobre fraude en comercio electrónico, identificaron que las técnicas de *machine learning* han adquirido un papel cada vez más visible en este campo por su capacidad para procesar información compleja y mejorar la identificación de comportamientos sospechosos. En una línea semejante, Ali et al. (2022) destacan que los modelos basados en aprendizaje automático se han consolidado como una de las principales rutas de avance en la detección de fraude financiero, precisamente por su capacidad para adaptarse a escenarios donde los patrones delictivos cambian con rapidez.

Asimismo, los hallazgos de este estudio también se relacionan con trabajos que han destacado la utilidad de la inteligencia artificial para reconocer patrones irregulares que difícilmente pueden ser detectados mediante enfoques convencionales. Pang et al. (2021) sostienen que los métodos de detección de anomalías basados en aprendizaje profundo ofrecen ventajas importantes cuando se trata de identificar comportamientos atípicos, especialmente en contextos donde las irregularidades son escasas, variables o complejas de modelar. Esta idea resulta consistente con los resultados obtenidos en las dimensiones rapidez del análisis y capacidad de anticipación, que fueron las mejor valoradas por los participantes.

Del mismo modo, Zhang et al. (2022) señalan que la detección de fraude en comercio electrónico exige modelos capaces de captar relaciones estructurales complejas entre transacciones, usuarios y comportamientos, mientras que Chen et al. (2024) subrayan que los enfoques recientes basados en aprendizaje auto-supervisado e inteligente muestreo pueden fortalecer el rendimiento de los sistemas de detección. Desde esa perspectiva, los datos de esta investigación refuerzan la idea de que la inteligencia artificial es percibida como una herramienta especialmente útil cuando el análisis requiere rapidez, sensibilidad frente a patrones atípicos y apoyo para decidir con mayor oportunidad.

Por otra parte, los resultados también pueden interpretarse a la luz de antecedentes más amplios sobre la evolución de los sistemas de detección de fraude. Abdallah et al. (2016) ya

advertían que estos sistemas enfrentaban desafíos persistentes, entre ellos el desbalance de los datos, la evolución constante de los esquemas fraudulentos y la necesidad de respuestas más adaptativas que las ofrecidas por métodos tradicionales. En la misma línea, Ngai et al. (2011) destacaban que las técnicas de minería de datos constituían una base importante para el reconocimiento de patrones de fraude financiero, sobre todo en entornos donde la complejidad de la información supera la capacidad de revisión manual. Más recientemente, Kanika et al. (2022) y Tong y Shen (2024) han insistido en que la detección eficaz del fraude en transacciones digitales depende en gran medida de la capacidad de los modelos para enfrentar datos desbalanceados y estructuras relacionales complejas. En este sentido, los resultados del presente estudio no aparecen como un hallazgo aislado, sino como una evidencia empírica que se integra de manera coherente con una línea de investigación que viene señalando, desde hace años, el valor de los sistemas inteligentes para mejorar la respuesta frente al fraude digital.

No obstante, también es importante reconocer que existen diferencias metodológicas entre esta investigación y varios de los estudios con los que se la compara. Mientras buena parte de la literatura previa se ha centrado en revisiones sistemáticas, análisis técnicos, desarrollos algorítmicos o validaciones de modelos computacionales, el presente estudio se apoyó en la percepción de una muestra integrada por estudiantes y profesionales vinculados a áreas afines a la tecnología, el análisis de datos, la ciberseguridad, el comercio electrónico y la gestión de riesgos. Por ello, la comparación no debe entenderse como una equivalencia directa entre diseños, sino como una convergencia razonable entre la evidencia técnica acumulada y la valoración empírica recogida en esta investigación. En otras palabras, si estudios como los de Rao et al. (2022), Dichev et al. (2025) y Compagnino et al. (2025) han mostrado el potencial técnico y analítico de la inteligencia artificial para fortalecer la detección de fraude, los resultados aquí obtenidos permiten afirmar que ese potencial también es reconocido desde una

perspectiva operativa por una población relacionada con los contextos donde estas herramientas encuentran aplicación práctica.

Implicaciones de los resultados

Los hallazgos obtenidos en esta investigación tienen implicaciones relevantes tanto en el plano práctico como en el académico. Desde una perspectiva aplicada, la relación positiva y significativa entre el uso de inteligencia artificial y la optimización de la detección de riesgos de fraude sugiere que estas herramientas pueden constituir un recurso valioso para fortalecer los sistemas de monitoreo y control en entornos de comercio electrónico. En términos operativos, esto implica que la incorporación de soluciones basadas en inteligencia artificial no solo podría contribuir a procesar grandes volúmenes de información con mayor rapidez, sino también a mejorar la identificación temprana de patrones sospechosos y la capacidad de respuesta ante posibles incidentes. Esta lectura coincide con lo planteado por Almazroi y Ayub (2023), quienes destacan que los modelos de aprendizaje automático aplicados al fraude en pagos en línea ofrecen ventajas importantes para mejorar la detección en escenarios digitales complejos, y con Odufisan et al. (2025), quienes subrayan que la integración de inteligencia artificial en procesos de prevención y control puede fortalecer de manera significativa la gestión del fraude en contextos contemporáneos.

En el plano académico, los resultados aportan evidencia empírica sobre un tema que mantiene alta relevancia dentro de la investigación actual en comercio electrónico, fraude digital y tecnologías inteligentes. El estudio permite observar que el uso de inteligencia artificial no solo es valorado positivamente desde una perspectiva técnica, sino también como un elemento que se asocia con mejoras concretas en dimensiones clave del proceso de detección, como la rapidez del análisis, la capacidad de anticipación y el apoyo a la toma de decisiones. Esto amplía la comprensión del fenómeno desde una mirada cuantitativa y se articula con estudios recientes que han insistido en la necesidad de seguir conectando el

desarrollo técnico de los modelos con sus implicaciones prácticas en escenarios reales de detección y gestión del riesgo (Ali et al., 2022; Dichev et al., 2025). En ese sentido, la investigación no solo confirma una tendencia previamente identificada en la literatura, sino que también aporta evidencia desde una muestra vinculada a contextos donde estas herramientas pueden tener aplicación directa.

Asimismo, los resultados tienen implicaciones metodológicas que también merecen ser consideradas. El hecho de haber trabajado con un diseño cuantitativo, no experimental, correlacional y de corte transversal permitió obtener evidencia estadística que respalda la relación entre las variables analizadas, aportando un nivel de objetividad importante al estudio. Al mismo tiempo, la confiabilidad alcanzada por el instrumento refuerza la consistencia de la medición y ofrece una base útil para futuras investigaciones que deseen profundizar en esta línea temática. Esto resulta especialmente valioso si se considera que uno de los retos actuales en el estudio del fraude digital no consiste únicamente en desarrollar modelos más sofisticados, sino también en construir instrumentos y diseños que permitan comprender cómo estas tecnologías son percibidas y valoradas en contextos aplicados. Por ello, el estudio no solo genera información pertinente sobre la relación entre inteligencia artificial y detección de fraude en comercio electrónico, sino que también deja abierta la posibilidad de nuevas investigaciones que amplíen el análisis hacia otras poblaciones, sectores o enfoques metodológicos más complejos.

Conclusión

La investigación permitió analizar la incidencia del uso de inteligencia artificial en la optimización de la detección de riesgos de fraude en entornos de comercio electrónico, y los resultados mostraron una relación positiva alta y estadísticamente significativa entre ambas variables. Este hallazgo confirmó la hipótesis general planteada y mostró que, dentro de la

muestra estudiada, una mayor valoración del uso de herramientas de inteligencia artificial se asoció con una mejor percepción de la capacidad para detectar riesgos de fraude. En este sentido, el estudio logró responder de manera coherente al problema formulado y al propósito central que orientó la investigación.

De igual forma, los resultados permitieron avanzar en los objetivos específicos del estudio. Por una parte, se reafirmó que el fraude constituye un problema vigente en los entornos de comercio electrónico y que su detección exige mecanismos cada vez más ágiles y precisos. Por otra, se identificó que los elementos mejor valorados del uso de la inteligencia artificial estuvieron relacionados con su capacidad analítica, su utilidad en la gestión del riesgo y su aporte al procesamiento oportuno de información. A ello se suma que, dentro de la variable dependiente, las dimensiones con medias más altas fueron rapidez del análisis y capacidad de anticipación, lo que sugiere que los participantes reconocen en estas herramientas un apoyo importante para identificar señales de riesgo y actuar con mayor oportunidad frente a posibles eventos de fraude.

En conjunto, los hallazgos aportan evidencia empírica relevante para comprender el papel de la inteligencia artificial en procesos de detección de riesgos de fraude dentro del comercio electrónico. Aunque los resultados deben interpretarse dentro de los límites de un diseño no experimental, correlacional y de una muestra no probabilística, el estudio ofrece una base útil para futuras investigaciones y para la reflexión sobre la incorporación de tecnologías inteligentes en contextos donde la seguridad digital, la prevención del fraude y la confianza en las transacciones resultan fundamentales. De esta manera, la investigación no solo permitió responder a los objetivos planteados, sino también destacar el valor estratégico que puede tener la inteligencia artificial en el fortalecimiento de los procesos de análisis y control en entornos digitales.

Referencias bibliográficas

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). *Fraud detection system: A survey*. *Journal of Network and Computer Applications, 68*, 90–113. https://https://doi:10.1016/j.jnca.2016.04.007

Adewumi, A. O., & Akinyelu, A. A. (2017). *A survey of machine-learning and nature-inspired based credit card fraud detection techniques*. *International Journal of System Assurance Engineering and Management, 8*(2), 937–953. https://doi:10.1007/s13198-016-0551-y

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:10.3390/app12199637

Almazroi, A. A. A., & Ayub, N. (2023). *Online payment fraud detection model using machine learning techniques*. *IEEE Access, 11*, 137188–137203. https://doi:10.1109/ACCESS.2023.3339226

Anita, Pontoh, G. T., & Pagalung, G. (2025). *Systematic literature review: Detection of financial fraud based on machine learning*. *UNIMAS Review of Accounting and Finance, 9*(1), 103–123. https://doi:10.33736/uraf.9939.2025

Casanova-Villalba, C. I., & Casanova-Villalba, L. A. (2024). Uso de análisis de datos avanzados para la detección de fraudes financieros. *Revista Científica Ciencia Y Método, 2*(3), 1–12. https://doi.org/10.55813/gaea/rcym/v2/n3/44

Casanova-Villalba, C. I., Herrera-Sánchez, M. J., & Almeida-Blacio, J. H. (2025). Aplicaciones de inteligencia artificial en la auditoría financiera contemporánea. *Revista Científica Ciencia Y Método, 3*(2), 30–43. https://doi.org/10.55813/gaea/rcym/v3/n2/3

Chen, C.-T., Lee, C., Huang, S.-H., & Peng, W.-C. (2024). *Credit card fraud detection via intelligent sampling and self-supervised learning*. *ACM Transactions on Intelligent Systems and Technology, 15*(2), Article 35, 1–29. https://doi:10.1145/3641283

Compagnino, A. A., Maruccia, Y., Cavuoti, S., Riccio, G., Tutone, A., Crupi, R., & Pagliaro, A. (2025). *An introduction to machine learning methods for fraud detection*. *Applied Sciences, 15*(21), 11787. https://doi:10.3390/app152111787

Dichev, A., Zarkova, S., & Angelov, P. (2025). *Machine learning as a tool for assessment and management of fraud risk in banking transactions*. *Journal of Risk and Financial Management, 18*(3), 130. https://doi:10.3390/jrfm18030130

Gruezo-Realpe, M. S., Torres-Galves, G. D., & Lascano-Rivera, S. B. (2026). Ciberseguridad predictiva basada en inteligencia artificial contra ataques generativos. *Revista Científica Enfoques Del Conocimiento, 3*(2), 16–28. https://doi.org/10.55813/gaea/revistacec/v3/n2/2

Herrera-Sánchez, M. J., & Casanova-Villalba, C. I. (2024). Inteligencia artificial y su impacto en la transformación de la gestión financiera. *Space Scientific Journal of Multidisciplinary, 2*(1), 52–64. https://doi.org/10.63618/omd/ssjm/v2/n1/43

Herrera-Sánchez, M. J., Casanova-Villalba, C. I., Concha-Ramirez, J. A., & López-Pérez, P. J.

(2024). Impacto de la inteligencia artificial en los procesos de auditoría contable. *Innova Science Journal, 2*(1), 1–14. https://doi.org/10.63618/omd/isj/v2/n1/28

Hurtado-Guevara, R. F., & Casanova-Villalba, C. I. (2022). La auditoría forense como herramienta para la detección de fraudes financieros en Ecuador. *Revista Científica Zambos, 1*(1), 33–50. https://doi.org/10.69484/rcz/v1/n1/52

Kanika, Singla, J., Bashir, A. K., Nam, Y., UI Hasan, N., & Tariq, U. (2022). *Handling class imbalance in online transaction fraud detection*. *Computers, Materials & Continua, 70*(2), 2861–2877. https://doi:10.32604/cmc.2022.019990

Li, Z., Hui, P., Zhang, P., Huang, J., Wang, B., Tian, L., Zhang, J., Gao, J., & Tang, X. (2021). *What happens behind the scene? Towards fraud community detection in e-commerce from online to offline*. In *Companion Proceedings of the Web Conference 2021* (pp. 105–113). https://doi:10.1145/3442442.3451147

Montalván-Vélez, C. L., Mogrovejo-Zambrano, J. N., Romero-Vitte, I. J., & Pinargote-Carrera, M. L. D. C. (2024). Introducción a la inteligencia artificial: Conceptos básicos y aplicaciones cotidianas. *Journal of Economic and Social Science Research, 4*(1), 173–183. https://doi.org/10.55813/gaea/jessr/v4/n1/93

Mutemi, A., & Bação, F. (2024). *E-Commerce fraud detection based on machine learning techniques: Systematic literature review*. *Big Data Mining and Analytics, 7*(2), 419–444. https://doi:10.26599/BDMA.2023.9020023

Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). *Application of artificial intelligence for fraudulent banking operations recognition*. *Big Data and Cognitive Computing, 7*(2), 93. https://doi:10.3390/bdcc7020093

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). *The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature*. *Decision Support Systems, 50*(3), 559–569. https://doi:10.1016/j.dss.2010.08.006

Odufisan, O. I., Abhulimen, O. V., & Ogunti, E. O. (2025). *Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria*. *Journal of Economic Criminology, 7*, 100127. https://doi:10.1016/j.jeconc.2025.100127

Pang, G., Shen, C., Cao, L., & van den Hengel, A. (2021). *Deep learning for anomaly detection: A review*. *ACM Computing Surveys, 54*(2), Article 38, 1–38. https://doi:10.1145/3439950

Plakandaras, V., Gogas, P., Papadimitriou, T., & Tsamardinos, I. (2022). *Credit card fraud detection with automated machine learning systems*. *Applied Artificial Intelligence, 36*(1), 2086354. https://doi:10.1080/08839514.2022.2086354

Rao, S. X., Zhang, S., Han, Z., Zhang, Z., Min, W., Chen, Z., Shan, Y., Zhao, Y., & Zhang, C. (2022). *xFraud: Explainable fraud transaction detection on heterogeneous graphs*. *Proceedings of the VLDB Endowment, 15*(3), 427–436. https://doi:10.14778/3494124.3494128

Razaque, A., Ben Haj Frej, M., Bektemyssova, G., Amsaad, F., Almiani, M., Alotaibi, A., Jhanjhi, N. Z., Amanzholova, S., & Alshammari, M. (2023). *Credit card-not-present fraud detection and prevention using big data analytics algorithms*. *Applied Sciences, 13*(1), 57. https://doi:10.3390/app13010057

Sánchez-Aguayo, M., Urquiza-Aguiar, L., & Estrada-Jiménez, J. (2021). *Fraud detection using the fraud triangle theory and data mining techniques: A literature review*. *Computers, 10*(10), 121. https://doi:10.3390/computers10100121

Sharma, P., Banerjee, S., Tiwari, D., & Patni, J. C. (2021). *Machine learning model for credit card fraud detection—A comparative analysis*. *The International Arab Journal of Information Technology, 18*(6), 789–796. https://doi:10.34028/iajit/18/6/6

Tong, G., & Shen, J. (2024). *Financial transaction fraud detector based on imbalance learning and graph neural network*. *Applied Soft Computing, 149*(Part A), 110984. https://doi:10.1016/j.asoc.2023.110984

Wijaya, M. G., Pinaringgi, M. F., Zakiyyah, A. Y., & Meiliana. (2024). *Comparative analysis of machine learning algorithms and data balancing techniques for credit card fraud detection*. *Procedia Computer Science, 245*, 677–688. https://doi:10.1016/j.procs.2024.10.294

Xiang, S., Zhu, M., Cheng, D., Li, E., Zhao, R., Ouyang, Y., Chen, L., & Zheng, Y. (2023). *Semi-supervised credit card fraud detection via attribute-driven graph representation*. *Proceedings of the AAAI Conference on Artificial Intelligence, 37*(12), 14557–14565. https://doi:10.1609/aaai.v37i12.26702

Xuan, S., Liu, G., Li, Z., Zheng, L., Wang, S., & Jiang, C. (2018). *Random forest for credit card fraud detection*. In *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)* (pp. 1–6). https://doi:10.1109/ICNSC.2018.8361343

Zhang, G., Li, Z., Huang, J., Wu, J., Zhou, C., Yang, J., & Gao, J. (2022). *EFraudCom: An e-commerce fraud detection system via competitive graph neural networks*. *ACM Transactions on Information Systems, 40*(3), Article 47, 1–29. https://doi:10.1145/3474379