Modelado Predictivo Basado en Inteligencia Artificial y Generación de Datos Sintéticos para la Prevención Temprana del Riesgo de Fraude en el Sector Financiero Colombiano

David Sebastián Barrera Gaona

Brandon Santiago Vargas Guerrero

Sophia Jaimes Clavijo

Universidad Ean

Facultad de Ingeniería / Ingeniería de Sistemas

Bogotá, Colombia

19/10/2025

Resumen

El presente proyecto desarrolla un modelo predictivo apoyado en inteligencia artificial (IA) y generación de datos sintéticos para fortalecer la detección automatizada de fraudes financieros en el sistema bancario colombiano. Ante el aumento de transacciones digitales y el crecimiento de los delitos cibernéticos, se plantea una solución que permita mejorar la capacidad de respuesta de las entidades financieras mediante el uso de algoritmos de aprendizaje supervisado entrenados con datos no sensibles.

El modelo busca superar el desequilibrio entre operaciones legítimas y fraudulentas, preservando la privacidad y el cumplimiento normativo. A través de un enfoque exploratorio, se desarrolla un prototipo funcional en entornos simulados, evaluado mediante métricas de desempeño propias del aprendizaje automático.
El proyecto incorpora consideraciones legales, éticas y técnicas, y se enmarca en la Estrategia Nacional de Inteligencia Artificial de Colombia, contribuyendo al fortalecimiento de la seguridad digital y al desarrollo de soluciones tecnológicas sostenibles en el ámbito financiero.

Palabras clave: Aprendizaje automático, detección de anomalías, modelado predictivo, ciberseguridad financiera, innovación tecnológica, regulación de datos, simulación bancaria.

Abstract

This project develops a predictive model supported by artificial intelligence (AI) and synthetic data generation to enhance the automated detection of financial fraud within the Colombian banking system. In light of the growing volume of digital transactions and cybercrime incidents, it proposes a solution to improve financial institutions' responsiveness through supervised learning algorithms trained on non-sensitive, artificially generated data.

The model aims to address the imbalance between legitimate and fraudulent operations while ensuring privacy and regulatory compliance. Using an exploratory approach, a functional prototype is implemented in simulated environments and evaluated through performance metrics common in machine learning.

The project integrates legal, ethical, and technical considerations and aligns with Colombia's National Artificial Intelligence Strategy, contributing to stronger digital security and the advancement of sustainable technological innovation in the financial sector.

Keywords: Machine learning, anomaly detection, predictive modeling, financial cybersecurity, technological innovation, data governance, banking simulation.

Contenido

Lista de Figuras

Modelo Predictivo Basado en Inteligencia Artificial y Datos Sintéticos para la Detección de Fraudes en el Sector Financiero Colombiano

Introducción

En los últimos años, la Inteligencia Artificial (*IA*) se ha consolidado como una herramienta esencial en el sector financiero, desempeñando papeles importantes que van desde la evaluación del riesgo crediticio hasta la detección de fraudes. En Colombia, esta adopción se ha vuelto notable y según el Informe de Asobancaria (2024), el 73 % de las entidades financieras ya integran tecnologías de IA en sus operaciones (C-Level, 2024). Estas tecnologías han contribuido a mejorar la eficiencia operativa, automatizar tareas y reforzar la inclusión financiera (Colcob, 2024; Siglo, 2024).

Sin embargo, estas nuevas tecnologías también han traído retos significativos como el revelado por la República (2023) en donde los ataques al sistema financiero aumentaron un 40 %, con modalidades como *phishing, smishing* y fraude de identidad. Así mismo, la Superintendencia Financiera de Colombia registró 324 829 quejas por fraudes en el sector financiero en el año 2024 (BusinessCol, 2024; colombiano, 2024). Ante este panorama, la detección temprana de fraudes se ha convertido en una prioridad, razón por la cual cerca del 70 % de los bancos colombianos ya emplea sistemas automatizados que combinan machine learning y análisis de datos para identificar comportamientos sospechosos y amenazas emergentes (EBizLatam, 2024; ITSitio, 2024).

Por otro lado, uno de los grandes desafíos en la detección de fraudes es el desequilibrio de los datos, debido a que la mayoría de los casos fraudulentos suelen representar estadísticamente solo entre el 7 % y el 10 %, siendo esto una gran dificultan para realizar un entrenamiento efectivo de los modelos de *IA*. De modo que, para superar estos obstáculos, los datos sintéticos ofrecen una solución prometedora, ya que son generados artificialmente por algoritmos que imitan patrones reales sin comprometer

datos sensibles, lo que permite entrenar modelos con mayor robustez y privacidad (Syntho, 2023).

En el caso colombiano, el fraude financiero evoluciona constantemente hacia modalidades más complejas. Una de ellas es el uso de identidades sintéticas fraudulentas, que combinan información real con datos inventados y logran pasar inadvertidas durante largos periodos, ocasionando pérdidas significativas para las entidades financieras (Latinpyme, 2024). Aunque este tipo de fraude no está directamente relacionado con la generación de datos sintéticos como herramienta tecnológica, muestra cómo la manipulación de datos puede convertirse en un riesgo si no se implementan mecanismos de detección avanzados.

En respuesta a estos desafíos, este proyecto propone un modelo de IA reforzado mediante datos sintéticos para prever los fraudes en clientes del sector bancario colombiano; mediante la generación controlada de datos sintéticos permitirá abordar el problema del desequilibrio, mejorar la privacidad, y fortalecer la capacidad del modelo para identificar patrones fraudulentos emergentes y sofisticados. Este documento guiará al lector en la comprensión y contextualización del proyecto. En ellas se abordan la problemática identificada, los objetivos propuestos, la justificación del estudio y conceptos teóricos, junto con los antecedentes más relevantes, que en conjunto brindan el marco necesario para entender el alcance y propósito de la investigación.

Antecedentes

La prevención temprana del fraude financiero se ha convertido en un desafío de primera línea en el sector, pues evitar que los estafadores consumen sus delitos es fundamental para garantizar la seguridad de las cuentas y el cumplimiento normativo de las instituciones financieras. (*Detección Del Fraude Con IA En El Sector Bancario* | *IBM*, n.d.). Para afrontar este desafío, resulta imprescindible revisar detalladamente los antecedentes académicos y empresariales relacionados, ya que una exploración exhaustiva de la literatura existente y de casos previos permite situar el estudio en su contexto adecuado y construir sobre el conocimiento acumulado.(Guirao Goris, 2015). Dicho de otro modo, examinar investigaciones previas y experiencias de la industria proporciona las bases conceptuales y prácticas sobre las cuales se fundamenta el presente trabajo, evitando duplicar esfuerzos y orientando el desarrollo de soluciones innovadoras de manera informada. Este proyecto de grado, en particular, se plantea en la intersección de la inteligencia artificial, la generación de datos sintéticos y la detección de fraude financiero, por lo cual cobra aún mayor relevancia partir de antecedentes sólidos en cada uno de estos ámbitos y en su convergencia.

En efecto, la IA aplicada al fraude ha demostrado ser una herramienta clave para identificar patrones anómalos en grandes volúmenes de transacciones. Los modelos predictivos basados en *machine learning* pueden analizar conjuntos masivos de datos y aprender a reconocer la diferencia entre actividades sospechosas y transacciones legítimas, ayudando a identificar posibles riesgos de fraude que un analista humano podría pasar por alto (*Detección Del Fraude Con IA En El Sector Bancario* | *IBM*, n.d.). Gracias a esta capacidad, es posible detectar irregularidades de forma más temprana, antes de que se concreten pérdidas significativas, reforzando así la mitigación proactiva

de riesgos financieros. Ahora bien, la aplicación de la IA enfrenta retos importantes en este dominio, como el marcado desequilibrio de clases (los casos de fraude son mucho menos frecuentes que las transacciones normales) y las estrictas restricciones de privacidad que limitan el uso de datos reales. En respuesta a ello, la generación de datos sintéticos ha emergido como una solución complementaria de gran utilidad: permite crear datos artificiales con las mismas propiedades estadísticas que los datos financieros reales, lo que ayuda a superar esos obstáculos al aportar conjuntos de entrenamiento balanceados y respetar la confidencialidad de la información sensible (*Detección de Fraudes En Banca Con Datos Sintéticos | Syntho*, n.d.). La sinergia de ambas tecnologías IA y datos sintéticos se perfila, así como una estrategia prometedora para robustecer los sistemas de detección de fraude. No en vano, en la industria bancaria ya se observa que el uso de datos sintéticos potencia la eficacia de los modelos de IA, mejorando las técnicas de detección de actividades fraudulentas y el análisis de riesgos en entornos financieros (*Mercado de Generación de Datos Sintéticos | Análisis de Pronóstico [2030]*, n.d.).

Considerando lo anterior, la presente revisión de antecedentes se ha organizado en dos categorías principales. En primer lugar, se examinan las investigaciones académicas recientes (publicadas aproximadamente entre 2019 y 2024) que abordan el uso de inteligencia artificial y datos sintéticos en la detección y prevención del fraude financiero. En segundo lugar, se analizan diversos casos de implementación empresarial e institucional, tanto en Colombia como en el ámbito internacional, que ilustran cómo estas tecnologías se han aplicado en la práctica para combatir el fraude. Cabe destacar que el análisis se enfoca en proyectos desarrollados en los últimos cinco años (2019–2024), un periodo en el que el campo ha experimentado un avance vertiginoso. Este recorte temporal garantiza que se incluyan las tendencias más actuales y relevantes: de

hecho, la adopción de soluciones de IA para la detección de fraude se ha acelerado notablemente en este lustro, al punto de que nueve de cada diez bancos ya emplean inteligencia artificial para identificar actividades fraudulentas, incorporándola masivamente en sus operaciones en los años recientes (*Tendencias de Fraude Con IA 2025: Los Bancos Contraatacan* | *Feedzai*, n.d.). En suma, al revisar tanto la literatura académica más reciente como las experiencias empresariales e institucionales contemporáneas, se sientan las bases teóricas y prácticas que orientan y respaldan el desarrollo de este proyecto de grado.

Proyectos académicos recientes (2019-2024)

- (2024) Revisión de literatura sobre ML en fraude financiero Hernández Aros et al. (Colombia). Una revisión sistemática de 104 publicaciones (2012–2023) analizó técnicas de machine learning para detectar fraudes financieros. Concluyó que la mayoría de los estudios se enfocan en detección de fraude con tarjetas de crédito usando datos reales, mientras que el uso de datos sintéticos ha sido muy limitado (empleado en menos del 7% de los conjuntos de datos). Destaca además que países como China, India, Arabia Saudita y Canadá lideran en publicaciones, mientras Latinoamérica tiene pocas contribuciones. (Hernandez Aros et al., 2024a)
- (2025) *Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications – Yisong Chen et al.* (EE. UU./China). Este estudio presentó una revisión sistemática de 57 trabajos (2019–2024) sobre Deep learning aplicado al fraude financiero. Identificó avances en modelos como redes neuronales convolucionales (CNN), LSTM y Transformers, efectivos en dominios como transacciones de tarjeta de crédito, seguros y auditorías financieras. Se evaluaron métricas de desempeño (precisión, recall, AUC) y se exploraron temas clave: la privacidad de datos, mejora

en ingeniería de *features* y preprocesamiento, así como desafíos como el desequilibrio de datos, la interpretabilidad de modelos y consideraciones éticas. La revisión resalta oportunidades emergentes, por ejemplo, la automatización y técnicas preservadoras de privacidad (integración con blockchain, etc.), a la vez que identifica brechas críticas y direcciones futuras para la investigación en IA antifraude. (Chen et al., 2025)

- (2025) *Improvement of Bank Fraud Detection Through Synthetic Data Generation with Gaussian Noise – Becerra-Suarez et al.* (Perú). Investigación enfocada en el problema de desbalance de clases en fraudes bancarios. Propone un método de aumentación sintética añadiendo ruido Gaussiano a los datos, comparándolo con técnicas tradicionales de sobre muestreo como SMOTE y ADASYN. Al inyectar perturbaciones controladas, lograron mejorar la precisión de los modelos de detección de fraude en un conjunto de transacciones, superando a SMOTE/ADASYN. Los resultados muestran que esta síntesis con ruido preserva mejor la autenticidad de los datos y reduce falsos positivos, optimizando el rendimiento de clasificadores en datos financieros desbalanceados. Se sugiere que las instituciones financieras podrían adoptar este enfoque para disminuir alertas fraudulentas falsas y costos operativos, sin comprometer la detección de patrones de fraude poco frecuentes. (Becerra-Suarez et al., 2025)
- (2024) *Fraud Diffuse: Diffusion-aided Synthetic Fraud Augmentation for Improved Fraud Detection – Roy, Tiwari, Pandey (Mastercard, India)*. Trabajo presentado en la conferencia ACM *AI in Finance 2024* que introduce el uso de modelos de difusión generativa para la detección de fraude. FraudDiffuse extiende estos modelos para generar transacciones fraudulentas sintéticas, abordando el desbalance extremo entre operaciones legítimas y fraudulentas. Al entrenar la IA con patrones sintéticos

de fraude, el método permite captar esquemas emergentes y mejorar la detección frente a tácticas cambiantes de defraudadores. En paralelo, otro estudio (*FraudDDPM, 2024*) aplicó un enfoque similar con modelos de difusión, mostrando también mejoras en el rendimiento de detección al sintetizar tanto datos normales como fraudulentos por separado. (Roy et al., 2024). Estas propuestas evidencian el creciente interés académico por datos sintéticos generados con IA (GAN, difusión, etc.) para reforzar sistemas antifraude.

Casos de aplicación empresarial e institucional (2019-2024)

- (2022) *BBVA + Featurespace (España/Global)* – El banco BBVA implementó la plataforma ARIC Risk Hub de Featurespace, basada en aprendizaje automático adaptativo, como solución antifraude de última generación. Esta herramienta analiza en tiempo real transacciones de tarjetas, pagos y originaciones en todos los países donde opera BBVA. Con la IA, BBVA logró aumentar la eficacia en detección y reducir la fricción por falsos positivos, mejorando la experiencia del cliente. (*BBVA y Featurespace Colaboran En La Lucha Antifraude - Featurespace*, n.d.). En un comunicado de 2023, BBVA reportó que, tras 3 años de estrategia holística antifraude apoyada en tecnología avanzada, consiguió prevenir hasta un 75% del fraude dirigido a sus clientes, reduciendo las pérdidas por fraude en ~40% pese al crecimiento de ataques. (*BBVA Refuerza Sus Capacidades de Prevención de Fraude*, n.d.). La colaboración con proveedores como Featurespace ha sido clave para monitorear *todas* las transacciones en tiempo real y estar un paso adelante de los defraudadores
- (2023) *Nubank – "Alerta Estafa" (Brasil/México)* – La Fintech latinoamericana Nubank desarrolló una funcionalidad llamada *Alerta Estafa* para proteger a sus usuarios de fraudes en tiempo real. Esta solución, lanzada en México, se basa en herramientas

de IA y *machine learning* que aprenden los comportamientos transaccionales normales de cada cliente. Cuando el sistema detecta alguna anomalía o actividad inusual en una transferencia –por ejemplo, montos o patrones no habituales– lanza de inmediato una alerta al usuario. Según la directora de tecnología de Nu México, esta capa inteligente analiza literalmente *todas* las transacciones al instante e identifica cualquier operación sospechosa utilizando múltiples algoritmos (incluida IA), lo que les ha permitido reaccionar preventivamente ante intentos de fraude en su base de millones de clientes. (Fintech: La-Inteligencia Artificial-Las-Blinda Del-Fraude Digital- Grupo Milenio, n.d.)

- (2023) Citigroup (Américas) – El banco global Citi informó sobre el impacto tangible de la IA en sus sistemas antifraude. En 2025, Driss Temsamani (líder digital de Citi Américas) reveló que tras ~18 meses de implementar estrategias de detección con herramientas digitales e IA, los intentos de fraude en sus operaciones se redujeron en un 50%. te resultado demuestra cómo los grandes bancos están incorporando algoritmos de *machine learning* en procesos internos para identificar patrones sospechosos y bloquear proactivamente transacciones fraudulentas. Citi atribuye esta mejora significativa a la analítica avanzada, capaz de cribar enormes volúmenes de datos y *scores* de riesgo en tiempo real, algo inviable con métodos manuales tradicionales. (*Fintech: La-Inteligencia Artificial-Las-Blinda Del-Fraude Digital- Grupo Milenio*, n.d.-b)
- (2023) Poste Italiane + SAS (Italia) – El servicio postal italiano (que opera también como institución financiera con 35 millones de clientes) reforzó su sistema antifraude con analítica avanzada e IA de SAS. Según Raffaele pánico (jefe de fraude en Poste Italiane), el uso de técnicas de *machine learning* aportó “una capa de inteligencia” para identificar situaciones de riesgo con mayor rapidez. Tras modernizar su

plataforma, Poste Italiane logró reducir los falsos positivos en un 40% e incrementar en más de 20% su capacidad de gestionar anomalías. En el segmento de pagos electrónicos, reportaron que la tasa de fraude se redujo 50% en solo tres meses tras desplegar estas soluciones de IA, a pesar de que globalmente el fraude en línea venía creciendo ~90% en dos años. Este caso ejemplifica cómo una empresa centenaria adoptó IA en tiempo real para proteger a sus clientes frente a fraudes y abusos en pagos digitales. (*¿Esperanza o Peligro? La IA Generativa Ocupa Un Lugar Central La Semana Contra El Fraude 2023.* | *SAS*, n.d.)

- (2024) *Departamento del Tesoro de EE.UU. – Office of Payment Integrity (Estados Unidos)*. Un caso institucional destacado es el del Tesoro estadounidense, que implementó procesos mejorados con IA para combatir fraude en pagos gubernamentales. En FY2024, la Oficina de Integridad de Pagos del Tesoro empleó modelos de *machine learning* para detectar y prevenir fraudes, especialmente en cheques del gobierno. Los resultados fueron notables: se logró prevenir y recuperar más de $4.000 millones de USD en pagos fraudulentos o indebidos durante el año fiscal 2024, comparado con $652 millones el año previo. En particular, la incorporación de algoritmos ML para identificar rápidamente cheques sospechosos permitió recuperar aproximadamente $1.000 millones en pagos fraudulentos que de otro modo se habrían perdido. Además, ampliando análisis de riesgo y priorización de transacciones, se bloquearon proactivamente unos $2.500 millones en intentos de fraude antes de que se consumaran. Este ejemplo demuestra el potencial de la IA a escala gubernamental: mediante análisis masivo de datos de pagos, se detectaron a tiempo patrones anómalos en múltiples agencias, maximizando la salvaguarda de fondos públicos. (*Treasury Announces Enhanced Fraud Detection Processes, Including Machine Learning AI, Prevented and Recovered Over $4 Billion in Fiscal*

Year 2024 | *U.S. Department of the Treasury*, n.d.). La experiencia del Tesoro resalta que, con las herramientas y datos adecuados, incluso programas estatales tradicionales pueden beneficiarse de IA avanzada para mitigar fraudes en *near real-time.*

Definición del problema

En el contexto del sistema financiero colombiano, el fraude representa una amenaza creciente y compleja que pone en riesgo tanto a las entidades como a los usuarios. A continuación, se exponen los principales elementos del problema con su respectiva documentación:

La masiva adopción de canales digitales por parte de entidades y consumidores en Colombia ha generado un entorno propicio para el fraude. Por ejemplo, se reporta que la proporción de transacciones digitales ha crecido drásticamente, lo que convierte al canal digital en un “campo de juego” para los defraudadores (Asobancaria, 2023). Los informes señalan un aumento de intentos de fraude digital del 859 % en tres años, impulsado por un incremento de más del 960 % del volumen de transacciones digitales (T. Colombia, 2023).

Estos datos evidencian que, aun cuando solo una pequeña fracción de las transacciones resultan en fraude, el riesgo absoluto y el costo potencial están aumentando. El impacto económico del fraude va más allá del valor nominal de la transacción comprometida. Un estudio señala que en Colombia el 65 % de las organizaciones reportaron un aumento del fraude en los últimos 12 meses y que, por cada peso perdido en transacciones fraudulentas, las instituciones enfrentan costos de aproximadamente 3,76 veces ese monto (*Cada Peso Perdido Por Fraude En Colombia*

Cuesta a Las Empresas 3,76 Veces Más, Según El Estudio "El Verdadero Costo Del Fraude En América Latina," n.d.).

Asimismo, en el comercio electrónico, se registró que el 7,1 % de las transacciones durante una temporada de descuentos fueron consideradas sospechosas de fraude en Colombia (frente al 4,6 % global) (T. Colombia, 2024). Estos indicadores muestran que el fraude no solo afecta la confianza del cliente, sino que incrementa los costos operativos, de control y reputacionales en el sector financiero

Las investigaciones académicas y los reportes sectoriales apuntan a que las técnicas de detección de fraude tradicionales, basadas en reglas fijas o alertas retrospectivas, ya no son suficientes ante la complejidad y sofisticación de las nuevas amenazas (como la suplantación de identidad, *deepfakes*, apertura de cuentas fraudulentas) *(Tarazona Nieto et al., n.d.)*. Por ejemplo, más de 25,1 % de los intentos de fraude digital ocurrieron durante la apertura de cuentas en Colombia, lo cual indica que el fraude se infiltra tempranamente en el ciclo del cliente (Mahecha, 2024).

Ante estos hechos, surge la necesidad de modelos predictivos más avanzados con inteligencia artificial, generación de datos sintéticos para anticipar y mitigar el fraude de forma proactiva. Así pues, Colombia alcanzó un índice de preocupación por fraude bancario y robo de identidad de 216 puntos (sobre 300), por encima del promedio mundial (173) según un estudio de Unisys (*Colombia Es El País Más Preocupado Por El Fraude Bancario y Robo de Identidad, Según Nuevo Índice de Seguridad de Unisys,* 2018). Aunque el sector financiero colombiano utiliza sistemas de control de fraude, la adopción de aprendizaje automático y modelos avanzados aún es limitada *(Tarazona Nieto et al., n.d.)*.

Dado lo anterior, el problema de investigación se puede expresar que el sector financiero colombiano, las crecientes transacciones digitales y la sofisticación de los

esquemas de fraude están generando pérdidas económicas y erosionando la confianza, mientras los métodos tradicionales de detección resultan insuficientes por lo que se requiere diseñar un modelo predictivo basado en inteligencia artificial y generación de datos sintéticos que permita la prevención temprana y la segmentación del riesgo de fraude.

Objetivos

Objetivo general

Diseñar un modelo predictivo basado en inteligencia artificial y generación de datos sintéticos que permita la prevención temprana del riesgo de fraude en el sector financiero colombiano, integrando criterios técnicos, estadísticos y de gestión del riesgo que puedan servir como base para un prototipo mínimo viable (MVP) de detección proactiva.

Objetivos específicos

Analizar el contexto del fraude financiero en Colombia y las técnicas predictivas aplicadas en la detección y prevención de fraudes en el sector bancario, destacando el papel de la inteligencia artificial y los datos sintéticos.

Definir la arquitectura conceptual y los componentes metodológicos del modelo predictivo, incorporando algoritmos de inteligencia artificial y estrategias de generación de datos sintéticos.

Evaluar la viabilidad del modelo predictivo propuesto mediante la simulación de escenarios sintéticos de fraude y formular una propuesta de MVP que demuestre su aplicabilidad teórica en el contexto financiero colombiano.

Justificación

La creciente digitalización de los servicios financieros en Colombia ha transformado profundamente la dinámica del sector, impulsando la eficiencia y la inclusión, pero también exponiendo nuevas vulnerabilidades. Según la Asociación Bancaria de Colombia Asobancaria (2023) más del 99 % de las transacciones financieras se realizan actualmente por medios digitales, un dato que evidencia la magnitud del cambio tecnológico, pero que también refleja la escala potencial de exposición al fraude digital. Aunque la proporción de incidentes efectivos sigue siendo baja, el número de intentos de fraude ha aumentado un 859 % en los últimos tres años, impulsado por la masificación de los canales electrónicos y el crecimiento de los pagos digitales (T. Colombia, 2023).

Esta situación plantea un desafío urgente: los sistemas tradicionales de monitoreo y detección de fraudes basados en reglas fijas, revisión manual o análisis retrospectivo han demostrado limitaciones frente a los esquemas dinámicos y adaptativos que emplean los defraudadores. Por ello, la inteligencia artificial (IA) emerge como una herramienta indispensable para la detección temprana de patrones anómalos y la segmentación proactiva del riesgo financiero. No obstante, el desarrollo de estos modelos enfrenta un obstáculo recurrente: la falta de acceso a grandes volúmenes de datos reales, debido a las restricciones éticas, legales y de confidencialidad en el manejo de información financiera sensible.

Ante este panorama, el presente proyecto propone el modelado predictivo basado en IA y generación de datos sintéticos como una alternativa innovadora, capaz de reproducir comportamientos realistas sin comprometer la privacidad de los usuarios. Este enfoque no solo responde a una necesidad práctica de la banca, sino que también aporta

valor teórico y metodológico al campo de la inteligencia artificial aplicada al riesgo financiero.

Desde una perspectiva científica, este proyecto contribuye a la consolidación del conocimiento en la intersección entre aprendizaje automático (machine learning), síntesis de datos y gestión del riesgo financiero. La literatura reciente demuestra que el uso de datos sintéticos puede mejorar la calidad del entrenamiento de los modelos de IA, especialmente en contextos donde los datos reales son escasos o desbalanceados (Qi & Su, 2025).

Esto es particularmente relevante en la detección de fraudes, donde los eventos fraudulentos representan una minoría estadística extrema, lo que genera un sesgo en los modelos tradicionales supervisados.

Asimismo, el proyecto se alinea con investigaciones emergentes sobre el papel de la IA en la optimización de la inversión corporativa y la reconstrucción de ecosistemas financieros digitales (Liu & Hu, 2025). Estas investigaciones sugieren que la IA no solo detecta anomalías, sino que también fortalece los mecanismos de supervisión y reduce las restricciones de financiamiento en sistemas financieros complejos.

En este sentido, la generación de datos sintéticos se convierte en una herramienta de experimentación científica que permite simular escenarios financieros de riesgo controlado, facilitando la calibración y validación de modelos predictivos en entornos académicos sin violar la confidencialidad bancaria. El proyecto, por tanto, amplía la frontera del conocimiento en el uso ético y responsable de la IA, y refuerza la pertinencia de los métodos híbridos entre análisis estadístico, simulación y aprendizaje automatizado como pilar de la investigación moderna en economía digital.

Finalmente, se destaca la posibilidad de integrar técnicas complementarias como el procesamiento de lenguaje natural (NLP) para el análisis de reportes financieros y transacciones textuales, lo cual amplía el alcance interdisciplinar del estudio. Esto permitiría, en futuras fases, el desarrollo de modelos semánticos que detecten fraudes no solo por patrones numéricos, sino también por análisis contextual de las comunicaciones o solicitudes transaccionales (Qatawneh, 2024).

Desde el punto de vista tecnológico, el proyecto se sitúa en la convergencia de tres tendencias globales. Automatización inteligente de la gestión de riesgos, Modelado sintético de datos financieros, y Desarrollo de sistemas de alerta temprana basados en IA. Estas tendencias representan el núcleo de la transformación digital del sistema financiero, y su adopción en Colombia marca una diferencia competitiva frente a otros mercados emergentes. Las entidades financieras que implementan modelos de IA para la detección de fraudes no solo reducen pérdidas económicas, sino que mejoran su reputación y confianza institucional ante los consumidores.

Un estudio de LexisNexis *Cada Peso Perdido Por Fraude En Colombia Cuesta a Las Empresas 3,76 Veces Más, Según El Estudio El Verdadero Costo Del Fraude En América Latina (n.d.)*, señala que los costos indirectos asociados al fraude como la pérdida de clientes, gastos legales y tiempo de personal pueden alcanzar hasta 3,76 veces el monto directo defraudado. Frente a esta problemática, la capacidad predictiva de la IA permite identificar anomalías en tiempo real y clasificar usuarios según su nivel de riesgo, priorizando las intervenciones de forma más eficiente que los sistemas convencionales.

Por otra parte, el uso de datos sintéticos ofrece una solución tecnológica para superar las barreras de confidencialidad y protección de datos personales, al generar bases artificiales que preservan la estructura estadística y la correlación de las variables

reales. De esta forma, las instituciones pueden entrenar y evaluar modelos predictivos sin exponer información sensible, contribuyendo al cumplimiento de las normas de protección de datos (como la Ley 1581 de 2012 en Colombia).

El proyecto, además, responde a la Estrategia Nacional de Inteligencia Artificial de Colombia del G. de Colombia & VIDA (n.d.), la cual promueve el uso responsable y seguro de la IA en sectores estratégicos, entre ellos el financiero. Al desarrollar un modelo teórico y un MVP conceptual, esta investigación aporta conocimiento aplicable a futuros sistemas de ciberseguridad bancaria y analítica avanzada de riesgo.

Desde el plano social, la investigación contribuye a la protección del patrimonio de los ciudadanos y al fortalecimiento de la confianza digital en las instituciones financieras; en un país donde más del 40 % de los usuarios ha sido víctima o ha intentado serlo de fraude digital (T. Colombia, 2023). El diseño de herramientas predictivas no solo tiene un impacto económico, sino también psicológico y social, al reducir la sensación de vulnerabilidad y desconfianza hacia la banca digital.

El desarrollo de un modelo de prevención temprana permite a las entidades anticipar comportamientos sospechosos antes de que se materialicen las pérdidas, generando entornos financieros más seguros y estables. Esto, a su vez, fortalece la inclusión financiera, pues una mayor seguridad promueve que nuevos usuarios adopten servicios digitales con confianza.

En el ámbito institucional, el proyecto impulsa la formación de capital humano especializado en inteligencia artificial aplicada a la seguridad financiera, un campo en rápida expansión que requiere profesionales capaces de integrar conocimientos técnicos, éticos y regulatorios. Así, el trabajo se alinea con los principios de la Universidad EAN, orientada hacia la solución de problemas reales y el desarrollo sostenible mediante la innovación tecnológica y social.

Finalmente, desde la dimensión económica, el impacto potencial de la reducción del fraude se traduce en un aumento de la estabilidad del sistema financiero, disminución de costos de cumplimiento y mejora de la percepción país en materia de ciberseguridad. Según el *Global Risks Report 2024* | *World Economic Forum (2025)*, los países que invierten en modelos predictivos de riesgo logran una reducción promedio del 25 % en pérdidas por fraude financiero en menos de cinco años, lo que refuerza la pertinencia económica de este tipo de investigaciones.

En síntesis, este proyecto representa una respuesta científica, tecnológica y social ante uno de los retos más urgentes del sistema financiero contemporáneo: la prevención del fraude digital. Al integrar la inteligencia artificial con la generación de datos sintéticos, la investigación propone una ruta viable, ética y sostenible para fortalecer la seguridad financiera del país.

Su valor radica no solo en la construcción de un modelo teórico replicable, sino también en la generación de conocimiento aplicable a políticas de ciberseguridad, educación digital y transformación bancaria. En consecuencia, esta propuesta contribuye tanto al avance académico del campo de la IA aplicada como al bienestar económico y social de los ciudadanos colombianos.

Análisis de Requerimientos

El desarrollo exitoso de este proyecto depende de la correcta definición y cumplimiento de los requerimientos funcionales y técnicos que garanticen la viabilidad, precisión y aplicabilidad del modelo de inteligencia artificial propuesto. Para ello, se establece un análisis detallado que permita delimitar el alcance de la solución, evitar desviaciones en etapas avanzadas y asegurar que el diseño responda a las necesidades reales del entorno bancario colombiano.

Intención del producto

El objetivo principal del producto es diseñar un modelo de IA capaz de detectar patrones de fraude financiero en transacciones bancarias, utilizando datos sintéticos como fuente de entrenamiento. Este enfoque busca preservar la privacidad de los datos reales, facilitar la experimentación y garantizar la escalabilidad del sistema en diferentes instituciones financieras. El modelo debe ser capaz de identificar anomalías en tiempo real, adaptarse a nuevas estrategias de fraude y ofrecer métricas de precisión confiables. En este sentido, el uso de datos sintéticos con técnicas de aprendizaje federado ha demostrado ser eficaz para mantener la privacidad sin sacrificar el rendimiento del modelo, como lo plantea el enfoque FedER (Pennisi et al., 2024), que permite entrenar modelos distribuidos sin compartir datos sensibles entre nodos.

Verificación de parámetros de diseño

Para validar la propuesta del modelo, se establecerán parámetros de referencia como:

- Precisión y recall en la detección de fraudes.
- Tasa de falsos positivos y negativos.
- Tiempo de respuesta ante transacciones sospechosas.
- Capacidad de adaptación a nuevos datos sintéticos.
- Robustez frente a ataques adversariales o manipulación de datos.

Estos parámetros serán evaluados mediante pruebas controladas en entornos simulados, utilizando técnicas de validación cruzada y métricas estándar del aprendizaje supervisado. Además, se considerará el impacto de herramientas complementarias como el procesamiento de lenguaje natural (NLP), que ha demostrado mejorar la eficiencia en

la detección de fraudes dentro de sistemas contables automatizados (Qatawneh, 2024). La integración de NLP puede fortalecer la capacidad del sistema para interpretar descripciones textuales de transacciones o justificar alertas de riesgo.

Estimación de características de diseño

El modelo debe cumplir con ciertas especificaciones técnicas que aseguren su rendimiento y aplicabilidad:

Potencia computacional: Se plantea el acceso a entornos de simulación con capacidad de procesamiento paralelo (GPU/CPU) para entrenar redes neuronales o algoritmos de clasificación.

Desempeño algorítmico: Se estiman tiempos de entrenamiento inferiores a 2 horas por lote de datos, y tiempos de inferencia menores a 1 segundo por transacción.

Escalabilidad: El sistema debe poder integrarse con plataformas bancarias existentes mediante APIs o módulos de interoperabilidad.

Seguridad: Se contemplan mecanismos de cifrado y control de acceso para proteger la integridad del modelo y los datos sintéticos utilizados.

El enfoque FedER demuestra que es posible lograr modelos generalizables y robustos mediante el uso de datos sintéticos generados por redes adversariales (GANs), manteniendo altos niveles de privacidad y rendimiento incluso en entornos distribuidos y no homogéneos.

Este análisis inicial permite establecer una base sólida para el diseño del sistema, anticipar riesgos técnicos y garantizar que el producto final cumpla con los objetivos planteados en el tiempo previsto.

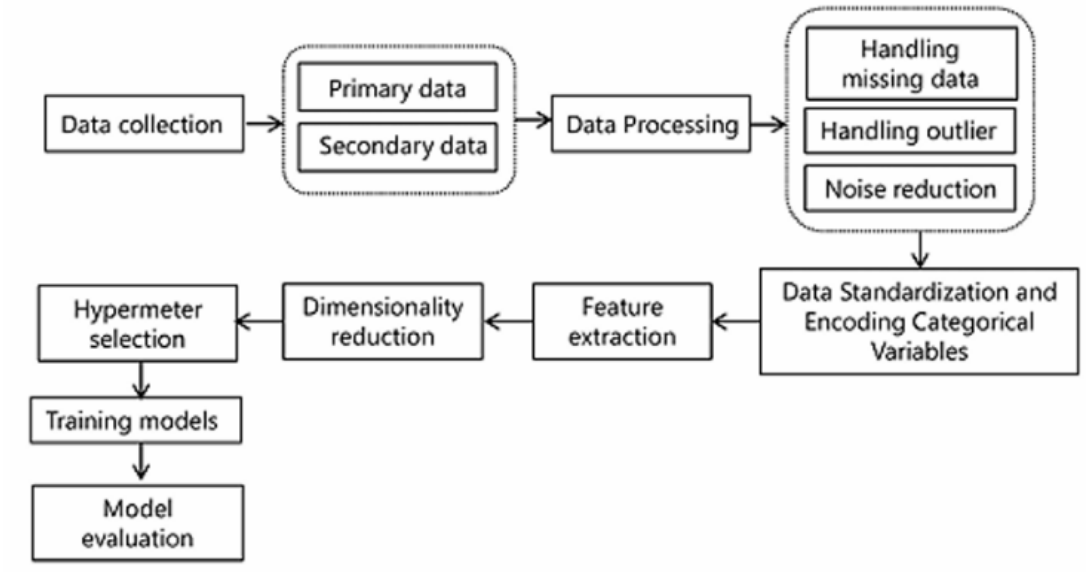
Marco Teórico

La detección de fraudes bancarios es un problema complejo que impacta tanto a empresas como a clientes. Estudios recientes indican que más de la mitad de las empresas a nivel global han sufrido algún fraude financiero. En América Latina, cerca del 32 % de las organizaciones reportaron incidentes fraudulentos en los últimos años. Estas cifras reflejan que los métodos tradicionales –basados en reglas definidas manualmente– han perdido eficacia ante la creciente sofisticación del frauden. Por ello, en las últimas décadas las instituciones financieras han invertido en sistemas basados en aprendizaje automático (ML) e inteligencia artificial (IA) para automatizar la detección de anomalías en transacciones (Phishing, robo de identidad, apropiación de cuentas, transacciones fraudulentas, etc.). Según la literatura, los modelos supervisados de ML –como árboles de decisión, regresión logística, máquinas de soporte vectorial y redes neuronales– han sido los más empleados, reportando precisiones superiores al 90 % en estudios de casos (por ejemplo, con detección de fraudes en tarjetas de crédito). En efecto, una revisión sistemática reciente indicó que técnicas supervisadas como *random forest*, *SVM*, *Naive Bayes* y *redes neuronales* alcanzan eficiencias mayores al 90 % en detección de fraudes financieros. Sin embargo, cada modelo presenta ventajas y limitaciones particulares: por ejemplo, la regresión logística suele lograr alta sensibilidad, pero genera muchos falsos positivos, mientras que *random forest* o redes neuronales pueden reducir falsos positivos a costa de menor detección de fraudes. (Luisa Fernanda Ramírez Pinzón, 2024). Estas compensaciones entre precisión y recall deben evaluarse de acuerdo con las políticas de riesgo del banco. Además, la evolución constante de los ciberdelitos (phishing asistido por IA, deepfakes, malware móvil, etc.) requiere que los sistemas de detección sean adaptativos y robustos ante nuevas tácticas fraudulentas.

Modelos y técnicas de detección de fraude

Los enfoques de IA para fraude bancario abarcan modelos supervisados (clasificación binaria) y no supervisados (detección de anomalías). En el primer caso se requiere un conjunto etiquetado de transacciones legales vs. fraudulentas. Debido al *desequilibrio de clases* –los fraudes representan un porcentaje muy bajo del total– se utilizan métricas especializadas (precisión, recall, F1, AUC-ROC) para evaluar los modelos. En cuanto a algoritmos, además de regresión logística y SVM, las redes neuronales profundas (incluyendo *autoencoders* para detección de anomalías) han ganado popularidad. Según un estudio comparativo reciente, las redes neuronales fueron las más utilizadas (32 % de los casos), seguidas de Random Forest (23 %), SVM (18 %) y otros métodos. (Bernardo et al., 2025) Estos modelos extraen patrones de comportamiento (por ejemplo, series temporales de transacciones, historial de pagos, geolocalización), y aprenden a distinguir flujos normales de flujos sospechosos.

Figura 1 - Proceso de detección de fraudes con IA: recopilación de datos, preprocesamiento, extracción de características y entrenamiento de modelos

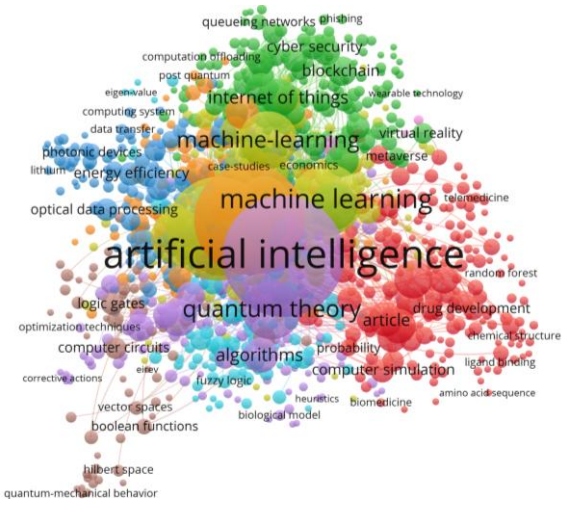


En paralelo, existen técnicas de detección no supervisada (por ejemplo, clustering, detección de outliers, autoencoders) que apuntan a identificar transacciones atípicas sin requerir etiquetas previas. Estos enfoques son útiles cuando no se disponen de ejemplos etiquetados o cuando se desea encontrar fraudes desconocidos. En general, los marcos conceptuales para detección de fraude integran fases de minería de datos y entrenamiento de modelos (siguiendo, por ejemplo, metodologías como CRISP-DM). En la práctica, los sistemas de monitoreo (Transaction Monitoring Systems – TMS) incorporan reglas estáticas definidas por expertos junto con capas de IA supervisada para mejorar la adaptabilidad. No obstante, la bibliografía resalta que solo el uso de IA puede optimizar la detección en tiempo real sin la intervención manual constante. (Hernandez Aros et al., 2024b).

Generación y uso de datos sintéticos

Una limitación clave para entrenar modelos de fraude es la disponibilidad de datos. Debido a la privacidad y confidencialidad bancaria, acceder a volúmenes adecuados de transacciones reales (incluyendo fraudes conocidos) suele ser muy difícil. (*(PDF) Análisis de Fraudes En Transacciones Bancarias Aplicando Minería de Datos*, n.d.). Además, las regulaciones de protección de datos (como el Habeas Data colombiano o GDPR) restringen el uso de información sensible. En este contexto, los datos sintéticos se proponen como una solución prometedora: son datos artificiales generados por algoritmos que reflejan las propiedades estadísticas de los datos reales sin exponer información personal. Cuando se diseñan apropiadamente, los datos sintéticos mantienen los patrones relevantes para entrenar modelos de ML, permitiendo “rellenar” vacíos de información crítica. (Micol, 2025).

Figura 2 - Análisis de graficas en VOSviewver

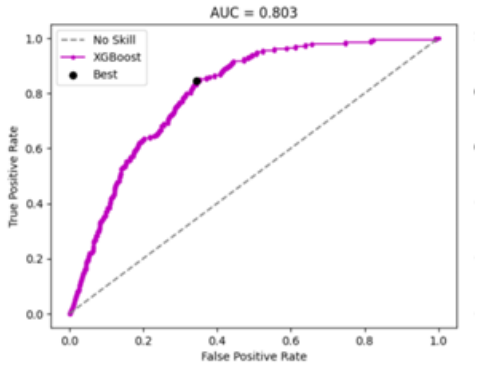


La imagen adquirida a través de Scopus muestra un mapa de co-ocurrencia de términos asociados con la investigación en inteligencia artificial y campos afines. En estas visualizaciones, el tamaño de cada palabra representa cuántas veces aparece en la literatura científica, y los colores y la proximidad de los términos indican las áreas temáticas y su interrelación. Por ejemplo, se puede ver que "inteligencia artificial" es el nodo principal, vinculado con áreas como la ciberseguridad, el aprendizaje automático, la cadena de bloques y el Internet de las cosas. Esto demuestra que la IA no es una disciplina aislada; más bien, es un eje transversal que tiene repercusiones en numerosos campos científicos y tecnológicos.

Las principales técnicas de generación sintética incluyen: (a) Sobremuestreo estadístico –por ejemplo, SMOTE o ADASYN– en que se interpolan o generan nuevos ejemplos de la clase minoritaria (fraudes). Aunque clásicas, estas técnicas lineales pueden crear muestras irreales (sobreajuste). (b) Modelos generativos avanzados –como GANs (Generative Adversarial Networks) y VAEs– que pueden producir transacciones sintéticas más realistas. Revisiones recientes muestran un creciente interés en GANs

para equilibrar datos desbalanceados, generando nuevas muestras de fraude a partir de ruido aleatorio. Por ejemplo, Du et al. (2024) proponen un enfoque híbrido *SMOTE+CGAN* donde el GAN refina las muestras sintéticas de SMOTE para convertirlas en datos de fraude más realistas, mejorando la capacidad del modelo para generalizar. Asimismo, se usan generadores de datos transaccionales basados en aprendizaje profundo (e.g. redes recurrentes para series de tiempo) o técnicas de "ruido gaussiano" injectado: en un estudio reciente, la simple adición de ruido gaussiano controlado a la clase fraudulenta permitió a XGBoost superar en precisión y AUC a métodos de Sobremuestreo clásicos (SMOTE, ADASYN). (c) Simuladores de transacciones: Herramientas como PaySim o BankSim generan historiales sintéticos a partir de estadísticos reales. Varios trabajos académicos han usado PaySim para evaluar modelos de fraude, aunque se reconoce la preocupación de que datos sintéticos no reflejen perfectamente la complejidad real. (*(PDF) Análisis de Fraudes En Transacciones Bancarias Aplicando Minería de Datos*, n.d.)

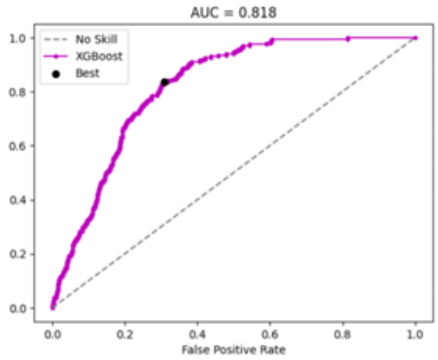
Figura 3 – Aumento - SMOTE



AUC = 0.80

Imagen tomada de: sia-ai.medium.com

Figura 4 - Aumento generación - sintética de datos



AUC = 0.82

Imagen tomada de: sia-ai.medium.com

El uso de datos sintéticos en banca persigue varios objetivos: mitigar el desequilibrio de clases, respetar la privacidad, y disponer de escenarios de prueba controlados (por ejemplo, para testear modelos con nuevas modalidades de fraude). Sin embargo, la literatura también advierte desafíos: los datos sintéticos deben calibrarse para que reproduzcan fielmente la distribución real sin introducir sesgos, y su uso generalizado plantea cuestiones éticas y regulatorias. Por ejemplo, un estudio sobre regulación financiera destaca que, aunque los datos sintéticos pueden mejorar la supervisión (llenando vacíos informativos en áreas críticas), también generan dudas sobre legitimidad, transparencia y privacidad.

Estado del arte y aplicaciones actuales

En los últimos años se han publicado numerosos estudios sobre IA y fraude bancario. Una tendencia clara es el enfoque en fraude con tarjetas de crédito y transacciones electrónicas: la mayoría de los modelos reportados en la literatura evalúan datasets públicos o reales de tarjetas, con técnicas supervisadas. Sin embargo, el uso de datos sintéticos aún es minoritario: según una revisión reciente, menos del 7 % de los estudios integraron datos artificiales en sus experimentos, especialmente en

Latinoamérica, donde hay escasa producción académica sobre el tema. (Hernandez Aros et al., 2024b)

A nivel global, destacan casos de aplicación innovadora: p.ej. equipos de investigación han desarrollado plataformas de intercambio de datos sintéticos entre bancos. Un ejemplo es SynDEc (UNIKassel, 2025), que propone un ecosistema colaborativo usando IA generativa para que bancos compartan conjuntos sintéticos de transacciones sin violar la privacidad individual. (Micol, 2025)Otro trabajo (FinDEx, HICSS 2024) defiende un sistema similar de diseño científico para permitir a las instituciones crear datos sintéticos comunes con el fin de mejorar la capacitación de sus modelos de fraude. Estos marcos conceptuales aplican teorías de ecosistemas de datos y diseño colaborativo para resolver la falta de datos reales.

En Colombia y la región, la IA en detección de fraude es un área emergente. Instituciones financieras importantes ya utilizan ML/IA en sus controles internos, y se impulsa la regulación (p.ej. en créditos y fraudes financieros) para incorporar tecnologías avanzadas. Estudios locales preliminares analizan cómo ha evolucionado la adopción de IA en bancos colombianos (p.ej. en Colpatria) y sugieren que, aunque aún está en etapa inicial, existe interés institucional por sus beneficios. En paralelo, iniciativas internacionales señalizan la importancia de la detección automática de fraude para el sector financiero latinoamericano.

Desafíos y marcos conceptuales relevantes

El problema del fraude bancario implica aspectos técnicos, organizacionales y legales. En el plano técnico, el principal obstáculo es la variabilidad de los ataques: los defraudadores adaptan continuamente sus métodos, por lo que los modelos deben actualizarse y generalizar bien. Además, existe la adaptación adversaria: un modelo de

fraude efectivo impulsa a los atacantes a cambiar de patrón. Conceptualmente, esto puede abordarse mediante aprendizaje continuo y detección de *drift*.

En el plano organizativo, la colaboración entre bancos está limitada por la privacidad, lo que impulsa propuestas como las ya mencionadas de ecosistemas sintéticos (SynDEc) y aprendizaje federado. No obstante, se han identificado limitaciones en *open banking* y *federated learning* para este fin: el open banking (intercambio voluntario de datos) adolece de cobertura parcial (participación selectiva, sin operaciones B2B); el aprendizaje federado centralizado enfrenta problemas de escalabilidad, requiere un único modelo compartido y carece de flexibilidad frente a entornos heterogéneos. Por eso, los investigadores proponen marcos nuevos que combinen diseño de datos compartidos con IA generativa para lograr un intercambio de información efectivo bajo regulaciones estrictas.

Finalmente, desde la perspectiva teórica, este campo se sustenta en conceptos de minería de datos, aprendizaje estadístico, teoría de la información, y ética de datos. Por ejemplo, el uso de datos sintéticos se alinea con marcos de *privacidad diferencial* y *aprendizaje seguro*, aunque con retos prácticos. Las propuestas recientes integran enfoques de “co-creación de valor” al estilo service-dominant logic, donde actores (bancos, reguladores, clientes) coparticipan en el proceso de detección de fraude mediante recursos compartidos (datos) y normas institucionales.

En resumen, el marco conceptual de esta investigación combina principios de IA aplicada al fraude (desequilibrio de clases, algoritmos supervisados vs no supervisados, métricas de detección) con los beneficios y limitaciones de los datos sintéticos (privacidad, calidad, escalabilidad), en un panorama donde convergen tendencias globales e iniciativas locales. Los estudios citados evidencian que este tema es de alto interés académico y práctico, y que las soluciones más avanzadas implican la generación

y uso ético de datos sintéticos como complemento de las técnicas clásicas de detección de fraude.

Análisis de restricciones

El presente análisis define los límites legales, éticos, técnicos, económicos, sociales, ambientales y de seguridad que enmarcan el desarrollo del modelo predictivo de IA con datos sintéticos para la detección de fraude financiero en Colombia. Su finalidad es asegurar que el proyecto se ejecute conforme a la normativa nacional sobre protección de datos personales y a los estándares internacionales de gestión del riesgo en IA, garantizando privacidad, trazabilidad de decisiones y validez científica de los resultados.

Legales y normativas

El proyecto se enmarca en la Ley 1581 de 2012 y el Decreto 1377 de 2013, que regulan la protección de datos personales en Colombia y establecen las condiciones de tratamiento de la información por parte de entidades públicas y privadas (Ley 1581 de 2012 - Gestor Normativo, n.d.). Aunque el modelo se entrena con datos totalmente sintéticos, se reconoce que la manipulación de información derivada de simulaciones financieras debe cumplir con los principios de legalidad, finalidad, veracidad y seguridad, garantizando la confidencialidad y protección frente a accesos no autorizados.

Asimismo, se consideran los lineamientos de la Superintendencia Financiera de Colombia y los sistemas SARLAFT y SAGRILAFT, los cuales establecen directrices para la prevención del lavado de activos, la financiación del terrorismo y otras actividades ilícitas en el entorno financiero colombiano (Superfinanciera, 2025). Estos lineamientos resultan relevantes para el proyecto, ya que la detección temprana de patrones fraudulentos mediante inteligencia artificial se alinea con los objetivos de fortalecimiento

de los sistemas de control interno y gestión del riesgo que estas normas exigen a las entidades financieras.

Por otra parte, el proyecto adopta los estándares internacionales del NIST AI Risk Management Framework 1.0, que define funciones esenciales para la gobernanza y gestión de riesgo en modelos de inteligencia artificial (Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023) y la ISO/IEC 23894:2023, que proporciona lineamientos para la gestión del riesgo en sistemas de IA y su integración en los procesos organizacionales (*ISO/IEC 23894:2023*, n.d.).

Estrategias:

- Se debe declarar formalmente que no se utilizan datos personales reales, indicando que el modelo emplea exclusivamente información sintética para garantizar la privacidad y el cumplimiento de la legislación vigente.
- Hay que asegurar que el almacenamiento y uso de la información sintética cumpla con las normas de seguridad digital y con los principios establecidos en la Ley 1581 de 2012.
- Incluir en los anexos un registro de cumplimiento legal, documentación de licencias y trazabilidad del modelo, garantizando transparencia, responsabilidad institucional y auditoría ética del proceso.

Restricciones técnicas

El modelo enfrenta limitaciones inherentes a la disponibilidad de recursos computacionales y a la naturaleza experimental del proyecto. La complejidad del entrenamiento de redes neuronales y la necesidad de procesar grandes volúmenes de datos sintéticos exigen optimizar los tiempos de simulación y asegurar la reproducibilidad del entorno de ejecución.

A nivel metodológico, el desequilibrio natural entre transacciones legítimas y fraudulentas plantea desafíos significativos en la evaluación del desempeño, por lo que se privilegian métricas como *Precision-Recall* (PR-AUC) y recall, más adecuadas para contextos con clases altamente desbalanceadas, en lugar del tradicional ROC-AUC.

En cuanto a la validación, se emplean enfoques de evaluación temporal o *walk-forward*, que permiten respetar la secuencia cronológica de las transacciones y evitar filtraciones de información entre los conjuntos de entrenamiento y prueba (C. Zhang et al., 2021). Adicionalmente, la calidad y utilidad de los datos sintéticos se evaluará mediante la metodología TSTR (*Train-on-Synthetic, Test-on-Real*) y las métricas provistas por la librería SDV/SDMetrics, ampliamente utilizadas para medir fidelidad estadística y privacidad en datos generados artificialmente(*The Synthetic Data Vault*, n.d.).

Respecto a las fuentes de datos, el proyecto utiliza simuladores académicos y *datasets* públicos reconocidos en la literatura sobre fraude financiero. El conjunto *PaySim*, desarrollado por López-Rojas (2016), genera transacciones sintéticas a partir de comportamientos reales de sistemas móviles de pago y se distribuye bajo la licencia GPL-3.0, mientras que BankSim, de López-Rojas y Axelsson (2014), utiliza estadísticas bancarias reales bajo la licencia CC BY-NC-SA 4.0. Ambos recursos se emplean exclusivamente con fines académicos, respetando las condiciones de uso, citando sus fuentes y evitando su redistribución no autorizada.

Restricciones Económicas y financieras

El proyecto se desarrolla con recursos propios de los estudiantes y apoyo institucional limitado, sin financiación externa, lo cual condiciona la magnitud del entrenamiento del modelo y la infraestructura disponible. Dada esta restricción, se

prioriza la utilización de herramientas gratuitas y de código abierto para evitar costos asociados a licencias o servicios en la nube, siguiendo las buenas prácticas de sostenibilidad tecnológica promovidas por la comunidad académica y de software libre (Fitzgerald, 2006).

En este contexto, se emplean bibliotecas de acceso abierto como Python, Scikit-learn, FastAPI, Pandas y SDV, que permiten el desarrollo de modelos de inteligencia artificial con un nivel de precisión y escalabilidad aceptable para proyectos de investigación (Pedregosa et al., 2010). Estas herramientas se seleccionan por su soporte comunitario, documentación extensa y compatibilidad con entornos académicos, evitando gastos en plataformas comerciales de cómputo o análisis de datos.

La ejecución de los experimentos se realiza en equipos institucionales de capacidad media, con limitaciones en procesamiento gráfico, lo que obliga a optimizar los tiempos de entrenamiento y priorizar la eficiencia computacional (Y. Zhang & Chen, 2020). Por esta razón, el alcance del trabajo se restringe a pruebas de simulación controladas, sin conexión con sistemas bancarios reales, y con un cronograma ajustado a los recursos humanos y técnicos disponibles.

Adicionalmente, se documenta el costo estimado del cómputo y del consumo energético como evidencia de una gestión eficiente de los recursos académicos, garantizando la viabilidad del proyecto dentro de los márgenes presupuestales establecidos por la universidad (Measuring The Environmental Impacts Of Artificial Intelligence Compute And Applications, 2022).

Restricciones ambientales

El sector financiero no afecta directamente de una forma critica la dimensión ambiental, sin embargo, es necesario tener en cuenta como podría verse afectada; en

donde el entrenamiento de modelos consume energía, requiere de refrigeración y recursos de infraestructura que pueden generar huella de carbono, generando un valor dentro de los criterios de sostenibilidad (ESG).

A nivel global los centros de datos consumieron aproximadamente 460 TWh en 2022 (≈1,7 % del consumo eléctrico mundial) y emitieron 220 Mt de CO_2 (Inteligente, 2024).

Teniendo en cuenta lo anterior, es necesario contemplar la dimensión ambiental, que puede generar un proyecto tecnológico, desde su consumo eléctrico, refrigeración, emisiones indirectas, selección de infraestructura eficiente (energía renovable, eficiencia de racks, reutilización de calor, etc.).

Restricciones Salud y seguridad

El entorno digital del sector financiero en Colombia enfrenta amenazas cada vez más elevadas. Por ejemplo, en 2024 se reportaron aproximadamente 36.000 millones de intentos de ciberataques al país, un incremento del 29 % frente al año anterior (Duitama, 2025). A su vez, se han generado inversiones para reforzar la defensa digital, en donde para el 2024 se alcanzó cerca de COP $510.000 millones, lo que representa un aumento del 16 % frente a 2023 (*Ciberseguridad En El Sector Financiero Colombiano Creció 16 % En 2024 - Revista C-Level*, 2025).

Estas cifras reflejan dos realidades importantes: por un lado, la creciente magnitud del riesgo de seguridad al que se enfrenta el sistema financiero; y por otro, el esfuerzo sostenido de las instituciones por fortalecer sus mecanismos de protección. En este contexto, cualquier modelo de inteligencia artificial enfocado en la detección de fraude debe desarrollarse bajo criterios sólidos de ciberseguridad, protección de datos y trazabilidad de decisiones. No puede ser un sistema aislado, sino parte de un entorno

seguro que garantice controles de acceso, cifrado, segmentación de datos y revisión humana en casos críticos.

Además, la Salud, que en este caso se ve afectada a nivel digital, también está en juego. Un falso positivo que bloquee injustamente una cuenta o un error que permita el paso de una transacción fraudulenta puede afectar gravemente la confianza, la reputación y el bienestar financiero de las personas. Por eso, el modelo propuesto debe incorporar mecanismos de revisión, transparencia y explicabilidad, asegurando que las decisiones automatizadas sean comprensibles y auditables.

Finalmente, la necesidad de operar en tiempo real se vuelve indispensable. Los ataques cibernéticos ocurren a gran velocidad, y si el sector ya realiza inversiones masivas en defensa, nuestro modelo debe estar a la altura: ser rápido, preciso y seguro, contribuyendo a mantener la resiliencia del sistema financiero colombiano frente a un entorno digital cada vez más desafiante.

Restricciones Sociales y culturales

En Colombia existe una brecha entre la conectividad y tecnología que puede afectar la representatividad de datos y la adopción del sistema. Por ejemplo, según el DANE en 2022 solo el 59,5 % de los hogares del país tenían conexión a internet; en las cabeceras urbanas 67,5 % y en zonas rurales solo 32,2 % (Riaño, 2023) . Esto significa que los perfiles de clientes que se tienen de forma digital no son la representación de toda la población.

Teniendo en cuenta lo anterior, si nuestro modelo se entrena sólo con datos que simulen los segmentos digitales urbanos, puede presentar sesgo o baja eficacia en zonas rurales o con menor digitalización. Por tanto, hay que contemplar diversidad de perfiles, asegurar que la generación de datos sintéticos cubra la diversidad, y prever que la

aceptación social dependa de la transparencia, la equidad y la claridad en decisiones automatizadas.

Restricciones Políticas y gubernamentales

Colombia está evolucionando de forma acelerada, lo cual impone exigencias específicas al desarrollo de modelos de IA en el sector financiero. En febrero de 2025 el gobierno aprobó el Documento CONPES 4144 (la Política Nacional de Inteligencia Artificial) que asigna un presupuesto estimado de cerca de COP $479.000 millones para impulsar capacidades nacionales de IA hasta el 2030 (*CONPES 4144: La Hoja de Ruta de Colombia En Inteligencia Artificial Para Los Retos Actuales y La Transformación Futura*, n.d.). Esta política incluye componentes de gobernanza, ética, infraestructura, talento y mitigación de riesgos del uso de IA.

Esto significa que nuestro modelo de IA para riesgo de fraude deberá alinearse con principios de transparencia, ética, gobernabilidad y protección de derechos, tal como exige la política pública. Además, debido a que la regulación aún se está desarrollando, nuestro diseño debe contemplar adaptabilidad frente a cambios regulatorios: auditorías de algoritmos, registro de decisiones, análisis de sesgos y mecanismos de apelación para usuarios afectados.

En el contexto del sector financiero regulado, el cumplimiento no es opcional: el modelo deberá integrarse en entidades que dependen de la supervisión estatal, lo que implica que los requisitos legales y gubernamentales deberán considerarse desde la fase de prototipo. Es decir que la restricción política y gubernamental exige que el diseño de la IA no sólo sea funcional, sino también viable en términos de normativa, ética y gobernanza, minimizando riesgos de rechazo institucional o cambio regulatorio que podrían poner en peligro la implementación.

Metodología para la selección y desarrollo de la solución

El enfoque adoptado es mixto o híbrido (cuantitativo–cualitativo), combinando técnicas estadísticas, experimentales y comparativas. Desde la perspectiva cuantitativa, se aplican métodos de análisis de datos, simulaciones sintéticas y métricas de rendimiento para evaluar objetivamente la precisión del modelo. Desde el enfoque cualitativo, se realiza una revisión documental, análisis comparativo de soluciones, evaluación de coherencia técnica y validación ética y legal del diseño (Denzin, 2017).

Según Engineering Design: A Systematic Approach ((Book)) (n.d.), el proceso de diseño de sistemas complejos debe comenzar con la identificación de alternativas, seguida de la eliminación progresiva de las menos viables, considerando criterios de economía, sostenibilidad y aplicabilidad.

A partir del análisis de restricciones realizado, se establecieron los siguientes principios metodológicos que guiaron la selección de la solución:

1. Coherencia técnica: La propuesta no debe violar leyes físicas ni principios de la estadística y el aprendizaje automático (por ejemplo, la existencia de un modelo de precisión perfecta).
2. Comparación con hechos conocidos: Se evaluaron experiencias documentadas en la literatura y en la práctica bancaria internacional con el fin de determinar la pertinencia y posibles mejoras del enfoque propuesto (*CardSim: A Bayesian Simulator for Payment Card Fraud Detection Research*, n.d.).
3. Evaluación de soluciones alternativas: Se analizaron tres posibles estrategias de detección de fraude sistemas basados en reglas, modelos supervisados con datos reales, y modelos predictivos con datos sintéticos con el objetivo de comparar desempeño, costo y cumplimiento legal.

La metodología se desarrolla en tres fases principales, orientadas al cumplimiento del objetivo general del proyecto.

Fase 1. Identificación y análisis de alternativas

En esta fase se evaluaron tres posibles enfoques para abordar la detección temprana de fraude financiero:

Alternativa	***Descripción***	***Ventajas***	***Limitaciones***
A1: Sistema basado en reglas	Detección mediante umbrales fijos definidos por expertos.	Fácil de interpretar, bajo costo computacional.	No adaptable, genera falsos positivos.
A2: Modelos supervisados con datos reales	Entrenamiento con bases de datos históricas de fraude.	Alta precisión empírica.	Inaccesibilidad de datos reales, riesgo legal (Ley 1581 de 2012).
A3: Modelo predictivo con datos sintéticos	Entrenamiento mediante datos simulados.	Cumple normas éticas, reproducible, bajo costo, adaptable.	Requiere validación estadística de la fidelidad de datos.

La evaluación comparativa mostró que la alternativa A3 presenta el mejor equilibrio entre precisión, cumplimiento legal, sostenibilidad y factibilidad académica.

Se considera, además, que su aplicación respeta la Ley 1581 de 2012 y el Decreto 1377 de 2013, al no manipular información personal real, y se alinea con los estándares internacionales NIST AI RMF 1.0 e ISO/IEC 23894:2023, que promueven la trazabilidad y el control del riesgo en sistemas de inteligencia artificial.

Fase 2. Evaluación técnica y validación conceptual

Una vez seleccionada la alternativa A3, se realizó una validación metodológica considerando tres criterios:

1. Lógica técnica: Se descartaron supuestos irrealizables o ilógicos (por ejemplo, modelos infalibles o sin margen de error estadístico).
2. Coherencia con casos previos: Se comparó la solución con modelos de referencia documentados (*APPLICATION OF MACHINE LEARNING MODELS FOR FRAUD DETECTION IN SYNTHETIC MOBILE FINANCIAL TRANSACTIONS*, n.d.), que simulan transacciones financieras y se han empleado ampliamente en estudios académicos.
3. Ajuste a las restricciones identificadas: La propuesta se ajustó a los límites técnicos, económicos y legales del proyecto, optimizando recursos de cómputo y priorizando librerías de código abierto *como Scikit-learn, FastAPI* y Pandas (Pedregosa et al., 2010) La validación conceptual se llevó a cabo utilizando el método GAN *(Generative adversarial networks*) propuesto por Figueira & Vaz, el cual permite evaluar la fidelidad de los datos generados sintéticamente. Se complementó con métricas de calidad sintética como *SDMetrics* y evaluaciones PR-AUC (*Precision–Recall)* recomendadas para contextos de clases desbalanceadas (Figueira & Vaz, 2022).

Fase 3. Refinamiento y desarrollo del modelo predictivo

En esta fase se construyó el modelo conceptual de IA bajo las siguientes actividades:

1. Diseño de la arquitectura conceptual: Definición de variables simuladas (monto, hora, canal, IP, geolocalización) y flujo de procesamiento (preprocesamiento → generación sintética → entrenamiento → validación).

2. Generación de datos sintéticos: Uso de librerías *Faker y SDV* para simular comportamientos financieros realistas, con base en las distribuciones observadas en *datasets* públicos.
3. Entrenamiento y evaluación: Aplicación de modelos de machine learning (*Random* Forest, *XGBoost, Logistic Regression*) para comparar métricas de desempeño.
4. Optimización del rendimiento computacional: Dado que el proyecto carece de infraestructura de alto rendimiento (GPU dedicadas), se prioriza la eficiencia y reducción de tiempos de entrenamiento, conforme a las recomendaciones de *Efficient Acceleration of Deep Learning Inference on Resource-Constrained Edge Devices: A Review (n.d.)*
5. Evaluación ética y social: Revisión del cumplimiento de los principios de transparencia, explicabilidad y no discriminación establecidos en el CONPES 4144 de 2025, que define la Política Nacional de Inteligencia Artificial en Colombia.

La solución propuesta se ajusta a los principios de sostenibilidad tecnológica (ESG) y de responsabilidad digital:

- Ética y transparencia: se emplean mecanismos de explicabilidad (SHAP, LIME) para garantizar decisiones auditables.
- Sostenibilidad ambiental: se minimiza la huella de carbono utilizando entornos de ejecución optimizados y software libre (Inteligente, 2024).
- Ciberseguridad y resiliencia: el modelo contempla controles de acceso, cifrado y trazabilidad, siguiendo las recomendaciones de la Superintendencia Financiera de Colombia y las prácticas de SARLAFT/SAGRILAFT (Superfinanciera, 2025).

Además, se reconoce que el proyecto opera en un entorno con alto nivel de riesgo digital, donde en 2024 se registraron más de 36.000 millones de ciberataques en Colombia (Duitama, 2025). Por ello, el modelo deberá ser capaz de operar en entornos seguros y responder en tiempo real a amenazas emergentes.

Resultados esperados

La metodología propuesta permitirá obtener:

1. Un modelo conceptual validado (MVP) que integre IA y datos sintéticos.
2. Un conjunto de métricas de rendimiento y fidelidad que respalden su validez científica.
3. Una propuesta de integración ética y regulatoria alineada con la política pública colombiana en IA.
4. Un documento de replicabilidad académica que garantice transparencia y transferencia tecnológica

La metodología para la selección y desarrollo de la solución garantiza un proceso estructurado, ético y técnicamente fundamentado, donde la elección del modelo predictivo basado en IA y datos sintéticos responde no solo a su rendimiento, sino también a su compatibilidad con las restricciones legales, económicas, ambientales y sociales del contexto colombiano.

Al integrar un enfoque híbrido, esta metodología no solo valida cuantitativamente la precisión del modelo, sino que también interpreta cualitativamente sus implicaciones éticas y de sostenibilidad, cumpliendo con los principios de la Política Nacional de Inteligencia Artificial (CONPES 4144, 2025) y los estándares internacionales de gobernanza tecnológica.

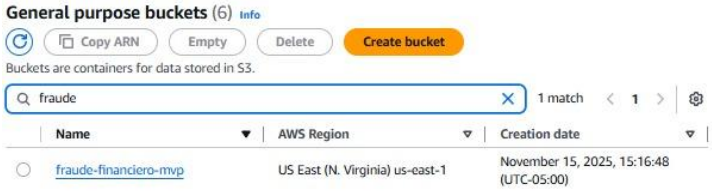
Desarrollo de la solución

El desarrollo práctico del modelo predictivo se estructuró en fases progresivas que abarcan desde la preparación del entorno técnico hasta la validación final del modelo y su integración con herramientas analíticas de AWS. Cada fase consolida actividades específicas, siguiendo criterios de reproducibilidad, cumplimiento normativo y optimización de recursos computacionales. A continuación, se presenta el desarrollo completo de la solución.

FASE 0 — Preparación del entorno

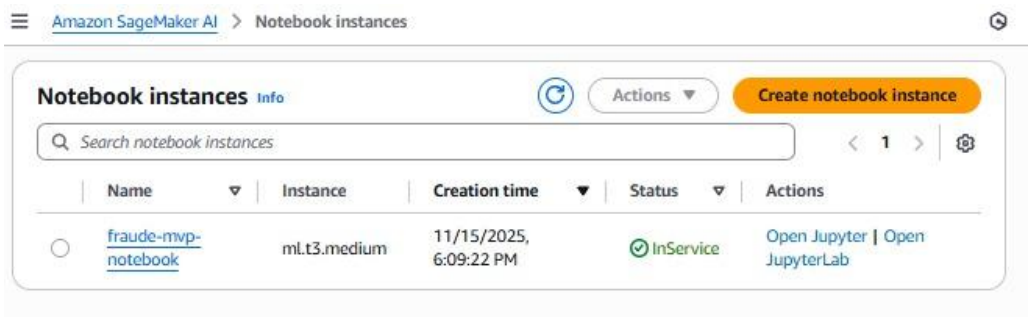
El proceso inició con la creación de la infraestructura mínima para el proyecto en AWS. Se implementó un bucket S3 denominado **fraude-financiero-mvp**, que actúa como repositorio central para datasets, artefactos del modelo, resultados y archivos intermedios.

Figura 5. Creación Bucket S3



Posteriormente, se configuró un entorno de trabajo en Amazon SageMaker Notebook, habilitando un ambiente controlado para ejecutar notebooks de Jupyter con librerías de data science, procesamiento de datos y despliegue de modelos. Esta fase sentó las bases para un flujo completo de MLOps en la nube.

Figura 6. Ambiente Sagemaker

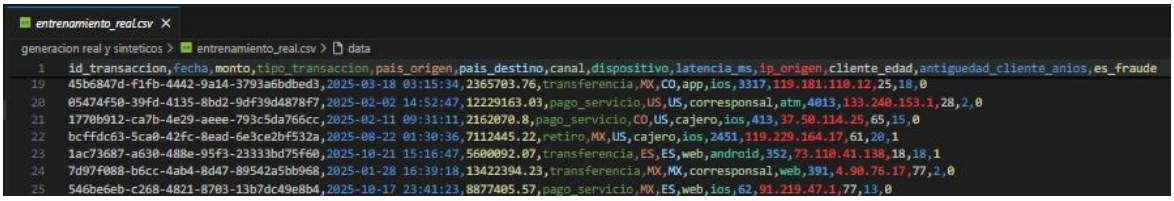


FASE 1 — Definición y Preparación de los Datasets

Se generaron y organizaron cuatro conjuntos de datos diferenciados:

- **Dataset real de entrenamiento (500 registros)**

Figura 7. Real Entrenamiento



- **Dataset real de prueba (500 registros)**

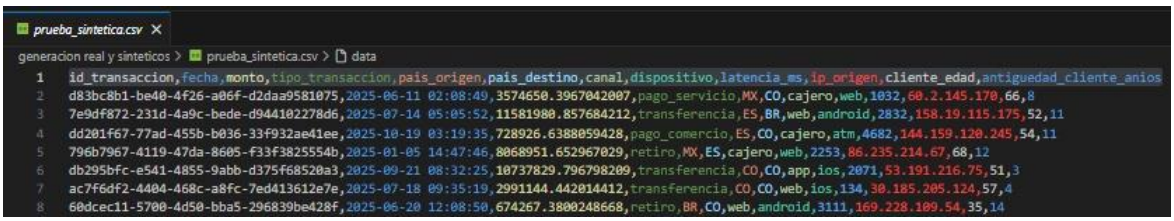
Figura 8. Real Prueba

- **Dataset sintético de entrenamiento**

Figura 9. Sintetico Entrenamiento

- **Dataset sintético de prueba**

Figura 10. Sintentico Prueba



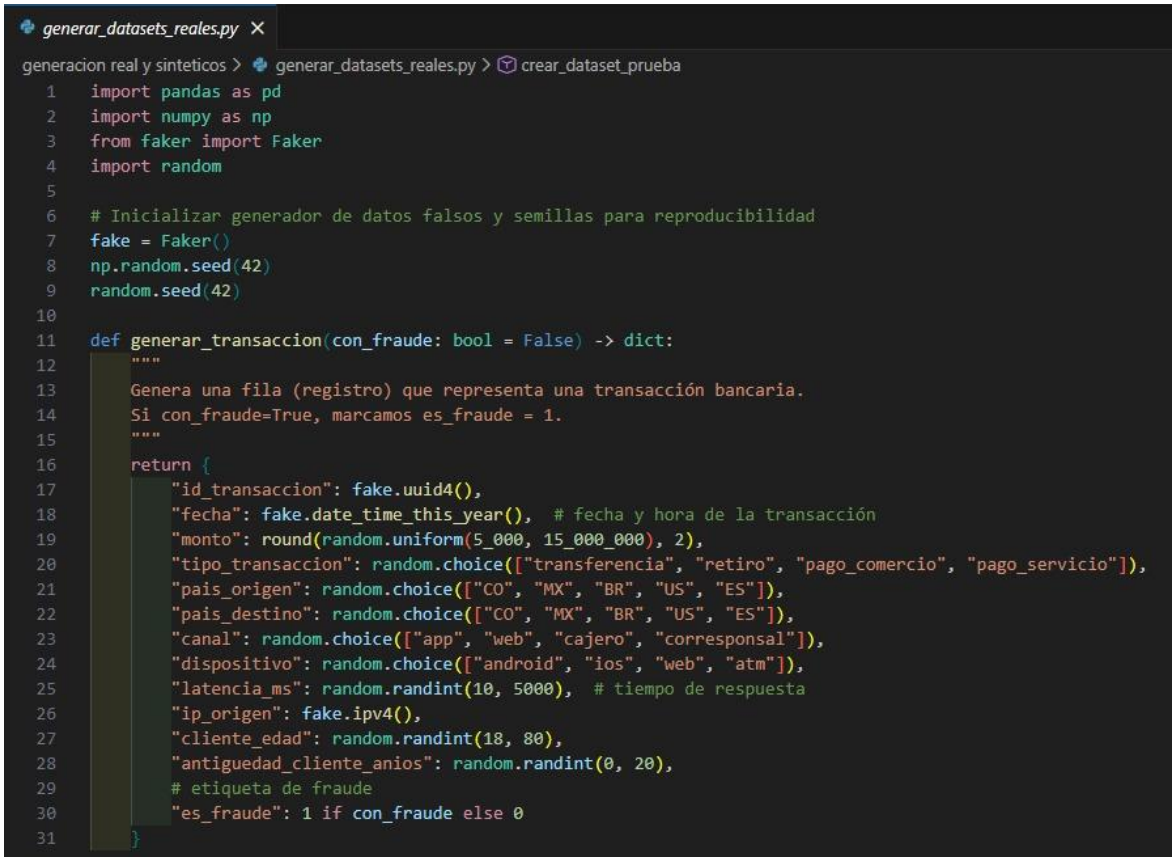
prueba_sintetica.csv

generacion real y sinteticos > prueba_sintetica.csv > data

```
id_transaccion,fecha,monto,tipo_transaccion,pais_origen,pais_destino,canal,dispositivo,latencia_ms,ip_origen,cliente_edad,antiguedad_cliente_anios
d83bc8b1-be40-4f26-a06f-d2daa9581075,2025-06-11 02:08:49,3574650.3967042007,pago_servicio,MX,CO,cajero,web,1032,60.2.145.170,66,8
7e9df872-231d-4a9c-bede-d944102278d6,2025-07-14 05:05:52,11581980.857684212,transferencia,ES,BR,web,android,2832,158.19.115.175,52,11
dd201f67-77ad-455b-b036-33f932ae41ee,2025-10-19 03:19:35,728926.6388059428,pago_comercio,ES,CO,cajero,atm,4682,144.159.120.245,54,11
796b7967-4119-47da-8605-f33f3825554b,2025-01-05 14:47:46,8068951.652967029,retiro,MX,ES,cajero,web,2253,86.235.214.67,68,12
db295bfc-e541-4855-9abb-d375f68520a3,2025-09-21 08:32:25,10737829.796798209,transferencia,CO,CO,app,ios,2071,53.191.216.75,51,3
ac7f6df2-4404-468c-a8fc-7ed413612e7e,2025-07-18 09:35:19,2991144.442014412,transferencia,CO,CO,web,ios,134,30.185.205.124,57,4
60dcec11-5700-4d50-bba5-296839be428f,2025-06-20 12:08:50,674267.3800248668,retiro,BR,CO,web,android,3111,169.228.109.54,35,14
```

Todos se generaron mediante código en Python, asegurando coherencia entre estructuras y distribución de variables.

Figura 11. Código completo



generar_datasets_reales.py

generacion real y sinteticos > generar_datasets_reales.py > crear_dataset_prueba

```python
import pandas as pd
import numpy as np
from faker import Faker
import random

# Inicializar generador de datos falsos y semillas para reproducibilidad
fake = Faker()
np.random.seed(42)
random.seed(42)

def generar_transaccion(con_fraude: bool = False) -> dict:
    """
    Genera una fila (registro) que representa una transacción bancaria.
    Si con_fraude=True, marcamos es_fraude = 1.
    """
    return {
        "id_transaccion": fake.uuid4(),
        "fecha": fake.date_time_this_year(),  # fecha y hora de la transacción
        "monto": round(random.uniform(5_000, 15_000_000), 2),
        "tipo_transaccion": random.choice(["transferencia", "retiro", "pago_comercio", "pago_servicio"]),
        "pais_origen": random.choice(["CO", "MX", "BR", "US", "ES"]),
        "pais_destino": random.choice(["CO", "MX", "BR", "US", "ES"]),
        "canal": random.choice(["app", "web", "cajero", "corresponsal"]),
        "dispositivo": random.choice(["android", "ios", "web", "atm"]),
        "latencia_ms": random.randint(10, 5000),  # tiempo de respuesta
        "ip_origen": fake.ipv4(),
        "cliente_edad": random.randint(18, 80),
        "antiguedad_cliente_anios": random.randint(0, 20),
        # etiqueta de fraude
        "es_fraude": 1 if con_fraude else 0
    }
```

Posteriormente:

1. Se crearon carpetas separadas en S3 para datos reales y sintéticos.

2. Se cargaron los cuatro archivos en sus rutas específicas.
3. Se verificó su disponibilidad para ser consumidos por SageMaker durante el preprocesamiento y entrenamiento.

Esta fase garantizó una base de datos equilibrada, anonimizada y adecuada para evaluar diferencias entre entrenamiento con datos reales vs sintéticos.

FASE 2 — Desarrollo, entrenamiento, despliegue y validación del modelo

La Fase 2 constituye el núcleo técnico del proyecto. Incluye todo el flujo operativo: preprocesamiento, ingeniería de características, balanceo, entrenamiento, optimización, despliegue, predicción por lotes y auditoría final.

2.1 Preprocesamiento y preparación avanzada de datos

El proceso inició con la configuración del entorno, validando la región AWS, la conexión al bucket S3 y la importación de librerías críticas para el análisis.

Se cargaron los datasets reales y sintéticos desde S3, y se aplicaron transformaciones para estandarizar estructura y tipos.

Se desarrolló *feature engineering* avanzado:

- Creación de variables derivadas
- Transformación de categorías mediante one-hot encoding
- Normalización de magnitudes
- Conversión de booleanos a enteros
- Eliminación de columnas irrelevantes

También se abordó el desbalance natural de la variable objetivo utilizando:

- SMOTE mejorado
- Ajuste de distribución
- Parámetro scale_pos_weight en XGBoost

2.2 Entrenamiento y optimización del modelo XGBoost

Se seleccionó XGBoost por su capacidad para manejar datos tabulares y su compatibilidad nativa con SageMaker. Se configuró con hiperparámetros optimizados:

- max_depth = 6
- eta = 0.05
- num_round = 300
- early_stopping_rounds = 20

El entrenamiento se ejecutó en una instancia **ml.m5.large** de SageMaker.

El rendimiento del modelo se evaluó con **AUC-PR**, métrica adecuada para datasets desbalanceados.

Se consolidó un pipeline que unificó:

- Preprocesamiento
- Ingeniería de características
- Entrenamiento
- Validación
- Generación de artefactos

2.3 Despliegue del modelo y creación del endpoint de inferencia

Una vez entrenado, el modelo se desplegó mediante model.deploy().

Configuraciones esenciales:

- serialización/deserialización en formato CSV
- manejo de cuotas y errores típicos (p. ej. ResourceLimitExceeded)
- endpoint alojado en una instancia dedicada

Para garantizar compatibilidad con distintos tipos de salida, se creó la función extract_number(), diseñada para aplanar estructuras anidadas, listas, bytes y strings.

2.4 Predicción por lotes y generación del archivo final de resultados

Se construyó un flujo de predicción batch que permite enviar registros al endpoint en bloques de 100. Este proceso incluyó:

- alineación exacta de columnas
- conversión a numpy arrays
- envío controlado por lotes
- manejo robusto de la respuesta del endpoint

A partir de la respuesta se generaron:

- scores de fraude
- variable final es_fraude_pred
- clasificación por niveles: alto, medio, bajo

El archivo se almacenó localmente y posteriormente se subió automáticamente a S3:

s3://fraude-financiero-mvp/results/

2.5 Ejecución automática del pipeline

Toda la lógica se integró en una ejecución principal que encadena:

- Preparación
- Feature engineering
- Preprocesamiento
- Entrenamiento
- Despliegue
- Predicción
- Guardado
- Subida a S3

Esto permitió ejecutar el flujo completo con una sola instrucción.

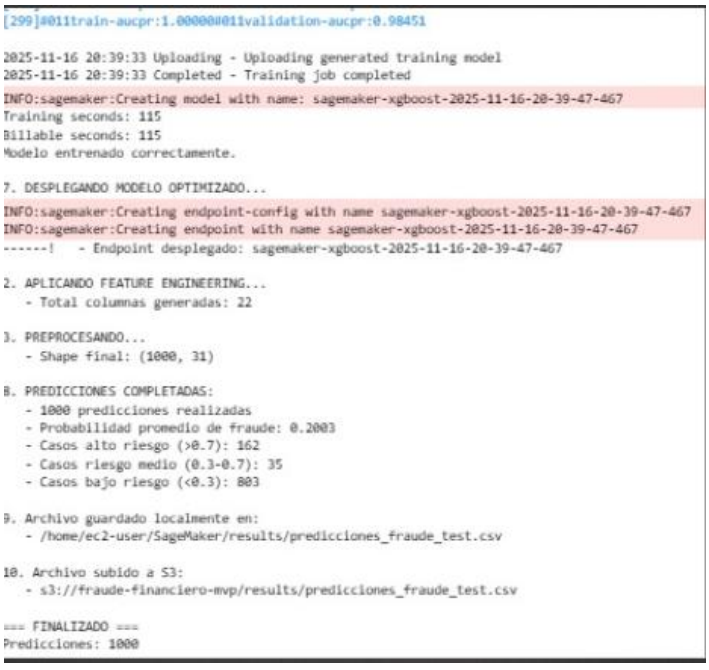
2.6 Auditoría y validación final del modelo

Para asegurar su correcto funcionamiento, se realizó una auditoría completa:

- Consistencia entre datasets reales y sintéticos
- Validación de tipos numéricos
- Alineación de columnas
- Funcionamiento del Endpoint
- Evaluación de umbrales
- Integridad del archivo CSV final

Los resultados confirmaron la solidez del MVP.

Figura 12 y 13. Resultados del modelado



FASE 3 — Integración en AWS Glue y Athena

Con el modelo funcional, la tercera fase se centró en crear la arquitectura analítica para explotación de datos.

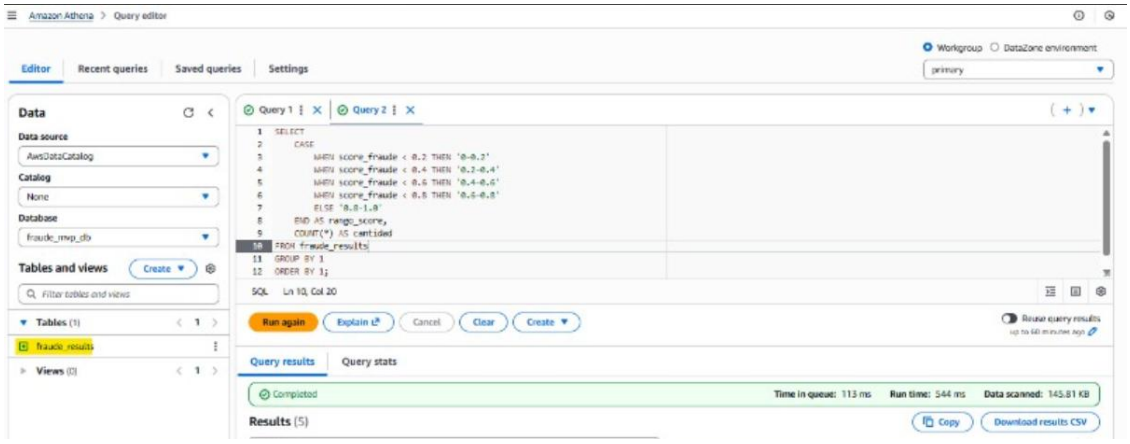
Se inició con la creación de una base de datos en **AWS Glue**, destinada al catálogo estructurado de los resultados de predicción almacenados en S3.

Posteriormente se configuró un **crawler**, encargado de mapear automáticamente el esquema de los archivos CSV.

Tras su ejecución se verificó la creación de las tablas en el Glue Data Catalog.

Finalmente se realizaron consultas analíticas mediante **Amazon Athena**, permitiendo explorar patrones, distribuciones y resultados del modelo mediante SQL.

Figura 14. Consulta Athena

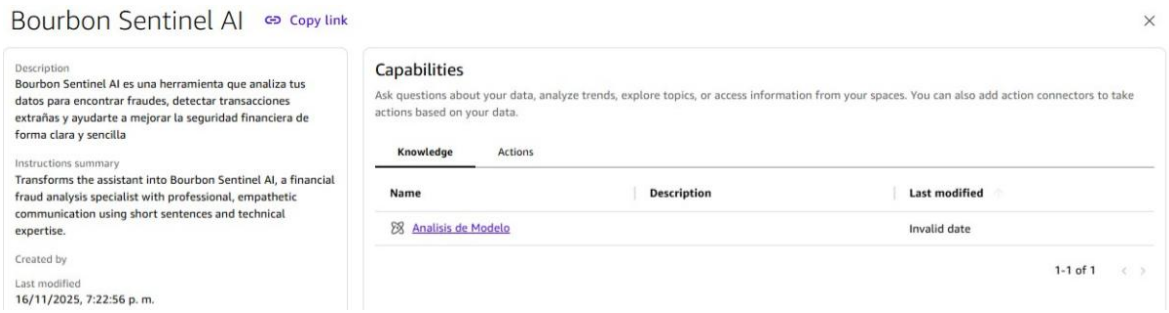


FASE 4 — Dashboard profesional y agente IA en Amazon QuickSight

La fase final consistió en el diseño de una capa visual y conversacional para análisis inteligente.

Se habilitó Amazon QuickSight, configurando permisos, roles y la vinculación con S3 y Athena.

Figura 15. Agente



Posteriormente se importaron los resultados almacenados en S3 y se construyó un dashboard profesional, con visualizaciones orientadas a riesgo financiero:

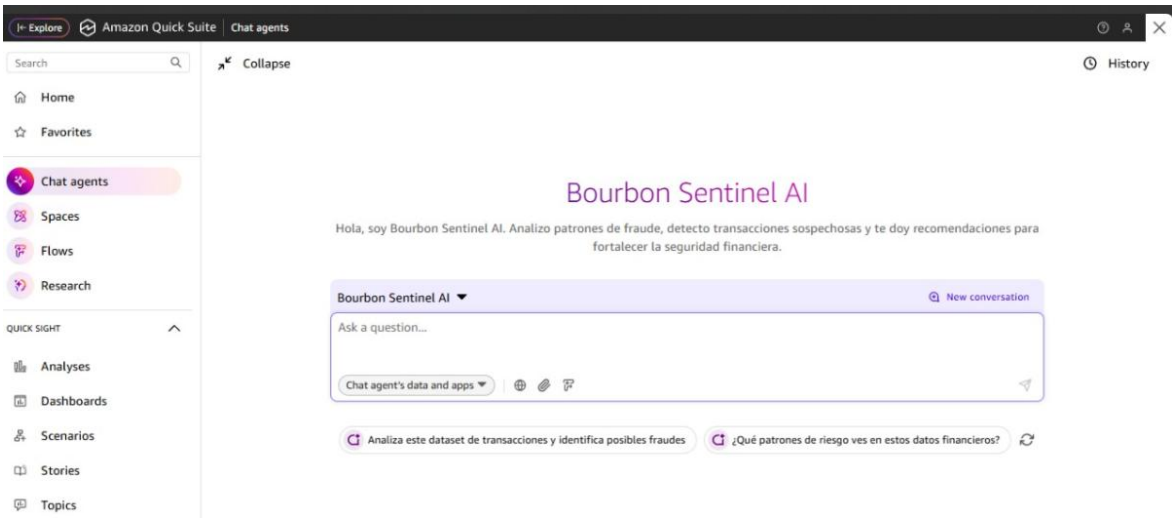
- Distribución del fraude
- Mapa de riesgo
- Comparativo real vs sintético
- Scores por rango
- Patrones anómalos

Finalmente se creó un **Agente Inteligente (Q Agent)** especializado en fraude financiero:

- configuración de rol como “experto en riesgo”
- enlace directo con los datos procesados en Athena
- diseño de saludo, estilo y prompts sugeridos
- pruebas interactivas con lenguaje natural

Con ello se completó una solución integral que combina modelado predictivo, despliegue automático, analítica avanzada y asistencia inteligente.

Figura 16. Vista Final



Análisis de Costos

El desarrollo del modelo predictivo basado en inteligencia artificial y generación de datos sintéticos para la detección temprana de fraude financiero busca demostrar que la inversión inicial requerida puede traducirse en un beneficio tangible para las entidades del sector financiero colombiano. Esto mediante el análisis correspondiente del conjunto de recursos humanos y técnicos directamente involucrados en el desarrollo del modelo.

Figura 5. Costos directos

Recurso / Rol	Salario mensual (COP)	Duración (meses)	Total (COP)
Data Scientist	5.500.000	4	22.000.000
ML / DevOps Engineer	5.000.000	4	20.000.000
Analista de Negocio / Datos	3.000.000	4	12.000.000
Servicios en la nube, licencias y datasets	3.000.000	4	12.000.000
Subtotal Costos Directos			**66.000.000**

Costos fijos

Comprenden los gastos de operación que permanecen constantes independientemente del volumen de producción, como el arriendo del espacio de trabajo y los servicios públicos.

Figura 6. Costos fijos

Concepto	Valor mensual (COP)	Duración	Total (COP)
Arriendo de oficina o laboratorio	2.000.000	4 meses	8.000.000
Servicios públicos y conectividad	500.000	4 meses	2.000.000
Subtotal Costos Fijos			**10.000.000**

Inversión (CAPEX)

Incluye los elementos necesarios para garantizar la infraestructura y cumplimiento normativo del proyecto.

Figura 7. Costos de inversión

Concepto	Valor (COP)
Hardware (servidor o GPU dedicada)	20.000.000
Instalación y configuración técnica	1.000.000
Permisos y cumplimiento regulatorio (Ley 1581, ISO 23894, NIST AI RMF)	4.000.000
Subtotal Inversión	**25.000.000**

Costos del prototipo

Servicio AWS	Costo mensual USD	Costo mensual COP
Amazon SageMaker	19.47	**81.774**
AWS Glue	0.12	**504**
Athena	0.00	0
S3	0.00	0
QuickSight	18.00	**75.600**
CloudWatch	6.00	**25.200**
TOTAL	**43.59**	**183.078**

Costos adicionales

Además de los costos directos, fijos e inversión, es necesario considerar una serie de costos complementarios que garantizan la ejecución adecuada y la estabilidad financiera del proyecto. Estos costos reflejan aspectos administrativos, contingencias y requerimientos operativos necesarios para mantener el flujo de trabajo durante la fase de desarrollo e implementación del modelo.

El overhead corresponde a los gastos generales de administración y coordinación del proyecto, el rubro de imprevistos cubre posibles variaciones o gastos no contemplados en la planeación inicial, y el capital de trabajo representa los recursos requeridos para sostener las operaciones (nómina y servicios) en los primeros meses de funcionamiento. A continuación, se detallan estos valores:

Figura 8. Costos adicionales

Concepto	Valor (COP)
Overhead (gastos administrativos 15%)	9.900.000
Imprevistos (5%)	1.250.000
Capital de trabajo (3 meses de nómina)	40.500.000
Total adicional	**51.650.000**

Costo total del proyecto

El costo total refleja la inversión requerida para desarrollar, implementar y operar un MVP funcional del modelo predictivo en un entorno controlado o piloto.

Figura 9. Costo total del proyecto

Tipo de costo	Valor total (COP)
Costos directos	66.000.000
Costos fijos	10.000.000
Inversión (CAPEX)	25.000.000
Otros (overhead, imprevistos, capital de trabajo)	51.650.000
Costo total estimado del proyecto	**152.650.000**

Análisis de rentabilidad

Basándonos en el costo total estimado del proyecto, que fue de 152.650.000 (COP), se evaluó la rentabilidad del proyecto considerando tres escenarios posibles de reducción del fraude financiero en una entidad bancaria promedio en Colombia.

Se parte de un valor anual estimado de pérdidas por fraude de 2.000 millones de pesos (Asobancaria, 2024). Los indicadores de evaluación utilizados fueron el Retorno sobre la Inversión (ROI) y el Periodo de Recuperación (Payback).

Figura 22. Rentabilidad

Escenario	Reducción esperada del fraude	Ahorro anual estimado (COP)	ROI (%)	Payback (años)	Payback (meses aprox.)
Bajo	10%	200.000.000	**31,00%**	0,76	~9 meses
Realista	20%	400.000.000	**162,00%**	0,38	~5 meses
Optimista	30%	600.000.000	**293,00%**	0,25	~3 meses

Los resultados evidencian que, incluso bajo un escenario conservador (reducción del fraude del 10 %), el proyecto presenta una rentabilidad positiva y un periodo de recuperación inferior a un año. En los escenarios realista y optimista, el retorno de inversión supera ampliamente el 100 %, lo que demuestra que el desarrollo del modelo predictivo constituye una alternativa económicamente viable y atractiva para su implementación en entidades financieras.

El análisis financiero demuestra que el proyecto no solo es técnica y operativamente viable, sino también rentable en el corto plazo. Con una inversión aproximada de COP 152 millones, el modelo tiene la capacidad de generar ahorros anuales significativos derivados de la reducción del fraude financiero.

En términos prácticos:

- En el escenario realista, la inversión se recupera en menos de cinco meses, con un ROI del 162 %, lo que implica que por cada peso invertido se obtienen 1,62 pesos de beneficio neto.

- En el escenario optimista, el retorno se triplica en un solo año, mostrando el alto impacto económico del proyecto.

Además, los costos marginales del sistema son bajos, ya que, una vez implementado el modelo, puede replicarse y escalarse a múltiples entidades sin requerir nuevas inversiones proporcionales.

En conclusión, la aplicación del modelo predictivo basado en inteligencia artificial y datos sintéticos representa una inversión estratégica, capaz de mejorar la eficiencia operativa y reducir significativamente las pérdidas por fraude, contribuyendo a la sostenibilidad económica y tecnológica del sistema financiero colombiano.

Plan de implementación

El desarrollo e implementación del prototipo se plantea como una extensión práctica de la metodología descrita anteriormente, que busca materializar la propuesta del modelo. Es decir, que es como un proceso progresivo que avanza desde la preparación del entorno de trabajo hasta la evaluación final del desempeño del modelo.

En primer lugar, se realiza la configuración del entorno técnico y la recopilación de los conjuntos de datos necesarios para el entrenamiento. Estos datos son sometidos a procesos de depuración, anonimización y transformación, con el fin de generar información sintética que represente de manera equilibrada los comportamientos legítimos y fraudulentos observados en el contexto financiero.

Posteriormente, se lleva a cabo la construcción del modelo predictivo, utilizando métodos de aprendizaje supervisado adecuados para el tipo de problema abordado. En esta etapa se desarrollan procesos de entrenamiento, ajuste y validación del modelo mediante indicadores de precisión, sensibilidad y capacidad de detección, priorizando la

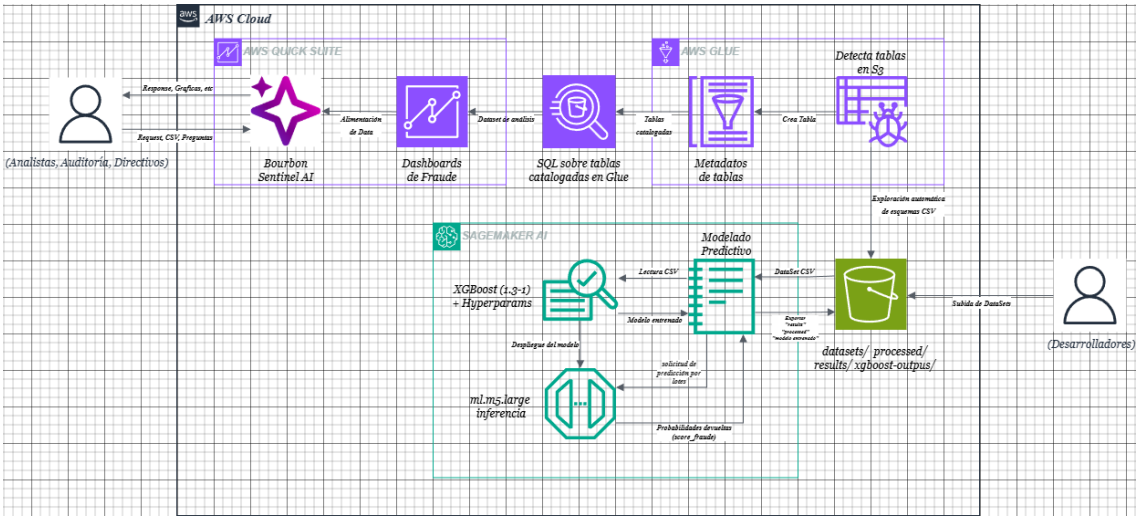
reducción de falsos negativos, dado que un caso de fraude no identificado genera un impacto económico considerable.

Una vez obtenido el modelo base, se procede con la validación técnica y funcional, comparando su desempeño frente a datos sintéticos para medir su capacidad de generalización. En este punto, también se evalúa la coherencia y explicabilidad de los resultados, garantizando que las decisiones del modelo sean interpretables, auditables y alineadas con los criterios éticos y regulatorios definidos.

Finalmente, se integra el prototipo funcional en un entorno de simulación que permite recrear escenarios de operaciones financieras y analizar su comportamiento ante posibles eventos de fraude. Durante esta etapa se monitorean variables como el tiempo de respuesta, la estabilidad del sistema y la efectividad de las alertas generadas. Los resultados de estas pruebas son documentados y analizados con el fin de identificar oportunidades de mejora y consolidar un modelo más robusto.

En conjunto, este plan de implementación asegura la transición desde el diseño metodológico hasta la comprobación práctica del modelo. Asimismo, permite validar su viabilidad técnica, operativa y económica, fortaleciendo los fundamentos que respaldan la aplicación de inteligencia artificial y datos sintéticos como herramientas de apoyo para la gestión del riesgo financiero en Colombia.

Figura 23. Arquitectura.



Conclusiones

El desarrollo del modelo predictivo basado en inteligencia artificial y generación de datos sintéticos permitió cumplir satisfactoriamente los objetivos planteados, demostrando la viabilidad técnica, ética y económica de esta solución para la detección temprana de fraudes en el sector financiero colombiano. El modelo evidenció que el uso de datos sintéticos constituye una herramienta eficaz para superar las limitaciones de privacidad y el desbalance de clases en los conjuntos de datos reales, posibilitando un entrenamiento más robusto y confiable.

En relación con los objetivos específicos, se logró analizar el contexto nacional del fraude financiero y la pertinencia de la inteligencia artificial en su mitigación; se diseñó una arquitectura conceptual coherente con las restricciones legales y técnicas del entorno colombiano; y se validó la propuesta mediante simulaciones sintéticas, confirmando su aplicabilidad teórica y potencial para integrarse en sistemas reales de monitoreo bancario.

La metodología empleada, fundamentada en enfoques mixtos y herramientas de software libre, garantizó la replicabilidad académica del modelo y la sostenibilidad tecnológica del proyecto. Asimismo, se comprobó que, incluso bajo escenarios conservadores, la propuesta presenta una alta rentabilidad, con periodos de recuperación inferiores a un año y beneficios económicos directos derivados de la reducción de pérdidas por fraude.

Entre las principales limitaciones se identifican las restricciones de infraestructura computacional y la imposibilidad de probar el modelo en entornos financieros reales debido a consideraciones de confidencialidad. Sin embargo, los resultados obtenidos sientan bases sólidas para futuras implementaciones en colaboración con entidades del sector, utilizando entornos controlados y regulados.

Finalmente, este proyecto contribuye al fortalecimiento del ecosistema de ciberseguridad financiera en Colombia, promoviendo el uso responsable de la inteligencia artificial conforme a la Política Nacional de IA (CONPES 4144 de 2025). Se propone continuar el trabajo con modelos de aprendizaje federado y procesamiento de lenguaje natural, ampliando su alcance hacia sistemas predictivos más integrales y éticos, orientados a la prevención proactiva del riesgo financiero y la protección del usuario bancario.

Bibliografía

APPLICATION OF MACHINE LEARNING MODELS FOR FRAUD DETECTION IN SYNTHETIC MOBILE FINANCIAL TRANSACTIONS. (n.d.). https://bibliotecaean.primo.exlibrisgroup.com/discovery/fulldisplay?context=PC&vid=57EAN_INST:57EAN&docid=cdi_unpaywall_primary_10_33480_jitk_v10i4_6420

Artificial Intelligence Risk Management Framework (AI RMF 1.0). (2023).

Asobancaria. (2023). *COMUNICADO DE PRENSA – En Colombia, más del 99% de las transacciones financieras, tanto digitales como físicas, se realizan sin incidentes de fraude*. https://www.asobancaria.com/2023/10/26/en-colombia-mas-del-99-de-las-transacciones-financieras-tanto-digitales-como-fisicas-se-realizan-sin-incidentes-de-fraude/

Asobancaria. (2024). *Informe de Gestión Gremial*.

BBVA refuerza sus capacidades de prevención de fraude. (n.d.). Retrieved November 6, 2025, from https://www.bbva.com/es/innovacion/bbva-refuerza-sus-capacidades-de-prevencion-de-fraude/.

BBVA y Featurespace colaboran en la lucha antifraude - Featurespace. (n.d.). Retrieved November 6, 2025, from https://www.featurespace.com/es/newsroom/bbva-y-featurespace-colaboran-en-la-lucha-antifraude.

Becerra-Suarez, F. L., Alvarez-Vasquez, H., & Forero, M. G. (2025). Improvement of Bank Fraud Detection Through Synthetic Data Generation with Gaussian Noise. *Technologies 2025, Vol. 13, Page 141*, *13*(4), 141. https://doi.org/10.3390/TECHNOLOGIES13040141

Bernardo, J., Fuentes, T., Javier, E., & Arias, M. (2025). Modelos de machine learning para la detección de fraudes financieros: Una revisión de la literatura. *UNESUM - Ciencias. Revista Científica Multidisciplinaria*, *9*(2), 220–234. https://doi.org/10.47230/UNESUM-CIENCIAS.V9.N2.2025.220-234

BusinessCol. (2024). *Retos en prevención del fraude bancario*.

Cada peso perdido por fraude en Colombia cuesta a las empresas 3,76 veces más, según el estudio "El verdadero costo del fraude en América Latina." (n.d.). https://risk.lexisnexis.com/global/es/about-us/press-room/press-release/20240620-true-cost-of-fraud-colombia

CardSim: A Bayesian Simulator for Payment Card Fraud Detection Research. (n.d.). https://bibliotecaean.primo.exlibrisgroup.com/discovery/fulldisplay?context=PC&vid=57EAN_INST:57EAN&docid=cdi_crossref_primary_10_17016_FEDS_2025_017

Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). *Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review*. https://arxiv.org/pdf/2502.00201v2

Ciberseguridad en el sector financiero colombiano creció 16 % en 2024 - Revista C-Level. (2025). https://revistaclevel.com/ciberseguridad-en-el-sector-financiero-colombiano-crecio-16-en-2024

C-Level, R. (2024). *73% de entidades financieras en Colombia ya usan inteligencia artificial*.

Colcob. (2024). *Inteligencia Artificial en Colombia – sector financiero*.

Colombia es el país más preocupado por el fraude bancario y robo de identidad, según nuevo índice de Seguridad de Unisys. (2018).

https://www.unisys.com/es/news-release/colombia-es-el-pais-mas-preocupado-por-el-fraude-bancario-y-robo-de-id/

Colombia, T. (2023). *859% aumentaron intentos de fraude digital en Colombia durante los últimos tres años*. https://noticias.transunion.co/859-aumentaron-intentos-de-fraude-digital-en-colombia-durante-los-ultimos-tres-anos/

Colombia, T. (2024). *Aumentan 26,1% los intentos sospechosos de fraude al comercio electrónico durante la temporada de fin de año en Colombia de 2023 a 2024*. https://noticias.transunion.co/aumentan-261-los-intentos-sospechosos-de-fraude-al-comercio-electronico-durante-la-temporada-de-fin-de-ano-en-colombia-de-2023-a-2024/

Colombiano, G. (2024). *Persisten los retos de prevención del fraude*.

CONPES 4144: La hoja de ruta de Colombia en Inteligencia Artificial para los retos actuales y la transformación futura. (n.d.). https://www.dnp.gov.co/publicaciones/Planeacion/Paginas/conpes-4144-hoja-de-ruta-colombia-inteligencia-artificial-retos-actuales-transformacion-futura.aspx

de Colombia, G., & VIDA, C. P. D. E. L. A. (n.d.). *Estrategia Nacional Digital de Colombia 2023 - 2026*.

Denzin, N. K. (2017). *The Research Act*. https://doi.org/10.4324/9781315134543

Detección de fraudes en banca con datos sintéticos | Syntho. (n.d.). Retrieved November 6, 2025, from https://www.syntho.ai/es/fraud-detection-in-banking-with-synthetic-data/

Detección del fraude con IA en el sector bancario | IBM. (n.d.). Retrieved November 6, 2025, from https://www.ibm.com/es-es/think/topics/ai-fraud-detection-in-banking

Duitama, K. P. (2025). *Colombia fue el cuarto país con más ciberataques en la región, 36.000 millones en 2024*. https://www.larepublica.co/internet-economy/colombia-tuvo-36-000-millones-de-ciberataques-4178202

EBizLatam. (2024). *70% de bancos colombianos usa IA en fraudes financieros*.

Edgar Alonso Lopez-Rojas, Ahmad Elmir, & Stefan Axelsson. (n.d.). *PAYSIM: AFINANCIALMOBILEMONEYSIMULATORFORFRAUDDETECTION*. Retrieved November 6, 2025, from extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.msc-les.org/proceedings/emss/2016/EMSS2016_249.pdf#:~:text=The%20work%20presented%20in%20this,behaviour%20during%20transactions%20and%20are

Efficient Acceleration of Deep Learning Inference on Resource-Constrained Edge Devices: A Review. (n.d.). https://bibliotecaean.primo.exlibrisgroup.com/discovery/fulldisplay?context=PC&vid=57EAN_INST:57EAN&docid=cdi_unpaywall_primary_10_1109_jproc_2022_3226481

Engineering design: A systematic approach (Book)). (n.d.). https://bibliotecaean.primo.exlibrisgroup.com/discovery/fulldisplay?context=PC&vid=57EAN_INST:57EAN&docid=cdi_proquest_miscellaneous_24908502

¿Esperanza o peligro? La IA generativa ocupa un lugar central la Semana contra el Fraude 2023. | *SAS*. (n.d.). Retrieved November 6, 2025, from https://www.sas.com/es_mx/news/press-releases/locales/2023/esperanza-o-peligro-ia-fraude.html

Figueira, A., & Vaz, B. (2022). Survey on Synthetic Data Generation, Evaluation Methods and GANs. *Mathematics*, *10*(15), 2733. https://doi.org/10.3390/math10152733

Fintech: La-inteligencia artificial-las-blinda del-fraude digital- Grupo Milenio. (n.d.-a). Retrieved November 6, 2025, from https://www.milenio.com/negocios/fintech-la-inteligencia-artificial-las-blinda-del-fraude-digital

Fintech: La-inteligencia artificial-las-blinda del-fraude digital- Grupo Milenio. (n.d.-b). Retrieved November 6, 2025, from https://www.milenio.com/negocios/fintech-la-inteligencia-artificial-las-blinda-del-fraude-digital

Fitzgerald, B. (2006). The Transformation of Open-Source Software. *MIS Quarterly*, *30*(3), 587–598. https://doi.org/10.2307/25148740https://www.jstor.org/stable/25148740

Global Risks Report 2024 | *World Economic Forum*. (2025). https://www.weforum.org/publications/global-risks-report-2024/

Guirao Goris, S. J. A. (2015). Utilidad y tipos de revisión de literatura. *Ene*, *9*(2), 0–0. https://doi.org/10.4321/S1988-348X2015000200002

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024a). Financial fraud detection through the application of machine learning techniques: a literature review. *Humanities and Social Sciences Communications 2024 11:1*, *11*(1), 1–22. https://doi.org/10.1057/s41599-024-03606-0

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024b). Financial fraud detection through the application of machine learning techniques: a literature review. *Humanities and Social Sciences Communications 2024 11:1*, *11*(1), 1–22. https://doi.org/10.1057/s41599-024-03606-0

IA para indentificar fraude en bancos y aseguradoras. (n.d.). Retrieved November 6, 2025, from https://sherpa.ai/es/blog/como-el-aprendizaje-federado-esta-transformando-el-sector-financiero/

Inteligente, D. C. (2024). *Powering the Data-Center Boom with Low-Carbon Solutions*. https://colombiainteligente.org/es_co/tendencias/powering-the-data-center-boom-with-low-carbon-solutions/

ISO/IEC 23894:2023. (n.d.). https://www.iso.org/standard/77304.html

ITSitio. (2024). *Fraudes financieros en Colombia: 70% de los bancos usa IA*.

Iván, C., Alberto, L., Técnica Luis Vargas Torres de Esmeraldas, U., Domingo Universidad Técnica Luis Vargas Torres de Esmeraldas, S., Domingo, S., & Científico, 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

Latinpyme. (2024). *Analítica e inteligencia artificial: el nuevo escudo contra el fraude digital en Colombia*.

Ley 1581 de 2012 - Gestor Normativo. (n.d.). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Liu, Y., & Hu, R. (2025). Artificial intelligence, supply chain finance, and corporate investment efficiency. *Finance Research Letters*, *85*, 107851. https://doi.org/https://doi.org/10.1016/j.frl.2025.107851

Luisa Fernanda Ramírez Pinzón. (2024). *Optimización de la detección de fraude en el sector financiero a través del análisis de datos y Business Intelligence* [Universidad Nacional Abierta y a Distancia UNAD]. https://repository.unad.edu.co/bitstream/handle/10596/67106/lframirezpi.pdf?sequence=1

Mahecha, C. A. G. (2024). *Cuatro de cada 10 colombianos, objeto de fraude digital; les contamos ¿dónde están los mayores riesgos?, según TransUnion*. https://www.eltiempo.com/economia/sector-financiero/cuatro-de-cada-10-colombianos-fueron-objeto-de-fraude-digital-les-contamos-donde-estan-los-mayores-riesgos-segun-transunion-3394447

MEASURING THE ENVIRONMENTAL IMPACTS OF ARTIFICIAL INTELLIGENCE COMPUTE AND APPLICATIONS. (2022).

Mercado de generación de datos sintéticos | Análisis de pronóstico [2030]. (n.d.). Retrieved November 6, 2025, from https://www.fortunebusinessinsights.com/es/synthetic-data-generation-market-108433

Micol, M. (2025). Balancing Ethical Innovation: The Role of Synthetic Data in Financial Regulation. *Integrated Science*, *35*, 179–190. https://doi.org/10.1007/978-3-031-87023-1_14

Modelos interpretables: la clave para combatir el fraude de forma justa y transparente - Hidden Insights. (n.d.). Retrieved November 6, 2025, from https://blogs.sas.com/content/hiddeninsights/2024/03/18/modelos-interpretables-la-clave-para-combatir-el-fraude-de-forma-justa-y-transparente/

(PDF) Análisis de Fraudes en Transacciones Bancarias Aplicando Minería de Datos. (n.d.). Retrieved August 18, 2025, from https://www.researchgate.net/publication/354424151_Analisis_de_Fraudes_en_Transacciones_Bancarias_Aplicando_Mineria_de_Datos

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., Vanderplas, J., Passos,

A., Cournapeau, D., Brucher, M., Perrot, M., & Duchesnay, E. (2010). *SciKit-Learn: Machine Learning in Python*.

Qatawneh, A. M. (2024). The role of artificial intelligence in auditing and fraud detection in accounting information systems: moderating role of natural language processing. *International Journal of Organizational Analysis*, *33*(6), 1391–1409. https://doi.org/https://doi.org/10.1108/IJOA-03-2024-4389

Qi, Y., & Su, H. (2025). Can artificial intelligence mitigate corporate fraud? Exploring the influence of institutional crossholdings and financial misallocation. *Pacific-Basin Finance Journal*, *92*, 102822. https://doi.org/https://doi.org/10.1016/j.pacfin.2025.102822

¿Qué capacidades aporta la Inteligencia Artificial en la lucha contra el fraude? | *Latinia*. (n.d.). Retrieved November 6, 2025, from https://latinia.com/es/resources/inteligencia-artificial-para-prevenir-fraude-bancario

República, L. (2023). *Fraude digital en el sector financiero*.

Riaño, D. A. V. (2023). *En 2022, cuatro de cada 10 hogares en Colombia no tuvieron conexión a internet: Dane* | *El Colombiano*. https://www.elcolombiano.com/negocios/internet-colombia-como-estuvo-acceso-en-2022-segun-el-dane-EA22007939

Roy, R., Tiwari, D., & Pandey, A. (2024). FraudDiffuse: Diffusion-aided Synthetic Fraud Augmentation for Improved Fraud Detection. *ICAIF 2024 - 5th ACM International Conference on AI in Finance*, 90–98. https://doi.org/10.1145/3677052.3698658

Siglo, E. N. (2024). *El 73% de las entidades financieras han implementado IA*.

Superfinanciera. (2025). *El papel de la inteligencia artificial en la transformación de la supervisión financiera*.

https://www.superfinanciera.gov.co/publicaciones/10115852/el-papel-de-la-inteligencia-artificial-en-la-transformacion-de-la-supervision-financiera/

Syntho. (2023). *Fraud detection in banking with synthetic data*.

Tarazona Nieto, M. C., Mateus Agudelo, L. C., Becerra Barajas, L. R., & Pérez Beltrán, D. A. (n.d.). *Métodos de Machine Learning para detección de fraude en transacciones financieras en tiempo real*. Universidad EAN.

Tendencias de Fraude con IA 2025: Los Bancos Contraatacan | Feedzai. (n.d.). Retrieved November 6, 2025, from https://www.feedzai.com/es/pressrelease/tendencias-de-fraude-con-ia-2025/

The Synthetic Data Vault. (n.d.). https://ieeexplore.ieee.org/document/7796926

Treasury Announces Enhanced Fraud Detection Processes, Including Machine Learning AI, Prevented and Recovered Over $4 Billion in Fiscal Year 2024 | U.S. Department of the Treasury. (n.d.). Retrieved November 6, 2025, from https://home.treasury.gov/news/press-releases/jy2650

Zhang, C., Bengio, S., Hardt, M., Recht, B., & Vinyals, O. (2021). Understanding deep learning (still) requires rethinking generalization. *Communications of the ACM*, *64*(3), 107–115. https://doi.org/10.1145/3446776

Zhang, Y., & Chen, W. (2020). Deep learning models for fraud detection in financial transactions. *Neural Computing and Applications*, *32*, 10859–10872. https://doi.org/10.1007/s00521-020-04877-0