Identificación De las Principales Prácticas Implementadas por las Entidades Financieras para Combatir el Fraude Financiero

Jessica Lorena Cárdenas Justinico

Jeison Felipe Cárdenas Saavedra

Universidad EAN

Facultad de Administración, Finanzas y Ciencias Económicas

Maestría en Inteligencia de Negocios

Maestría en Administración de Empresas - MBA

Bogotá, Colombia

05/05/2025

Identificación De las Principales Prácticas Implementadas por las Entidades Financieras para Combatir el Fraude Financiero

Jessica Lorena Cárdenas Justinico

Jeison Felipe Cárdenas Saavedra

Trabajo de grado presentado como requisito para optar al título de:

Magister en Inteligencia de Negocios

Magister en Administración de Empresas

Director (a):

Omar Alonso Patiño

Modalidad:

Consultoría Profesional

Universidad EAN

Facultad de Administración, Finanzas y Ciencias Económicas

Maestría en Inteligencia de Negocios

Maestría en Administración de Empresas - MBA

Bogotá, Colombia

05/05/2025

Nota de aceptación:

Firma del jurado

Firma del jurado

Firma del director del trabajo de grado

Bogotá D.C., 16/05/2025

Dedicatoria

A Dios, por ser mi guía y fortaleza en cada paso de este camino.

A mis padres, por su apoyo incondicional a lo largo de este proceso.

A mi esposo, por su amor, paciencia y por estar siempre a mi lado, animándome a seguir adelante, siendo un ejemplo y no permitiéndome rendirme en ningún momento. Te amo Vida

Y muy especialmente a mi hijo Santiago. Te amo, hijo. Gracias por tu paciencia y apoyo incondicional. Tu amor y comprensión han sido mi mayor motivación.

Jessica Cárdenas

A mis padres, por su amor inmenso y apoyo incondicional en cada momento, acompañándome siempre en la búsqueda de ser una mejor persona y profesional.

También a mi hermano, por ser un faro de fuerza y resiliencia, siempre mostrándome que, sin importar las adversidades, es posible seguir adelante con determinación y esperanza.

Jeison Cárdenas

Agradecimientos

Agradecemos en primer lugar a Dios, quien nos ha brindado la fortaleza, la salud y las oportunidades para llegar hasta este punto. Su guía y su luz nos han acompañado en cada etapa de este proceso, incluso en los momentos más desafiantes.

Nuestro agradecimiento eterno a nuestra familia, quienes son el pilar de nuestra vida y nuestro mayor soporte. Sin su apoyo incondicional, no sería posible culminar esta etapa de nuestras vidas.

De manera especial, expresamos nuestra gratitud al Doctor en Ciencias Empresariales Omar Alonso Patiño, director de esta tesis. Su experiencia, paciencia y orientación constante han sido esenciales para dar forma a esta investigación. Sus observaciones precisas y consejos fueron clave para alcanzar los objetivos trazados. Su apoyo incondicional ha sido fundamental para lograr la culminación exitosa de este trabajo de grado.

.

Resumen

El presente trabajo analiza las principales prácticas implementadas por las entidades financieras para combatir el fraude financiero, con un enfoque especial en el Banco Itaú Colombia. Este fenómeno, potenciado por la digitalización y los avances tecnológicos, representa un desafío creciente tanto a nivel global como en América Latina. Mediante una revisión sistemática de literatura y el análisis de casos reales, se identificaron patrones de fraude interno y externo, así como metodologías basadas en aprendizaje automático, minería de datos y técnicas avanzadas como redes neuronales y algoritmos de detección de anomalías. Los resultados muestran que las herramientas tecnológicas, combinadas con controles internos efectivos y una cultura organizacional y una estructura de Gobierno de Datos sólida, son clave para mitigar los riesgos de fraude y mejorar la sostenibilidad de las operaciones bancarias. Este estudio ofrece recomendaciones prácticas y un marco metodológico para fortalecer la gestión de riesgos financieros en las instituciones.

Palabras Claves: Fraude financiero, Detección de anomalías, Modelos predictivos, Gobierno de Datos, Control Interno.

Abstract

The present study analyzes the main practices implemented by financial institutions to combat financial fraud, with a particular focus on Banco Itaú Colombia. This phenomenon, driven by digitalization and technological advancements, poses a growing challenge both globally and in Latin America. Through a systematic literature review and the analysis of real cases, patterns of internal and external fraud were identified, as well as methodologies based on machine learning, data mining, and advanced techniques such as neural networks and anomaly detection algorithms. The results demonstrate that technological tools, combined with effective internal controls, a strong organizational culture, and a robust Data Governance structure, are essential to mitigating fraud risks and improving the sustainability of banking operations. This study provides practical recommendations and a methodological framework to strengthen financial risk management within institutions.

Keywords: Financial fraud, Anomaly detection, Predictive models, Data Governance, Internal control.

Tabla de contenido

Lista de Figuras

Pág.

Lista de Tablas

Pág.

1. Introducción

1.1. Tema de Investigación

El presente trabajo titulado "Identificación de las Principales Prácticas Implementadas por las Entidades Financieras para Combatir el Fraude Financiero", es una consultoría realizada en el marco de la Maestría en Inteligencia de Negocios y la Maestría en Administración de Empresas de la Universidad EAN. El enfoque de la consultoría es evaluar las tecnologías emergentes y metodologías analíticas más eficaces para la detección y prevención del fraude financiero interno y externo, y cómo estas pueden ser integradas en las estrategias actuales del Banco Itaú Colombia.

1.2. Problema de Investigación

1.1.1. Antecedentes

Los avances tecnológicos y la cantidad creciente de datos generados han creado un entorno propicio para el aumento significativo del fraude, especialmente en el ámbito bancario. Los delincuentes siempre encuentran formas de eludir las medidas de seguridad, aunque no de forma inmediata, eventualmente logran alcanzar su objetivo principal: robar. (Delarue, 2020), en su informe, concuerda en que las empresas disponen de una mayor

cantidad de datos, aunque en vez de ver un problema, lo plantea como una oportunidad para detectar fraudes mediante el uso y análisis de estos datos y técnicas forenses. Además, se resalta el papel crucial que desempeñan los auditores en la actualidad, quienes pueden identificar transacciones o comportamientos inusuales y patrones que podrían sugerir o predecir fraude.

Un control deficiente da pie a casos como lo es el de la empresa Wirecard, (De León Obrador, 2022), que en 2020 fue acusada de inflar sus cuentas de respaldos en aproximadamente 1.900 millones de euros que nunca existieron. Este escándalo no solo implicó fraude contable, sino también la manipulación de auditorías por parte de los altos ejecutivos y la falta de control interno adecuado. De manera similar, otro escándalo financiero muy popular fue el de Wells Fargo en 2016 (Lilly et al., 2021), donde se reveló que más de 30.000 empleados habían participado en la apertura de aproximadamente dos millones de cuentas sin el consentimiento de los clientes.

El fraude financiero en Wells Fargo involucró la apertura sistemática y no autorizada de cuentas bancarias y productos financieros, generando tarifas e intereses fraudulentos que ascendieron a 3 mil millones de dólares. La falta de controles internos permitió que el esquema pasara desapercibido durante años. Como consecuencia, el banco sufrió sanciones financieras y un daño significativo a su reputación, obligándolo a implementar reformas para recuperar la confianza del público y mejorar sus prácticas de gobernanza. De manera similar, en Dinamarca, el escándalo de Danske Bank (Vinther Daugaard et al., 2024) involucró el procesamiento de aproximadamente 200.000 millones de euros de origen sospechoso a través de sus sucursales en Estonia

entre 2007 y 2015. La detección del fraude se logró mediante una combinación de auditorías internas y análisis de datos transaccionales.

Los fraudes más comunes a nivel mundial incluyen la manipulación de transacciones internas, la gestión engañosa de proveedores y la apropiación indebida de fondos, todo esto debido a un control interno poco efectivo que no previene o detecta a tiempo los comportamientos inusuales de los empleados al interior de las entidades bancarias (Usman, Abdullahi, et al., 2024).

El panorama Latinoamérica, presenta un comportamiento similar al de nivel mundial en cuanto en temas de fraude financiero, no obstante, presenta un comportamiento en mayor medida. El informe (Cybersource, n.d.), señala que las empresas latinoamericanas son cada vez más conscientes de los riesgos asociados, especialmente debido a la creciente digitalización. Este fenómeno ha llevado a un aumento en la adopción de tecnologías avanzadas de detección y prevención de fraudes, como el uso de herramientas de aprendizaje automático y análisis de datos.

El estudio "Mitigating Financial Fraud Using Data Science" destaca cómo el análisis de datos y la ciencia de datos se están utilizando para mitigar el fraude financiero, con un enfoque particular en el fraude con tarjetas de crédito. Las técnicas incluyen redes neuronales y máquinas de vectores de soporte (SVM), que han demostrado ser efectivas para reducir los falsos positivos y mejorar la precisión en la detección de fraudes.

En Colombia, el Banco Itaú CorpBanca ha sido un ejemplo destacado de cómo las instituciones financieras enfrentan desafíos relacionados con el fraude financiero. La manipulación de transacciones internas y la apropiación indebida de fondos son dos

de los problemas más comunes. La adopción de sistemas de inteligencia artificial y análisis de datos ha sido fundamental para la detección temprana de estas actividades fraudulentas, permitiendo al banco identificar patrones sospechosos y tomar medidas correctivas a tiempo (W. Li et al., 2020).

Un estudio sobre el impacto del control interno en la detección y prevención de fraudes en Colombia resalta la importancia de fortalecer los sistemas de control interno. Este estudio sugiere que la implementación de mejores prácticas de gobernanza y auditoría, así como el uso de herramientas avanzadas de análisis de datos, puede mejorar significativamente la capacidad de las instituciones para detectar y prevenir el fraude (Leal et al., 2014).

En este orden de ideas, el fraude financiero, tanto interno como externo, es un desafío creciente a nivel global, latinoamericano y colombiano. La digitalización y la sofisticación de los delincuentes exigen el uso de tecnologías avanzadas como el aprendizaje automático y el análisis de Big Data para proteger los activos financieros y mantener la confianza de los clientes. Las instituciones deben seguir innovando en sus estrategias de prevención y detección de fraudes para enfrentar eficazmente estas amenazas. Por esta razón, las metodologías o técnicas de detección de fraude son esenciales para identificar a los delincuentes una vez que las medidas de prevención han fallado (Assunção et al., 2015; Joyanes, 2019).

Un caso notable de fraude interno es la manipulación de transacciones internas, donde empleados con accesos privilegiados alteran registros financieros para crear cuentas ficticias y desviar fondos. Este tipo de actividad fraudulenta se ha identificado a través del análisis de Big Data, que permite detectar patrones anómalos en los flujos

de transacciones, facilitando así la detección temprana de estas prácticas fraudulentas (Perdomo Maldonado, 2017; Valenzuela et al., 2022a).

Otro ejemplo relevante es el fraude en la gestión de proveedores, en el cual empleados internos coluden con proveedores externos para inflar facturas o cobrar por servicios no prestados. La detección de este fraude ha sido posible gracias al uso de análisis avanzados de datos, que comparan detalles de facturación con registros de servicios efectivamente realizados. Algoritmos de aprendizaje automático han sido clave para identificar discrepancias que revelan actividades fraudulentas (OEA & ASOBANCARIA, 2020; Perdomo Maldonado, 2017; Valenzuela et al., 2022a).

Finalmente, la apropiación indebida de fondos es otro caso común de fraude interno, en el que los empleados sustraen fondos directamente de las cuentas de la institución. Un caso destacado incluye el uso de sistemas de inteligencia artificial para monitorear y analizar patrones de acceso a sistemas críticos, identificando comportamientos sospechosos, como accesos fuera de horarios normales o desde ubicaciones inusuales (Valenzuela et al., 2022a).

1.1.2. Planteamiento del Problema

El Banco Itaú CorpBanca Colombia S. A., brazo local de la institución financiera brasileña Itaú Unibanco (Itaú, 2023c), ha cimentado su presencia en Colombia ofertando servicios como cuentas de ahorro, corriente, tarjetas de débito, crédito, préstamos

hipotecarios, rotativos, libranza, inversiones, seguros y fiducias a personas naturales o negocios corporativos (Itaú, 2023a). Aunque a lo largo de dos décadas el Banco Itaú Colombia ha experimentado una serie de adquisiciones o fusiones (Itaú, 2016), el establecimiento bancario ha logrado posicionarse como el décimo mejor banco de Colombia gracias a su total de activos de casi 30 billones de dólares (Itaú, 2022). Adicional a esto, la entidad financiera siempre está en búsqueda de adaptarse al cambio que experimenta el mercado y la innovación tecnológica que caracteriza a la entidad financiera. Por eso es que con base a su objetivo principal de migrar cerca del 60% de sus cargas de trabajo a la Nube y bajo el lema "La tecnología no sólo da soporte, es la base de la transformación", la marca Itaú se ha logrado posicionar como la número 1 en América Latina y la 261 en el mundo, según el Brand Finance Global Ranking Global 2024 (Haigh, 2024).

Ahora bien, el Banco Itaú Colombia, al igual que otros actores del sistema financiero, debe hacerle frente a la grave problemática del fraude financiero con el fin de hacer sostenibles los logros que hasta el momento ha alcanzado. Se calcula que sólo para el año 2023 se produjeron casi $ 11.000 MM de pérdidas netas a causa de este tipo de riesgo operacional (Itaú, 2023b), donde el fraude externo abarca una cantidad de $ 6.345 MM (58%) y el fraude interno una cantidad de casi $ 3.000 MM (28%) a causa de la ejecución de procesos o relaciones laborales, siendo estos dos últimos los conflictos internos más relevantes. Mientras que, las exposiciones más importantes a considerar en el fraude externo se contemplan la estafa en tarjetas de créditos o débitos, y la suplantación de identidad en el portal web o la aplicación del celular.

No obstante, Itaú CorpBanca Colombia S.A. ha estado tratando este problema en el 2023 por medio de la promoción de una cultura de prevención de fraudes y de un Sistema de Gestión Antisoborno según la norma ISO 310000(Itaú, 2023b). De esta forma, las pérdidas operacionales se han reducido aproximadamente en $6.000 MM (40%) respecto al año 2022, en el cual las pérdidas netas asociadas al fraude financiero fueron de $18.657 MM (Itaú, 2022). Principalmente, esto se puede deber a que el sistema bancario aún debe mejorar los modelos de predicción de fraude en tiempo real para prevenir ataques externos acarreados en gran medida por la transformación digital.

Dentro de los desafíos que afronta el Banco Itaú esta mejorar la capacidad de detectar y prevenir el fraude en tiempo real, pues con el crecimiento de las transacciones digitales, es fundamental contar con modelos predictivos que puedan identificar patrones y comportamientos fraudulentos de manera rápida y precisa, ya que, a medida que más usuarios migran hacia plataformas digitales para realizar sus operaciones bancarias, la cantidad de datos generados aumenta exponencialmente, lo que presenta retos significativos en términos de procesamiento y análisis de datos. Sin embargo, la complejidad de los datos y la velocidad a la que se producen las transacciones plantean desafíos adicionales en términos de procesamiento y análisis de datos en tiempo real (Pandey et al., 2024).

Además, con el aumento de canales digitales, se está transformando cómo los usuarios interactúan con los servicios financieros, impulsando la demanda de experiencias integradas, personalizadas y coherentes a través de canales transaccionales digitales. Este cambio se ha visto reflejado en la adaptación de entidades financieras colombianas como Bancolombia y Davivienda, quienes han validado la importancia de ajustarse a las

expectativas cambiantes de los consumidores en la era digital (Vargas Rojas & Luna, 2020).

Del mismo modo, para el banco Itaú la transformación digital es uno de sus objetivos principales, sin embargo, esto le genera nuevos desafíos asociados a la mejora de la eficiencia y la cobertura de productos financieros, la adaptación de los colaboradores a las nuevas tecnologías, la aplicación de estrategias efectivas de innovación y, sobre todo, enfocados en garantizar la seguridad de las transacciones en línea, especialmente en lo que respecta a la detección y prevención del fraude (Pandey et al., 2024).

Por otro lado, para el Banco Itaú se presenta otro desafío para adaptarse a las tácticas cambiantes de los delincuentes, pues a medida que evolucionan las tecnologías de seguridad, los delincuentes también están desarrollando nuevas formas de eludir los sistemas de detección que emplean las entidades. Esto requiere una mejora continua de los modelos predictivos de fraude para mantenerse al día con las últimas amenazas y tácticas utilizadas por los delincuentes (Pandey et al., 2024).

Adicionalmente, el Banco Itaú se enfrenta el reto de equilibrar la seguridad con la experiencia del cliente. Si bien es fundamental protegerse contra el fraude, también es importante garantizar una experiencia de servicio fluida y sin fricciones. Esto significa implementar medidas de seguridad robustas garantizando que estas no obstaculicen la experiencia del cliente. Para abordar estos desafíos, el Banco Itaú necesita desarrollar y mejorar sus capacidades en análisis de datos e implementación de inteligencia artificial, lo que implica invertir en la inclusión de tecnologías avanzadas de procesamiento de datos, como pueden ser el aprendizaje automático y el análisis predictivo, los cuales contribuyen en la mejora de la detección de patrones de fraude (Wu et al., 2023).

Por eso, este trabajo, buscará realizar un análisis de la situación actual a nivel global para identificar riesgos internos y externos que afrontan las entidades financieras; con esto, analizar los casos reales de fraude que han afrontado distintos actores del sector financiero, para identificar los patrones de riesgo al interior de estas entidades. Por otro lado, se investigará acerca de las buenas prácticas que han desarrollado las entidades financieras para combatir el fraude interno, así como, también se investigará sobre los modelos que las entidades han adoptado para hacer frente a esta problemática. Finalmente, con la investigación y el análisis desarrollado, se propondrá una metodología para seleccionar el modelo adecuado que permita la detección de fraudes, con el objeto de que el banco lo pueda implementar y así, aportar a la disminución de la pérdida neta que enfrenta la entidad por los fraudes internos.

1.1.3. Pregunta de Investigación

¿Qué tecnologías emergentes y metodologías analíticas han demostrado ser más eficaces en la detección y prevención del fraude financiero en entidades bancarias?

2. Objetivos de investigación

2.1. Objetivo general

Identificar las principales prácticas implementadas por las entidades financieras para combatir el fraude financiero.

2.2. Objetivos específicos

- Identificar casos reales de fraude interno/externo en entidades financieras a nivel Mundial.
- Analizar la información relevante para identificar los patrones en los casos reales de fraude interno en las entidades financieras a nivel Global.
- Describir modelos que se han propuesto o desarrollado para el análisis de los datos que permite la detección de fraude en las entidades financieras.
- Proponer una metodología para la selección de un modelo de predicción de fraude en entidades financieras.

3. Justificación

En la era actual de la transformación digital, los avances tecnológicos han revolucionado la forma en que las instituciones financieras operan y cómo los clientes interactúan con ellas. Sin embargo, esta digitalización también ha dado lugar a un aumento significativo en los casos de fraude financiero, representando una amenaza constante para la integridad del sistema financiero y la confianza del cliente. En este contexto, la implementación de modelos de detección de fraude y/o comportamientos inusuales se presenta como una herramienta indispensable para el Banco ITAÚ. Principalmente porque puede mitigar riesgos operacionales, mejorar prácticas y optimizar servicios.

La importancia del análisis del fraude interno en las entidades financieras a nivel Mundial radica en que estas pueden desarrollar su capacidad para identificar patrones y estar a la vanguardia en las buenas prácticas que otras entidades puedan desarrollar para detectar y prevenir el fraude a su interior. En el caso del Banco Itaú Colombia, donde la confianza del cliente y la integridad del sistema son fundamentales, el análisis del fraude interno no solo es una medida preventiva, sino también un desarrollo estratégico para la protección de activos e incrementar la reputación.

Al mitigar el fraude mediante el estudio y análisis de casos reales de fraude financiero, el banco puede reducir significativamente el riesgo operacional asociado con transacciones fraudulentas, esto se traduce en menores pérdidas financieras, evitando la necesidad de reembolsar a clientes afectados y minimizando el impacto negativo en la rentabilidad y la sostenibilidad a largo plazo del banco. Además, al identificar y prevenir

actividades fraudulentas de manera oportuna, se fortalece la confianza del cliente y se preserva la reputación del banco como una institución segura y confiable.

La investigación de casos reales de fraude interno en entidades financieras a nivel Mundial también tiene un impacto positivo en la mejora de las prácticas internas del banco. Al analizar y comprender los patrones de fraude, la institución puede detectar vulnerabilidades en sus sistemas y procesos existentes, permitiendo así realizar ajustes y mejoras continuas en la seguridad y la gestión de riesgos. Esto no solo mejora la eficiencia operativa, sino que también garantiza el cumplimiento de regulaciones y estándares de seguridad cada vez más rigurosos. Además, al asegurar la seguridad de las transacciones, se fomenta la adopción de servicios financieros digitales, lo que impulsa la innovación y el crecimiento del banco en un mercado cada vez más competitivo.

En términos de viabilidad, este proyecto es pertinente y factible en tiempo, recursos financieros, humanos y materiales. Principalmente, porque la investigación en la literatura científica no requiere mano de obra adicional ni una inversión económica para la adquisición de equipos. En definitiva, la investigación propuesta para la identificación de casos reales de fraude interno y de las acciones desarrolladas a nivel Mundial para la detección y prevención de fraude en el Banco ITAÚ no solo es esencial para mitigar riesgos y proteger activos, sino que también representa una oportunidad para mejorar prácticas, optimizar servicios y fortalecer la posición competitiva del banco en el mercado. Con el apoyo adecuado y un enfoque estratégico, este proyecto tiene el potencial de generar beneficios significativos a corto y largo plazo para el banco y sus clientes.

4. Marco Institucional

Itaú, un banco con un siglo de experiencia en el ámbito financiero mundial, ha consolidado su posición como líder en banca privada en América Latina. Para el 2023, se destacó como la marca más valiosa en la región y se ubicó en el puesto 242 a nivel mundial. Con su sede central en Brasil, Itaú tiene presencia en 18 países, siendo Itaú Unibanco su principal accionista (Banco Itaú, 2024).

El banco Itaú tuvo sus inicios en Colombia en 1912 con el Banco Alemán Antioqueño. En 1963, tuvo una participación accionaria en el Banco de Crédito, en 1992 se transformó en Bancoquia y en 1997 se fusionó con el Banco Santander. Posteriormente, en 2009 tuvo presencia en el país con la compra de Helm Bank, en 2013 realizó la fusión con CorpBanca, dándose la llegada de Itaú a Colombia en 2017. Para 2024, Itaú cumple 7 años como marca en el país, posicionándose como el décimo banco más grande por tamaño de activos (Banco Itau, 2024).

Desde su llegada al país, la misión del Banco Itaú ha sido convertirse en un aliado estratégico para sus clientes, ofreciendo productos y servicios financieros que satisfagan sus necesidades y contribuyan a su bienestar económico. Su visión es consolidarse como un referente de excelencia en el sector bancario colombiano, destacado por su cercanía con los clientes, la innovación y sostenibilidad en sus productos. Los valores fundamentales que orientan la actuación del banco en el país son la ética, la transparencia, el trabajo en equipo, la responsabilidad social y la diversidad, asegurando así una gestión integral y sostenible en el tiempo (Banco Itau, 2024).

El Banco Itaú Colombia se rige por sólidas políticas de gobierno corporativo, asegurando la transparencia, la sostenibilidad y la responsabilidad a largo plazo de la organización. Su junta directiva está integrada por profesionales de distintas áreas con una amplia trayectoria en el sector financiero que supervisan y orientan las decisiones estratégicas de la entidad. Además, su estructura organizacional en Colombia se caracteriza por su eficiencia y adaptabilidad a las dinámicas del mercado financiero. En 2024, se creó la vicepresidencia de Digital, Operaciones, Tecnología y Transformación (DOTT), sumándose a las vicepresidencias de Administrativa y Financiera, Riesgos, Tesorería y Global Markets, Digital y Marketing, Banca Minorista, Banca Mayorista, Gestión Humana, Jurídica, Tecnología, Cumplimiento, Operaciones y Auditoría (Banco Itau, 2024).

4.1. Sector Financiero Colombiano y Posición en el Mercado

El sector financiero colombiano ha experimentado una evolución significativa en las últimas décadas, caracterizándose por un crecimiento estable, una regulación rigurosa y la adopción de tecnologías innovadoras (Ocampo, 2021). En este contexto, Itaú ha logrado posicionarse como una entidad relevante, integrando tecnología avanzada para mejorar la experiencia del cliente y optimizar la gestión de riesgos. Su participación en el mercado está orientada hacia la banca personal, corporativa y de inversiones, con una fuerte presencia en sectores estratégicos de la economía colombiana.

Un factor determinante en la posición del banco ha sido la digitalización y la seguridad cibernética. El informe de la Organización de Estados Americanos (OEA) sobre ciberseguridad en el sistema financiero colombiano señala que el 97% de las entidades financieras del país han implementado protocolos de seguridad robustos para mitigar los riesgos asociados a fraudes digitales (OEA & ASOBANCARIA, 2020). En este sentido, Itaú ha adoptado prácticas avanzadas de protección de datos y transacciones para garantizar la seguridad de sus clientes.

4.2. Productos y Servicios

El modelo de negocio de Itaú Colombia está segmentado en soluciones especializadas para personas naturales y empresas. Dentro de la banca personal, el banco ofrece productos como cuentas corrientes y de ahorro, tarjetas de crédito, fiducias, inversiones y préstamos de consumo e hipotecarios. Para la banca corporativa, ofrece cuentas empresariales, inversiones, leasing y créditos estructurados. Además, cuenta con filiales como Itaú Comisionista de Bolsa Colombia, Itaú Fiduciaria Colombia, Itaú Panamá e Itaú Corredor de Seguros, que refuerzan su oferta integral de servicios financieros (Banco Itaú, 2024).

4.3. Tendencias y Retos del Sector

El sector bancario colombiano enfrenta diversos retos, entre ellos la transformación digital, la regulación financiera y la inclusión bancaria. Según el informe "La reinvención financiera en la era digital", la digitalización de los servicios financieros es una prioridad para el sector, ya que permite mejorar la eficiencia operativa y ampliar el acceso a servicios bancarios (Valenzuela et al., 2022b). Adicionalmente, el "Proyecto F" destaca la importancia de reducir el uso de efectivo y fomentar los medios de pago electrónicos para fortalecer la transparencia y la formalización de la economía (Perdomo Maldonado, 2017).

Asimismo, Asobancaria en su Informe de Gestión Gremial (IGG), entre varios desafíos que presenta el sector, destaca la transformación digital y la innovación dado que se está promoviendo el uso de medios digitales mediante tecnologías como inteligencia artificial y big data, lo que ha generado un aumento en las operaciones digitales y la implementación del modelo Open Finance, que consiste en el intercambio de información entre distintas entidades financieras. Esta transformación abre la puerta al desafío de mantener la seguridad y protección del usuario (existen 43 ciberataques por segundo), por lo que el sector ha realizado inversiones importantes en ciberseguridad, $463 mil millones para 2022, y alianzas entre los sectores públicos y privados, que acompañado con el modelo Open Finance, han permitido mantener el fraude en 0.6 pesos por cada 10.000 pesos transados (Malagón González et al., 2023).

5. Marco Conceptual y Contextual

El fraude en el sector financiero es un problema grave que puede resultar en pérdidas significativas para instituciones financieras, inversionistas y consumidores. Para abordar este desafío, se han desarrollado modelos y técnicas de minería de datos y aprendizaje automático. En este marco conceptual, se explora cómo estos modelos se aplican en la predicción de fraudes financieros, comenzando con la definición de fraude y sus diferentes tipos, seguido por cómo se utilizan los modelos supervisados y no supervisados para identificar y prevenir actividades fraudulentas en el sector financiero.

5.1. Definición de Fraude

El fraude se refiere a cualquier acción intencional y engañosa realizada para obtener beneficios personales a expensas de otra persona o entidad. En el contexto financiero, el fraude puede manifestarse de diversas formas, incluyendo el fraude de tarjetas de crédito, el fraude de seguros, la corrupción, el lavado de dinero, entre otros. Es importante destacar que el fraude puede ser perpetrado tanto por individuos externos como internos a una institución financiera, lo que lleva a la necesidad de detectar y prevenir tanto el fraude externo como el interno (Tripathi & Pavaskar, 2012). (Ver Tabla 5-1).

Tabla 5-1

Tipos de Fraudes Financieros

Tipo de Fraude	Descripción
Fraude de tarjeta de crédito	Uso no autorizado de tarjetas de crédito robadas o perdidas, así como la adquisición fraudulenta de tarjetas mediante identidades falsas.
Fraude de seguros	Presentación de reclamaciones de seguros falsas o infladas para obtener indemnizaciones de forma fraudulenta.
Corrupción	Abuso de poder o posición para obtener beneficios personales a expensas de una organización o entidad.
Lavado de dinero	Proceso de ocultar o disfrazar el origen ilícito de fondos obtenidos a través de actividades ilegales.
Robo de identidad	Uso indebido de la información personal de otra persona para cometer fraudes financieros.

Nota. Esta tabla presenta una clasificación de los tipos de fraudes financieros, destacando su descripción y características principales. La información ha sido extraída de las fuentes citadas: (Bozkuş Kahyaoğlu Editor, 2022; Tripathi & Pavaskar, 2012).

5.1.1. Fraude Interno

El fraude interno se refiere a las actividades fraudulentas llevadas a cabo por individuos que forman parte de la institución en la que se comete el fraude, siendo considerado de alto nivel si proviene de la gerencia y de bajo nivel si es operativo (Abdallah et al., 2016a). Este tipo de fraude se puede dividir en dos categorías principales:

Actividades no autorizadas. Estas actividades implican operaciones realizadas por empleados de la institución sin la debida autorización. Esto puede incluir la ejecución de transacciones no reveladas intencionalmente, operaciones no autorizadas que resultan en pérdidas monetarias para la institución, y la valoración errónea intencional de posiciones financieras para beneficio personal (Varmedja et al., 2019).

Hurto y fraude. Esta categoría abarca una amplia gama de actividades fraudulentas, que van desde el fraude crediticio y la apropiación indebida de activos hasta la falsificación de documentos y la utilización de identidades falsas. Incluye acciones como el hurto de activos, la malversación de fondos, la extorsión, el robo de identidad y la destrucción dolosa de activos, entre otros (Varmedja et al., 2019).

5.1.2. Prevención y Detección

La prevención y detección del fraude interno requiere un enfoque multifacético que incluya controles internos sólidos, una cultura organizacional ética, capacitación adecuada

para el personal y el uso de tecnología avanzada para monitorear y detectar actividades sospechosas.

La minería de datos, un campo interdisciplinario que combina la estadística, la inteligencia artificial y la informática, se centra en descubrir patrones y relaciones significativas en grandes conjuntos de datos. Uno de los pilares fundamentales de la minería de datos es la utilización de modelos de aprendizaje automático, que pueden clasificarse en dos categorías principales: modelos supervisados y no supervisados. Estos modelos desempeñan un papel crucial en la predicción y detección de patrones en datos financieros, como en la detección de fraudes (CHEN et al., 2006).

6. Diseño Metodológico de la Consultoría para el Banco Itaú

6.1. Enfoque de la Investigación

El enfoque de esta investigación se desarrolla desde una perspectiva cualitativa, ya que se busca realizar un análisis sobre el fraude en el sector financiero para identificar las prácticas más comunes de fraude y cómo las entidades financieras están actuando para prevenir y detectar los casos relacionados con este fenómeno. Esta investigación tiene un fin descriptivo, realizando un análisis de la información recopilada para detectar los métodos de prevención y detección de fraude, así como las buenas prácticas desarrolladas por las entidades financieras para hacer frente a esta problemática.

6.2. Fases de la Consultoría

La estrategia de trabajo se estructura en seis fases principales, cada una diseñada para cumplir con los objetivos establecidos. En cada fase se detallan las actividades necesarias para recopilar y analizar la información, con un enfoque en la elaboración de un estado del arte sólido sobre los fraudes internos en el sector bancario y en la identificación de las mejores prácticas para su prevención y detección (ver Tabla 6-1).

Tabla 6-1

Esquema del Diseño Metodológico

Componente	Objetivo	Actividades
Comprensión de la Situación Actual del Sector Bancario en Colombia y Latinoamérica	Analizar el contexto actual del sector bancario en términos de fraudes internos.	- Recopilación de informes y documentos de diversas instituciones bancarias. - Análisis de estudios y reportes sobre fraudes en el sector bancario en Colombia y América Latina. - Investigación de artículos académicos y publicaciones relevantes. - Evaluación de casos de estudio y análisis comparativos.
Diagnóstico del Estado Actual de la Seguridad y Gestión de Fraudes	Identificar las mejores prácticas y tendencias actuales en la gestión de fraudes internos.	- Revisión de procesos y controles existentes. - Comparación de enfoques y metodologías empleadas en diferentes bancos.
Desarrollo de Modelos de Predicción de Fraude (Revisión Bibliográfica)	Realizar un análisis exhaustivo de los modelos de predicción de fraude utilizados en el sector bancario.	- Identificación de técnicas de Machine Learning y algoritmos estadísticos. - Análisis de publicaciones académicas y técnicas. - Evaluación de ventajas y desventajas de diferentes enfoques y algoritmos.
Calibración de Modelos de Predicción (Revisión Bibliográfica)	Investigar las metodologías de calibración de modelos predictivos en el contexto de fraudes bancarios.	- Análisis de métodos de calibración de modelos de predicción. - Evaluación de la efectividad de técnicas de calibración. - Síntesis de mejores prácticas en la calibración de modelos predictivos.
Validación de Algoritmos (Revisión Bibliográfica)	Analizar las metodologías de validación de algoritmos de predicción de fraudes.	- Investigación sobre técnicas de validación. - Estudio de la implementación de pruebas piloto.

		- Comparación de estudios de caso sobre validación de algoritmos.
Consolidación de la información y Entregables	Identificar los criterios para la selección de algoritmos y proponer la metodología para la selección de modelos de detección de fraudes basados en el estado del arte.	- Definición de criterios para la selección de algoritmos. - Evaluación de algoritmos basados en precisión, eficiencia y aplicabilidad. - Elaboración de la metodología de selección de modelos de predicción de fraude. - Presentación de recomendaciones y mejores prácticas.

Nota. Esta tabla presenta el diseño metodológico propuesto para la investigación, incluyendo los componentes, objetivos y actividades específicas. Se destacan las etapas clave, como la comprensión del contexto, el diagnóstico de la seguridad y gestión de fraudes, y el desarrollo, calibración y validación de modelos de predicción de fraude**.**

Elaboración propia

6.3. Procedimientos y Técnicas para el Diagnóstico

En este apartado se describen los procesos y métodos aplicados para recoger y analizar la información relevante en el diagnóstico. Se enfoca en detallar las estrategias utilizadas para obtener datos confiables, así como las técnicas analíticas que permiten interpretar la información recopilada. El objetivo principal es garantizar un análisis

exhaustivo que respalde la identificación de modelos predictivos efectivos y prácticas óptimas para la prevención del fraude financiero.

6.3.1. Procedimientos

Revisión Sistemática de Literatura. Selección de estudios relevantes garantizando un análisis exhaustivo del contexto.

Benchmarking General del Sector. Identificación de tendencias emergentes y mejores prácticas documentadas en el sector financiero.

Análisis Comparativo de Modelos. Evaluación de la eficacia, precisión y requerimientos computacionales de modelos predictivos.

Análisis de Compatibilidad Tecnológica. Revisión de modelos compatibles con AWS.

6.3.2. Técnicas

Modelado Predictivo. Utilización de algoritmos de aprendizaje automático.

Análisis de Viabilidad Computacional. Evaluación de infraestructura tecnológica y capacidad operativa.

Benchmarking. Comparación con prácticas líderes en el sector financiero.

6.3.3. Metodología Utilizada para el Diagnóstico

Se ha seleccionado la metodología de diagnóstico integral que evalúa la permite consolidar la información recolectada con el propósito de proporcionar una visión integral que permita identificar brechas y proponer soluciones adaptadas al contexto del sector financiero, considerando la viabilidad teórica y computacional.

Diseño del Plan de la Consultoría

Inicio del Proyecto. Definición de alcance, cronograma y objetivos específicos.

Recolección de Información. Implementación de instrumentos validados a partir de revisiones bibliográficas y bases públicas**.**

Análisis y Diagnóstico. Procesamiento de datos e identificación de brechas, con énfasis en la comparación de modelos predictivos.

Desarrollo de Recomendaciones. Propuesta de modelos predictivos y buenas prácticas adaptables basadas en información sectorial.

Evaluación Teórica de Modelos. Análisis comparativo de la viabilidad teórica de los modelos propuestos.

Socialización de Resultados. Presentación de hallazgos, recomendaciones teóricas y discusión sobre posibles escenarios de implementación futura.

7. Diagnostico Organizacional

Para realizar el diagnóstico organizacional del Banco Itaú, se llevaron a cabo tres etapas principales: (1) Revisión de la literatura científica sobre prácticas financieras a nivel mundial y latinoamericano, (2) Investigación de casos reales de fraude en entidades financieras y (3) Generación de una metodología para la selección de modelos de predicción de fraudes financieros. La metodología utilizada se basa en una Revisión Sistemática de la Literatura (SLR), siguiendo el modelo propuesto por Kitchenham permitiendo un enfoque integral al identificar modelos predictivos más efectivos y adaptables a la infraestructura tecnológica del banco.

7.1. Revisión de la literatura científica sobre las prácticas financieras bajo el contexto mundial

7.1.1. Estrategia de Búsqueda

La revisión sistemática de la literatura (SLR) se lleva a cabo en el contexto latinoamericano de las prácticas financieras, siguiendo el modelo propuesto por Kitchenham. En este enfoque, la evidencia o los resultados se definen como una síntesis de los estudios científicos más reconocidos sobre el tema específico o relacionado con el tema de investigación específico.

El propósito de esta revisión es examinar métodos, técnicas, modelos, guías marco y/o buenas prácticas existentes en el sector financiero en América Latina y Colombia. Se establecen dos componentes clave: la estrategia de búsqueda y el marco para analizar las publicaciones encontradas. Para garantizar una revisión sistemática adecuada (Velásquez, 2015a), sugiere pasos básicos, para no divagar e identificar las acciones. En la Tabla 7-1 se muestran las preguntas que se formularon para esta investigación:

***T*abla 7-1**

Preguntas de Investigación para la Revisión Sistemática de la Literatura.

	Pregunta	Objetivo y Esquema de Clasificación	Palabras Clave
RQ1	¿Cuáles son los modelos de predicción de fraudes financieros más utilizados en la literatura científica y cómo se comparan en términos de precisión y eficacia?	Identificar los modelos de predicción de fraudes financieros más citados y comparar su precisión y eficacia en estudios científicos.	Modelos de Predicción, Fraudes Financieros, Precisión, Eficacia
RQ2	¿Qué metodologías y enfoques se han empleado para desarrollar modelos de detección de fraudes financieros?	Explorar las metodologías y enfoques utilizados en el desarrollo de modelos de detección de fraudes financieros en la literatura científica.	Metodologías, Enfoques, Modelos de Detección, Fraudes Financieros,
RQ3	¿Cuáles son las principales características y elementos clave que se consideran en los modelos de predicción de fraudes financieros?	Identificar las características y elementos clave considerados en los modelos de predicción	Características, Elementos Clave, Modelos de Predicción, Fraudes Financieros

		de fraudes financieros en la literatura científica.	
RQ4	¿Cuáles son los desafíos y limitaciones comunes asociados con los modelos de predicción de fraudes financieros, y cómo se abordan en la literatura?	Identificar los desafíos y limitaciones comunes en los modelos de predicción de fraudes financieros y examinar cómo se abordan en la literatura científica.	Desafíos, Limitaciones, Modelos de Predicción, Fraudes Financieros
RQ5	¿Cómo se evalúan y validan los modelos de detección de fraudes financieros en entornos del mundo real?	Explorar los métodos de evaluación y validación de modelos de detección de fraudes financieros en aplicaciones del mundo real según la literatura científica.	Evaluación, Validación, Modelos de Detección, Fraudes Financieros, Mundo Real, Literatura Científica
RQ6	¿Qué papel juegan los factores contextuales, como la regulación financiera y las características del mercado, en el diseño y la implementación de modelos de predicción de fraudes financieros?	Analizar el papel de los factores contextuales, como la regulación financiera y las características del mercado, en el diseño e implementación de modelos de predicción de fraudes financieros según la literatura científica.	Regulación Financiera, Características del Mercado, Diseño, Implementación, Modelos de Predicción, Fraudes Financieros,
RQ7	¿Cuáles son las tendencias emergentes en el desarrollo de modelos de detección de fraudes financieros, y qué áreas de investigación están ganando atención en la literatura actual?	Identificar las tendencias emergentes y áreas de investigación en desarrollo de modelos de detección de fraudes financieros en la literatura científica actual.	Tendencias Emergentes, Áreas de Investigación, Modelos de Detección, Fraudes Financieros

RQ8	¿Qué diferencias existen en la implementación de modelos de predicción de fraudes financieros entre diferentes sectores financieros, como la banca, los seguros y la inversión?	Examinar las diferencias en la implementación de modelos de predicción de fraudes financieros entre diferentes sectores financieros según la literatura científica.	Implementación, Sectores Financieros, Modelos de Predicción, Fraudes Financieros,

Nota. Esta tabla detalla las preguntas de investigación formuladas para orientar el análisis y la revisión sistemática sobre modelos de detección y predicción de fraudes financieros. Cada pregunta está acompañada de su objetivo específico, enfocado en identificar características clave, metodologías, limitaciones, tendencias emergentes y diferencias sectoriales. Adaptado de "*Una Guía Corta para Escribir Revisiones Sistemáticas de Literatura Parte 3"(Velásquez, 2015).*

Después de tener las palabras claves identificadas, se definió la siguiente ecuación de búsqueda: ("Financial Fraud" OR "financial risk" OR fraud) AND ("Prediction*" OR "Detection Models") AND bank* contemplando un rango de 10 años, periodo el cual, permitirá mapear e identificar las lecciones aprendidas a implementar en el caso Itaú Colombia (Velásquez, 2015b).

7.2. Investigación sobre casos reales de fraude en entidades financieras

Para explorar los casos reales de fraude en el sector financiero, es crucial llevar a cabo una investigación en la literatura científica sobre casos reales reportados e investigados en el sector, validando un entorno Latinoamericano.

En primer lugar, resulta fundamental realizar una revisión exhaustiva en la literatura científica, apoyándose en investigaciones previas, estudios, artículos y libros disponibles en las bases académicas; con el objetivo de identificar teorías, marcos conceptuales y modelos desarrollados para comprender el accionar de las entidades financieras frente al fraude.

Además, con la investigación realizada se busca identificar patrones en los casos de fraude reales reportados, para poder perfilar los comportamientos inusuales al interior de las entidades financieras que desencadenen en fraudes materializados.

Por último, se realiza la identificación de las lecciones aprendidas que han ido recopilando las entidades financieras con los casos reales de fraude que se han materializado, con el fin de detectar las buenas prácticas que se han adoptado en el sector para la detección y prevención de fraude, con esto identificar las más apropiadas para el banco Itaú Colombia.

7.3. Generación de la metodología para la selección de modelos de predicción de fraudes financieros

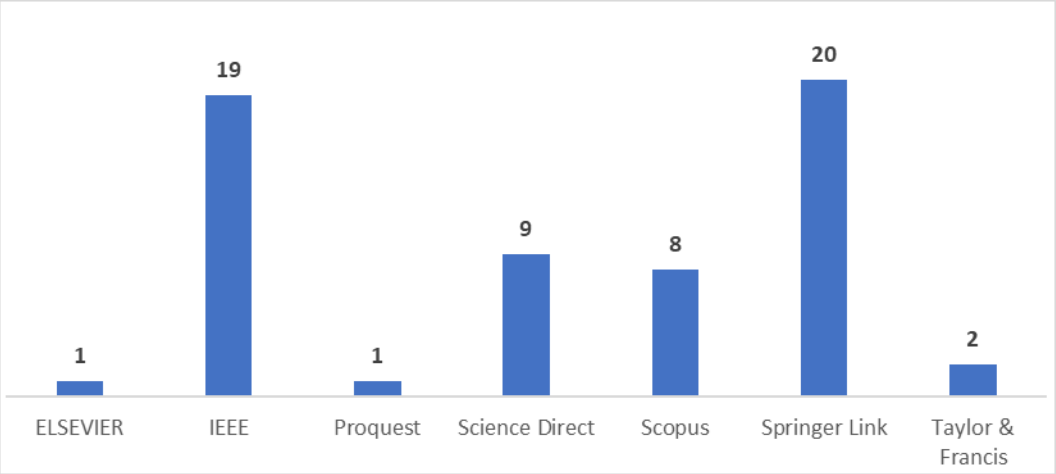
Finalmente, se genera la documentación con el resumen de la investigación realizada para que el banco pueda realizar la consulta, asimismo, se establece la metodología de selección del modelo óptimo para que el banco la pueda adoptar y esta le sirva para la detección de fraudes e identificar las prácticas que le permitan mejorar su acción frente al fraude financiero. Por esto se hace necesario documentar los casos reales de fraude que se han presentado en entidades financieras, los modelos desarrollados para identificar y prevenir el fraude financiero y las buenas prácticas adoptadas por las entidades financieras, los cuales se documentan en la sección 5 y 6 del presente documento.

Por otro lado, se realizará la socialización con el banco para exponer la información encontrada para que este aporte al objetivo que tiene el banco de mitigar el fraude interno.

Con el fin de obtener una significativa cantidad de información que permita responder a la pregunta de investigación y alcanzar los objetivos propuestos, se optó por realizar un análisis detallado de modelos de detección de fraudes financieros. Para la recolección de información, se revisaron diversas bases de datos y se seleccionaron 60 artículos que abordan esta problemática (Ver Anexo A). En la Figura 7-1 se presenta la distribución de los artículos con base a las revistas consultadas. Siendo IEEE y Springer Link las que más aportaron a la investigación.

Figura 7-1

Consolidado de Revistas Científicas Consultada.

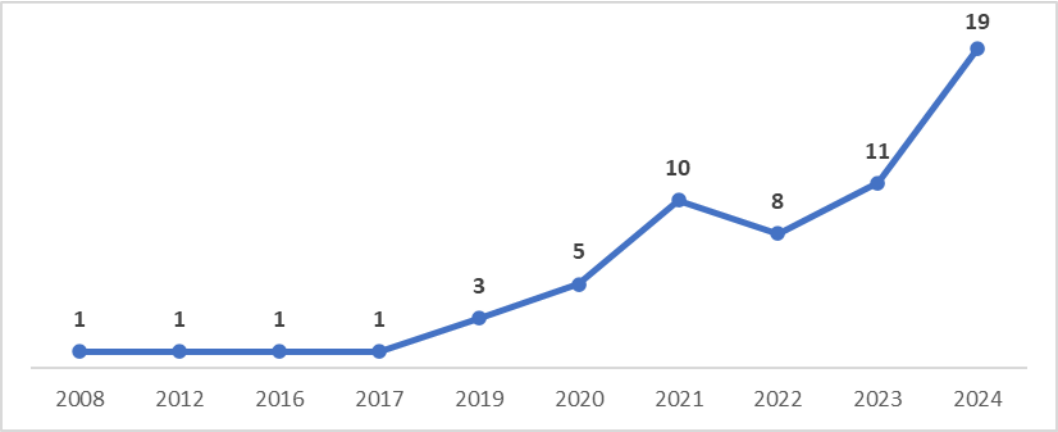


Nota. La figura muestra la distribución de los artículos científicos consultados durante el estudio, según las revistas académicas de origen. Esta visualización destaca las fuentes más relevantes para la investigación sobre modelos de detección y predicción de fraudes financieros. Elaboración Propia.

En la Figura 7-2 se presenta la distribución de los artículos con base al año de publicación; aunque, inicialmente, se planteó revisar la literatura científica de los últimos 10 años, se realizó un enfoque en los años post-pandemia, ya que esta generó una evolución en cuanto a la digitalización de los procesos y esto trae consigo nuevas metodologías de fraude y, asimismo, nuevos métodos de detección de fraude para hacer frente a los modos de fraude emergentes.

Figura 7-2

Cronología de los artículos.



Nota. La figura muestra la cronología de los artículos seleccionados para el estudio, destacando su distribución a lo largo del tiempo. Este análisis temporal permite identificar tendencias y el incremento en la producción académica relacionada con los modelos de detección y predicción de fraudes financieros. Elaboración Propia.

Los métodos analizados incluyen técnicas de aprendizaje automático, modelos híbridos y enfoques basados en redes neuronales. Además, se consideraron distintos conjuntos de datos, con énfasis en bases de datos públicas como Kaggle. Se encontraron modelos como submuestreo aleatorio, sobre muestreo de minorías sintéticas (SMOTE), redes neuronales artificiales, algoritmos genéticos y técnicas de optimización de hiperparámetros.

7.4. Procesamiento de Datos

En los diferentes artículos coinciden en que la arquitectura e ingeniería de datos, junto con la gobernanza de datos, son pilares fundamentales para la implementación efectiva de modelos de detección de fraudes. Se destaca la necesidad de infraestructuras escalables, técnicas de preprocesamiento robustas y sistemas que aseguren la transparencia y la seguridad de los datos. Estos factores no solo mejoran el rendimiento de los modelos, sino también garantizan su cumplimiento con las normativas y expectativas éticas en el sector financiero (Bose et al., 2019; Kancharla & Madhu Kumar, 2023). En este contexto, los casos de Banco Itaú en Chile y Brasil se consolidan como referentes clave al demostrar cómo una estrategia de datos bien estructurada puede traducirse en ventajas competitivas tangibles, especialmente en el ámbito de la analítica avanzada aplicada a la detección y mitigación del fraude interno.

7.4.1. La Gobernanza de Datos como Pilar para la Detección de Fraude

En la actual era digital, caracterizada por la explosión de datos y el avance de tecnologías disruptivas, la gobernanza de datos ha adquirido una importancia estratégica esencial para las organizaciones modernas, en especial el sector financiero. Más allá del cumplimiento normativo, la gobernanza de datos se concibe como un conjunto de principios, procesos, roles, políticas y tecnologías orientados a asegurar la integridad, disponibilidad, privacidad y valor de los activos de información (Sheokand et al., 2024a).

Una gestión adecuada de los datos permite mejorar la toma de decisiones, fortalecer los mecanismos de control interno y mitigar los riesgos de fraude financiero.

La relación entre gobernanza de datos, gobierno corporativo y prevención del fraude ha sido ampliamente discutida en la literatura reciente (Muslim, 2025a) señala que muchas organizaciones presentan deficiencias estructurales en sus controles internos, incluyendo falta de supervisión efectiva, conflictos de interés en los comités de auditoría y priorización de resultados financieros sobre la ética organizacional. Casos emblemáticos como los de Volkswagen y Wirecard (mencionados anteriormente) demuestran que, incluso en contextos regulatorios estrictos, las fallas en la implementación práctica de controles y en la gobernanza de datos permiten la ocurrencia de fraudes de gran escala.

Adicionalmente, el modelo tradicional del "triángulo del fraude" (presión, oportunidad y racionalización) ha sido complementado por enfoques más integradores que consideran también factores psicológicos y organizacionales. Estos nuevos modelos explican cómo presiones internas, culturas organizativas tóxicas y falta de valores éticos consolidados pueden fomentar conductas fraudulentas (Muslim, 2025a). Así, se reconoce que una gobernanza de datos sólida no debe limitarse a aspectos técnicos o regulatorios, sino que debe estar basada en una cultura organizacional basada en la transparencia, la responsabilidad y la ética.

Factores Clave para una Gobernanza de Datos Efectiva

A partir de los documentos revisados, se identifican factores esenciales para establecer una gobernanza de datos sólida. Ver Tabla 7-2.

Tabla 7-2

Factores Clave de la Gobernanza de Datos

Factor Crítico	Descripción
Definición de roles y responsabilidades	Creación de figuras como Data Owners y Chief Data Officers para asignar responsabilidades claras sobre la calidad y protección de los datos.
Políticas de acceso, seguridad y retención	Adopción de políticas estrictas para proteger los activos de datos y facilitar el cumplimiento de normativas regulatorias.
Auditoría del linaje de datos	Monitoreo del ciclo de vida de los datos para detectar inconsistencias y fraudes de manera temprana.
Cultura organizacional basada en la ética	Promoción de una cultura organizacional orientada a la transparencia y rendición de cuentas para prevenir fraudes.
Soporte tecnológico avanzado	Uso de tecnologías como blockchain, inteligencia artificial y plataformas distribuidas para automatizar controles y mejorar la gobernanza.
Capacitación continua	Formación regular en gobernanza de datos y auditoría para fortalecer la resiliencia frente a riesgos emergentes.

Nota. La tabla presenta los factores críticos para fortalecer la gobernanza de datos en las organizaciones, considerando su impacto en la prevención del fraude financiero. Se abordan dimensiones clave como la definición estructurada de responsabilidades, la implementación de políticas de acceso y resguardo de datos, la auditoría integral del ciclo de vida de la información, el fortalecimiento de principios éticos en la cultura organizacional, el aprovechamiento de tecnologías emergentes, y el desarrollo continuo de competencias técnicas en el talento humano. Adaptado de los artículos (Bernardo et al., 2024; Muslim, 2025b; Sheokand et al., 2024b).

Gobernanza de Datos como Defensa Contra el Fraude

La implementación de un marco de gobernanza de datos robusto refuerza la capacidad de las organizaciones para resistir tentaciones fraudulentas. Como explica (Muslim, 2025b), cuando la gobernanza se limita al cumplimiento normativo superficial y no se internalizan valores éticos, se crean condiciones propicias para el fraude. Por el contrario, una gobernanza efectiva asegura la transparencia de los procesos, mejora la calidad de la información y facilita auditorías internas y externas eficientes.

Normativas y Calidad de Datos

Finalmente, (Bernardo et al., 2024) resaltan que la adhesión a estándares internacionales de calidad de datos es fundamental para construir confianza y garantizar que los datos utilizados en decisiones financieras sean íntegros, exactos y verificables. Una gestión descuidada de los datos no solo incrementa los riesgos operativos, sino que también expone a las organizaciones a sanciones regulatorias y pérdidas reputacionales.

7.4.2. Casos Itaú Chile y Brasil: Buenas Prácticas en Acción

Los casos de Banco Itaú en Chile y Brasil representan dos aproximaciones exitosas y complementarias en cuanto a la implementación de tecnologías habilitadas por Amazon Web Services (AWS) que colocan la gobernanza de datos en el centro de su estrategia:

- Itaú Chile ha adoptado una arquitectura basada en un Data Lake centralizado, complementado con servicios de Machine Learning, lo cual ha facilitado la estandarización de datos y una mayor eficiencia en el despliegue de modelos de detección de fraude, reduciendo los tiempos de implementación de tres meses a tres semanas.
- En contraste, Itaú Brasil ha optado por una arquitectura de Data Mesh, que permite la descentralización del procesamiento de datos entre los diferentes dominios organizacionales, sin sacrificar la integridad ni el control. Esta estrategia ha posibilitado la migración de 8 petabytes de datos y la integración lógica de fuentes diversas en un marco robusto de gobernanza federada.

Ambos modelos demuestran cómo la tecnología de AWS (como Lake Formation, IAM, CloudTrail, Amazon S3, y SageMaker), puede ser aprovechada no solo para construir arquitecturas resilientes, sino también para operacionalizar la gobernanza de datos, mediante la definición clara de accesos, responsabilidades, linaje y políticas de uso de datos. En la Tabla 7-3, se comparan ambos enfoques, destacando diferencias y similitudes en gestión de datos, descentralización y eficiencia operativa. Ambas estrategias han optimizado el rendimiento de los modelos analíticos, logrando una integración lógica de datos distribuidos y brindando mayor autonomía a los equipos de negocio en la toma de decisiones.

Tabla 7-3

Paralelo Tecnología Implementada por Banco Itaú Chile y Banco Itaú Brasil

Aspecto	Itaú Chile	Itaú Unibanco Brasil
Enfoque Principal	Mejora en la eficiencia operativa y despliegue rápido de modelos de analítica en AWS.	Arquitectura Data Mesh para descentralizar el acceso y procesamiento de datos en toda la organización.
Motivación	Reducir tiempos de implementación de modelos y mejorar la calidad de los datos.	Optimizar el uso de datos en distintas unidades de negocio y mejorar la personalización de servicios.
Tecnología Clave	Data Lake, Machine Learning (ML) en AWS, Amazon BI y Lake Foundation.	Data Mesh, descentralización de datos con AWS, integración de múltiples fuentes de información.
Impacto en el negocio	Reducción del 75% en el tiempo de despliegue de modelos (de 3 meses a 3 semanas).	Migración de 8 petabytes de datos comprimidos a AWS.
	Mayor transparencia y control en la gestión de datos.	Reducción de procesos analíticos de 15 horas a 45 minutos.
	Optimización en procesos normativos y regulatorios.	Aceleración en la adopción de soluciones analíticas en toda la organización.
Retos superados	Creación de arquitecturas escalables y flexibles.	Superación de la centralización de datos mediante Data Mesh.
	Agilización del procesamiento de datos.	Gobernanza y seguridad en un entorno descentralizado.

	Despliegue más rápido de modelos predictivos.	Optimización de costos en el manejo de grandes volúmenes de datos.
		Integración de datos de diferentes unidades de negocio.
Casos de Uso en Analítica Avanzada	Implementación de modelos de Machine Learning para predecir fraude en transacciones bancarias.	Uso de análisis de datos en tiempo real para optimizar la respuesta a riesgos macroeconómicos.
Resultados Clave	Estandarización y mejora en la calidad de datos.	Autonomía de los equipos en la gestión de datos.
	Reducción de costos y mejora en el gobierno de datos.	Integración lógica de datos descentralizados.
	Mayor velocidad en la ejecución de procesos analíticos.	Expansión de los negocios basados en datos.

Nota. Paralelo entre ambos enfoques, destacando sus principales diferencias y similitudes en términos de gestión de datos, tiempos de procesamiento, descentralización y beneficios operativos. Adaptado de los videos (Itaú Acelera El Despliegue de Modelos En Un 75% Con Infraestructura AWS, n.d.; Itaú Unibanco Adopta Una Arquitectura de Malla de Datos y Confía En El Soporte de AWS, n.d).

Itaú Colombia también se encuentra en proceso de actualización tecnológica. Siguiendo los pasos de sus filiales en Chile y Brasil, ha seleccionado a Amazon Web Services (AWS) como su aliado estratégico para impulsar su transformación digital en Colombia, con el objetivo de mejorar la experiencia del cliente.

Si bien el propósito de este documento es identificar las principales técnicas y modelos para la mitigación y detección efectiva del fraude interno, es fundamental comprender cómo aprovechar este tipo de tecnología a favor del análisis de fraudes

financieros. En este contexto, la detección eficaz de anomalías en grandes volúmenes de datos es clave para fortalecer los modelos de prevención y control (K. Chen et al., 2019; Joyanes, 2019).

La falta de acceso a datos financieros por confidencialidad limita el desarrollo de modelos predictivos efectivos. Dentro de la revisión de la literatura científica se encontraron diferentes trabajos basados en un conjunto de datos libre del sitio web www.kaggle.com, que consta de 284.315 transacciones que se realizaron en Europa, de las cuales 492 corresponden a fraudes comprobados, es decir, el 0.172% corresponden a transacciones fraudulentas. Esto supone un desafío en cuanto al desequilibrio de los datos, por lo que, varios estudios se centran en este problema para optimizar los modelos de detección de fraude (Itoo et al., 2021a).

Para abordar el problema del desbalance de datos, (Mashrur et al., 2020), exploraron múltiples técnicas de preprocesamiento y modelos de aprendizaje automático, destacando Random Forest y redes neuronales profundas como enfoques efectivos. Por su parte, en (Itoo et al., 2021b), se implementó un submuestreo aleatorio y se compararon Regresión Logística (LR), Naïve Bayes (NB) y K-Vecinos más Cercanos (KNN), concluyendo que LR fue el modelo más efectivo con una precisión del 95%. Estos ejemplos resaltan la importancia de contar con arquitecturas de datos flexibles y escalables que faciliten la implementación de dichas técnicas, garantizando así un equilibrio adecuado entre el desempeño de los modelos y el cumplimiento de principios éticos y normativos. La regresión logística (LR) alcanzó una precisión del 95% cuando (Almhaithawi et al., 2020a), implementaron la técnica de Sobremuestreo de minorías

sintéticas (SMOTE) para equilibrar datos y el riesgo mínimo de Bayes (BMR) para optimizar predicciones, logrando ahorros del 97%.

(Ileberi et al., 2022a) compararon varios modelos y encontraron que el bosque aleatorio obtuvo la mayor exactitud (99,98%) al emplear algoritmos genéticos para seleccionar características. (W. Li et al., n.d.) aplicó la técnica de Sobremuestreo de minorías sintéticas (SMOTE) y el submuestreo basado en conglomerados (CUS) para abordar el desbalance de datos en un modelo de bosque aleatorio, obteniendo una precisión del 99,8% empleando un algoritmo genético para seleccionar características 252:7. (Tayebi et al., 2022) analizaron hiperparámetros óptimos y concluyeron que LR mantiene su estabilidad con una exactitud del 96% sin importar el algoritmo metaheurístico utilizado. (Flondor et al., 2024) aplicaron Decision Tree Classifier sobre dos conjuntos de datos sintéticos, obteniendo 96% y 99% de exactitud, destacando su bajo tiempo computacional.

(Zioviris et al., 2022), incorporaron SMOTE y una autocodificadora variable en una red neuronal convolucional (CNN), alcanzando un 97,67%. (Venkata et al., 2024), desarrollaron SpinalNet con normalización de cuantiles y técnicas de selección de características, logrando una precisión de 89,10%. (Benchaji et al.) ajustaron datos con un modelo de Aproximación y Proyección de Variedad Uniforme (UMAP), reduciendo la dimensionalidad y, aplicaron una red neuronal recurrente de memoria a corto-largo plazo (LSTM), alcanzando una exactitud de 96,7% y una precisión del 98,9%.

Las redes generativas antagónicas (GANs) se utilizan para detectar fraudes generando datos sintéticos mediante un generador y un discriminador. (Zhao et al., 2024a) emplearon conjuntos de datos de 284,807 y 1,048,576 transacciones (492 y 1,042 fraudulentas, respectivamente) para diseñar el modelo SAGAN, logrando una precisión del

82%. Por su parte, (Xie et al., 2023a) destacó la integración de datos dinámicos y contextuales para mejorar la detección de patrones transaccionales fraudulentos externos. Estos modelos optimizan el análisis de datos complejos y detectan anomalías ocultas con alta precisión.

(Krishnavardhan, Govindarajan, Rao, et al., 2024) integraron Grey Wolf Optimization (GWO) y Fireworks Algorithm (FW) en un modelo ANFIS, alcanzando 99,87% en préstamos fraudulentos, 99,96% en tarjetas de crédito y 99,85% en fraudes de seguro. (Innan et al., 2024a) combinaron Isolation Forest (IF) y GWO para detectar anomalías, logrando 93,52% de precisión y una mejora en la reducción de falsos positivos.

(Tang & Liang, 2024) aplicaron redes neuronales de grafos (GNN) para garantizar la confidencialidad de datos financieros entre instituciones, obteniendo 95,99% y 81,60% de precisión en dos conjuntos de datos. (Wang, Qi, et al., 2019) desarrollaron un sistema federado que mejora detección en tiempo real, con un 99% de precisión en banca europea.

(Lopez, 2017) utilizó simulación basada en agentes múltiples (MABS) para generar datos sintéticos replicando fraudes financieros, permitiendo la mejora de modelos sin comprometer información real. (Maulana et al., 2021), combinaron Big Data y arquitectura SOA para detectar fraudes en banca electrónica en tiempo real, aumentando la eficiencia operativa.

Los artículos revisados se categorizaron según los enfoques empleados para la detección de fraudes. Destacan los modelos de aprendizaje profundo, como las redes neuronales convolucionales (CNN) y una red neuronal de memoria bidireccional a largo y corto plazo (BiLSTM), que alcanzaron niveles de precisión superiores al 97%. No obstante, modelos más tradicionales, como la regresión logística y los bosques aleatorios,

mostraron resultados comparables con menores requerimientos computacionales. En la Tabla 7-4 se presentan los modelos más implementados junto con datos clave, útiles para una futura implementación.

Tabla 7-4

Modelos de Detección de Fraude

Método	Tipo de Fraude	Precisión Promedio	Requiere Menor Costo Computacional	Estructura Solida Gobernanza de Datos	Lenguaje de Programación Utilizado	Tecnologías AWS Relacionadas	Referencia
Hidden Markov Model (HMM)	Interno	92%	No	Si	Python	Amazon SageMaker, AWS Lambda, Amazon EMR	(Dewi et al., 2017a; Zioviris et al., 2022)
Graph Attentive Network	Interno	94%	No	Si	Python	Amazon Neptune, SageMaker, AWS Glue	(Kafila et al., 2024; Krishnavardhan, Govindarajan, Rao, et al., 2024; Wang, Lin, et al., 2019; Xie et al., 2023b; Zhao et al., 2024b)
Graph Neural Networks	Interno	98%	No	Si	Python	Amazon Neptune, SageMaker, Amazon S3, AWS Step Functions	(Krishnavardhan, Govindarajan, & Rao, 2024;

							Kurshan et al., 2020)
Regresión Logística	Interno y Externo	95%	Sí	No	Python	Amazon SageMaker, AWS Glue, Amazon Athena	(Ali et al., 2024; Almhaithawi et al., 2020b; Balaji et al., 2024; Ding, 2023; Hajek, Abedin, et al., 2023; Ileberi et al., 2022b; Innan et al., 2024b; Itoo et al., 2021a; Krishnavardhan et al., 2023; W. Li et al., 2022; Shukla et al., 2023a; Tong & Shen, 2023)
K-Nearest Neighbor	Interno	88%	Sí	No	Python	Amazon SageMaker, Amazon RDS, AWS Batch	(Balaji et al., 2024; Ding, 2023; Itoo et al., 2021a; Krishnavardhan et al., 2023; RB & KR, 2021)
Máquinas de Soporte Vectorial (SVM)	Interno	96%	No	No	Python	Amazon SageMaker, AWS Batch, Amazon EC2 Spot Instances	(Abadlia & Smairi, 2024; Khalid et al., 2024; W. Li et al., 2022; RB & KR, 2021; Saha et al., 2023; Xiong et al., 2022)
Árboles de Decisión y Bosques Aleatorios	Interno y Externo	97%	Sí	Si	R, Python	Amazon SageMaker, AWS Glue, Amazon S3, Amazon Kinesis	(Abadlia & Smairi, 2024; Ali et al., 2024; Almhaithawi et al., 2020b; Ashfaq, Khalid, Yahaya, Aslam, Azar, et al., 2022; Ding, 2023; Fu et al., 2022; Ileberi et al., 2022b; Innan et al., 2024b; Saha et al., 2023; Xiong et al., 2022)

Redes Generativas Antagónicas (GANs)	Externo	99%	No	Si	Tensor Flow, Python	Amazon SageMaker, AWS Deep Learning Containers, Amazon FSx para Lustre	(Ali et al., 2024; Cherif et al., 2024; Chhabra et al., 2024; Usman, Abdullahi, et al., 2024; Zhao et al., 2024b)

Nota. La tabla presenta un resumen de los modelos de detección de fraude, sus características principales y tecnologías relacionadas. Aunque la columna de "Tecnologías AWS Relacionadas" no está explícitamente detallada en la literatura revisada, se realizó una adaptación basada en los hallazgos de la investigación, considerando las capacidades tecnológicas disponibles en el banco y las tecnologías de AWS más relevantes para implementar estos modelos. Elaboración propia.

Continuando y centrándose en los resultados obtenidos para los fraudes internos en el sector financiero, este fenómeno abarca una amplia gama de prácticas, desde la manipulación de informes financieros hasta la alteración de transacciones y la apropiación indebida de activos (Zhu et al., 2024). Los modelos de detección han demostrado ser efectivos en la identificación de estos patrones fraudulentos, utilizando técnicas avanzadas como redes neuronales, aprendizaje profundo y análisis de patrones mediante reglas de asociación (Afriyie et al., 2023a; Kute et al., 2021). Sin embargo, la implementación de estos modelos enfrenta múltiples desafíos, como la calidad y disponibilidad de los datos, la detección de nuevas estrategias de fraude y la necesidad de mejorar la interpretabilidad de los modelos de detección para facilitar su aplicación en entornos reales (Dewi et al., 2017b; Y. Li et al., 2022). Estos retos resaltan la importancia de combinar enfoques supervisados y no supervisados, junto con estrategias de optimización de hiperparámetros y validación cruzada, para mejorar la precisión y reducir los falsos positivos en la identificación de fraudes internos en instituciones financieras (Benchaji et al., 2021; Tang & Liang, 2024).

Para enfrentar estos desafíos, diversos modelos han sido aplicados con éxito en la detección de fraudes internos, abordando factores como la manipulación de cuentas, accesos no autorizados y la simulación de transacciones ficticias (Zhu et al., 2024). Modelos basados en aprendizaje profundo, como Redes Neuronales Codificadoras-Decodificadoras, han permitido transformar datos en representaciones latentes, facilitando la detección de irregularidades en patrones transaccionales (Y. Li et al., 2022). Asimismo, los modelos de aprendizaje no supervisado, como Isolation Forest y técnicas de optimización como Grey Wolf Optimizer (GWO), han sido efectivos en la identificación

de anomalías sin necesidad de datos previamente etiquetados, reduciendo el impacto de la escasez de información sobre fraudes detectados en entidades financieras (Afriyie et al., 2023a; Kute et al., 2021).

En el análisis de fraudes internos, técnicas avanzadas como Procesamiento de Lenguaje Natural (PLN) con Word2Vec han sido utilizadas para identificar inconsistencias en informes financieros, revelando la manipulación de ingresos o la omisión de pasivos (Zhu et al., 2024). Por otro lado, el uso de Redes Neuronales de Grafos (GNN) ha demostrado ser eficiente para modelar relaciones transaccionales y detectar conexiones sospechosas en la red interna de una institución bancaria(Tang & Liang, 2024). Complementariamente, modelos híbridos como el Hidden Markov Model (HMM) han sido implementados para evaluar secuencias de eventos y detectar manipulaciones en procesos crediticios internos (Dewi et al., 2017b).

Las conductas fraudulentas internas más recurrentes incluyen la alteración de informes contables, la generación de activos ficticios, la autorización indebida de préstamos y el desvío de fondos. Modelos basados en árboles de decisión y bosques aleatorios han demostrado una alta precisión en la detección de estas prácticas, logrando identificar patrones en la asignación de recursos financieros y en la ejecución de transacciones inusuales dentro de las organizaciones (Afriyie et al., 2023a), en la Tabla 7-5 se muestra las conductas más recurrentes y los modelos que se implementaron para mitigar estas conductas. Sin embargo, la detección temprana sigue siendo un desafío debido a la sofisticación de los métodos empleados por los defraudadores y la necesidad de combinar múltiples fuentes de datos en un análisis integral.

Tabla 7-5

Modelos Implementados para Mitigar Conductas Fraudulentas.

Conducta Fraudulenta Interna	Modelo Implementado	Tecnologías Clave de AWS
Manipulación de Informes Financieros	Modelos de PLN como Word2Vec y aprendizaje automático supervisado con Máquinas de Soporte Vectorial (SVM).	- Amazon Comprehend para análisis de texto. - Amazon SageMaker para entrenar y desplegar modelos SVM. - AWS Glue para ETL de datos financieros.
Generación de Ganancias Ficticias	Algoritmos de clasificación supervisada y redes neuronales profundas.	- Amazon SageMaker para entrenar redes neuronales profundas. - Amazon S3 para almacenamiento de datos. - AWS Batch para procesamiento escalable.
Creación de Activos Falsos o Sobrevaloración	Modelos de auditoría automatizada con aprendizaje automático y detección de anomalías.	- AWS Audit Manager para auditorías automatizadas. - Amazon Lookout for Metrics para detección de anomalías. - Amazon SageMaker para entrenar modelos de ML.
Divulgación de Información Errónea o Engañosa	Análisis semántico con algoritmos basados en PLN y autoencoders.	- Amazon Comprehend para análisis semántico. - Amazon SageMaker para entrenar autoencoders. - AWS Glue para integrar múltiples fuentes de datos.

Apropiación Indebida de Activos	Algoritmos de detección de anomalías basados en redes neuronales y reglas de asociación.	- Amazon SageMaker con detección de anomalías. - Amazon Neptune para análisis de relaciones transaccionales. - AWS Lambda para ejecutar reglas personalizadas en tiempo real.
Manipulación de Procesos Internos	Algoritmo Hidden Markov Model (HMM) para rastrear desviaciones en procesos.	- Amazon SageMaker para implementar HMM. - AWS Step Functions para coordinar flujos de procesos. - Amazon DynamoDB para almacenar datos de procesos en tiempo real.
Accesos Inusuales y Manipulación de Cuentas	Sistemas de detección de intrusos con algoritmos bayesianos y reglas de asociación.	- Amazon GuardDuty para detección de accesos sospechosos. - AWS Security Hub para centralizar hallazgos de seguridad. - Amazon SageMaker para algoritmos bayesianos.
Alteración de Transacciones Internas	Modelos de Random Forest y Árboles de Decisión.	- Amazon SageMaker para implementar Random Forest. - Amazon Kinesis para procesamiento en tiempo real. - Amazon Athena para análisis ad-hoc de transacciones.
Autorización Indebida de Préstamos	Redes neuronales profundas combinadas con SMOTE.	- Amazon SageMaker para entrenar redes neuronales profundas. - AWS Data Wrangler para preprocesamiento con SMOTE.

		- Amazon S3 para almacenamiento seguro de datos de préstamos.
Manipulación de Inventarios y Bonificaciones	Modelos de aprendizaje automático con análisis de correlación.	- Amazon SageMaker con análisis de correlación. - AWS Glue para limpieza y transformación de datos de inventarios. - Amazon Quicksight para visualización de patrones.
Encubrimiento de Fraude Mediante Lenguaje Técnico	PLN con análisis de legibilidad textual y detección de anomalías.	- Amazon Comprehend para analizar texto técnico. - Amazon SageMaker para modelos de PLN avanzados. - AWS Glue para preparar informes financieros.
Fraude Interno en Tarjetas de Crédito	Redes neuronales profundas y bosques aleatorios.	- Amazon SageMaker para entrenar y desplegar ambos modelos. - Amazon Kinesis para análisis de transacciones en tiempo real. - Amazon Athena para consultas rápidas sobre datos históricos.
Simulación de Transacciones para Cumplimiento	Redes neuronales convolucionales (CNN) y técnicas de grafos.	- Amazon Neptune para grafo de transacciones. - Amazon SageMaker para entrenar redes CNN. - AWS Lambda para ejecución de análisis en tiempo real.

Falsificación de Documentación Contable	Análisis forense digital con redes neuronales profundas.	- Amazon Rekognition para análisis de documentos digitales. - Amazon SageMaker para entrenar modelos avanzados. - AWS CloudTrail para monitorear accesos a documentación crítica.
Omisión de Pasivos y Manipulación de Ratios	Algoritmos de aprendizaje automático no supervisado.	- Amazon SageMaker para entrenar modelos no supervisados. - AWS Glue para preprocesar estados financieros. - Amazon Lookout for Metrics para identificar irregularidades en ratios financieros.

Nota. La tabla presenta una relación entre las conductas fraudulentas internas, los modelos implementados para detectarlas y las tecnologías clave de AWS que podrían emplearse para su mitigación. Al igual que en la Tabla 5-2, se propone el uso de tecnologías AWS con base en la literatura revisada. (Afriyie et al., 2023a; Dewi et al., 2017a; S. H. Li et al., 2012a; Usman, Abdullahi, et al., 2024).

Dado este contexto, la combinación de enfoques supervisados y no supervisados, gjunto con la optimización de hiperparámetros y la validación cruzada, representan el futuro en la lucha contra el fraude interno en el sector financiero. A medida que las instituciones implementan tecnologías más avanzadas para la detección temprana de fraudes, será fundamental fortalecer los mecanismos de auditoría y monitoreo, garantizando la transparencia y seguridad en las operaciones bancarias.

8. Resultados de la Solución

8.1. Metodología para la selección del modelo óptimo de detección de fraude

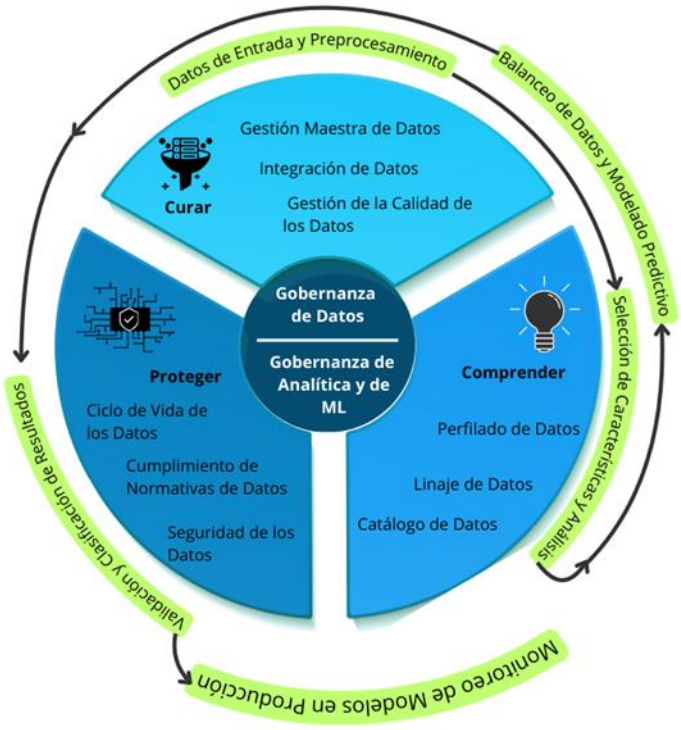
Con base en la literatura consultada en el desarrollo de la investigación, en la Figura 8-1 se presenta una metodología propuesta para la selección de un modelo óptimo para la detección de fraudes financieros. Esta metodología se configura como un proceso clave que involucra múltiples etapas secuenciales e interrelacionadas, iniciando desde la recolección y preparación de datos hasta alcanzar la fase de monitoreo y evaluación continua del desempeño del modelo.

De manera distintiva, en la presente propuesta se incorpora de manera transversal el componente de Modelo de Gobernanza de Datos de AWS, como un eje estratégico que asegura la calidad, integridad, trazabilidad, seguridad y cumplimiento normativo en cada fase del proceso. La inclusión de la gobernanza no solo responde a requisitos regulatorios como el GDPR o estándares internacionales como ISO/IEC 38505-2, sino que también actúa como un factor habilitador que incrementa la fiabilidad, transparencia y sostenibilidad de los modelos de detección de fraudes en entornos financieros (Bernardo et al., 2024; Sheokand et al., 2024b) .

Así, cada una de las etapas metodológicas contempla no solo los aspectos técnicos propios del procesamiento y análisis de datos, sino también los mecanismos de control, documentación, validación y monitoreo de la calidad de los datos empleados, en concordancia con buenas prácticas de gobernanza de datos.

Figura 8-1

Metodología para la selección y validación del modelo óptimo.



Nota. El diagrama ilustra la metodología consolidada para la selección, validación y monitoreo continuo de modelos de detección de fraude, basada en los enfoques más empleados en los artículos revisados. Se incluyen procesos como preprocesamiento de datos, selección de características, balanceo de datos y evaluación del modelo. Fuente: Adaptado de (Amazon Web Services, 2025).

A continuación, se presenta un detalle de cada una de las etapas contempladas en la metodología propuesta:

8.1.1. Curar

En esta primera etapa, la prioridad es preparar los datos que alimentarán a los modelos de fraude. Para ello, se requiere:

- Integrar múltiples fuentes bancarias (por ejemplo: sistemas transaccionales, registros de tarjetas, bases de usuarios).
- Realizar limpieza, estandarización y validación de datos.
- Garantizar la calidad y consistencia de los datos utilizados.

El pilar Curar se centra en asegurar que los datos ingresados son confiables, completos y aptos para el análisis, minimizando errores de entrada que puedan comprometer el modelo.

8.1.1.1. Recolección y Preparación de Datos

En esta fase de la metodología, se identifican las características de los datos disponibles para la detección de fraudes y se aplican técnicas de preprocesamiento que garanticen su calidad y relevancia. Este proceso incluye la transformación de variables para estandarizar y normalizar los datos, así como la selección de características clave para optimizar el rendimiento de los modelos analíticos. (Ver Tabla 8-1).

Tabla 8-1

Métodos de Recolección y Preparación de Datos

Proceso	Descripción	Métodos utilizados
Transformación de Variables	Ajustar las variables numéricas y categóricas para garantizar consistencia y adecuación al modelo	- Normalización: Escalar las variables numéricas en un rango específico (por ejemplo, entre 0 y 1). Min-Max Scaling (Dewi et al., 2017a) - Estandarización: Transformar las variables numéricas para que tengan una media de 0 y una desviación estándar de 1. Z-Score Standardization (Afriyie et al., 2023b) - Codificación de variables categóricas: Transformación de datos categóricos en datos numéricos para su posterior análisis y procesamiento en algoritmos estadísticos o de aprendizaje automático. o One-Hot Encoding (S. H. Li et al., 2012a), Label Encodingn (Usman, Adfullahi, et al., 2024)4), transformaciones logarítmicas(Xia et al., 2018), Escalamiento robusto(Krishnavardhan, Govindarajan, & Rao, 2024)
Selección de Características	Identificar las relaciones y relevancia entre las características de los datos para eliminar aquellas redundantes o irrelevantes, mejorando la eficiencia del modelo.	- Análisis de correlación: Eliminar características altamente correlacionadas(Afriyie et al., 2023b) - Análisis de Componentes Principales (PCA): Reducir la dimensionalidad transformando las características originales en componentes principales que capturan la mayor parte de la información(Hong et al., 2023) - Prueba de Fisher: Evaluar la independencia entre dos variables, partiendo de la hipótesis nula de que son independientes(S. H. Li et al., 2012b)

Nota. La tabla presenta una descripción de los métodos utilizados en la transformación y selección de variables para mejorar la calidad y eficiencia de los modelos de análisis. Las

referencias citadas corresponden a estudios que han documentado la efectividad de estos métodos.

8.1.2. Comprender

En esta fase se enfoca en entender, documentar y rastrear los datos que se utilizan en el análisis, asegurando que el flujo de la información sea trazable, auditable y contextualizado. El pilar Comprender proporciona el marco que permite:

- Mantener la trazabilidad de las variables seleccionadas.
- Registrar las transformaciones aplicadas a los datos.
- Documentar la historia de los datos (linaje de datos) desde su origen hasta su uso en el modelo.

8.1.2.1. Selección de Características y Análisis de Variables

La etapa de Selección de Características y Análisis de Variables constituye un proceso crítico dentro del flujo metodológico para la detección de fraudes financieros, orientado a optimizar la calidad del conjunto de datos empleados en el modelado predictivo. Durante esta fase, se desarrollan las siguientes actividades esenciales:

- **Identificación y selección de variables relevantes.** Se seleccionan aquellas variables predictivas que presentan mayor relevancia estadística o analítica respecto a la variable objetivo, ya sea a través de técnicas de análisis de correlaciones, medidas de importancia de características (feature importance) o métodos de evaluación basados en modelos preliminares.

- **Documentación de procesos de transformación y selección.** Cada transformación aplicada a los datos, así como los criterios utilizados para la selección o eliminación de variables, son documentados de forma exhaustiva. Esta práctica garantiza la replicabilidad de los experimentos analíticos y permite la auditoría completa del flujo de trabajo.
- **Aplicación de técnicas de reducción dimensional.** Cuando es necesario, se aplican métodos como el Análisis de Componentes Principales (PCA) o técnicas basadas en la varianza explicada, con el objetivo de simplificar la estructura del conjunto de datos, preservar la información relevante y mejorar la eficiencia de los modelos.

8.1.3. Curar y Comprender

La fase de balanceo de datos y modelado predictivo integra ambos pilares debido a la criticidad de garantizar calidad y trazabilidad al mismo tiempo.

Durante esta etapa:

- Se genera de manera responsable datos sintéticos (por ejemplo, mediante SMOTE) para corregir el desequilibrio de clases (pocos fraudes frente a muchas transacciones legítimas).
- Se documentan todos los experimentos realizados: versión de los datos utilizados, parámetros del balanceo, arquitectura de los modelos.

Curar garantiza que los datos balanceados sean confiables, mientras que Comprender permite auditar y justificar cada paso en el entrenamiento de los modelos.

8.1.3.1. Equilibrar los Datos

Como se validó en la literatura consultada lo más frecuente en los conjuntos de datos que tienen disponibles las entidades financieras es que los fraudes ser mucho menos frecuentes que las transacciones legítimas, es por esto que, para aumentar la eficiencia del modelo, se debe equilibrar el conjunto de datos, para esto existen distintas técnicas:

- ***Submuestreo.*** Tiene como objetivo eliminar el sesgo que se puede generar en el modelo hacia la clase mayoritaria del conjunto de datos (transacciones legitimas). Este tiene desventajas como: pérdida de información y sobreajuste del modelo (Hajek, Mohammad, et al., 2023).

- ***Sobremuestreo.*** Su objetivo es aumentar el número de muestras de la clase minoritaria (fraudes financieros), por medio de la creación de datos sintéticos a partir de la data original (Ashfaq, Khalid, Yahaya, Aslam, Taher Azar, et al., 2022).

Ahora bien, con los resultados obtenidos una de las técnicas más empleadas y que aportó a mejorar el rendimiento de los modelos es el sobremuestro de minorías sintéticas (SMOTE, Synthetic Minority Over-sampling Technique), que por medio de un proceso de interpolación entre las muestras cercanas de la clase minoritaria (fraudes), genera nuevos datos sintéticos de esta clase minoritaria (Almhaithawi et al., 2020c ; W. Li et al., n.d.).

8.1.4. Selección del Modelo

Después del preprocesamiento de los datos, es fundamental seleccionar el modelo más adecuado para la detección de fraudes. Con base en la literatura revisada, a continuación, se presentan los modelos más utilizados en este campo (Ver Tabla 8-2).

Tabla 8-2

Comparación de Modelos Tradicionales y Avanzados para la Detección de Fraudes

Tipo de Modelo	Modelo	Descripción
Modelos Tradicionales	Regresión Logística (LR)	Se emplea cuando las relaciones entre las variables del conjunto de datos son relativamente simples.
	Random Forest (RF)	Modelo basado en bosques aleatorios que combina múltiples árboles de decisión para generar un resultado único. Es eficaz con datos tabulares y relaciones no lineales.
	Máquinas de Soporte Vectorial (SVM)	Algoritmo eficaz en problemas de clasificación complejos, especialmente cuando existen márgenes claros entre las clases.
Modelos Avanzados	Redes Neuronales (ANN)	Modelo ampliamente utilizado en la detección de fraudes financieros. Es útil cuando el conjunto de datos es de gran volumen y presenta relaciones no lineales complejas.
	Deep Learning	Modelos basados en aprendizaje profundo que mejoran su eficiencia con el uso continuo. Son ideales para datos secuenciales. Ejemplos: Redes Neuronales Convolucionales (CNN), Redes de Memoria a Corto y Largo Plazo (LSTM) y Redes Neuronales Gráficas (GNNs).

Nota. La tabla presenta una comparación entre modelos tradicionales y avanzados utilizados en la detección de fraudes financieros. Mientras que los modelos tradicionales, como la Regresión Logística y Random Forest, son efectivos en problemas con relaciones relativamente simples, los modelos avanzados, como las Redes Neuronales y el Deep Learning, ofrecen mayor precisión en conjuntos de datos complejos y de gran volumen.

Una vez se ha seleccionado el modelo para trabajar, en función de la cantidad de datos y las características de estos se hace necesario entrenar el modelo para que realice su aprendizaje, para esto es necesario dividir el conjunto de datos en dos: entrenamiento y validación. El porcentaje sugerido para el entrenamiento oscila entre 70% y 80% del conjunto de datos, el restante se debe emplear para probar el modelo (Itoo et al., 2021b; Shukla et al., 2023b).

8.1.5. Proteger

En la fase de validación y clasificación de resultados, se busca asegurar la protección de los datos sensibles y garantizar la integridad de los resultados del modelo. En eta parte del proceso se asegura que:

- Los datos de validación estén blindados contra accesos no autorizados.
- La clasificación de fraudes sea auditable y cumpla las normativas de protección de datos.

8.1.5.1. Validación del Modelo

Culminado el proceso de entrenamiento y aprendizaje del modelo, se debe validar el rendimiento de este, (Tang & Liang, 2024; Yang et al., 2019) sugieren realizarlo con las siguientes métricas:

- ***Exactitud (Accuracy).*** Permite determinar la proporción de predicciones correctas, pero puede ser engañosa en datos desbalanceados, y se calcula con:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

- ***Precisión.*** Permite determinar la proporción de verdaderos positivos identificados correctamente respecto al total de casos positivos, se calcula con:

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

- ***Recall (Sensibilidad).*** Permite determinar la proporción de verdaderos positivos identificados correctamente respecto al total de casos positivos reales, se calcula con:

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

- ***F1-score***. Esta métrica combina precisión y recall y mide la exactitud del modelo cuando las clases están desequilibradas, se calcula con:

$$F1 = \frac{2*Precision*Recall}{Precision+Recall} \quad (4)$$

8.1.6. Proteger y Comprender

En la fase de monitoreo y mejora continua de los modelos en producción, se combinan los pilares de Proteger y Comprender. Durante esta etapa:

- Se supervisa el comportamiento de los modelos desplegados en entornos productivos para detectar desviaciones de desempeño (concept drift o data drift).
- Se audita el acceso y uso de los modelos y sus predicciones.
- Se mantienen registros actualizados y auditables para asegurar conformidad normativa.

Este proceso es clave para mantener la resiliencia operativa y cumplir con los estándares regulatorios y éticos.

8.1.6.1. Monitoreo y Mejora Continua

Una vez se ha seleccionado e implementado el modelo adecuado para la predicción de fraude financiero, es muy importante realizar un monitoreo y control periódico para validar que este siga cumpliendo con las necesidades de la entidad, asimismo, este proceso genera mejoras en el modelo para mantenerlo a la vanguardia frente a los nuevos comportamientos de fraude. Algunas actividades que aportan eso son:

- ***Monitoreo en tiempo real.*** Las métricas propuestas para la validación del modelo deben ser monitoreadas continuamente, con esto, se tendrá la seguridad de que el modelo esté identificando fraudes correctamente en tiempo real.

- ***Actualización periódica.*** Dado que los comportamientos fraudulentos mantienen un ritmo constante de cambio, se hace necesario reentrenar el modelo de forma periódica con nuevos datos para que este se adapte a los cambios en los patrones de fraude.

Con la desagregación de las actividades descritas anteriormente el modelo seleccionado se hace más eficaz y su tiempo de ejecución va a ir reduciendo, adicionalmente, entre más tiempo lleve en marcha el modelo seleccionado se puede iniciar un proceso de combinación de modelos, por medio de la implementación de modelos híbridos, los cuales se caracterizan por combinar características y algoritmos de aprendizaje automático para aumentar el rendimiento y la precisión de las predicciones.

La implementación de un sistema efectivo de detección de fraude en entornos financieros como el de Banco Itaú requiere más que técnicas avanzadas de Machine Learning; exige una sólida infraestructura de gobernanza de datos que garantice la calidad, trazabilidad y protección de la información en cada etapa del proceso analítico.

A lo largo de este capítulo, se ha demostrado que la adecuada articulación de los pilares de Curar, Comprender y Proteger no solo habilita el correcto funcionamiento de los modelos predictivos, sino que también se convierte en un elemento estratégico esencial para:

- Maximizar la confianza en los modelos mediante datos íntegros y procesos auditables.
- Garantizar el cumplimiento normativo frente a regulaciones financieras nacionales e internacionales.
- Optimizar la detección temprana de actividades fraudulentas, mejorando la capacidad de respuesta de la organización.
- Promover la transparencia, la ética y la responsabilidad en el uso de analítica avanzada y algoritmos de decisión automatizada.
- De esta manera, la gobernanza de datos deja de ser concebida únicamente como una barrera de control, para consolidarse como un verdadero motor habilitador de eficiencia, resiliencia e innovación en el entorno bancario digitalizado.

La Tabla 8-3 sintetiza la relación entre las principales fases del proceso de detección de fraude y los pilares de gobernanza de datos basados en las mejores prácticas de Amazon Web Services (AWS), proporcionando una guía estructurada para la correcta implementación de la metodología propuesta:

Tabla 8-3

Relación entre las Fases del Proceso de Detección de Fraude y los Pilares de Gobernanza de Datos de AWS

Fase del Proceso de Detección de Fraude	Pilares de Gobernanza AWS Relacionados	Función Principal
Datos de Entrada y Preprocesamiento	Curar	Integrar múltiples fuentes bancarias, asegurar la calidad, consistencia y preparación adecuada de los datos antes de su uso analítico.

Selección de Características y Análisis	Comprender	Mantener la trazabilidad de las variables seleccionadas, registrar las transformaciones de los datos y documentar el linaje para auditorías futuras.
Balanceo de Datos y Modelado Predictivo	Curar y Comprender	Garantizar la generación responsable de datos sintéticos (por ejemplo, mediante SMOTE) y documentar exhaustivamente los experimentos de entrenamiento de modelos.
Validación y Clasificación de Resultados	Proteger	Asegurar que los datos de validación estén protegidos contra accesos no autorizados, mantener la integridad de los resultados y auditar las decisiones predictivas.
Monitoreo de Modelos en Producción	Proteger y Comprender	Supervisar el acceso a los modelos y sus predicciones, detectar desviaciones o deterioros de desempeño, y mantener registros auditables que respalden el cumplimiento normativo.

Nota. La tabla resume la vinculación estratégica entre las fases del proceso de detección de fraude y los pilares de gobernanza de datos propuestos por AWS. Cada fase operacional está alineada con uno o varios pilares fundamentales (Curar, Comprender y Proteger) que aseguran la calidad, trazabilidad y seguridad de los datos. Esta articulación no solo optimiza el desempeño de los modelos analíticos, sino que también fortalece la transparencia, el cumplimiento normativo y la resiliencia operativa en el entorno bancario digital.

9. Conclusiones y Recomendaciones

A continuación, se presentan las conclusiones derivadas de la consultoría académica realizada para el banco Itaú Colombia, así como las recomendaciones correspondientes. Estas conclusiones abordan el problema planteado y se fundamentan en los resultados obtenidos a lo largo del estudio, los patrones identificados, los modelos de detección revisados y la metodología propuesta.

9.1. Conclusiones

La investigación realizada ha proporcionado una visión integral sobre la relevancia de los casos reales de fraude financiero para el desarrollo de sistemas robustos, como los de Danske Bank, Wells Fargo, Wirecard y el esquema Ponzi del expresidente de NASDAQ, reveló el alto impacto económico y reputacional que los fraudes financieros generan en las instituciones y sus clientes. Estos casos evidencian que, sin sistemas de detección de fraudes sólidos y adaptables, las organizaciones están expuestas a pérdidas millonarias y al deterioro de la confianza pública. Además, se identificaron patrones de fraude recurrentes que pueden ser detectados anticipadamente mediante modelos predictivos adecuados.

La evolución de los patrones de fraude financiero en el entorno digital postpandemia, los fraudes financieros aumentaron un 33% en el Reino Unido y un 35% en los Estados Unidos, impulsados principalmente por la digitalización del sector financiero. El estudio identificó 15 patrones específicos de fraude interno, que van desde la manipulación de informes financieros hasta la simulación de transacciones. Estos patrones resaltan la necesidad de modelos predictivos que permitan una detección temprana y precisa de las irregularidades dentro de las instituciones.

La investigación y la revisión comparativa con estudios previos, deja en evidencia la diversidad de modelos de detección de fraude y efectividad de enfoques híbridos, demostraron que no existe un modelo único para la detección de fraudes financieros (Abdallah et al., 2016b; Hilal et al., 2022; Motie & Raahemi, 2024). La elección del modelo depende del tipo de fraude, el tiempo de respuesta requerido y las características del conjunto de datos. Se observo que los modelos basados en redes neuronales gráficas (GNN) y redes generativas antagónicas (GAN) ofrecen niveles de precisión de hasta 98% y 99%, respectivamente. No obstante, se concluye que un enfoque híbrido, que combine múltiples técnicas, resulta más eficaz para abordar la diversidad y complejidad de los fraudes financieros.

Como propuesta de una metodología integral para la selección del modelo óptimo

Se propone una metodología, compuesta por cinco etapas clave:

- Recolección y preparación de datos
- Equilibrado de datos (para manejar desbalances en las clases)
- Selección del modelo
- Validación del modelo

- Monitoreo y mejora continua

Esta metodología, similar a la propuesta por (Krishnavardhan, Govindarajan, Rao, et al., 2024), destaca la importancia de la mejora continua, ya que los fraudes evolucionan constantemente, lo que obliga a los modelos a adaptarse a nuevos patrones de comportamiento fraudulento, teniendo en cuenta también la importancia de contar con una buena gobernanza de datos (Bozkuş Kahyaoğlu Editor, 2022b; Grove & Basilico, 2008).

A pesar de limitaciones como la falta de acceso a datos reales y un enfoque teórico debido a restricciones de confidencialidad, la investigación aporta significativamente al sector financiero. Se propone un marco metodológico holístico que integra múltiples modelos y fuentes de datos, permitiendo a las instituciones financieras, como el banco Itaú Colombia, contar con una guía adaptable para la detección de fraudes. Esta contribución supera enfoques anteriores, que se centraron únicamente en modelos individuales, al ofrecer una estrategia más amplia y flexible.

9.2. Recomendaciones

Desarrollar sistemas de detección robustos basados en el análisis de casos reales, en donde el banco Itaú Colombia debe reforzar sus sistemas de detección tomando como referencia los casos reales analizados. Es fundamental implementar modelos predictivos robustos que se ajusten a los patrones de fraude identificados, minimizando así el impacto económico y reputacional. Se recomienda la adopción de tecnologías que permitan actualizaciones dinámicas en los sistemas de monitoreo para anticipar nuevas formas de fraude.

También es necesario expandir el análisis hacia nuevas modalidades de fraude, considerando el aumento del fraude en el entorno digital, se sugiere ampliar el campo de investigación hacia modalidades poco exploradas, como el fraude en seguros y el fraude en inversiones, líneas de negocio clave para el banco. Esta ampliación permitirá diseñar estrategias específicas para cada modalidad, incrementando la capacidad de respuesta del banco frente a diversas amenazas.

En cuanto a la implementación con enfoques híbridos para la detección de fraudes, dado que no existe un modelo universalmente aplicable, se recomienda adoptar enfoques híbridos que combinen múltiples modelos de detección, como GNN y GAN, aprovechando sus altos niveles de precisión. La combinación de estos modelos permitirá abordar eficazmente la diversidad y complejidad de los fraudes financieros, incrementando la eficiencia y exactitud de los procesos de detección.

Se sugiere que el banco Itaú Colombia implemente la metodología integral propuesta, asegurando el cumplimiento de cada una de sus etapas, desde el preprocesamiento de datos hasta el monitoreo continuo del modelo seleccionado. Esta metodología garantizará que los modelos predictivos se mantengan actualizados y adaptables, mejorando su efectividad en la detección de nuevos patrones fraudulentos.

Ante la imposibilidad de acceder a datos reales por razones de confidencialidad, se recomienda el uso de datos públicos o la generación de datos sintéticos. Además, se sugiere desarrollar modelos predictivos personalizados para cada tipo de fraude, lo que permitirá resultados más precisos y alineados a las necesidades específicas de cada línea de negocio del banco Itaú Colombia.

10. Referencias Bibliográficas

(43) Itaú acelera el despliegue de modelos en un 75% con infraestructura AWS - YouTube. (n.d.). Retrieved January 31, 2025, from https://www.youtube.com/watch?v=vSHXS4q82v0

(43) Itaú Unibanco adopts the data mesh architecture and relies on AWS support - English - YouTube. (n.d.). Retrieved January 31, 2025, from https://www.youtube.com/watch?v=mSUO9-SUuB4

Abadlia, H., & Smairi, N. (2024). Enhanced particle swarm optimization-based hyperparameter optimized stacked autoencoder for credit card fraud detection. *International Journal of Data Science and Analytics*, 1–15. https://doi.org/10.1007/S41060-024-00524-X/FIGURES/14

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

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

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023a). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, *6*, 100163. https://doi.org/10.1016/J.DAJOUR.2023.100163

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023b). A supervised machine learning algorithm for

detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, *6*, 100163. https://doi.org/10.1016/J.DAJOUR.2023.100163

Ali, N. T., Hasan, S. J., Ghandour, A., & Al-Hchimy, Z. S. (2024). Improving credit card fraud detection using machine learning and GAN technology. *BIO Web of Conferences*, *97*. https://doi.org/10.1051/bioconf/20249700076

Almhaithawi, D., Jafar, A., & Aljnidi, M. (2020a). Example-dependent cost-sensitive credit cards fraud detection using SMOTE and Bayes minimum risk. *SN Applied Sciences*, *2*(9), 1–12. https://doi.org/10.1007/S42452-020-03375-W/FIGURES/6

Almhaithawi, D., Jafar, A., & Aljnidi, M. (2020b). Example-dependent cost-sensitive credit cards fraud detection using SMOTE and Bayes minimum risk. *SN Applied Sciences*, *2*(9). https://doi.org/10.1007/s42452-020-03375-w

Almhaithawi, D., Jafar, A., & Aljnidi, M. (2020c). Example-dependent cost-sensitive credit cards fraud detection using SMOTE and Bayes minimum risk. *SN Applied Sciences*, *2*(9). https://doi.org/10.1007/s42452-020-03375-w

Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors*, *22*(19). https://doi.org/10.3390/s22197162

Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Taher Azar, A., Alsafari, S., & Hameed, I. A. (2022). *A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism*. https://doi.org/10.3390/s22197162

Assunção, M. D., Calheiros, R. N., Bianchi, S., Netto, M. A. S., & Buyya, R. (2015). Big Data computing and clouds: Trends and future directions. *Journal of Parallel and Distributed Computing*, *79–80*, 3–15. https://doi.org/10.1016/J.JPDC.2014.08.003

Balaji, K., Saxena, N., Behera, N. R., Kiran Kumar, M., Prasad, H. K., & Gedamkar, P. R. (2024). Improved Fraud Detection in Banking Systems through Machine Learning

and Big Data Analytics with Management Key Components. *Proceedings - 3rd International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2024*. https://doi.org/10.1109/ACCAI61061.2024.10601803

Banco Itau. (2024). *Presentación institucional*.

Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2021). *Enhanced credit card fraud detection based on attention mechanism and LSTM deep model*. https://doi.org/10.1186/s40537-021-00541-8

Bose, R., Chakraborty, S., & Roy, S. (2019). Explaining the Workings Principle of Cloud-based Multi-factor Authentication Architecture on Banking Sectors. *Proceedings - 2019 Amity International Conference on Artificial Intelligence, AICAI 2019*, 764–768. https://doi.org/10.1109/AICAI.2019.8701317

Bozkuş Kahyaoğlu Editor, S. (2022a). *Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application*. https://link.springer.com/bookseries/13615

Bozkuş Kahyaoğlu Editor, S. (2022b). *Accounting, Finance, Sustainability, Governance & Fraud: Theory and Application*. https://link.springer.com/bookseries/13615

Chen, K., Seshadri, S., & Zhang, L.-J. (Eds.). (2019). *Big Data – BigData 2019* (Vol. 11514). Springer International Publishing. https://doi.org/10.1007/978-3-030-23551-2

CHEN, R.-C., CHEN, T.-S., & LIN, C.-C. (2006). A NEW BINARY SUPPORT VECTOR SYSTEM FOR INCREASING DETECTION RATE OF CREDIT CARD FRAUD. *International Journal of Pattern Recognition and Artificial Intelligence*, *20*(02), 227–239. https://doi.org/10.1142/S0218001406004624

Cherif, A., Ammar, H., Kalkatawi, M., Alshehri, S., & Imine, A. (2024). Encoder–decoder graph neural network for credit card fraud detection. *Journal of King Saud University - Computer and Information Sciences*, *36*(3). https://doi.org/10.1016/j.jksuci.2024.102003

Chhabra, R., Goswami, S., & Ranjan, R. K. (2024). A voting ensemble machine learning based credit card fraud detection using highly imbalance data. *Multimedia Tools and Applications*, *83*(18), 54729–54753. https://doi.org/10.1007/S11042-023-17766-9/FIGURES/19

Cybersource. (n.d.). *2023 Global Ecommerce Payments And Fraud Report*.

De Leon Obrador, M. (2022). *WIRECARD FRAUD: ANALYSIS AND PROPOSED PREVENTION STRATEGIES*.

Delarue, M. L. (2020). *Preventing and detecting fraud*. https://www.ey.com/es_co/assurance/preventing-and-detecting-fraud-how-to-strengthen-the-roles-of-companies-auditors-and-regulators

Dewi, R., Sarno, R., Fatichah, C., & Dwi, S. (2017a). Fraud detection on event log of bank financial credit business process using Hidden Markov Model algorithm. *Proceeding - 2017 3rd International Conference on Science in Information Technology: Theory and Application of IT for Education, Industry and Society in Big Data Era, ICSITech 2017*, *2018-January*, 35–40. https://doi.org/10.1109/ICSITECH.2017.8257082

Dewi, R., Sarno, R., Fatichah, C., & Dwi, S. (2017b). Fraud detection on event log of bank financial credit business process using Hidden Markov Model algorithm. *Proceeding - 2017 3rd International Conference on Science in Information Technology: Theory and Application of IT for Education, Industry and Society in Big Data Era, ICSITech 2017*, *2018-January*, 35–40. https://doi.org/10.1109/ICSITECH.2017.8257082

Ding, Z. (2023). Construction and Exploration of a Financial Risk Control Model Based on Machine Learning. *2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques, EASCT 2023*. https://doi.org/10.1109/EASCT59475.2023.10393547

Flondor, E., Donath, L., & Neamtu, M. (2024). Automatic Card Fraud Detection Based on Decision Tree Algorithm. *Applied Artificial Intelligence*, *38*(1). https://doi.org/10.1080/08839514.2024.2385249/SUPPL_FILE/UAAI_A_2385249_SM7315.BIB

Fu, B., Yu, X., & Feng, T. (2022). CT-GCN: a phishing identification model for blockchain cryptocurrency transactions. *International Journal of Information Security*, *21*(6), 1223–1232. https://doi.org/10.1007/s10207-022-00606-6

Grove, H., & Basilico, E. (2008). Fraudulent Financial Reporting Detection: Key Ratios Plus Corporate Governance Factors. *International Studies of Management & Organization*, *38*(3), 10–42. https://doi.org/10.2753/IMO0020-8825380301

Haigh, R. (2024). *Global 500 2024 | The Annual Brand Value Ranking | Brandirectory*. https://brandirectory.com/rankings/global/

Hajek, P., Abedin, M. Z., & Sivarajah, U. (2023). Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework. *Information Systems Frontiers*, *25*(5), 1985–2003. https://doi.org/10.1007/s10796-022-10346-6

Hajek, P., Mohammad, ·, Abedin, Z., & Sivarajah, · Uthayasankar. (2023). *Fraud Detection in Mobile Payment Systems using an XGBoost-based Framework*. *25*, 1985–2003. https://doi.org/10.1007/s10796-022-10346-6

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. *Expert Systems with Applications*, *193*, 116429. https://doi.org/10.1016/J.ESWA.2021.116429

Hong, Z., Tu, B., Tong, X., Pan, H., Zhou, R., Zhang, Y., Han, Y., Wang, J., Yang, S., & Ma, Z. (2023). A Fast Large-Scale Path Planning Method on Lunar DEM Using Distributed Tile Pyramid Strategy. *IEEE Journal of Selected Topics in Applied Earth*

Observations and Remote Sensing, *16*, 344–355. https://doi.org/10.1109/JSTARS.2022.3226527

Ileberi, E., Sun, Y., & Wang, Z. (2022a). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1). https://doi.org/10.1186/s40537-022-00573-8

Ileberi, E., Sun, Y., & Wang, Z. (2022b). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1). https://doi.org/10.1186/s40537-022-00573-8

Innan, N., Sawaika, A., Dhor, A., Dutta, S., Thota, S., Gokal, H., Patel, N., Khan, M. A. Z., Theodonis, I., & Bennai, M. (2024a). Financial fraud detection using quantum graph neural networks. *Quantum Machine Intelligence*, *6*(1), 1–18. https://doi.org/10.1007/S42484-024-00143-6/FIGURES/23

Innan, N., Sawaika, A., Dhor, A., Dutta, S., Thota, S., Gokal, H., Patel, N., Khan, M. A. Z., Theodonis, I., & Bennai, M. (2024b). Financial fraud detection using quantum graph neural networks. *Quantum Machine Intelligence*, *6*(1), 1–18. https://doi.org/10.1007/S42484-024-00143-6/FIGURES/23

Itaú. (2016). *Presentación Institucional*.

Itaú. (2022). *Presentación Institucional dic 22*.

Itaú. (2023a). *Banco Itaú - Banca Personas - Banco Itaú Colombia - Banco Itaú*. https://banco.itau.co/

Itaú. (2023b). *Bonos subordinados*.

Itaú. (2023c). *Presentación institucional*.

Itoo, F., Meenakshi, & Singh, S. (2021a). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection.

International Journal of Information Technology (Singapore), *13*(4), 1503–1511. https://doi.org/10.1007/s41870-020-00430-y

Itoo, F., Meenakshi, & Singh, S. (2021b). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *International Journal of Information Technology (Singapore)*, *13*(4), 1503–1511. https://doi.org/10.1007/s41870-020-00430-y

Joyanes. (2019). *BIG DATA: ARQUITECTURA, ECOSISTEMA HADOOP Y OPEN DATA)*.

Kafila, Hassan, M., Veena, C., Singla, A., Joshi, A., & Lourens, M. (2024). Fraud Detection in IoT-Based Financial Transactions Using Anomaly Detection Techniques. *Proceedings - 3rd International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2024*. https://doi.org/10.1109/ACCAI61061.2024.10602423

Kancharla, J. R., & Madhu Kumar, S. D. (2023). Breaking Down Data Silos: Data Mesh to Achieve Effective Aggregation in Data Localization. *2023 International Conference on Computer, Electronics and Electrical Engineering and Their Applications, IC2E3 2023*. https://doi.org/10.1109/IC2E357697.2023.10262765

Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach. *Big Data and Cognitive Computing 2024, Vol. 8, Page 6*, *8*(1), 6. https://doi.org/10.3390/BDCC8010006

Krishnavardhan, N., Govindarajan, · M, Rao, · S V Achutha, Govindarajan, M., & Rao, S. V. A. (2024). *An intelligent credit card fraudulent activity detection using hybrid deep learning algorithm*. *83*, 87621–87646. https://doi.org/10.1007/s11042-024-18793-w

Krishnavardhan, N., Govindarajan, M., & Rao, S. V. A. (2023). Flower pollination optimization algorithm with stacked temporal convolution network-based classification for financial anomaly fraud detection. *Soft Computing*, 1–14. https://doi.org/10.1007/S00500-023-08732-6/TABLES/16

Krishnavardhan, N., Govindarajan, M., & Rao, S. V. A. (2024). An intelligent credit card fraudulent activity detection using hybrid deep learning algorithm. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-18793-w

Kurshan, E., Shen, H., & Yu, H. (2020). Financial Crime Fraud Detection Using Graph Computing: Application Considerations Outlook. *Proceedings - 2020 2nd International Conference on Transdisciplinary AI, TransAI 2020*, 125–130. https://doi.org/10.1109/TransAI49837.2020.00029

Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering-A Critical Review. In *IEEE Access* (Vol. 9, pp. 82300–82317). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2021.3086230

Leal, L. F., Luis, B., & Ferrer, G. (2014). *IMPORTANCIA DEL CONTROL INTERNO PARA LA PREVENCIÓN DEL FRAUDE MALVERSACIÓN DE ACTIVOS*.

Li, S. H., Yen, D. C., Lu, W. H., & Wang, C. (2012a). Identifying the signs of fraudulent accounts using data mining techniques. *Computers in Human Behavior*, *28*(3), 1002–1013. https://doi.org/10.1016/J.CHB.2012.01.002

Li, S. H., Yen, D. C., Lu, W. H., & Wang, C. (2012b). Identifying the signs of fraudulent accounts using data mining techniques. *Computers in Human Behavior*, *28*(3), 1002–1013. https://doi.org/10.1016/j.chb.2012.01.002

Li, W., Wu, C. S., & Ruan, S. M. (2022). CUS-RF-Based Credit Card Fraud Detection with Imbalanced Data. *Journal of Risk Analysis and Crisis Response*, *12*(3), 110–123. https://doi.org/10.54560/jracr.v12i3.332

Li, W., Wu, C.-S., & Ruan, S.-M. (n.d.). CUS-RF-Based Credit Card Fraud Detection with Imbalanced Data. *Journal of Risk Analysis and Crisis Response*, *2022*(3), 110–123. https://doi.org/10.54560/jracr.v12i3.332

Li, W., Zhu, J., Zhang, Y., & Zhang, S. (2020). Design and implementation of intelligent traffic and big data mining system based on internet of things. *Journal of Intelligent & Fuzzy Systems*, *38*(2), 1967–1975. https://doi.org/10.3233/JIFS-190558

Li, Y., Chen, Z., Zha, D., Zhou, K., Jin, H., Chen, H., & Hu, X. (2022). Automated Anomaly Detection via Curiosity-Guided Search and Self-Imitation Learning. *IEEE Transactions on Neural Networks and Learning Systems*, *33*(6), 2365–2377. https://doi.org/10.1109/TNNLS.2021.3105636

Lilly, J., Durr, D., Grogan, A., & Super, J. F. (2021). Wells Fargo: Administrative evil and the pressure to conform. *Business Horizons*, *64*(5), 587–597. https://doi.org/10.1016/J.BUSHOR.2021.02.028

Lopez, R. E. A. (2017). A review of computer simulation for fraud detection research in financial datasets. *FTC 2016 - Proceedings of Future Technologies Conference*, 932–935. https://doi.org/10.1109/FTC.2016.7821715

Malagón González, J., Malagón, J., Presidente, G., Vera, A., Vicepresidente, S., Germán, T., & Moreno, M. (n.d.). *Principales hitos y desafíos de la banca colombiana: Informe de Gestión Gremial 2023*.

Mashrur, A., Luo, W., Zaidi, N. A., & Robles-Kelly, A. (2020). Machine learning for financial risk management: A survey. In *IEEE Access* (Vol. 8, pp. 203203–203223).

Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2020.3036322

Maulana, L. R., Fajar, A. N., & Meyliana. (2021). Extending the Design of Smart Mobile Application to Detect Fraud Theft of E-Banking Access Using Big Data Analytic and SOA. *Proceedings - 2021 IEEE 5th International Conference on Information Technology, Information Systems and Electrical Engineering: Applying Data Science and Artificial Intelligence Technologies for Global Challenges During Pandemic Era, ICITISEE 2021*, 360–364. https://doi.org/10.1109/ICITISEE53823.2021.9655805

Motie, S., & Raahemi, B. (2024). Financial fraud detection using graph neural networks: A systematic review. *Expert Systems with Applications*, *240*, 122156. https://doi.org/10.1016/J.ESWA.2023.122156

Ocampo, J. A. (2021). *SISTEMA FINANCIERO COLOMBIANO 1870-2021*. www.mnrediciones.com

OEA, & ASOBANCARIA. (2020). *Estado de la ciberseguridad en el sistema financiero colombiano*.

Pandey, D. K., Hassan, M. K., Kumari, V., Zaied, Y. Ben, & Rai, V. K. (2024). Mapping the landscape of FinTech in banking and finance: A bibliometric review. *Research in International Business and Finance*, *67*, 102116. https://doi.org/10.1016/J.RIBAF.2023.102116

Perdomo Maldonado, S. (2017). *Proyecto F Diagnóstico del uso del efectivo en Colombia*. www.comunicaciongraficalegis.com

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

Saha, P., Aanand, S., Shah, P., Khatwani, R., Mitra, P. K., & Sekhar, R. (2023). Comparative Analysis of ML Algorithms for Fraud Detection in Financial Transactions. *2023 1st International Conference on Advances in Electrical, Electronics and Computational Intelligence, ICAEECI 2023*. https://doi.org/10.1109/ICAEECI58247.2023.10370930

Shukla, P., Aggarwal, M., Jain, P., Khanna, P., & Rana, M. K. (2023a). Financial Fraud Detection and Comparison Using Different Machine Learning Techniques. *Proceedings - International Conference on Technological Advancements in Computational Sciences, ICTACS 2023*, 1205–1210. https://doi.org/10.1109/ICTACS59847.2023.10390165

Shukla, P., Aggarwal, M., Jain, P., Khanna, P., & Rana, M. K. (2023b). Financial Fraud Detection and Comparison Using Different Machine Learning Techniques. *Proceedings - International Conference on Technological Advancements in Computational Sciences, ICTACS 2023*, 1205–1210. https://doi.org/10.1109/ICTACS59847.2023.10390165

Tang, Y., & Liang, Y. (2024). *Credit card fraud detection based on federated graph learning*. https://doi.org/10.1016/j.eswa.2024.124979

Tayebi, M., Said, ·, & Kafhali, E. (2022). *Performance analysis of metaheuristics based hyperparameters optimization for fraud transactions detection*. *17*, 921–939. https://doi.org/10.1007/s12065-022-00764-5

Tong, G., & Shen, J. (2023). Financial transaction fraud detector based on imbalance learning and graph neural network. *Applied Soft Computing*, *149*, 110984. https://doi.org/10.1016/J.ASOC.2023.110984

Tripathi, K. K., & Pavaskar, M. A. (2012). *Survey on Credit Card Fraud Detection Methods*. www.ijetae.com

Usman, A. U., Abdullahi, S. B., Liping, Y., Alghofaily, B., Almasoud, A. S., & Rehman, A. (2024). Financial Fraud Detection Using Value-at-Risk With Machine Learning in Skewed Data. *IEEE Access*, *12*, 64285–64299. https://doi.org/10.1109/ACCESS.2024.3393154

Usman, A. U., Adfullahi, S. B., & Luping, Y. (2024). *Financial Fraud Detection Using Value-at-Risk With Machine Learning in Skewed Data*. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10507824

Valenzuela, M., Julián, G., Rojas Castañeda, A., Hernando, P., Gómez, J., Vicepresidente, R., José, J., Gómez, M., Directora, S., Normativa, J., Ovalle, A. M., Directora, H., Operacional, J., María, I., & Ordóñez, M. (2022a). *La reinvención financiera en la era digital*.

Valenzuela, M., Julián, G., Rojas Castañeda, A., Hernando, P., Gómez, J., Vicepresidente, R., José, J., Gómez, M., Directora, S., Normativa, J., Ovalle, A. M., Directora, H., Operacional, J., María, I., & Ordóñez, M. (2022b). *La reinvención financiera en la era digital*.

Vargas Rojas, L., & Luna, L. (2020). *La transformación digital en el sector bancario y la atención al cliente en épocas de pandemia Leidy*.

Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., & Anderla, A. (2019). Credit Card Fraud Detection - Machine Learning methods. *2019 18th International Symposium INFOTEH-JAHORINA, INFOTEH 2019 - Proceedings*. https://doi.org/10.1109/INFOTEH.2019.8717766

Velásquez, J. D. (2015a). A short guide to writing systematic literature reviews. Part 4. In *DYNA (Colombia)* (Vol. 82, Issue 190, pp. 9–12). Universidad Nacional de Colombia. https://doi.org/10.15446/dyna.v82n190.49511

Velásquez, J. D. (2015b). Una Guía Corta para Escribir Revisiones Sistemáticas de Literatura Parte 3. *DYNA*, *82*(189), 9–12. https://doi.org/10.15446/dyna.v82n189.48931

Venkata, V., Reddy, K., Vijaya, R., Reddy, K., Siva, M., Munaga, K., Karnam, B., Kumar Maddila, S., & Kolli, C. S. (2024). Deep learning-based credit card fraud detection in federated learning. *Expert Systems With Applications*, *255*, 124493. https://doi.org/10.1016/j.eswa.2024.124493

Vinther Daugaard, T., Bisgaard Jensen, J., Kauffman, R. J., & Kim, K. (2024). Blockchain solutions with consensus algorithms and immediate finality: Toward Panopticon-style monitoring to enhance anti-money laundering. *Electronic Commerce Research and Applications*, *65*, 101386. https://doi.org/10.1016/J.ELERAP.2024.101386

Wang, D., Lin, J., Peng, C., & Quanhui, J. (2019). *A Semi-Supervised Graph Attentive Network for Financial Fraud Detection*. https://ieeexplore.unalproxy.elogim.com/document/8970829

Wang, D., Qi, Y., Lin, J., Cui, P., Jia, Q., Wang, Z., Fang, Y., Yu, Q., Zhou, J., & Yang, S. (2019). A semi-supervised graph attentive network for financial fraud detection. *Proceedings - IEEE International Conference on Data Mining, ICDM*, *2019-November*, 598–607. https://doi.org/10.1109/ICDM.2019.00070

Wu, B., Lv, X., Alghamdi, A., Abosaq, H., & Alrizq, M. (2023). Advancement of management information system for discovering fraud in master card based intelligent supervised machine learning and deep learning during SARS-CoV2. *Information Processing & Management*, *60*(2), 103231. https://doi.org/10.1016/J.IPM.2022.103231

Xia, D., Lu, X., Li, H., Wang, W., Li, Y., & Zhang, Z. (2018). A MapReduce-Based Parallel Frequent Pattern Growth Algorithm for Spatiotemporal Association Analysis of Mobile Trajectory Big Data. *Complexity*, *2018*. https://doi.org/10.1155/2018/2818251

Xie, Y., Li, A., Hu, B., Gao, L., & Tu, H. (2023a). A Credit Card Fraud Detection Model Based on Multi-Feature Fusion and Generative Adversarial Network. *Computers, Materials and Continua*, *76*(3), 2707–2726. https://doi.org/10.32604/cmc.2023.037039

Xie, Y., Li, A., Hu, B., Gao, L., & Tu, H. (2023b). A Credit Card Fraud Detection Model Based on Multi-Feature Fusion and Generative Adversarial Network. *Computers, Materials and Continua*, *76*(3), 2707–2726. https://doi.org/10.32604/cmc.2023.037039

Xiong, T., Ma, Z., Li, Z., & Dai, J. (2022). The analysis of influence mechanism for internet financial fraud identification and user behavior based on machine learning approaches. *International Journal of System Assurance Engineering and Management*, *13*, 996–1007. https://doi.org/10.1007/s13198-021-01181-0

Yang, W., Zhang, Y., Ye, K., Li, L., & Xu, C. Z. (2019). FFD: A federated learning based method for credit card fraud detection. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11514 LNCS*, 18–32. https://doi.org/10.1007/978-3-030-23551-2_2/TABLES/4

Zhao, C., Sun, X., Wu, M., & Kang, L. (2024a). Advancing financial fraud detection: Self-attention generative adversarial networks for precise and effective identification. *Finance Research Letters*, *60*. https://doi.org/10.1016/j.frl.2023.104843

Zhao, C., Sun, X., Wu, M., & Kang, L. (2024b). Advancing financial fraud detection: Self-attention generative adversarial networks for precise and effective identification. *Finance Research Letters*, *60*. https://doi.org/10.1016/j.frl.2023.104843

Zhu, S., Wu, H., Ngai, E. W. T., Ren, J., He, D., Ma, T., & Li, Y. (2024). *A Financial Fraud Prediction Framework Based on Stacking Ensemble Learning*. https://doi.org/10.3390/systems12120588

Zioviris, G., Kolomvatsos, K., Stamoulis, G., & Stamoulis georges, G. (2022). Credit card fraud detection using a deep learning multistage model. *The Journal of Supercomputing*, *78*, 14571–14596. https://doi.org/10.1007/s11227-022-04465-9

Anexo A: Matriz de Consulta Bibliográfica

Se presenta la matriz de los 60 artículos consultados.

Revista	Articulo	Año	Modelo Implementado	Descripción Entidad Financiera	Resultados	Desafíos
IEEE	Una revisión de la simulación por computadora para la investigación de detección de fraudes en conjuntos de datos financieros	2016	Multi-Agent Based Simulation, MABS	Trasacciones Financieras	Pruebas de diferentes algoritmos de detección de patrones de fraude, como lavado de dinero	1. Falta de datos reales 2. Requiere iteración continua para mejorar la precisión del modelo
IEEE	Detección de fraudes en el registro de eventos del proceso de negocio de crédito financiero bancario mediante el algoritmo del modelo oculto de Markov	2017	Modelo de Markov Oculto (Hidden Markov Model)	Detección de fraude en el proceso de crédito	Alta probabilidad en la detección de fraudes	1. Identificar y diferenciar entre comportamientos normales y fraudulentos 2. Riesgo de errores debido a datos limitados en casos de fraude
ELSEVIER	Identificación de señales de cuentas fraudulentas mediante técnicas de minería de datos	2012	Bayesian Classification and Association Rules	Banco con cuentas personales, enfocado en detectar cuentas fraudulentas utilizadas en estafas telefónicas de cajeros automáticos (ATM).	Tasa de detección del 65% en la identificación de cuentas fraudulentas	1. Dependencia de datos precisos y preprocesados. 2. Implementación en sistemas bancarios basados en COBOL. 3. Complejidad de análisis continuo.

Scopus	Mejora en la detección de fraudes con tarjetas de crédito mediante el aprendizaje automático y la tecnología GAN	2024	Modelo hibrido de Machine Learning	Transacciones en línea con tarjeta de crédito	Accuracy: 99,9%	Software especializado
IEEE	Una red de atención gráfica semisupervisada para la detección de fraudes financieros	2019	Semi-Supervised Graph Attentive Network (SemiGNN)	Plataforma de pagos digitales con más de 400 millones de usuarios que analiza relaciones sociales y atributos financieros.	Mayor precisión en la detección de fraudes financieros mediante datos etiquetados y no etiquetados	1. Manejo de heterogeneidad en datos multivista 2. Necesidad de interpretabilidad en los resultados
Springer Link	FFD: Un método basado en el aprendizaje federado para la detección de fraudes con tarjetas de crédito	2019	Federated Fraud Detection (FFD)	Bancos participantes en Europa colaboraron mediante un modelo de aprendizaje federado sin compartir datos sensibles.	10% de mejora en AUC frente a métodos tradicionales, alcanzando una precisión del 95.5%.	1. Costos de comunicación. 2. Coordinación entre bancos. 3. Manejo de distribución de datos desequilibrada.
IEEE	Cómo encontrar cuentas con errores en los estados financieros mediante razonamiento ontológico	2019	Ontological reasoning using OWL and SWRL to analyze relationships between financial accounts.	Identificación de anomalías en ingresos, gastos y provisiones para préstamos con explicaciones interpretables.	Identificación de anomalías en ingresos, gastos y provisiones para préstamos con explicaciones interpretables.	Calidad de los datos, complejidad en la modelización y limitaciones históricas.

IEEE	Aprendizaje automático para la gestión de riesgos financieros: una encuesta	2020	Semi-Supervised Graph Attention Network	Modelo de red neuronal gráfica para detección de fraudes	Identificación precisa de actividades fraudulentas en redes financieras complejas	1. Manejo de datos heterogéneos en grandes volúmenes 2. Necesidad de interpretabilidad de resultados
IEEE	Un enfoque comparativo del análisis predictivo con aprendizaje automático para la detección de fraudes en datos financieros en tiempo real	2020	Enfoque Comparativo de Analítica Predictiva con ML	Detección de fraude en datos financieros en tiempo real	Comparación de técnicas de ML, incluyendo redes neuronales y árboles de decisión, para detectar fraudes con alta precisión en datos en tiempo real	1. Procesamiento de grandes volúmenes de datos en tiempo real 2. Optimización de tasas de falsos positivos. 3.Modelos Cambiantes constantemente
Taylor & Francis	Detección de informes financieros fraudulentos: indicadores clave y factores de gobernanza corporativa	2008	Probit Statistical Model utilizando índices financieros (GMI, SGI, DSRI) y factores cualitativos de gobernanza corporativa	Corporaciones públicas cuyas prácticas fueron investigadas por la U.S. Securities and Exchange Commission (SEC) y autoridades europeas.	Combinación de análisis financiero y cualitativo para mayor precisión. Identificación de patrones clave para red flags. Detección temprana del 76% con un bajo margen de error. Requiere análisis exhaustivo de ratios financieros (margen bruto, crecimiento de ventas, cuentas por cobrar) para generar alertas tempranas	Dependencia de datos financieros precisos. - Complejidad para integrar datos cualitativos y cuantitativos. - Necesidad de expertos en gobernanza corporativa.

IEEE	Detección de fraudes y delitos financieros mediante computación gráfica: consideraciones de aplicación y perspectivas	2020	Computación Gráfica con Redes Neuronales (Graph Neural Networks - GNNs)	Bancos y Procesadores de Pagos, Instituciones de Servicios Financiero, Billeteras Digitales y Proveedores de Pagos Electrónicos	Detección precisa de patrones anómalos en redes de cuentas, mejora en tiempo de respuesta en sistemas dinámicos	1. Procesar grafos dinámicos en tiempo real 2. Robustez frente a ataques adversariales 3. Limitaciones en datos etique
Springer Link	Comparación y análisis de algoritmos de regresión logística, Naïve Bayes y KNN machine learning para la detección de fraudes con tarjetas de crédito	2020	1. Regresión Logistica 2. KNN, algoritmo K vecinos más cercanos 3.Naive Bayes	Banca Europea, transacciones de tarjetas de crédito	Accuracy: 95,9% 91,5% 75,1% Sensibilidad: 87,8% 75,7% 68,7% Especifidad 100% 100% 78,9% Precisión: 100% 100% 70,1% Medida F: 91,3% 84,6% 69,4% AUC: 91,8% 86% 67,8%	1. Lenguage Python 2, Desequilibrio de datos (Submuestreo) 3. Perdida de información
Springer Link	Ejemplo de detección de fraude con tarjetas de crédito sensibles a los costos dependientes mediante SMOTE y el riesgo mínimo de Bayes	2020	1. Regresión Logistica (LR) 2. Bosques Aleatorios (RF) 3. XGBoost 4. CatBoost	Banca Europea, transacciones de tarjetas de crédito	F1-Score: 98% 100% 98,8% 100% AUC: 99,7% 99,9% 99,9% 99,9% Savings: 92,8% 97% 94% 97%	1. Lenguage R-Python 2, Desequilibrio de datos (SMOTE y BMR) 3. Ajuste conforme a necesidad

IEEE	Ampliación del diseño de aplicaciones móviles inteligentes para detectar fraudes y robos de acceso a banca electrónica mediante análisis de big data y SOA	2021	Análisis de Big Data con Arquitectura Orientada a Servicios (SOA)	Entidades financieras que operan con servicios de banca electrónica y cuentas digitales inactivas (dormant accounts), con alta dependencia de plataformas móviles y digitales	Identificación en tiempo real de fraudes en cuentas inactivas mediante alertas automáticas enviadas a gerentes de sucursales.	1. Integración de SOA con sistemas bancarios tradicionales.2. Manejo de datos estructurados y no estructurados en Big Data.3. Capacitación del personal para la gestión de alertas.
IEEE	Detección automática de anomalías mediante búsqueda guiada por curiosidad y aprendizaje por autoimitación	2021	AutoAD: Neural networks with curiosity-driven search and self-imitation learning.	Empresas o instituciones que necesitan detectar anomalías en datos financieros desbalanceados y complejos.	Identificación precisa de anomalías mediante arquitecturas optimizadas, con una mejora en la eficiencia de detección.	1. Requiere altos recursos computacionales. 2. Sensibilidad a configuraciones iniciales y ajuste de hiperparámetros.
IEEE	Técnicas de aprendizaje profundo e inteligencia artificial explicable aplicadas a la detección del lavado de dinero: una revisión crítica	2021	Deep learning models and XAI (Explainable Artificial Intelligence) for fraud detection.	Instituciones enfocadas en la detección de lavado de dinero y fraudes internos mediante análisis avanzado de transacciones.	Mejora en la identificación de transacciones sospechosas y anomalías en flujos de dinero, con explicaciones interpretables para auditorías.	1. Acceso limitado a datos etiquetados y actualizados. 2. Complejidad en la implementación de XAI. 3. Dificultades para manejar datos desbalanceados.

IEEE	Modelo de atención de dos niveles de aprendizaje de representación para la detección de fraudes	2021	Hybrid Model: Integration of Hidden Markov Model and Gradient Boosting Classifier	Bancos que buscan mejorar la detección de fraudes mediante análisis predictivo y monitorización en tiempo real de transacciones financieras.	Incremento significativo en la precisión de detección y reducción de falsos positivos en comparación con métodos tradicionales	1. Complejidad de integrar ambos modelos. 2. Requiere recursos computacionales elevados. 3. Ajuste de hiperparámetros para optimizar resultados.
Scopus	Modo de bosque aleatorio mejorado para la detección de transacciones fraudulentas en línea	2021	Bosque Aleatorio (RF)	Banco en China, transacciones Online	Precision: 97,8% Tasa de Recuerdo: 95%	1. Software 2. Desequilibrio de datos (Bagging Balance)
Science Direct	Detección de fraudes con tarjetas de crédito empleando redes neuronales artificiales	2021	ANN (Red Neuronal Artificial)	Banca Europea, transacciones de tarjetas de crédito	Accuraccy: 99,9%	1. Software 2. Desequilibrio de datos (Submuestreo) 3. Tiempo de aprendizaje
Springer Link	El análisis del mecanismo de influencia para la identificación del fraude financiero en Internet y el comportamiento de los usuarios basado en enfoques de aprendizaje automático	2021	Red Neuronal	Banco en China, transacciones Online	Accuracy: 96,4%	Software especializado
Springer Link	Estrategias de aprendizaje incremental para la detección de fraudes con tarjetas de crédito	2021	Red Neuronal Densa (NN)	Transacciones en línea	Aumenta precisión en 1,3%	1. Software especializado 2. Desequilibrio de datos 3. Tiempo de respuesta

Springer Link	Detección mejorada de fraudes con tarjetas de crédito basada en el mecanismo de atención y el modelo profundo de LSTM	2021	Red Neuronal Recurrente Profunda (RNN)	Tarjetas de crédito	Accuracy: 96,7% Precisión: 98,9%	1. Desequilibrio de datos 2. Software especializado (Python)
Springer Link	Un sistema inteligente de detección de fraudes con tarjetas de pago	2021	Árboles potenciados por gradiente (GBT)	Transacciones en línea	AUC: 93,7%	Software especializado
Springer Link	Detección de fraudes en sistemas de pago móvil utilizando un marco basado en XGBoost	2022	Refuerzo de Gradiente Extremo (XGBoosT)	Pagos Móviles	Accuracy: 99,9%	1. Desequilibrio de datos 2. Software especializado (Python)
Springer Link	Un nuevo método mejorado para la lucha contra el fraude en el crédito en línea	2022	Regresión Logistica	Tarjetas de crédito	Exactitud: 97,3%	Software especializado
Springer Link	CT-GCN: un modelo de identificación de phishing para transacciones de criptomonedas blockchain	2022	Red Neuronal Convolucional de Grafos (GCN)	Plataforma descentralizada de Criptomoneda	Accuracy: 88,02%	Software especializado
Proquest	Una detección de fraude con tarjetas de crédito basada en el aprendizaje automático que utiliza el algoritmo GA para la selección de características	2022	Bosque Aleatorio (RF)	Banca Europea, transacciones de tarjetas de crédito	Accuracy: 99,98%	1. Desequilibrio de datos 2. Software especializado (Google Colab)

Scopus	Un mecanismo eficiente de detección de fraudes basado en aprendizaje automático y blockchain	2022	Bosque Aleatorio (RF)	Plataforma descentralizada de Criptomoneda	Precision: 92%	1. Desequilibrio de datos 2. Software especializado
Scopus	Detección de fraudes con tarjetas de crédito basada en CUS-RF con datos desequilibrados	2022	Bosque Aleatorio (RF)	Tarjetas de crédito	Precisión: 99,8%	Software especializado
Springer Link	Análisis de rendimiento de la optimización de hiperparámetros basada en metaheurísticas para la detección de transacciones fraudulentas	2022	Regresión Logistica	Banca Europea, transacciones de tarjetas de crédito	Accuracy: 96%	1. Software 2. Desequilibrio de datos
Springer Link	Detección de fraudes con tarjetas de crédito empleando un modelo multietapa de aprendizaje profundo	2022	Red Neuronal Convolucional (CNN)	Banca Europea, transacciones de tarjetas de crédito	Exactitud: 97,67%	Software especializado
IEEE	Modelado predictivo basado en aprendizaje automático para la detección de fraudes en la banca digital	2023	Hybrid Model: Hidden Markov Model and Gradient Boosting Classifier	Bancos que buscan mejorar la detección de fraudes mediante modelos predictivos y análisis en tiempo real.	Precisión del modelo del 96.27%, recuperación del 89.38% y F1 del 21.18%, destacando mejoras en la detección de anomalías.	. Procesar grandes volúmenes de datos en tiempo real. 2. Manejo de conjuntos desbalanceados. 3. Ajuste de hiperparámetros para optimizar el modelo híbrido.

IEEE	Utilización de sistemas biométricos para mejorar la ciberseguridad en el sector bancario: un análisis sistemático	2023	Biometric systems with AI and blockchain integration	Instituciones que buscan prevenir fraudes mediante autenticación biométrica y tecnologías avanzadas como blockchain.	Alta precisión en la detección de accesos no autorizados y fraudes en línea, mejorando la protección de datos sensibles.	1. Coste elevado de implementación. 2. Complejidad en la integración con infraestructuras existentes. 3. Resistencia a ataques sofisticados.
IEEE	Construcción y Exploración de un Modelo de Control de Riesgo Financiero Basado en Machine Learning	2023	Machine Learning Models: Logistic Regression, Decision Trees, SVM, Neural Networks	Instituciones que buscan mejorar la evaluación de riesgos y la detección de fraudes mediante aprendizaje automático.	Precisión del modelo del 94%, mejora en la capacidad de detección de fraudes y evaluación de crédito.	1. Calidad de los datos.2. Interpretabilidad de los modelos.3. Adaptación a cambios en patrones de fraude.
IEEE	Análisis comparativo de algoritmos ML para detección de fraudes en transacciones financieras	2023	Random Forest, Decision Trees, K-Nearest Neighbors (KNN), Logistic Regression, Naive Bayes	Instituciones que buscan optimizar la detección de fraudes en transacciones mediante algoritmos de aprendizaje automático.	Random Forest logró una precisión del 99% y una recuperación del 100% al detectar patrones complejos en transacciones financieras.	1. Procesamiento eficiente de grandes volúmenes de datos. 2. Optimización de hiperparámetros. 3. Adaptación a nuevas técnicas de fraude.

IEEE	Detección y comparación de fraudes financieros mediante diferentes técnicas de aprendizaje automático	2023	Random Forest, Decision Trees, K-Nearest Neighbors (KNN), Logistic Regression, Naive Bayes	Instituciones financieras que implementan técnicas de aprendizaje automático para optimizar la detección de fraudes financieros.	Random Forest logró una precisión del 96.1% y un AUC del 98.9%, destacándose como el modelo más eficiente en la detección de fraudes financieros.	1. Procesamiento de grandes volúmenes de datos. 2. Adaptación a datos desbalanceados. 3. Optimización para detección en tiempo real.
Springer Link	Un modelo antifraude semisupervisado basado en XGBoost y BiGRU integrados con red de autoatención: una aplicación para la detección de fraudes en préstamos por Internet	2023	XGBoost y BiGRU integrados con red de autoatención	Banca Digital	Aumento significativo en la precisión de detección en datos desbalanceados, identificando patrones fraudulentos con alta sensibilidad.	Requiere infraestructura avanzada, complejidad en la integración con sistemas existentes y desafíos en la recolección de datos para fraudes internos.
Springer Link	Algoritmo de optimización de la polinización de flores con clasificación basada en red de convolución temporal apilada para la detección de fraudes de anomalías financieras	2023	Flower Pollination Optimization (FPO) y Queue Convolutional Neural Network (QCNN)	Instituciones que procesan grandes volúmenes de transacciones de tarjetas, seguros y préstamos para detectar anomalías.	Precisión del 99.95%, recuperación del 77% y F1 del 86%. Supera enfoques previos en detección de fraudes financieros.	Optimización del modelo para adaptarse a patrones internos y reducir falsos positivos en conjuntos de datos heterogéneos.

Springer Link	Un conjunto de votación basado en el aprendizaje automático de la detección de fraudes con tarjetas de crédito utilizando datos altamente desequilibrados	2024	Voting Ensemble (Random Forest, Logistic Regression, KNN) con Oversampling y Undersampling	Empresas investigadas por la SEC y organismos europeos	Precisión de 99.99% en la detección de fraudes con tarjetas de crédito. Uso de técnicas de balanceo de clases (ROS y RUS) para manejar datos desbalanceados. Implementación de votación ponderada para combinar clasificadores.	Adaptación para escenarios internos requiere modificar criterios de selección de características. Requiere infraestructura computacional avanzada.
Science Direct	Un modelo de detección de fraude con tarjetas de crédito basado en la fusión de múltiples funciones y la red generativa de adversarios	2023	Fusion of multiple features with Generative Adversarial Networks (GANs)	No especificado. Aplicación generalizada para bancos y entidades de tarjetas de crédito.	Alta precisión en detección de fraude externo, mejora en la identificación de patrones complejos en datos desbalanceados.	Adaptación para fraude interno, escalabilidad en tiempo real y necesidad de equilibrar datos altamente desbalanceados.

Science Direct	Detector de fraude de transacciones financieras basado en el aprendizaje de desequilibrios y redes neuronales de grafos	2023	Financial Transaction Fraud Detector: Graph Neural Networks (GNN) integrated with imbalance learning techniques	Entidades Financieras que buscan mejorar la detección de anomalías en transacciones mediante redes neuronales gráficas y técnicas avanzadas de aprendizaje automático.	Precisión del modelo del 98.45%, F1 del 94.7%, con significativa mejora en datos desbalanceados.	Procesamiento de grandes volúmenes de datos, integración de GNN con sistemas existentes y ajuste continuo de hiperparámetros.
Science Direct	Un algoritmo de aprendizaje automático supervisado para detectar y predecir fraudes en transacciones con tarjetas de crédito	2023	Random Forest, Decision Tree, Logistic Regression	Instituciones financieras que buscan identificar y prevenir fraudes internos mediante algoritmos ML	Random Forest alcanzó una precisión del 96%, sensibilidad del 97% y especificidad del 96%.Uso de SMOTE y remuestreo para datos desbalanceados.	Procesamiento eficiente de datos en tiempo real y ajuste de hiperparámetros para escenarios específicos
IEEE	Detección de fraudes mejorada en sistemas bancarios mediante aprendizaje automático y análisis de big data con componentes clave de gestión	2024	Random Forest, SVM, Decision Trees, Deep Learning	Entidades financieras que buscan prevenir fraudes en transacciones mediante análisis predictivo y big data.	Integración de big data, optimización de modelos predictivos, sistemas de alertas tempranas	Procesar datos masivos en tiempo real y garantizar la calidad de los datos provenientes de múltiples fuentes.

IEEE	Detección de fraude financiero mediante el uso del valor en riesgo con aprendizaje automático en datos sesgados	2024	Valor en riesgo (VaR) K-Nearest Neighbor (KNN	Banco	Precisión del 91.67%, una tasa de verdaderos positivos (TP) del 95% y una puntuación F1 del 93.33%. Estos resultados destacan la capacidad del modelo para detectar fraudes en datos sesgados, manejando de forma eficiente patrones de transacciones sospechosas y minimizando falsos positivos.	Disponibilidad limitada de datos; Manejo de datos altamente sesgados y complejidad en la simulación histórica.
IEEE	Detección de fraudes en transacciones financieras basadas en IoT mediante técnicas de detección de anomalías	2024	Redes neuronales convolucionales (CNN), recurrentes (RNN), y autoencoders	Instituciones que procesan transacciones financieras habilitadas por dispositivos IoT, con énfasis en sistemas de análisis en tiempo real.	Precisión del modelo de detección mejorada, métricas de AUC y F1 superiores al 90%. Detecta actividades anómalas y transacciones no autorizadas.	Procesamiento de grandes volúmenes de datos IoT; ajuste de hiperparámetros para diferentes entornos transaccionales.
Springer Link	BiLSTM integrado en la capa de atención para la predicción de fraudes financieros	2024	Redes de aprendizaje de secuencias (BiLSTM)	Banca Europea, transacciones de tarjetas de crédito	Accuracy: 99,96%	1. Software2. Desequilibrio de datos

Springer Link	Detección de fraudes financieros mediante redes neuronales de grafos cuánticos	2024	Redes Neuronales de Grafos Cuánticos (QGNNs), Circuitos Cuánticos Variacionales (VQC), Topological Data Analysis (TDA).	Banca Europea	Precisión del 94.5% y AUC de 0.85. Sobresale frente a modelos clásicos en la detección de transacciones anómalas en datos reales.	Costo computacional y limitaciones actuales en la tecnología cuántica.
Springer Link	Autocodificador apilado optimizado con hiperparámetros para la detección de fraudes con tarjetas de crédito	2024	L-PSO-SAE (Stacked Autoencoder + L-PSO)	Institución con grandes volúmenes de transacciones electrónicas con tarjetas de crédito	Precisión: 96.3%, AUC: 97.8%, Sensibilidad: alta	Manejo de datos desbalanceados y optimización de hiperparámetros
Springer Link	Detección de fraudes con tarjetas de crédito mediante la hibridación del bosque de aislamiento con el algoritmo optimizador Grey Wolf	2024	IF-GWO (Isolation Forest + Grey Wolf Optimizer)	Institución que gestiona grandes volúmenes de transacciones electrónicas con tarjetas de crédito	Precisión: 93.52%, AUC: 94.17%, G-mean: 94.10%. Reducción significativa de falsos positivos y negativos.	Manejo de datos desbalanceados y optimización de parámetros para grandes conjuntos de datos complejos.
Scopus	Un enfoque inteligente para detectar y predecir transacciones de fraude en línea utilizando el algoritmo XGBoost	2024	Algoritmo XGBoost	Institución financiera enfocada en optimizar la detección de fraudes en transacciones en línea.	Precisión del modelo: 98.12%. Capacidad de detección alta en datos desbalanceados.	Ajuste de hiperparámetros y manejo de conjuntos de datos con ruido.

Scopus	Modelo de detección de fraude bancario en línea en tiempo real mediante fusión de aprendizaje no supervisado	2024	Sistema de aprendizaje no supervisado basado en fusión (K-Means + DBSCAN + Redes neuronales autoasociativas)	Institución que gestiona grandes volúmenes de transacciones bancarias en línea	Precisión del 95%, reducción significativa de falsos positivos	Gestión de big data y ajuste de parámetros
Scopus	Mejora de la detección de fraudes en las transacciones con tarjeta de crédito mediante un modelo de aprendizaje federado optimizado	2024	Aprendizaje supervisado basado en algoritmos metaheurísticos. (COA)	Transacciones con tarjetas de crédito	Exactitud: 96,85%	Software y hardware especializado Privacidad de los datos
Scopus	Detección de fraude corporativo basada en vectores de legibilidad lingüística: aplicación a empresas financieras en China	2023	Naive Bayes, Random Forest, SVM + Word2Vec	Compañías que cotizan en las bolsas de Shanghái y Shenzhen. Estas empresas pertenecen al sector financiero bajo la clasificación de la Comisión Reguladora de Valores de China.	Mejora de 31.17% en precisión para SVM; F1-score y AUC también mejorados significativamente.	Gestión de grandes volúmenes de texto; reducción de la pérdida semántica durante la vectorización de datos.

Science Direct	Avances en la detección de fraudes financieros: redes adversarias generadoras de autoatención para una identificación precisa y eficaz	2024	Redes Generativas Adversarias (SAGAN)	Transacciones con tarjetas de crédito	Precisión: 82%	Entrenamiento del modelo
Science Direct	Red neuronal de grafos codificador-decodificador para la detección de fraudes con tarjetas de crédito	2024	Red neuronal gráfica codificadora y decodificadora	Institución que gestiona operaciones con tarjetas de crédito	Precisión: 97.4%. Reducción significativa de falsos positivos y tiempos de procesamiento optimizados	Complejidad computacional y necesidad de ajustar hiperparámetros debido a patrones dinámicos.
Science Direct	Datos desequilibrados de detección de fraudes con tarjetas de crédito: una solución basada en una red neuronal híbrida y una técnica de submuestreo basada en clústeres	2024	HNN-CUHIT (Red Neuronal Híbrida + Submuestreo Basado en Agrupamiento)	Institución financiera que gestiona transacciones con tarjetas de crédito	F1-Score: 0.0572, Precisión mejorada respecto a CNN	Optimización de parámetros y gestión de grandes volúmenes de datos.
Science Direct	Detección de fraudes con tarjetas de crédito basada en deep learning en el aprendizaje federado	2024	JNBO-Spinal Net	Transacciones en línea con tarjeta de crédito	Accuracy: 89,10%	Software especializado (MATLAB)
Taylor & Francis	Detección automática de fraudes con tarjetas basada en el algoritmo del árbol de decisión	2024	Árboles de deciisión	Validación de 2 conjuntos de datos de transacciones con tarjetas de creédito	Accuracy Primer conjunto: 96% Segundo conjunto: 99%	Software especializado (Python)

Springer Link	Una detección inteligente de actividades fraudulentas de tarjetas de crédito mediante un algoritmo híbrido de aprendizaje profundo	2024	Sistema de Inferencia neuro borroso adaptativo (ANFIS) GWO+FW	Se validaron 3 conjuntos de datos: prestamos fraudulentos, tarjteas de crédito y fraude de seguros	Accuracy Prestamos: 99,87% Accuracy T. Crédito: 99,96% Accuracy Fraude seguros: 99,85%	1. Desequilibrio de datos 2. Software especializado
Science Direct	Detección de fraudes con tarjetas de crédito basada en el aprendizaje de grafos federados	2024	Red Neuronal de Grafos (GNN)	Se realizaó el análisis sobre 2 conjunto de datos de transacciones en línea con tarjetas de crédito	Accuracy: 95,99% (primer conjunto de datos) 81,60% (segundo conjunto de datos)	1. Desequilibrio de datos 2. Software especializado