Optimización de la detección de fraude en el sector financiero a través del análisis de datos y Business Intelligence

Luisa Fernanda Ramírez Pinzón

Asesor

Edgar Andrés Villabón Aldana

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Ciencia de Datos y Analítica

2024

Dedicatoria

Quiero dedicar este logro, en primer lugar, a Dios, quien ha hecho posible que llegue a este momento tan importante en mi vida. A mi madre, por ser mi mayor fuente de inspiración y el ejemplo que me guía cada día. A Carlitos, por estar siempre a mi lado, brindándome apoyo y orientándome en cada decisión que tomo. A mi padre, por ser un modelo de vida, con sus sabios consejos y su perseverancia diaria.

También dedico este triunfo a mis hermanas, Isabella y Paula, por su apoyo incondicional durante todo este proceso, siempre dispuestas a compartir sus conocimientos y su tiempo cada semestre. A mi esposo, Andrés Guerra, por estar a mi lado en cada paso, por su presencia en cada obstáculo y logro, y por impulsarme constantemente a perseguir mis sueños y alcanzar mis metas.

Agradecimientos

En primer lugar, agradezco a Dios por cada paso que he dado en mi vida, por guiarme en todas las decisiones que he tomado y por darme la motivación y fortaleza necesarias para llevar a cabo esta especialización y trabajo de grado, que será un pilar importante para mi futuro.

También quiero expresar mi gratitud a mis padres, Myriam Pinzón, Carlos Ramírez y Carlos Salgado, por haberme apoyado a lo largo de todo el proceso de elaboración de este proyecto de vida, y por siempre estar dispuestos a ayudarme a alcanzar lo que deseo. Ellos son mi mayor fuente de inspiración y los que me brindan la fuerza para cumplir todas mis metas.

Agradezco profundamente a mis hermanas, Paula Ramírez e Isabella Salgado, por su infinita paciencia y apoyo en la creación de este proyecto. Cada una de sus enseñanzas y colaboraciones fue esencial para el éxito de este proceso tan significativo.

A mi tutor, Edgar Andrés Villabón, quien estuvo siempre pendiente del desarrollo de esta monografía, ofreciendo su ayuda incondicional y acompañándome en cada etapa. Su disposición para compartir su conocimiento fue invaluable y siempre me apoyó sin reservas.

Extiendo también mi agradecimiento a la Universidad Nacional Abierta y a Distancia, por todos los aprendizajes y experiencias a lo largo de la Especialización, así como a cada uno de los profesores que contribuyeron a mi formación profesional y a lo que soy hoy.

Resumen

El sector financiero enfrenta grandes desafíos en la detección y prevención del fraude debido a la creciente sofisticación de las tácticas fraudulentas, impulsadas por avances tecnológicos. El aumento de transacciones electrónicas ha permitido a los delincuentes encontrar nuevas formas de robar información, afectando tanto a usuarios como a entidades financieras.

En respuesta, el análisis de datos y la Inteligencia de Negocios emergen como herramientas clave para enfrentar este reto. Estas metodologías permiten identificar transacciones inusuales y patrones sospechosos mediante el análisis de anomalías, así como desarrollar modelos predictivos basados en datos históricos para prever comportamientos fraudulentos. Además, la segmentación de datos ayuda a detectar áreas de riesgo específicas, y la visualización de datos facilita la identificación de tendencias que podrían indicar fraude.

No obstante, para que estas herramientas sean efectivas, es esencial comprender mejor cómo utilizarlas. Aunque su potencial es reconocido, la falta de conocimiento sobre su aplicación limita la capacidad de las instituciones financieras para proteger sus activos y garantizar la seguridad de sus clientes. Por lo tanto, es crucial investigar cómo estas técnicas pueden optimizar la detección de fraude y fortalecer la confianza en el sector financiero.

Palabras claves: Fraude, Sector Financiero, Business Intelligence, Análisis de Datos

Abstract

The financial sector faces significant challenges in detecting and preventing fraud due to the increasing sophistication of fraudulent tactics, driven by technological advancements. The rise of electronic transactions has enabled criminals to find new ways to steal information, affecting both users and financial institutions.

In response, data analysis and Business Intelligence have emerged as key tools to address this challenge. These methodologies allow for the identification of unusual transactions and suspicious patterns through anomaly detection, as well as the development of predictive models based on historical data to anticipate fraudulent behavior. Additionally, data segmentation helps detect specific risk areas, and data visualization facilitates the identification of trends that may indicate fraud.

However, for these tools to be effective, it is essential to better understand how to use them. Although their potential is recognized, the lack of knowledge regarding their application limits the ability of financial institutions to protect their assets and ensure the security of their customers. Therefore, it is crucial to research how these techniques can optimize fraud detection and strengthen confidence in the financial sector.

Keywords: Fraud, Financial Sector, Business Intelligence, Data Analysis

Tabla de Contenido

Introducción 8

Planteamiento del Problema 10

Justificación 13

Objetivos 15

Objetivo General 15

Objetivos Específicos 15

Marco Conceptual y Teórico 16

Tendencias y Tipos de Fraude Financiero 22

Aplicaciones del Análisis de Datos e Inteligencia de Negocios en la Detección y Prevención de Fraude Financiero 28

Bosquejar un Conjunto de Estrategias a partir de la Inteligencia de Negocios y el Análisis de Datos para la Detección y Prevención del Fraude Financiero en Colombia 34

Conclusiones 39

Recomendaciones 41

Referencias Bibliográficas 42

Lista de Figuras

Figura 1 *Tipos de Fraude Financiero* 17

Figura 2 *Distribución de Fraudes por Modalidad: Digitales vs. Físicos* 18

Figura 3 *Cantidad Denuncias Delitos Informáticos* 19

Figura 4 *Fraude por Medios Electrónicos* 20

Figura 5 *Datos de Lavado de Activos en Estados Unidos* 26

Figura 6 *Modelos PaySim y Banksim* 32

Figura 7 *Puntuaciones modelos PaySim y Banksim* 33

Figura 8 *Fraudes Digitales* 34

Figura 9 *Desafíos para la Detección del Fraude Financiero* 35

Introducción

El sector financiero ha experimentado transformaciones significativas en las últimas décadas debido al avance de las tecnologías digitales. Sin embargo, estos avances han traído consigo nuevos retos, particularmente en la detección y prevención del fraude. A medida que las transacciones electrónicas se incrementan y los sistemas financieros adoptan tecnologías más complejas, los delincuentes han encontrado formas innovadoras de explotar vulnerabilidades y cometer fraudes que afectan tanto a los usuarios como a las instituciones financieras.

La sofisticación de las tácticas fraudulentas ha superado las capacidades de los métodos tradicionales de prevención, lo que ha llevado a un reconocimiento creciente de la necesidad de implementar tecnologías más avanzadas. En este escenario, el análisis de datos e Inteligencia de Negocios (BI) se presentan como herramientas clave para abordar este desafío. Estas tecnologías permiten procesar grandes volúmenes de información en tiempo real, identificar patrones anómalos y desarrollar modelos predictivos que prevén comportamientos fraudulentos antes de que ocurran.

No obstante, el potencial de estas herramientas depende en gran medida de cómo se utilicen. Aunque su valor ha sido ampliamente reconocido, la falta de conocimiento sobre su implementación limita la capacidad de las instituciones financieras para proteger sus activos y garantizar la seguridad de sus clientes. Por ello, es crucial investigar cómo el análisis de datos y el BI pueden optimizar la detección del fraude financiero, mejorando la eficiencia de las estrategias de prevención y fortaleciendo la confianza en el sector financiero.

Esta monografía tiene como objetivo explorar las aplicaciones de estas herramientas tecnológicas en la detección y prevención del fraude en el sector financiero colombiano, proponiendo estrategias basadas en el análisis de datos históricos, la identificación de patrones

fraudulentos y la implementación de modelos predictivos adaptados a las necesidades del entorno financiero local.

Planteamiento del Problema

El sector financiero es uno de los que enfrenta mayores desafíos frente al fraude, una problemática intensificada por los avances tecnológicos y las formas en que los usuarios realizan sus transacciones diarias. En este contexto, el desarrollo de portales virtuales y herramientas digitales ha facilitado a los clientes el acceso a servicios financieros, como cuentas bancarias y tarjetas de crédito, pero también ha dado lugar a nuevas modalidades de fraude, cada vez más sofisticadas y diversificadas, esto último como lo menciona (Torres Gallón, 2022).

Estos incrementos, también se han generado debido al aumento de las transacciones electrónicas, ya que las personas prefieren generar sus pagos y realizar todo tipo de transacciones a través de los medios electrónicos y no de medios tradicionales, esto es afirmado a su vez por (Torres Gallón, 2022)"…este aumento de las transacciones electrónicas no solo representa riesgos que afecten a las entidades bancarias sino también a los usuarios debido a la pérdida de información y violación de políticas de seguridad que conlleva a la pérdida de ingresos, y esto a su vez afecta la confianza" (p. 14).

Por otra parte, se puede reconocer que los métodos tradicionales, mediante los cuales se pretende seguir combatiendo el fraude financiero, ya no son suficientes, por tanto, se deben buscar otras opciones, como el BI que, a través de grandes volúmenes de data, pueden verificar nuevas metodologías de fraude. Según (Singh , Singh, Gahlawat , & Prabha, 2023) , las tecnologías emergentes, como las herramientas de Big Data, son fundamentales para gestionar los riesgos financieros asociados con las transacciones bancarias.

Estas tecnologías permiten a las instituciones actualizar sus enfoques obsoletos y desarrollar soluciones innovadoras que respondan a las exigencias del entorno financiero actual,

marcando una diferencia significativa en la manera en que se enfrentan los desafíos tecnológicos del sector.

Por su parte, el análisis de datos y las herramientas de BI han nacido como tecnologías promisorias para abordar este desafío al que las entidades financieras y usuarios nos vemos enfrentados y así, tomar decisiones estratégicas, tal y como lo menciona (Arguello Montes, 2017)"…el Business Intelligence permite desarrollar decisiones eficaces a los diferentes departamentos de las empresas con cierta facilidad; permite transformar grandes cantidades de datos en información útil para la toma de las decisiones estratégicas de las empresas" (p. 32).

Mediante estas nuevas herramientas se pueden realizar algoritmos de aprendizaje automático y análisis predictivo, que puedan prever el fraude antes de que ocurra, identificando patrones y comportamientos sospechosos en tiempo real. A su vez, tienen la capacidad de procesar grandes volúmenes de datos en tiempo real permitiendo una detección más rápida y eficiente del fraude, lo que reduce el riesgo de pérdidas significativas. Por otra parte, se considera relevante la aplicación de técnicas de segmentación de clientes, la cual permite adaptar los modelos de detección de fraude a las características individuales de cada cliente, mejorando así la precisión y reduciendo los falsos positivos.

Sin embargo, a pesar de que ya existen técnicas avanzadas y modelos específicos aplicados en la detección de fraude en el sector financiero, su implementación efectiva aún presenta desafíos significativos. Por lo tanto, surge la pregunta:

¿Cómo pueden las técnicas avanzadas de análisis de datos y la Inteligencia de Negocios ser utilizadas de manera efectiva para optimizar la detección de fraude en el sector financiero? Este planteamiento del problema guiará la investigación hacia la identificación de estrategias y

técnicas que permitan a las instituciones financieras mejorar sus sistemas de detección de fraude, protegiendo así los activos financieros y la confianza del cliente en el sector

Justificación

La presente investigación se enfoca en la optimización de la detección de fraude en el sector financiero a través del análisis de datos e inteligencia de negocios, dada su creciente relevancia en el contexto actual. Este fenómeno no solo amenaza la integridad financiera y reputacional de las instituciones en Colombia, sino que también impacta negativamente la confianza en varios sectores económicos, desestabilizando economías y afectando el costo de vida de las personas, independientemente de su estrato socioeconómico (Lozano Prada & Huertas Meneses, 2023). Además, según (Hernández Botero, 2020) las entidades financieras enfrentan riesgos operativos, legales y reputacionales como consecuencia de la materialización de fraudes, lo que subraya la necesidad de estrategias efectivas para mitigar estos impactos.

Este problema, ha ido generando un incremento en los tipos de fraude perpetrados por los ladrones, (Torres Ontibón, 2022), indica que los avances tecnológicos, los cuales inicialmente buscaban facilitar la realización de cualquier tipo de transacciones a los usuarios, también originaron nuevos tipos de fraudes por medio de estos sistemas electrónicos y el phishing, malware o spyware. Por su parte, (Álvarez Sánchez & Mejía Zapata, 2021) reafirman dicha teoría, mencionando que: "…el fraude electrónico es un delito cuya proporción ha ido aumentando en los últimos años, a pesar de los avances e implementaciones tecnológicas para mitigarlo. Además, este tiene diferentes modalidades, por ello es importante conocer su clasificación y cuáles son las diferentes formas utilizadas para cometer el fraude" (p.5).

Teniendo en cuenta lo anterior, se considera necesario para este trabajo de investigación, mejorar los métodos de detección de fraude, ya que los tipos de fraude van evolucionando y, por tanto, las soluciones no pueden ser estáticas y la detección temprana, permiten a las entidades actuar anticipadamente, (Castiblanco Castro, 2020) menciona: "La detección temprana de los

fraudes puede presentarse implementando una estrategia de prevención, detección y monitoreo llegando a tener un efecto beneficioso para la organización, evitando y mitigando el riesgo reputacional, legal, económico" (p.27).

El análisis de datos y las herramientas de BI brindan un enfoque avanzado y efectivo para detectar fraudes, ya que permiten a través de grandes volúmenes de datos identificar patrones o tendencias en las actividades fraudulentas ocasionadas en el Sistema Financiero, generando así beneficios para las entidades como la reducción de pérdidas económicas, el progreso de la reputación del sector y por ende, el incremento en la confianza de los clientes, tal y como se reconoce por (Chen, Chiang, & Storey, 2012), p.1165), la Inteligencia de Negocios, ha tomado una gran relevancia para la resolución de problemas que pueden ser identificados a través de la data en las organizaciones empresariales.

Por su parte, el Big Data ha cobrado una importancia crucial en la detección y análisis del fraude, así como en la gestión de riesgos a los que se enfrentan las entidades financieras. Esta tecnología tiene el potencial de transformar significativamente el sector, mejorando la capacidad predictiva de los modelos de riesgo, optimizando los tiempos de respuesta y aumentando la eficiencia de los sistemas. Además, permite una cobertura más integral de los riesgos y contribuye a reducir costos operativos de manera sustancial (Singh , Singh, Gahlawat , & Prabha, 2023).

Objetivos

Objetivo General

Proponer estrategias para mejorar la detección y prevención del fraude en el sector financiero mediante el análisis de datos y la Inteligencia de Negocios.

Objetivos Específicos

Identificar las tendencias y tipos de fraudes financieros a través de referentes bibliográfico y datos históricos.

Evaluar las aplicaciones del análisis de datos e Inteligencia de Negocios en la detección y prevención de fraude financiero.

Bosquejar un conjunto de estrategias a partir de la Inteligencia de Negocios y el análisis de datos para la detección y prevención del fraude financiero en Colombia.

Marco Conceptual y Teórico

La comprensión y la identificación de las diversas técnicas y tipos de fraude que pueden ocurrir en el sector financiero son de gran importancia para desarrollar estrategias efectivas de detección y prevención. Cada tipo de fraude puede tener características únicas que requieren enfoques específicos para su detección. Al analizar estas técnicas y tipos de fraude, es posible identificar patrones y tendencias que pueden mejorar los sistemas de detección.

Teniendo en cuenta lo anterior, es importante iniciar definiendo el fraude, de acuerdo con el Diccionario de Derecho de Merriam Webster (1996), citado en (Abdullahi, Mansor, & Shahir Nuhu, 2015) el fraude puede definirse como: "Cualquier acto, expresión, omisión u ocultación calculado para engañar a otro en su perjuicio, específicamente, una falsificación u ocultación con referencia a algún hecho material para una transacción que se realiza con conocimiento de su falsedad y/o con total desprecio por su veracidad o falsedad y con la intención de engañar a otro y que es razonablemente confiado por el otro que resulta perjudicado por ello" (p.31).

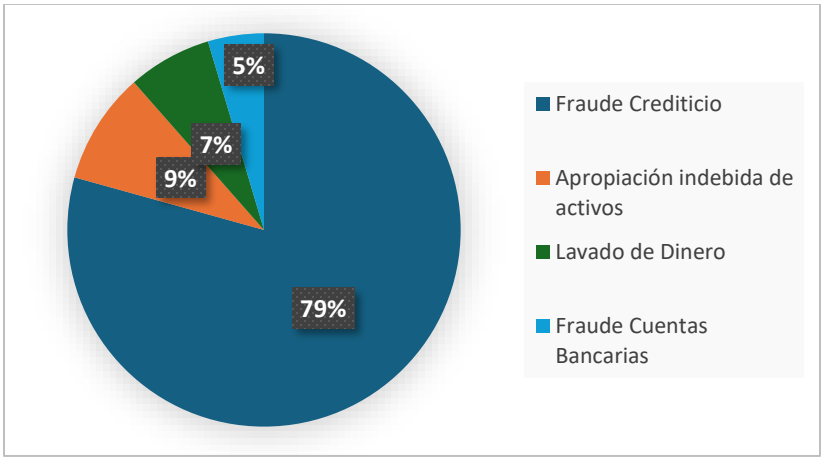
Por otra parte, y debido a que los fraudes han cobrado gran relevancia en las pérdidas económicas de las entidades financieras y que a razón de esto se han venido desarrollando sistemas y estrategias para la identificación y la prevención del fraude financiero, se reconoce que: “el aprendizaje automático tiene un gran potencial como medio para identificar y evitar actividades fraudulentas. Puede ayudar a las empresas a ofrecer un entorno más seguro para sus clientes, y a los clientes a mantenerse abiertos a los avances tecnológicos del sector financiero como resultado. Implementar la detección de fraudes con aprendizaje automático puede ser fácil y eficiente con modelos de datos bien diseñados y reglas comerciales consistentes”. (Dalal, Seth, Radulescu, Secara, & Tolea, 2022).

Es importante destacar que los métodos de aprendizaje automático desempeñan un papel fundamental en la identificación de fraudes en la actualidad. Según (Adewumi & Akinyelu, 2016), la mayoría de las técnicas utilizadas para la detección de fraudes con tarjetas de crédito están basadas en enfoques de aprendizaje supervisado, aunque también existen algunas que emplean aprendizaje semi-supervisado.

Sin embargo, y con el fin de poder realizar dichos modelos de aprendizaje automático se requieren identificar ciertos elementos a través de la investigación que permitan un buen desarrollo de los modelos de tipificación de fraudes, como se menciona en la siguiente figura1:

Figura 1

Tipos de Fraude Financiero



Nota. Tomada de (Sanusi, Firdaus, & Mat Isa, 2015)

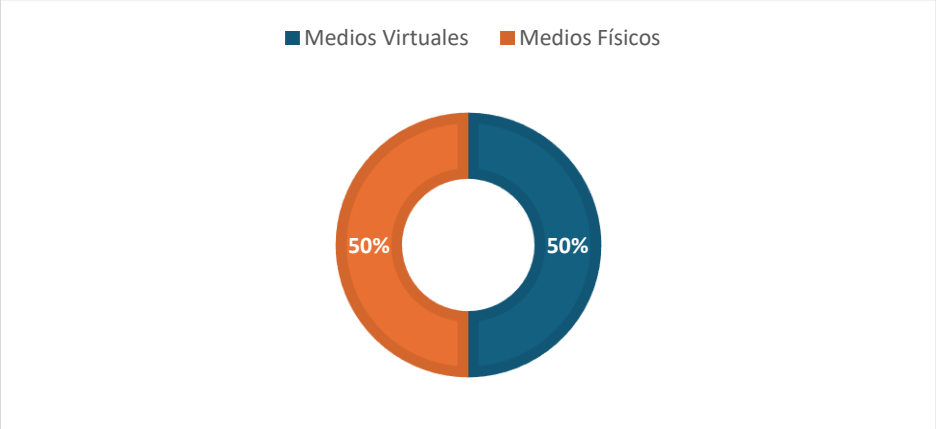
Al considerar estas definiciones y hallazgos, se destaca la importancia de comprender y estar al tanto de las diversas formas en que el fraude puede manifestarse en el sector financiero para poder implementar estrategias efectivas de detección y prevención.

Otro de los temas relevantes para tener en cuenta para el análisis de datos son los medios por los cuales se realizan los fraudes financieros, ya que, debido al aumento de las transacciones

digitales, es importante distinguir entre los medios digitales y físicos a través de los cuales se realizan las transacciones. Los fraudes pueden ocurrir tanto en el ámbito y medios digitales como en los físicos, y cada medio puede presentar diferentes desafíos y riesgos. Por ejemplo, el fraude digital puede incluir phishing, malware o ataques de ingeniería social, mientras que el fraude físico puede involucrar robo o clonación de tarjetas, así como aspectos relacionados con cheques. Al analizar los diferentes medios, se pueden implementar medidas de seguridad adecuadas para cada uno y mejorar la detección de fraude en ambos entornos:

Figura 2

Distribución de Fraudes por Modalidad: Digitales vs. Físicos



Nota. Tomada de (Lozano Prada & Huertas Meneses, 2023)(p.32)

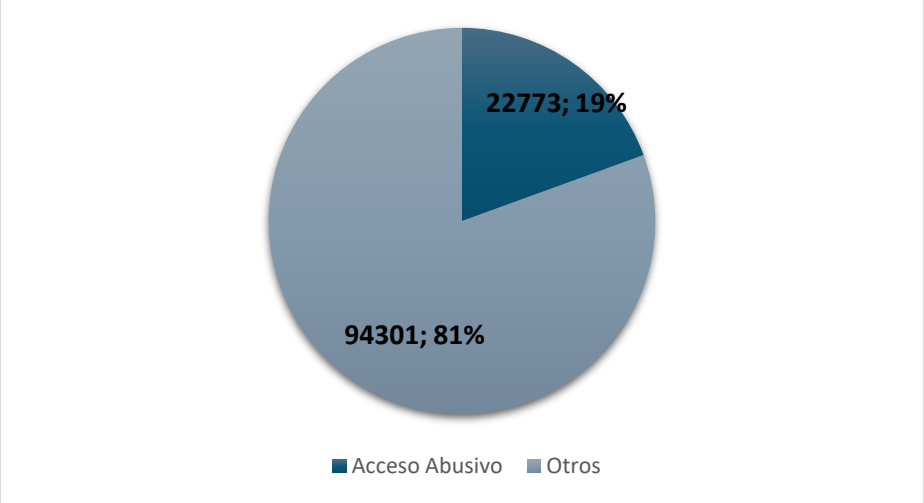
Según lo indicado previamente el 50% de los fraudes se realiza por medios digitales y el otro 50% por medios físicos, sin embargo, por su parte Asobancaria (2022) manifiesta que: "Con el aumento de la bancarización digital se vienen retos grandes para el sector financiero alrededor del mundo. Dos desafíos aparentemente en contradicción se nos aparecen al frente: ¿cómo generar entre los usuarios del sistema financiero una confianza en que la banca digital llegó para quedarse y al mismo tiempo crear en ellos una cultura de prácticas digitales sanas de autocuidado

para reducir su exposición al fraude? Alertar sobre los riesgos de los fraudes digitales podría ahuyentar a los usuarios del sistema financiero a hacer un mayor uso de los medios electrónicos para manejar sus productos financieros."(p.4).

Lo que ayudaría a confirmar que el fraude digital va en aumento debido a que la gran mayoría de las transacciones bancarias se pueden realizar por medios digitales, dándole entrada a los delincuentes para buscar formas y métodos para realizar fraude a través de estos medios. Esta afirmación se ve respaldada por (Asobancaria, 2023), en su documento de Política Pública para reducir el hackeo informa sobre unos datos relevantes relacionados con el fraude digital, en el cual mencionan los siguientes datos:

Figura 3

Cantidad Denuncias Delitos Informáticos



Nota. Tomada de (Asobancaria, 2023) (p.4)

Otro dato relevante para la investigación y teniendo en cuenta cifras importantes relacionadas con los tipos de fraude se encuentra lo mencionado por (Vélez Medina & Ortíz

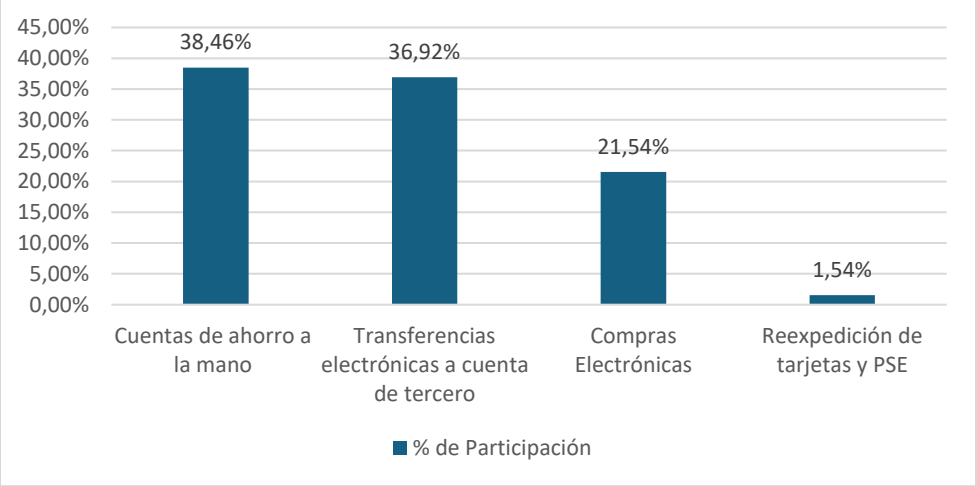
Morales, 2020) los cuales mencionan que: "…en Colombia se genera un promedio de ataques informáticos diarios, de los cuales 39,56% los sufre el sector financiero." (s.p).

Por otra parte, y debido a la importancia de conocer las transacciones mediante las cuales se realiza un gran volumen de fraudes ya sean digitales o electrónico, ya que se considera que las transacciones financieras son el punto de entrada para muchas actividades fraudulentas. El análisis de las transacciones puede dar a conocer los comportamientos sospechosos, así como los patrones inusuales de gasto, transferencias inesperadas o transacciones no autorizadas. Al monitorear y analizar las transacciones, las entidades financieras pueden identificar anomalías y, por tanto, tomar medidas rápidas para mitigar el riesgo de fraude.

En cuanto a los medios electrónicos más frecuentes, se encuentra:

Figura 4

Fraude por Medios Electrónicos



Nota. Tomada de Álvarez y Mejía, citado en (Torres Gallón, 2022) (p. 12).

Otro aspecto relevante para la identificación de los tipos de fraude es el uso de Big Data, ya que permite obtener información clave para la detección de riesgos. Según (Wang, 2021), la

investigación crediticia basada en Big Data enfrenta diversos riesgos, como los legales, de gestión y de seguridad en red. Para mitigar estos riesgos, se sugieren medidas de prevención en tres áreas principales: mejorar la estructura de gobernanza y el control interno, fortalecer la autorregulación de la industria y reforzar la supervisión del sector.

Mediante este tipo de metodologías se identifican aspectos notables que permiten reconocer formas y estrategias de identificación del fraude, lo que sirve para mitigar estos aspectos, por su parte (González Díaz & Olaya Alfonzo, 2021): "Uno de los hallazgos más importante en la prevención y control del fraude es el manejo de esquemas de transacciones en línea y tiempo real, este mecanismo brinda la oportunidad de reacción oportuna, antes de la autorización bancaria, protegiendo al comercio y consumidor de sufrir un fraude con pérdidas financieras."(p. 24).

Estas metodologías y tecnologías avanzadas permiten identificar y comprender mejor las estrategias utilizadas en actividades fraudulentas, proporcionando herramientas clave para su mitigación. Así, el manejo en tiempo real y el análisis de transacciones en línea se perfilan como elementos esenciales, permitiendo una reacción oportuna ante intentos de fraude. En conjunto, estos hallazgos subrayan la importancia de adoptar enfoques tecnológicos robustos que fortalezcan la protección tanto de los consumidores como del sector financiero frente a los riesgos de fraude.

Tendencias y Tipos de Fraude Financiero

Comprender las amenazas actuales que enfrenta el sector financiero requiere un análisis detallado de las tendencias y tipos de fraudes financieros a lo largo del tiempo. A través de la revisión de la literatura y el análisis de datos históricos, es posible identificar patrones recurrentes y nuevas formas de fraude que han surgido debido a los avances tecnológicos. Los fraudes han evolucionado, pasando de modalidades tradicionales como el uso indebido de tarjetas, a esquemas más complejos como el lavado de dinero y las estafas en línea, lo que subraya la necesidad de desarrollar estrategias actualizadas para su detección y prevención.

Es importante iniciar definiendo qué es el fraude. De acuerdo con lo descrito “es un conjunto de acciones que se llevan a cabo por ambición y corrupción, donde se manejan los recursos tecnológicos y aplicaciones para generar el robo de datos de usuarios, mediante engaños a través medios telefónicos, correos electrónicos, mensajes de texto entre otros dejando ver vulnerables al sector financiero y sin poder ser evitado ni castigado generando desconfianza en el ámbito económico” (Torres, 2022, como se citó en (Lozano Prada & Huertas Meneses, 2023).

Con la definición mencionada previamente, se considera fundamental empezar a clasificar y definir los distintos tipos de fraude que afectan al sector financiero, ya que cada modalidad presenta características únicas y métodos de operación. Entre los fraudes más comunes se encuentran:

Fraude con tarjetas de crédito: Este es uno de los fraudes más comunes y es por el cual los estafadores usan sin autorización los datos de tarjetas de crédito para realizar compras o transacciones, dentro de este tipo de fraude se puede incluir la clonación de tarjetas o el uso de información robada a través de técnicas como el phishing. Tal y como lo menciona (Álvarez Sánchez & Mejía Zapata, 2021), el phishing es una técnica de fraude común que implica el robo

de información bancaria mediante enlaces falsos enviados a través de mensajes o correos electrónicos. Esto permite que los estafadores obtengan datos como usuarios, contraseñas y números de tarjetas de crédito. Así mismo, estos autores definen el phishing como una suplantación de identidad para obtener información confidencial a través de sitios web falsos.

Esta situación resalta la necesidad urgente de aumentar la concienciación entre los usuarios sobre la seguridad en línea y la importancia de implementar medidas robustas de protección, tanto a nivel personal como por parte de las entidades financieras, para mitigar los riesgos asociados con este tipo de fraude.

Solo a través de una mayor educación y vigilancia se podrá reducir el impacto de estos delitos y proteger los recursos de los usuarios y de las entidades financieras, ya que en muchas ocasiones la entidad financiera debe responder a su cliente con el valor de estás compras fraudulentas.

Fraude en línea o fraude electrónico: En el sector financiero, este tipo de fraude se muestra a través del robo de credenciales bancarias o de tarjetas de crédito mediante sitios web fraudulentos, phishing, o malware. Además, involucra transacciones no autorizadas y suplantación de identidad, donde los delincuentes realizan compras o transferencias sin el conocimiento del propietario legítimo. El crecimiento del comercio electrónico ha facilitado este tipo de fraudes, aprovechando la falta de medidas de seguridad por parte de los usuarios y, en ocasiones, de las instituciones.

De acuerdo con lo mencionado por (Álvarez Sánchez & Mejía Zapata, 2021), existen diferentes tipos de fraude electrónico dentro de los cuales se encuentran el malware, keyloggers, spyware, spam y el hacking.

Malware: Este tipo de fraude se refiere a cualquier programa o código creado para dañar un sistema o hacer que funcione mal. Aunque existan muchas medidas de protección, los estafadores siguen creando malware más avanzado para evadirlas. Esto significa que las amenazas continuarán creciendo, no solo a través de computadores, sino también en dispositivos móviles.

Keyloggers: Son pequeños programas que registran todo lo que una persona escribe en un computador. Los datos capturados, como contraseñas o mensajes, pueden guardarse en el mismo equipo o enviarse a otro controlado por el atacante.

Spyware: Es un fraude que también se conoce como el software espía, este tipo de programa se instala en el dispositivo de cualquier sin conocimiento de la misma. El objetivo principal se basa en el monitoreo de lo que la persona realiza en su computador y posteriormente, envía dicha información al atacante.

Spam: Es el envío de correos no deseados a personas sin su consentimiento. Normalmente, estos correos pueden ser maliciosos y los delincuentes se hacen pasar por instituciones financieras para obtener información personal o los datos de acceso a cuentas.

Hacking: El hacking malicioso, o cracking, es uno de los delitos informáticos más antiguos. Consiste en acceder ilegalmente a sistemas para robar datos confidenciales, causando daños financieros o de reputación a las víctimas.

Sin embargo, (Álvarez Sánchez & Mejía Zapata, 2021), también hablan de otro tipo de fraudes electrónicos como lo son:

Smishing, según Kang et al (2013) citado en (Álvarez Sánchez & Mejía Zapata, 2021) describe el smishing como una forma de phishing que utiliza mensajes de texto para distribuir

malware o engañar a las personas para que compartan información personal y financiera, ya sea a través de enlaces fraudulentos o mediante premios falsos.

Pharming, esta modalidad consiste en llevar al usuario a una página que no es la original, se da cuando al digitarla en el navegador, la IP se convierte en numérica logrando el robo de la información confidencial y posteriormente de los recursos monetarios (Brody, et al., 2007, como se cita en (Álvarez Sánchez & Mejía Zapata, 2021).

Finalmente, el vishing según Yeboah y Mateko (2014) citado en (Álvarez Sánchez & Mejía Zapata, 2021), consiste en que el criminal llama a un usuario haciéndose pasar por un empleado del banco para solicitarle información personal y financiera.

Lo anterior demuestra que el fraude en línea o electrónico ha evolucionado a la par que el crecimiento de las tecnologías digitales y el comercio electrónico, generando una diversidad de métodos utilizados por los delincuentes para acceder a información confidencial y recursos financieros. A medida que los fraudes tradicionales como el phishing y el malware se han vuelto más sofisticados, nuevas amenazas como el smishing, pharming y vishing han surgido, utilizando tácticas engañosas para aprovecharse de las vulnerabilidades tecnológicas y humanas. Esta creciente variedad de fraudes refleja la capacidad de los delincuentes de adaptarse a las nuevas tecnologías y la necesidad constante de reforzar las medidas de seguridad tanto para las instituciones financieras como para los usuarios. En este sentido, es crucial implementar estrategias de detección proactiva y educar a los usuarios sobre los riesgos, con el fin de mitigar los impactos de estos fraudes en el sector financiero.

Lavado de dinero: Este tipo de fraude financiero busca encubrir el origen ilícito de fondos mediante un proceso de "blanqueo" a través de complejas redes de transacciones. Las instituciones financieras pueden verse involucradas, directa o indirectamente, en estos esquemas

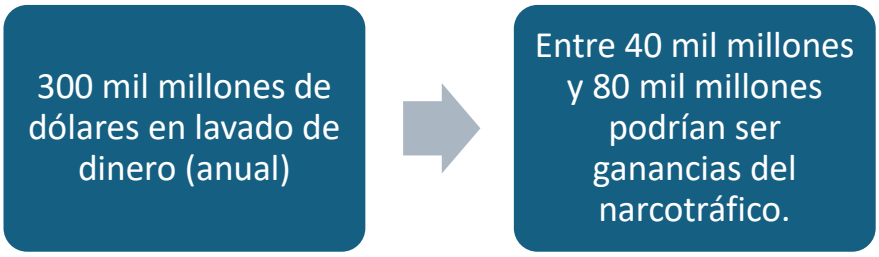
cuando no implementan controles adecuados para rastrear y verificar la legitimidad de los fondos. Esto puede incluir transferencias internacionales, empresas pantalla o cuentas bancarias en paraísos fiscales, todas diseñadas para ocultar el rastro del dinero ilícito.

Tal y como lo mencionan (Bolton & Hand, 2002): El lavado de dinero es el proceso de ocultar el origen, la propiedad o el uso de fondos, generalmente en efectivo, que son ganancias de actividades ilícitas.

Así mismo, la Figura 5 muestra la información sobre el lavado de activos a través de cifras alarmantes de aquella época donde en Estados Unidos el lavado de dinero en un año se reconocían las siguientes cifras:

Figura 5

Datos de Lavado de Activos en Estados Unidos



Nota. Tomada de (Bolton & Hand, 2002)

Las cifras mencionadas en la Figura 5 reflejan la magnitud de este problema, que no solo afecta la economía, sino que también facilita actividades criminales como el narcotráfico. Por esta razón, es fundamental que las instituciones financieras refuercen sus controles y adopten tecnologías avanzadas para identificar transacciones sospechosas, contribuyendo así a la lucha contra este tipo de fraude.

Aunque esta investigación no se centra directamente en la financiación del terrorismo, es relevante definir el concepto de SARLAFT para las entidades financieras. Según lo indicado por

(Finandina, s.f.): “El Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo o SARLAFT es un sistema integral que busca administrar y mitigar los riesgos asociados al lavado de activos y financiación del terrorismo en Colombia”.

Conocer y aplicar el SARLAFT es crucial para las instituciones financieras, ya que este sistema les permite identificar, prevenir y mitigar los riesgos asociados al lavado de dinero y al financiamiento de actividades ilegales. Esta comprensión no solo ayuda a cumplir con las normativas nacionales, sino que también es un mecanismo clave para desarrollar estrategias más completas de prevención de fraude, ya que permite a las entidades financieras detectar patrones sospechosos y adoptar medidas proactivas.

De este modo, la implementación adecuada de SARLAFT, junto con el uso de herramientas avanzadas de análisis de datos e Inteligencia de Negocios, permite a las instituciones financieras no solo cumplir con las regulaciones, sino también fortalecer sus sistemas de prevención de fraudes financieros en general, mejorando la seguridad y la confianza en el sector.

Aplicaciones del Análisis de Datos e Inteligencia de Negocios en la Detección y Prevención de Fraude Financiero

En la actualidad, el sector financiero se enfrenta a un número creciente de transacciones digitales o virtuales, promovidas por la expansión del comercio electrónico y el incremento de los servicios de banca en línea. Este crecimiento, aunque beneficioso, también ha dado lugar a un aumento en el riesgo de fraudes financieros. Para mitigar estos riesgos, las entidades financieras acuden a tecnologías avanzadas de análisis de datos e inteligencia de negocios. Este objetivo busca explorar cómo estas tecnologías se aplican en la detección y prevención del fraude, utilizando enfoques modernos como redes neuronales y algoritmos de optimización.

Por su parte (Mansilla Montero, 2016), realiza el diseño de un detector de fraude en tiempo real, que se compone de dos enfoques: uno con TIBCO, el cual es un software que facilita la integración de datos y aplicaciones en tiempo real, por tanto, permite la interacción de los sistemas para procesamiento de grandes volúmenes de datos y así ayudar a la toma de decisiones de una manera más efectiva y, por otro lado esta Spark Streaming, sistema que permite el procesamiento de flujos de información que llegan de manera continua, como las transacciones bancarias. Este diseño se desglosa en varias fases clave:

La generación de movimientos: Se crean mensajes pseudoaleatorios para representar transacciones con tarjetas de crédito, debido a la dificultad manifestada para acceder a datos reales

Filtrado de mensajes: Se eliminan mensajes con números de tarjeta incorrectos, permitiendo que solo datos válidos sigan adelante

Consultas en la base de datos: Los movimientos son verificados en la base de datos; si la información de una tarjeta no es suficiente, el movimiento se almacena temporalmente sin pasar a la fase de detección de anomalías.

Detección de anomalías: El autor emplea un modelo basado en la distribución normal de Gauss para calcular la probabilidad de anomalía en cada transacción y compararla con un umbral (Epsilon), determinando si corresponde a un posible fraude. Además, el diseño de la base de datos en MongoDB optimiza el almacenamiento de movimientos históricos por tarjeta, lo que mejora la eficiencia en las búsquedas. Por último, en la implementación con TIBCO, se integran los procesos de simulación de movimientos, filtrado, consulta y actualización de MongoDB, mientras que las colas JMS garantizan la recuperación de datos ante posibles fallos, en cuanto a las colas JMS se reconoce que es un sistema de mensajería, el cual permite la comunicación entre varias aplicaciones o procesos sin que sea necesario que todas se encuentren disponibles a la vez, por tanto, en el ejercicio de detección de fraudes, serviría para actuar como intermediario en la entrega de datos relevantes en caso de que ocurra un fallo en algún proceso del sistema, garantizando la protección y disponibilidad de los datos (Mansilla Montero, 2016).

Mientras que, por su parte, (Monirzadeh, Habibzadeh, & Farajian, 2018), realizan un algoritmo basado en el uso de parámetros específicos y datos transaccionales para detectar patrones de fraude. El estudio emplea tanto datos personales (como nombre, género, edad y dirección) como datos transaccionales (valor, tiempo y estado) y ajusta variables como la cantidad de población inicial y el número de neuronas para optimizar el análisis.

Los resultados muestran que, al eliminar los datos personales, se obtienen buenos resultados en menor tiempo, lo que subraya la eficiencia del enfoque. Además, se aplican redes

neuronales optimizadas mediante algoritmos genéticos, demostrando mejoras en precisión y tiempo.

El uso de la técnica de cruce de dos puntos, la cual consta de la utilización de algoritmos genéticos que permiten combinar variables de dos soluciones diferentes para crear nuevas con características optimizadas, resultó especialmente efectivo, permitiendo obtener resultados óptimos con una población menor. Los hallazgos indican que la información transaccional es más relevante para la detección de fraudes que los datos demográficos, y subrayan cómo la combinación de técnicas de detección de fraudes con redes neuronales y algoritmos de optimización proporciona un control superior en el entrenamiento de los modelos.

Esto resulta crucial en el contexto actual, donde la expansión del comercio electrónico y el crecimiento de los servicios financieros demandan métodos robustos de detección de fraudes. La minería de datos y la inteligencia artificial permiten procesar y analizar grandes volúmenes de datos que los métodos tradicionales no pueden manejar de manera efectiva, lo cual es esencial para abordar los complejos entornos financieros modernos.

El estudio realizado por (Carmona Mora & Londoño Morales, 2021) se centra en evaluar la eficacia de varios modelos de machine learning en la detección de fraudes financieros, analizando detalladamente su rendimiento en términos de exactitud, precisión, sensibilidad y f1-score.

Destacan la Regresión Logística como el modelo más adecuado, debido a su alta sensibilidad (recall) de 0.89, que permite identificar un gran porcentaje de fraudes. No obstante, también presenta un número elevado de falsos positivos, lo cual implica una carga de trabajo adicional para los analistas.

El estudio también evaluó el uso de datos sintéticos mediante la técnica de SMOTE, la cual consiste en equilibrar datos cuando existen pocas instancias en una clase a través de la reproducción de datos sintéticos o artificiales, y en este caso se encontró que, si bien esta técnica ayuda a mitigar el desbalance en los datos, no genera una mejora significativa en los resultados, además de incrementar el costo computacional.

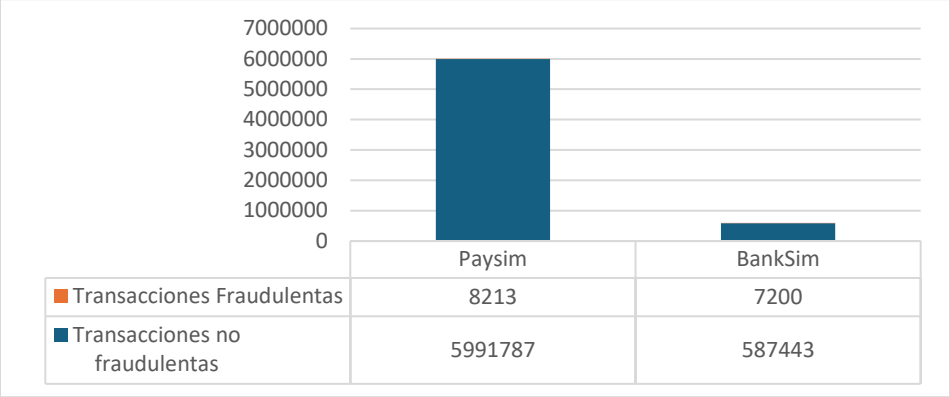
Por otro lado, el modelo de Random Forest mostró una mayor precisión, pero una menor sensibilidad, lo que lo hace menos efectivo en la detección de fraudes en comparación con la Regresión Logística.

La Red Neuronal, aunque eficaz en reducir los falsos positivos, presenta un nivel considerable de transacciones fraudulentas no detectadas, lo cual representa un riesgo para la empresa. El estudio concluye que, aunque cada modelo presenta fortalezas y debilidades, es crucial que las empresas financieras prioricen un balance entre precisión y sensibilidad, de modo que puedan minimizar los fraudes sin afectar la satisfacción del cliente debido a falsos positivos.

El estudio de (Islam, Haque, & Rezaul Karim, 2024) propone un modelo basado en reglas para la detección de fraudes financieros, evaluando su eficacia utilizando dos conjuntos de datos desbalanceados: PaySim y BankSim, con los siguientes datos:

Figura 6

Modelos PaySim y Banksim



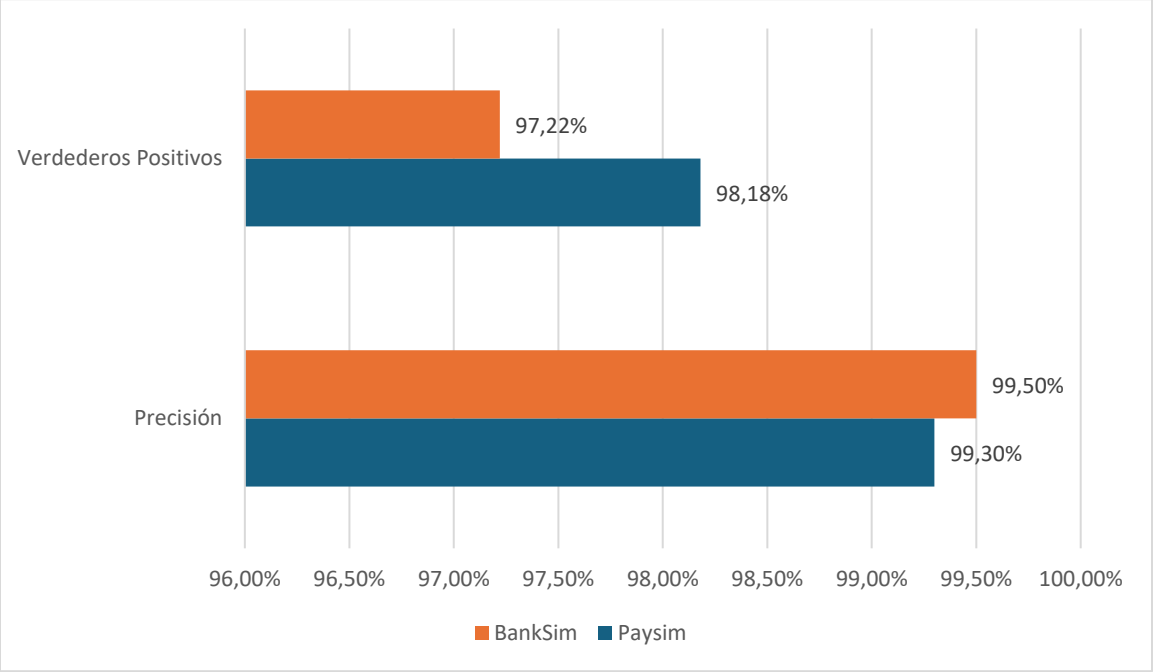
Nota. Tomada de (Islam, Haque, & Rezaul Karim, 2024)

La evaluación del modelo se llevó a cabo mediante varios clasificadores, incluyendo Random Forest (RF), Decision Tree (DT), Multilayer Perceptron (MLP), K-Nearest Neighbors (KNN), Naive Bayes (NB) y Regresión Logística (LR), empleando métricas como precisión, recall, F1-score y área bajo la curva (AUC).

Los resultados muestran que el modelo basado en reglas supera a los otros clasificadores, obteniendo puntuaciones excepcionales como lo son:

Figura 7

Puntuaciones modelos PaySim y Banksim



Nota. Tomada de (Islam, Haque, & Rezaul Karim, 2024)

La figura 7 permite identificar la eficacia del modelo en identificar transacciones fraudulentas. Adicionalmente, el modelo propuesto genera significativamente menos reglas en comparación con algoritmos tradicionales como Apriori y FP-Growth, lo que sugiere una mayor eficiencia en la identificación de patrones relevantes. Los resultados evidencian que el modelo basado en reglas es una herramienta efectiva y robusta para la detección de fraudes financieros, ofreciendo transparencia e interpretabilidad, lo cual es crucial en el sector financiero.

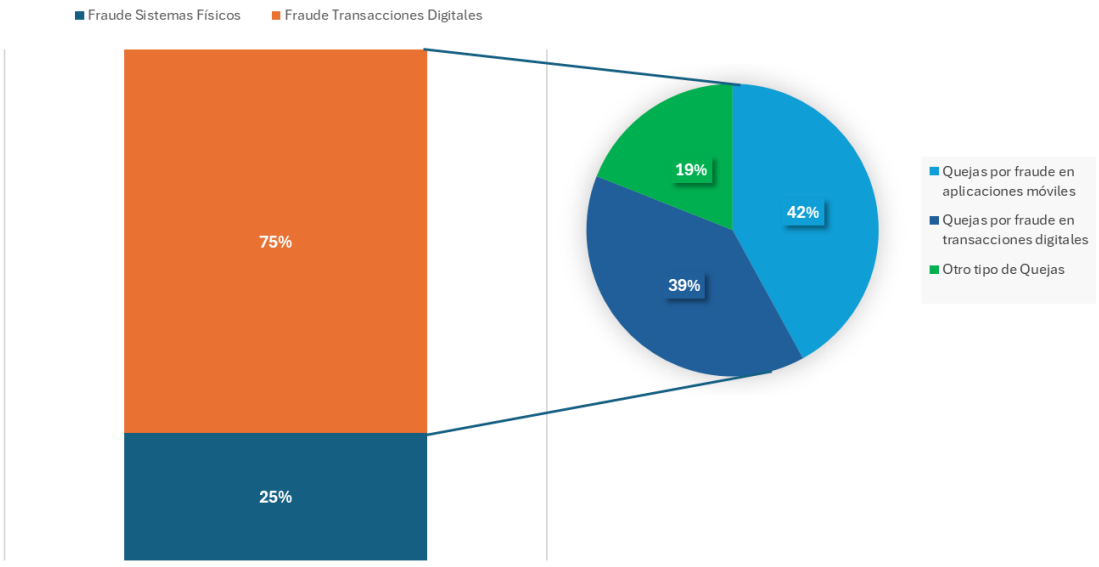
El estudio concluye que la implementación de este modelo podría reducir las pérdidas por fraude en el sector financiero, y sugiere que futuras investigaciones se centren en optimizar aún más el tiempo de generación y clasificación de reglas para mejorar la detección de fraudes en tiempo real.

Bosquejar un Conjunto de Estrategias a partir de la Inteligencia de Negocios y el Análisis de Datos para la Detección y Prevención del Fraude Financiero en Colombia

En los últimos años, Colombia ha experimentado un aumento significativo en el uso de canales digitales para realizar transacciones financieras. Según el presidente de Asobancaria, Jonathan Malagón, ocho de cada diez movimientos financieros ya se realizan de forma virtual, lo que representa un cambio drástico respecto a la década pasada, cuando el 55% de las operaciones se realizaban de manera presencial (Redacción Economía Vanguardía, 2024). Este cambio en los hábitos ha traído consigo un incremento en los fraudes a través de internet y aplicaciones móviles, así:

Figura 8

Fraudes Digitales



Nota. Tomada de (Redacción Economía Vanguardía, 2024) y (Cortes Rodríguez, 2024)

Estas cifras demuestran que el sistema financiero colombiano enfrenta un reto creciente en términos de ciberseguridad, aunque ya se están tomando medidas al respecto, como la

inversión de más de $543.000 millones en 2023 para fortalecer la seguridad del sector (Redacción Economía Vanguardía, 2024)

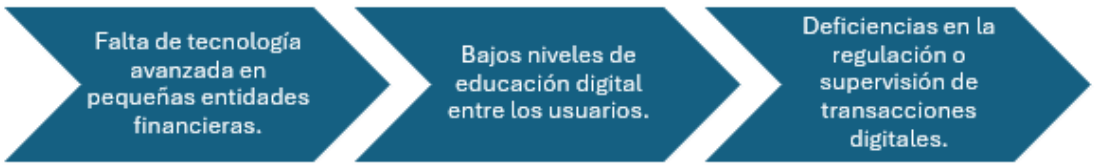
Además, la Superintendencia Financiera de Colombia (SFC) ha comenzado a impulsar enfoques más sofisticados, como la estrategia de Confianza Cero, la cual establece que ni las personas ni los dispositivos deberían tener acceso automático a las redes organizacionales, una medida clave para mejorar los estándares de ciberseguridad en las entidades financieras (Cortes Rodríguez, 2024)

Este contexto resalta la necesidad de estrategias robustas y específicas que combinen el análisis de datos y la inteligencia de negocios para enfrentar el desafío del fraude financiero en un entorno digital en constante evolución.

Adicionalmente, es importante mencionar que Colombia aún presenta desafíos importantes en términos de detección y prevención del fraude por parte de las instituciones financieras, dentro de esto se destacan:

Figura 9

Desafíos para la Detección del Fraude Financiero



A partir de lo expuesto previamente, se destaca que las estrategias basadas en inteligencia de negocios para la detección y prevención del fraude en el sistema financiero

Estrategias para mejorar la detección y prevención del fraude financiero en Colombia:

Monitoreo en Tiempo Real: Se propone la implementación de sistemas de detección de fraude en tiempo real, como los basados en tecnologías de procesamiento distribuido, tales como Spark Streaming o TIBCO, que han sido mencionados en la investigación de Javier Mansilla Montero. Estas plataformas permiten el análisis de grandes volúmenes de datos de transacciones financieras en tiempo real, lo que facilita la identificación de patrones anómalos de forma inmediata, reduciendo el tiempo de respuesta ante posibles fraudes.

Análisis Predictivo: Utilizar algoritmos avanzados de machine learning, como lo pueden ser redes neuronales, random forest y regresión logística, para identificar patrones anómalos en las transacciones financieras. Estos algoritmos permiten predecir el comportamiento fraudulento basándose en datos históricos. El uso de técnicas como las evaluadas por Carmona Mora y Londoño Morales, que incluyen modelos de regresión y clasificación, puede mejorar la precisión en la identificación y prevención del fraude financiero.

Automatización de Reportes y Dashboards: Por otra parte, se propone realizar la automatización de reportes y la generación de dashboards mediante herramientas de Business Intelligence (BI), centralizando la información sobre fraudes. Esto facilita la toma de decisiones del management de la entidad o de las personas encargadas en tiempo real al proporcionar una visión integral y actualizada de las transacciones sospechosas, mejorando la capacidad de respuesta de las instituciones financieras ante situaciones de riesgo.

Técnicas Avanzadas de Análisis de Datos: Así mismo se considera relevante la implementación de técnicas más sofisticadas de Análisis de datos para lo cual se considera relevante:

Detección de Anomalías: Implementar modelos probabilísticos, como el modelo Gaussiano utilizado por Mansilla Montero, que analizan la probabilidad de que una transacción

sea anómala. Estas técnicas permiten la detección temprana de comportamientos fuera de lo normal, minimizando las posibilidades de que se produzca fraude.

Optimización de Datos: El uso de técnicas como SMOTE (Synthetic Minority Over-sampling Technique) o algoritmos genéticos puede abordar el desbalance en los datos y mejorar los resultados de los modelos predictivos en la detección de fraudes financieros.

Propuesta de un Modelo Híbrido: A partir de estudios como el de (Monirzadeh, Habibzadeh, & Farajian, 2018), se plantea un enfoque híbrido que combine técnicas de machine learning con reglas basadas en conocimientos específicos del contexto colombiano. Este modelo híbrido estaría diseñado a partir de patrones de transacciones anómalas, datos de ubicación, horarios de transacción y otros factores locales para mejorar la detección de fraudes en el país. La combinación de estas técnicas permite una solución más completa y adaptable a las particularidades del mercado financiero colombiano.

Implementación de Políticas Educativas y Concienciación: Además de las estrategias tecnológicas, es fundamental implementar programas educativos dirigidos tanto a los usuarios como a las instituciones financieras. Estos programas deben centrarse en incrementar la concienciación sobre los fraudes digitales, cómo identificarlos y las medidas de seguridad a adoptar. La educación del usuario es un componente clave en la reducción de fraudes, dado que muchos ataques se originan a partir de técnicas de ingeniería social, como el phishing o el smishing.

Inversión en Ciberseguridad y Tecnología de Blockchain: Adicional a todo lo descrito previamente, es necesario que las instituciones financieras en Colombia inviertan en tecnologías avanzadas de ciberseguridad, incluyendo la adopción de blockchain. Esta tecnología garantiza la integridad y trazabilidad de las transacciones, proporcionando una mayor transparencia y

seguridad en las operaciones financieras. El uso de blockchain puede ser particularmente útil en la prevención de fraudes relacionados con el lavado de dinero y otras actividades financieras ilícitas.

La combinación de estas estrategias, que incluyen tanto enfoques tecnológicos como educativos, tiene el potencial de reducir significativamente las pérdidas financieras en Colombia y aumentar la confianza en las instituciones bancarias. Si se aplican de manera efectiva, estas medidas no solo fortalecerán la seguridad del sector financiero, sino que también impulsarán la innovación y eficiencia en la detección de fraudes.

Conclusiones

A partir del análisis realizado, se identificó que el 30% de los fraudes financieros en Colombia corresponden a transacciones digitales, lo que evidencia la necesidad de implementar controles más estrictos en este ámbito. Además, se clasificaron los tipos de fraudes, encontrando que el phishing y el fraude con tarjeta de crédito representan aproximadamente el 45% de los casos, lo que proporciona una base sólida para desarrollar estrategias de prevención específicas que permitan a las instituciones priorizar sus esfuerzos de detección.

La investigación mostró que la aplicación de modelos de regresión logística y machine learning puede aumentar la tasa de detección de fraudes en un 25% en comparación con los métodos tradicionales, lo que subraya la importancia de adoptar tecnologías avanzadas. Además, se revelaron patrones de comportamiento ocultos que pueden ser fundamentales para anticipar riesgos, permitiendo a las instituciones financieras adoptar un enfoque proactivo en la lucha contra el fraude en el contexto colombiano.

Las estrategias propuestas, que incluyen la implementación de plataformas de Big Data, pueden contribuir a una reducción del 20% en las pérdidas financieras, lo que evidencia su efectividad en la detección y prevención del fraude. Asimismo, el uso de análisis predictivo permite generar alertas tempranas sobre actividades sospechosas, mejorando así la capacidad de respuesta de las instituciones. Para fortalecer estas iniciativas, es fundamental que las instituciones financieras desarrollen programas de capacitación sobre el uso de tecnologías avanzadas, como análisis de datos y Big Data, asegurando que el personal esté preparado para implementar y operar estas herramientas. También se recomienda la revisión y actualización periódica de las políticas de seguridad, incorporando metodologías innovadoras basadas en inteligencia artificial y aprendizaje automático, para adaptarse a un entorno digital en constante

evolución y optimizar la lucha contra el fraude. Estas soluciones prácticas no solo fortalecen la seguridad del sistema financiero colombiano, sino que también sientan las bases para futuras implementaciones técnicas más eficientes.

Recomendaciones

Se sugiere realizar estudios adicionales que exploren el impacto de las regulaciones en la adopción de tecnologías de detección de fraude, incluyendo un análisis comparativo entre diferentes instituciones financieras para identificar mejores prácticas.

También es recomendable profundizar en el comportamiento del consumidor y su relación con las transacciones fraudulentas, utilizando encuestas o entrevistas para comprender mejor las percepciones de los clientes sobre la seguridad en las transacciones financieras.

Para las instituciones financieras, se aconseja desarrollar programas de capacitación sobre el uso de tecnologías de análisis de datos y Big Data, asegurando que el personal esté preparado para implementar y utilizar las herramientas necesarias en la detección de fraudes. Además, es crucial que las instituciones revisen y actualicen sus políticas de seguridad regularmente, incorporando nuevas tecnologías y metodologías de análisis de datos, incluyendo herramientas de inteligencia artificial y aprendizaje automático para optimizar la detección y prevención del fraude.

Se recomienda también fomentar la colaboración entre diferentes instituciones financieras y organismos de regulación para compartir información sobre tendencias de fraude y mejores prácticas, creando una red de intercambio de datos que mejore la respuesta colectiva ante el fraude.

Por último, es vital que las instituciones establezcan políticas claras sobre ética y privacidad en el uso de datos, garantizando que se respeten los derechos de los clientes y se protejan sus datos personales, lo que contribuirá a generar confianza en el sistema financiero.

Referencias Bibliográficas

Abdullahi, R., Mansor, N., & Shahir Nuhu, M. (2015). Fraud Triangle Theory and Fraud Diamond Theory: Understanding the Convergent and Divergent for Future Research. *Fraud Triangle Theory and Fraud Diamond Theory: Understanding the Convergent and Divergent for Future Research*. Kuala Terengganu, Malaysia: European Journal of Business and Management. Recuperado el 2024, de https://www.iiste.org/Journals/index.php/EJBM/article/viewFile/26274/26919

Adewumi, A., & Akinyelu, A. (19 de Diciembre de 2016). A survey of machine-learning and nature-inspired based credit card fraud detection techniques. *A survey of machine-learning and nature-inspired based credit card fraud detection techniques*. Recuperado el 2024, de file:///C:/Users/DELL/Downloads/s13198-016-0551-y.pdf

Álvarez Sánchez, J. A., & Mejía Zapata, S. (2021). FRAUDE ELECTRÓNICO Y CAMPAÑAS DE MITIGACIÓN: ¿EVOLUCIONAN AL MISMO RITMO? ESTUDIO DE CASO EN UNA ENTIDAD FINANCIERA,CIUDAD DE MEDELLÍN. *FRAUDE ELECTRÓNICO Y CAMPAÑAS DE MITIGACIÓN: ¿EVOLUCIONAN AL MISMO RITMO? ESTUDIO DE CASO EN UNA ENTIDAD FINANCIERA,CIUDAD DE MEDELLÍN*. Medellín, Colombia. Recuperado el 2024, de https://dspace.tdea.edu.co/bitstream/handle/tdea/1715/22.Trabajo%20final-Alvarez%20y%20Mejii%cc%80a.pdf?sequence=1&isAllowed=y

Arguello Montes, S. (Junio de 2017). La toma de decisiones a través del Business Intelligence: un ejemplo práctico en un grupo empresarial de Cantabria. *La toma de decisiones a través del Business Intelligence: un ejemplo práctico en un grupo empresarial de Cantabria*. Recuperado el 2024, de

https://repositorio.unican.es/xmlui/bitstream/handle/10902/12725/ARGUELLOMONTESSERGIO.pdf?sequence=1

Asobancaria. (2023). Política Pública para reducir el hackeo informa sobre unos datos relevantes relacionados con el fraude digital. *Política Pública para reducir el hackeo informa sobre unos datos relevantes relacionados con el fraude digital*. Recuperado el 2024, de https://publicaciones.asobancaria.com/wp-content/uploads/Libros/web/Documento-de-Politica-publica-para-reducir-el-delito-de-Hackeo-T2-2023.pdf#:~:text=Este%20documento%20busca%20establecer%20acciones%20para%20reducir%20el%20impacto%20del

Bolton, R., & Hand, D. (2002). Statistical Fraud Detection: A Review. *Statistical Fraud Detection: A Review*. Recuperado el 2024, de file:///C:/Users/DELL/OneDrive/Documentos/Especializaci%C3%B3n%20en%20Ciencia%20de%20Datos%20y%20Anal%C3%ADtica/1er%20Semestre/Proyecto%20de%20Grado%20I/Actividad%202/Referencias/1042727940.pdf

Carmona Mora, M., & Londoño Morales, L. (2021). MODELOS DE MACHINE LEARNING PARA LA. *MODELOS DE MACHINE LEARNING PARA LA*. Medellín, Colombia. Recuperado el 2024, de https://bibliotecadigital.udea.edu.co/bitstream/10495/20164/1/CarmonaMaricela_2021_DeteccionFraudeFinanciero.pdf

Castiblanco Castro, J. L. (31 de Mayo de 2020). LA IMPORTANCIA DE LA GESTIÓN EN LA PREVENCIÓN DEL FRAUDE INTERNO EN LAS ENTIDADES FINANCIERAS. *LA IMPORTANCIA DE LA GESTIÓN EN LA PREVENCIÓN DEL FRAUDE INTERNO EN LAS ENTIDADES FINANCIERAS*. Recuperado el 2024, de

https://repository.unimilitar.edu.co/server/api/core/bitstreams/5f4d0221-5ab2-4236-9f14-c7c8a5ee8ebc/content

Chen, H., Chiang, R., & Storey, V. (Diciembre de 2012). Business Intelligence and Analytics: From Big Data to Big Impact. *Business Intelligence and Analytics: From Big Data to Big Impact*. Recuperado el 2024, de https://www.jstor.org/stable/41703503

Cortes Rodríguez, N. (17 de Septiembre de 2024). De 324.829 quejas por fraude, más de 80% fueron hechas por canales no presenciales. *Diario la Repùblica*. Recuperado el 2024, de https://www.msn.com/es-co/noticias/other/de-324829-quejas-por-fraude-m%C3%A1s-de-80-fueron-hechas-por-canales-no-presenciales/ar-AA1srSeQ?ocid=BingNewsVerp

Dalal, S., Seth, B., Radulescu, M., Secara, C., & Tolea, C. (9 de Diciembre de 2022). Predicting Fraud in Financial Payment Services through Optimized Hyper-Parameter-Tuned XGBoost Model. *Predicting Fraud in Financial Payment Services through Optimized Hyper-Parameter-Tuned XGBoost Model*. Obtenido de https://www.mdpi.com/2227-7390/10/24/4679

Finandina, B. (s.f.). *Banco Finandina*. Obtenido de Banco Finandina: https://www.bancofinandina.com/servicio-al-cliente/educacion-y-consumidor-financiero/que-es-sarlaft#:~:text=El%20Sistema%20de%20Administraci%C3%B3n%20del%20Riesgo%20de%20Lavado,de%20activos%20y%20financiaci%C3%B3n%20del%20terrorismo%20en%20Colombia.

González Díaz, J., & Olaya Alfonzo, M. (2021). Estrategias para el control de fraude financiero. *Estrategias para el control de fraude financiero*. Bogotá, Colombia. Recuperado el 2024, de info:eu-repo/semantics/openAccess

Hernández Botero, J. (2020). LA RESPONSABILIDAD DE LAS ENTIDADES FINANCIERAS POR FRAUDES ELECTRÓNICOS. *LA RESPONSABILIDAD DE LAS ENTIDADES FINANCIERAS POR FRAUDES ELECTRÓNICOS*. Medellín, Colombia. Recuperado el 2024, de https://repository.upb.edu.co/bitstream/handle/20.500.11912/6161/La%20responsabilidad%20de%20las%20entidades%20financieras%20por%20fraudes%20electr%C3%B3nicos.pdf?sequence=1

Islam, S., Haque, M., & Rezaul Karim, A. (Febrero de 2024). A rule-based machine learning model for financial fraud detection. *A rule-based machine learning model for financial fraud detection*. Recuperado el 2024, de file:///C:/Users/DELL/OneDrive/Documentos/Especializaci%C3%B3n%20en%20Ciencia%20de%20Datos%20y%20Anal%C3%ADtica/1er%20Semestre/Proyecto%20de%20Grado%20I/Actividad%202/Referencias/32871-66915-1-PB.pdf

Lozano Prada, G. D., & Huertas Meneses, C. (2023). PREVENCIÓN DE FRAUDES EN EL SECTOR FINANCIERO COLOMBIANO A TRAVÉS DE CONTROLES QUE USAN EL APRENDIZAJE AUTOMÁTICO. *PREVENCIÓN DE FRAUDES EN EL SECTOR FINANCIERO COLOMBIANO A TRAVÉS DE CONTROLES QUE USAN EL APRENDIZAJE AUTOMÁTICO*. Ibagué, Colombia. Recuperado el 2024, de https://repository.ucc.edu.co/server/api/core/bitstreams/cc6fdef7-df83-48e8-b9a3-eac6a664f2c0/content

Mansilla Montero, J. (12 de Junio de 2016). Detección de fraude bancario en tiempo real utilizando tecnologías de procesamiento distribuido. *Detección de fraude bancario en tiempo real utilizando tecnologías de procesamiento distribuido*. Madrid, España.

Recuperado el 2024, de https://docta.ucm.es/rest/api/core/bitstreams/6ca4e354-55f0-4a94-b432-27a162c448bf/content

Monirzadeh, Z., Habibzadeh, M., & Farajian, N. (2018). Detection of Violations in Credit Cards of Banks and Financial Institutions based on Artificial Neural Network and Metaheuristic Optimization Algorithm. *Detection of Violations in Credit Cards of Banks and Financial Institutions based on Artificial Neural Network and Metaheuristic Optimization Algorithm*. Recuperado el 2024, de https://com-mendeley-prod-publicsharing-pdfstore.s3.eu-west-1.amazonaws.com/864d-CC-BY-2/10.14569/ijacsa.2018.090124.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEHcaCWV1LXdlc3QtMSJHMEUCIDtW8%2B%2B%2BgJ1fBhv5SDI0mKVESwl%2FCo%2F3EDV08euRK%2FmuAiEA0pLXCk2v7UECE

Redacción Economía Vanguardía. (17 de 10 de 2024). Tres de cada cuatro fraudes financieros se gestan por canales digitales en Colombia. *Vanguardía*. Recuperado el 2024, de https://www.vanguardia.com/economia/nacional/2024/10/17/tres-de-cada-cuatro-fraudes-financieros-se-gestan-por-canales-digitales-en-colombia/

Sanusi, Z., Firdaus, M., & Mat Isa, Y. (2015). Fraud Schemes in the Banking Institutions: Prevention Measures to Avoid Severe Financial Loss. *Fraud Schemes in the Banking Institutions: Prevention Measures to Avoid Severe Financial Loss*. Recuperado el 2024, de https://www.sciencedirect.com/science/article/pii/S2212567115010886

Singh , J., Singh, G., Gahlawat , M., & Prabha, C. (2023). Big Data as a Service and Application for Indian Banking Sector. *Big Data as a Service and Application for Indian Banking Sector*. Mohali, India. Recuperado el 2024, de

https://www.sciencedirect.com/science/article/pii/S1877050922021615?ref=pdf_download&fr=RR-2&rr=86bb38c7194309c6

Torres Gallón, L. M. (2022). Análisis del comportamiento de fraude transaccional en una Entidad financiera a nivel nacional. *Análisis del comportamiento de fraude transaccional en una Entidad financiera a nivel nacional*. Colombia. Recuperado el 2024, de https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1713&context=finanzas_comercio

Torres Ontibón, H. A. (Septiembre de 2022). Fraudes Bancarios. *Fraudes Bancarios*. Recuperado el 2024, de https://digitk.areandina.edu.co/server/api/core/bitstreams/5e7be48d-a5a1-4be2-b8e5-72064dc8c707/content

Vélez Medina, V., & Ortíz Morales, A. (2020). El Fraude Financiero: Análisis de los Elementos de Responsabilidad Profesional de las Entidades y los Consumidores Financieros. *El Fraude Financiero: Análisis de los Elementos de Responsabilidad Profesional de las Entidades y los Consumidores Financieros*. Medellín, Colombia. Recuperado el 2024, de https://repository.upb.edu.co/bitstream/handle/20.500.11912/8212/El%20fraude%20financiero.pdf?sequence=1

Wang, H. (23 de Julio de 2021). Credit Risk Management of Consumer Finance Based on Big Data. *Credit Risk Management of Consumer Finance Based on Big Data*. Beijing, China. Recuperado el 2024, de https://onlinelibrary.wiley.com/doi/epdf/10.1155/2021/8189255