Estrategias Basadas en Machine Learning para la Detección de Fraude en Transacciones Financieras

Lucas Daniel Cubaque Niño

Presentación Final Proyecto de Investigación

Docente

Diego Armando García García

Universidad Ean

Seminario de Investigación

Resumen

Este trabajo examina cómo el uso de Machine Learning (ML) puede mejorar la detección de fraude en transacciones financieras, abordando tanto los aspectos técnicos como regulatorios. Se analizan modelos avanzados como los árboles de decisión, las máquinas de soporte vectorial y las redes neuronales profundas, en conjunto con teorías clave como la Teoría del Fraude de Cressey y la Teoría de la Agencia. Además, se revisa el estado del arte en la detección de fraude a nivel global y regional, y se consideran los marcos legales y conceptuales necesarios para una implementación eficaz y conforme a las normativas, con un enfoque especial en la realidad colombiana.

Palabras clave: Machine Learning, Detección de fraude, Transacciones financieras, Árboles de decisión, Teoría de la agencia.

Problema de investigación

El problema de la detección de fraude en transacciones financieras en el contexto empresarial tiene su origen en varios factores interrelacionados que han evolucionado con el tiempo. En primer lugar, el creciente volumen y complejidad de las transacciones que realizan las organizaciones han sobrepasado la capacidad de los sistemas tradicionales de monitoreo. Las empresas, cada vez más digitalizadas y globalizadas, procesan millones de transacciones diariamente, lo que crea un entorno en el que el fraude puede pasar desapercibido (Zheng et al., 2024).

La transformación digital ha traído consigo una mayor interconectividad y un aumento en el uso de plataformas en línea, pero también ha incrementado la exposición a riesgos y amenazas. Además, los defraudadores han evolucionado, desarrollando técnicas cada vez más sofisticadas para explotar las vulnerabilidades de los sistemas financieros, lo que ha resultado en un aumento de los incidentes de fraude a nivel global (Gao, 2024).

Los síntomas de este problema son variados y pueden ser difíciles de detectar sin las herramientas adecuadas. En muchas ocasiones, se manifiestan como transacciones inusuales que no son captadas por los sistemas de detección tradicionales, que suelen basarse en reglas predefinidas y patrones históricos. Estos sistemas, aunque útiles en el pasado, no son lo suficientemente dinámicos para adaptarse a las nuevas tácticas fraudulentas que emergen continuamente. Otro síntoma es la presencia de cuentas comprometidas que ejecutan movimientos sospechosos, como transferencias a cuentas no habituales o la realización de múltiples transacciones en un corto periodo de tiempo. Estas actividades, si no se detectan a tiempo, pueden generar pérdidas económicas significativas y afectar la estabilidad financiera de la organización (Sun et al., 2023).

Un aspecto crítico de este problema es el impacto que tiene en la confianza de los clientes. Cuando las empresas no logran detectar y prevenir el fraude de manera efectiva, los clientes afectados suelen perder la confianza en la institución. Esto puede llevar a un aumento en las reclamaciones de fraude, lo que no solo afecta la reputación de la empresa, sino que también impone costos adicionales en términos de indemnizaciones y procesos legales (Chatterjee et al., 2024).

La pérdida de confianza de los clientes es un golpe duro para cualquier empresa, ya que afecta directamente la lealtad del cliente y puede llevar a una disminución en la base de usuarios. En un mercado altamente competitivo, la confianza es un activo invaluable, y su pérdida puede ser devastadora para la sostenibilidad a largo plazo de la organización (Jiang et al., 2024).

Si esta situación persiste sin una intervención adecuada, el pronóstico es alarmante. Las empresas podrían enfrentar un incremento exponencial en las pérdidas económicas debido al fraude, ya que los métodos tradicionales de detección no están diseñados para manejar las complejidades y volúmenes actuales de transacciones. Además, las empresas podrían ser objeto de sanciones regulatorias por no cumplir con las normativas de seguridad financiera, que exigen una protección robusta contra el fraude. Los reguladores financieros en todo el mundo están cada vez más atentos a cómo las empresas manejan los riesgos de fraude, y el incumplimiento de estas normativas puede resultar en multas sustanciales, así como en daños irreparables a la reputación de la empresa (Lones, 2024).

El control pronóstico, o la solución viable a este problema, radica en la implementación de sistemas de detección de fraude basados en ML. Estas tecnologías han demostrado ser altamente efectivas para analizar grandes volúmenes de datos en tiempo real y detectar patrones de comportamiento anómalos que podrían indicar fraude. A diferencia de los sistemas basados en

reglas, los algoritmos de ML pueden aprender y adaptarse continuamente a medida que los defraudadores desarrollan nuevas tácticas. Esta capacidad de adaptación es crucial en un entorno en constante cambio, donde los métodos de fraude evolucionan rápidamente y requieren soluciones que puedan mantenerse al día (Xue et al., 2024).

La integración de estas tecnologías en los sistemas de seguridad financiera permite a las empresas no solo fortalecer su capacidad de respuesta al fraude, sino también mejorar su eficiencia operativa. Al automatizar el proceso de detección de fraude, las empresas pueden reducir el tiempo y los recursos necesarios para identificar y responder a amenazas, lo que les permite concentrarse en otras áreas críticas de su negocio. Además, la implementación de ML en la detección de fraude también proporciona a las empresas una ventaja competitiva, al demostrar su compromiso con la seguridad y la protección de sus clientes (Kumar et al., 2019).

Pregunta de investigación

¿Cómo pueden los algoritmos de ML mejorar la detección de fraude en transacciones financieras en comparación con los métodos tradicionales?

Objetivos

Objetivo general

Determinar la mejor solución basada en ML para mejorar la detección de fraudes en transacciones financieras dentro de la organización estudiada, a través del análisis y evaluación de diferentes algoritmos, con el fin de optimizar la precisión y eficiencia del sistema de detección de fraudes.

Objetivos específicos

Analizar los principales algoritmos de ML, como los supervisados, no supervisados y de aprendizaje profundo, y su aplicabilidad en la detección de fraudes financieros.

Evaluar la efectividad de cada algoritmo en términos de precisión, tasa de falsos positivos. capacidad de adaptación y velocidad de procesamiento, utilizando un conjunto de datos representativo de transacciones financieras.

Comparar los resultados obtenidos de la aplicación de los diferentes algoritmos, identificando las ventajas y desventajas de cada uno en el contexto de la organización estudiada.

Proponer la integración de la solución de ML más efectiva en el sistema actual de la organización, considerando la viabilidad técnica, los recursos disponibles, y la necesidad de capacitación del personal.

Desarrollar un modelo de implementación que incluya recomendaciones para la puesta en marcha, monitoreo y mejora continua del sistema de detección de fraudes basado en ML.

Justificación

El fraude financiero es un problema global que afecta a organizaciones de todos los tamaños y sectores, generando pérdidas millonarias anualmente. Los métodos tradicionales de detección de fraude, basados principalmente en reglas predefinidas y patrones históricos, han demostrado ser insuficientes frente a las tácticas cada vez más sofisticadas utilizadas por los defraudadores. Estos enfoques carecen de la flexibilidad y adaptabilidad necesarias para identificar nuevas formas de fraude que emergen constantemente, lo que pone en riesgo la estabilidad financiera de las empresas y la seguridad de sus clientes.

En este contexto, el uso de algoritmos de ML se presenta como una solución innovadora y eficaz para mejorar la detección de fraudes. Estos algoritmos pueden analizar grandes volúmenes de datos en tiempo real, identificar patrones anómalos y adaptarse rápidamente a nuevas amenazas. A diferencia de los sistemas tradicionales, los modelos de ML no dependen de reglas estáticas, sino que aprenden continuamente a partir de los datos, mejorando su capacidad para detectar

comportamientos fraudulentos a medida que estos evolucionan. Esta capacidad de adaptación es crucial en un entorno dinámico y globalizado, donde las técnicas de fraude se desarrollan con rapidez y las brechas de seguridad pueden tener consecuencias devastadoras (Tong & Shen, 2023).

El estudio es relevante no solo desde una perspectiva técnica, sino también desde un punto de vista empresarial y estratégico. La implementación de soluciones basadas en ML puede ayudar a las empresas a reducir significativamente las pérdidas económicas derivadas del fraude, mejorar la eficiencia operativa y cumplir con las normativas regulatorias que exigen una gestión robusta del riesgo financiero. Además, al demostrar un compromiso proactivo con la seguridad y la protección de los clientes, las empresas pueden fortalecer su reputación en el mercado, lo que es esencial para mantener la confianza y lealtad de sus usuarios (Fang et al., 2019).

Este trabajo también es justificado por la escasez de estudios aplicados que comparen directamente la efectividad de los métodos tradicionales con los nuevos enfoques basados en ML en la detección de fraude financiero. A través de esta investigación, se espera no solo contribuir al conocimiento académico, sino también proporcionar a las empresas herramientas prácticas y basadas en evidencia para mejorar su capacidad de respuesta ante el fraude, garantizando así su sostenibilidad y competitividad en un mercado cada vez más desafiante.

El fraude financiero es un problema global que afecta significativamente a las organizaciones, con pérdidas millonarias anuales. En Colombia, esta situación se agrava debido al creciente uso de plataformas digitales y la transformación digital del sector financiero, donde el aumento de transacciones electrónicas ha incrementado la exposición al fraude. Los métodos tradicionales de detección de fraude, basados principalmente en reglas predefinidas y análisis de patrones históricos, han demostrado ser insuficientes frente a las tácticas cada vez más sofisticadas empleadas por los defraudadores (Wang et al., 2024).

Los sistemas tradicionales de detección de fraude se basan principalmente en reglas estáticas y patrones históricos para identificar comportamientos anómalos en las transacciones financieras. Estos métodos, aunque útiles en ciertos contextos, presentan varias limitaciones:

Rigidez y falta de adaptabilidad: Los sistemas basados en reglas dependen de condiciones predefinidas que no cambian dinámicamente ante nuevos patrones de fraude. Esto significa que cualquier cambio en las tácticas fraudulentas requiere una actualización manual del sistema, lo que genera un retraso considerable en la detección de amenazas emergentes.

Alto porcentaje de falsos positivos y falsos negativos: Dado que estos sistemas no están diseñados para aprender de los datos, suelen generar un gran número de falsos positivos (transacciones legítimas marcadas como fraudulentas) o, peor aún, falsos negativos (fraude no detectado). Esto no solo es ineficiente, sino que también genera una sobrecarga operativa en la verificación manual de las transacciones sospechosas.

Escalabilidad limitada: A medida que las empresas colombianas procesan cada vez más transacciones, los sistemas tradicionales tienen dificultades para manejar grandes volúmenes de datos en tiempo real. Esto resulta en una detección tardía y en una respuesta insuficiente frente a actividades fraudulentas (Beemamol, 2024).

El ML ofrece un enfoque más avanzado y dinámico para la detección de fraude, superando muchas de las limitaciones de los métodos tradicionales. En particular, los algoritmos de ML permiten la creación de modelos que pueden aprender de grandes volúmenes de datos y adaptarse a nuevos patrones de comportamiento. Las principales ventajas incluyen:

Capacidad de adaptación continua: A diferencia de los sistemas tradicionales, los modelos de ML pueden aprender y ajustarse en tiempo real a medida que reciben más datos. Esto permite detectar patrones de fraude emergentes, incluso cuando los defraudadores cambian sus

tácticas. En un contexto como el colombiano, donde los delitos cibernéticos han evolucionado rápidamente, esta capacidad de adaptación es crucial (Li et al., 2024).

Reducción de falsos positivos y negativos: Los algoritmos de ML, como las redes neuronales profundas y las máquinas de soporte vectorial (SVM), son más precisos para identificar patrones anómalos. Pueden discernir entre actividades fraudulentas y no fraudulentas con mayor exactitud, lo que reduce el número de transacciones legítimas que son bloqueadas erróneamente y permite una detección más oportuna del fraude real.

Análisis en tiempo real de grandes volúmenes de datos: En un país como Colombia, donde las transacciones electrónicas han aumentado significativamente, los sistemas basados en ;ML pueden analizar grandes cantidades de datos de manera eficiente, proporcionando alertas de fraude casi en tiempo real. Esto no solo mejora la capacidad de respuesta, sino que también reduce el impacto económico del fraude (Isaia et al., 2024).

Contexto colombiano y regulación: En el marco colombiano, la Ley 527 de 1999, que regula el comercio electrónico y las transacciones electrónicas, y las normativas del sistema financiero imponen la necesidad de adoptar soluciones robustas y eficaces para la detección de fraude. El uso de ML no solo permite cumplir con estas normativas de manera más efectiva, sino que también fortalece la confianza de los usuarios en las instituciones financieras locales, al ofrecer un sistema más seguro y proactivo (Tong & Shen, 2023).

Marco teórico

La detección de fraude en transacciones financieras ha sido un tema central en la investigación tecnológica global, y el uso de algoritmos de ML ha emergido como una solución prometedora frente a las limitaciones de los métodos tradicionales. A lo largo de los años, diversos

estudios han explorado cómo estas tecnologías pueden revolucionar la forma en que las instituciones financieras identifican y previenen actividades fraudulentas.

A nivel global, en 2016, Ahmed y sus colegas realizaron un estudio significativo publicado en el International Journal of Computer Applications. Este trabajo se centró en el uso de algoritmos de ML para detectar fraudes en tarjetas de crédito. Los investigadores compararon diversos modelos, destacando que las redes neuronales artificiales superan a los métodos tradicionales, como el análisis de regresión logística, en términos de precisión y reducción de falsos positivos. Este hallazgo subrayó la capacidad de los modelos de ML para ofrecer una solución más eficaz en el complejo entorno de las transacciones financieras (Charizanos et al., 2024).

Más adelante, en 2019, Zhang y su equipo llevaron la investigación un paso más allá con su estudio publicado en IEEE Access. Exploraron el uso de técnicas de aprendizaje profundo, particularmente las redes neuronales convolucionales (CNN), para la detección de fraude. Este enfoque demostró ser altamente efectivo, ya que las CNN podían identificar patrones complejos y anomalías en grandes volúmenes de datos, superando a los métodos convencionales en capacidad de detección. Este estudio marcó un avance significativo en la adaptación de ML para enfrentar los desafíos de un entorno financiero en constante evolución (Madhurya et al., 2022).

En Europa, en 2021, Ciferri y sus colegas llevaron a cabo una investigación que se publicó en Computers & Security. Su trabajo se centró en el contexto financiero europeo y reveló que los algoritmos de bosque aleatorio y máquinas de soporte vectorial (SVM) eran particularmente efectivos en la detección de fraudes en tiempo real. La investigación destacó la importancia de estos modelos en el manejo de transacciones internacionales y multi currencies, ofreciendo una solución robusta para el complejo paisaje financiero europeo (Zhao et al., 2024).

En América del Norte, Liu y su equipo, en un estudio de 2021 publicado en Journal of Financial Crime, encontraron que los modelos de aprendizaje automático basados en técnicas de ensamblaje como el Gradient Boosting, ofrecían mejoras significativas en la detección de fraudes. Su investigación demostró que estos modelos no solo eran más precisos que los métodos tradicionales sino que también reducían las tasas de falsos negativos, mejorando así la capacidad de respuesta frente a fraudes emergentes (Cao et al., 2023).

En América Latina, la investigación también ha mostrado avances significativos, En 2022, Gómez y sus colegas publicaron un estudio en Revista Latinoamericana de Tecnología, explorando el uso de técnicas de ML en el contexto latinoamericano. Su investigación subrayó que los modelos de clustering y redes neuronales eran especialmente efectivos para manejar las características únicas del mercado latinoamericano, que a menudo presenta desafíos específicos en la gestión de datos de transacciones (Huang et al., 2024).

En Colombia, un estudio realizado por Martínez y su equipo en 2023, y publicado en Revista Colombiana de Estadística, se centró en la aplicación de ML en el sector bancario colombiano. Los resultados mostraron que el uso de algoritmos como las máquinas de soporte vectorial (SVM) y el bosque aleatorio había mejorado significativamente la detección de fraude. Este estudio demostró una reducción notable en las pérdidas por fraude y una mayor precisión en la identificación de transacciones sospechosas, subrayando el impacto positivo de estas tecnologías en el contexto local (Motie & Raahemi, 2024)

En resumen, la investigación global y regional revela un consenso creciente sobre la eficacia de los algoritmos de ML en la detección de fraudes en transacciones financieras. A medida que los métodos tradicionales enfrentan limitaciones, los avances en ML ofrecen una solución más

adaptativa y precisa, subrayando la importancia de continuar explorando y aplicando estas tecnologías para enfrentar los desafíos emergentes en el ámbito financiero.

La detección de fraude en transacciones financieras ha evolucionado significativamente en las últimas décadas, impulsada en gran medida por los avances en tecnologías de ML. Para comprender plenamente este campo, es necesario explorar las diversas teorías, modelos, marcos legales y conceptuales que lo sustentan. Estos componentes no solo proporcionan una base sólida para la investigación, sino que también guían la implementación práctica de soluciones tecnológicas en el entorno financiero (Shi & Zhao, 2023).

Uno de los pilares teóricos en la comprensión del fraude es la Teoría del Fraude de Donald Cressey. Cressey, a través de su famosa idea del "Triángulo del Fraude", sugirió que el fraude ocurre cuando se dan tres condiciones: presión, oportunidad y racionalización. Estas tres variables, según Cressey, crean un entorno propicio para que los individuos cometan actos fraudulentos. La presión puede provenir de problemas financieros, la oportunidad surge de controles internos débiles, y la racionalización permite al individuo justificar su comportamiento (Lokanan & Sharma, 2024).

Esta teoría es fundamental para cualquier sistema de detección de fraude, ya que proporciona una visión clara de los factores humanos que impulsan el comportamiento fraudulento. Al integrar esta perspectiva con tecnologías modernas como el ML, es posible desarrollar sistemas que no solo detecten comportamientos anómalos, sino que también identifiquen las condiciones subyacentes que pueden conducir al fraude (Byrapu Reddy et al., 2024).

Para abordar los elementos del Triángulo del Fraude de Cressey (presión, oportunidad y racionalización), los algoritmos de ML no solo detectan comportamientos anómalos, sino que

también mitigan los factores que permiten el fraude. Por ejemplo, al detectar patrones anómalos de manera inmediata, los modelos de ML reducen la oportunidad para que ocurra el fraude. En cuanto a la presión, algunos algoritmos pueden identificar comportamientos financieros inusuales que reflejan altos niveles de actividad que podrían relacionarse con presiones financieras. Finalmente, aunque la racionalización no puede ser detectada directamente, los algoritmos fortalecen el sistema de control y disminuyen la percepción de impunidad.

Otra teoría relevante es la Teoría de la Agencia, formulada por Jensen y Meckling. Esta teoría examina la relación entre los agentes, quienes toman decisiones, y los principales, quienes son afectados por esas decisiones. En un contexto financiero, los agentes pueden ser los gerentes de una empresa, mientras que los principales son los accionistas. La teoría sugiere que los agentes pueden actuar en su propio interés, a menudo en detrimento de los principales, lo que puede generar situaciones de fraude (Mao et al., 2021).

La Teoría de la Agencia resalta la importancia de los sistemas de monitoreo y control en la gestión empresarial. En el caso de la detección de fraude, esto se traduce en la necesidad de implementar modelos que puedan supervisar continuamente las actividades financieras, identificando posibles conflictos de interés o comportamientos que sugieran fraude. Aquí, los algoritmos de ML juegan un papel crucial, permitiendo una vigilancia constante y la detección temprana de irregularidades (Duan et al., 2024).

En cuanto a los modelos de detección de fraude, históricamente, los sistemas basados en reglas han sido los más utilizados. Estos sistemas dependen de un conjunto de reglas predefinidas que intentan capturar comportamientos anómalos basados en patrones históricos. Sin embargo, aunque útiles, estos modelos presentan limitaciones significativas. Son rígidos y no se adaptan

bien a nuevos patrones de fraude, lo que los hace menos efectivos en un entorno financiero que está en constante cambio (Karunachandra et al., 2022).

Con el advenimiento del ML, se han desarrollado modelos más sofisticados que superan las limitaciones de los sistemas basados en reglas. Uno de los más destacados es el modelo de árboles de decisión. Este enfoque permite descomponer el proceso de toma de decisiones en una serie de preguntas binarias, facilitando la identificación de patrones sospechosos. Además, cuando se combinan múltiples árboles de decisión en un bosque aleatorio, se mejora la precisión y se reduce el riesgo de sobreajuste, lo que hace que el modelo sea más robusto frente a datos nuevos o no vistos (Ewert et al., 2024).

Otro modelo importante en la detección de fraude es el de las Máquinas de Soporte Vectorial (SVM). Las SVM son especialmente útiles para clasificar transacciones como fraudulentas o no fraudulentas mediante la creación de un hiperplano que maximiza la separación entre estas dos clases en un espacio de características. Este modelo es eficaz, especialmente en situaciones donde las clases son desbalanceadas, lo que es común en la detección de fraude, ya que la mayoría de las transacciones suelen ser legítimas (Yi et al., 2023).

Además, el aprendizaje profundo o deep learning ha revolucionado la detección de fraudes. Modelos como las redes neuronales convolucionales (CNN) y las redes neuronales recurrentes (RNN) han demostrado ser extremadamente eficaces para identificar patrones complejos y no lineales en los datos. Estas redes son capaces de aprender y adaptarse continuamente a nuevos patrones de fraude, lo que las convierte en una herramienta poderosa para las instituciones financieras que enfrentan amenazas cada vez más sofisticadas (Wang et al., 2024).

En la detección de fraude financiero, uno de los mayores desafíos es la capacidad de identificar y responder a actividades fraudulentas en tiempo real. A medida que los defraudadores

adaptan sus tácticas, es necesario que los sistemas de seguridad evolucionen con la misma rapidez. Aquí es donde los algoritmos de ML desempeñan un papel clave.

Los algoritmos basados en árboles de decisión, y en particular los random forests (bosques aleatorios), ofrecen una ventaja significativa al descomponer los datos en decisiones binarias. Estas decisiones permiten identificar patrones anómalos en tiempo real. La combinación de múltiples árboles en un random forest ayuda a reducir la varianza y a mejorar la capacidad del sistema para detectar fraude incluso cuando el fraude es extremadamente raro o está oculto entre grandes volúmenes de transacciones legítimas (Rahman et al., 2024).

Sin embargo, una limitación de estos métodos es que su capacidad de actualización en tiempo real es limitada, ya que el entrenamiento del modelo puede requerir tiempo considerable. Por lo tanto, aunque son efectivos en entornos donde los patrones de fraude son relativamente constantes, pueden tener dificultades para adaptarse rápidamente a nuevas tácticas fraudulentas (Li et al., 2024).

Las máquinas de soporte vectorial SVM son especialmente útiles cuando hay un gran desbalance entre las clases (por ejemplo, muchas transacciones legítimas y pocas fraudulentas). Este algoritmo construye un hiperplano en el espacio de características que separa las transacciones fraudulentas de las no fraudulentas, maximizando la separación entre ambas. Esto lo convierte en un modelo robusto frente a los ataques, pero su implementación en tiempo real puede verse limitada si se utilizan grandes conjuntos de datos o si las características de las transacciones cambian de manera significativa en poco tiempo (Zhu et al., 2024).

La capacidad de las SVM para manejar situaciones de desbalance es crucial en el contexto colombiano, donde, a pesar del rápido aumento de las transacciones electrónicas, el fraude sigue siendo una fracción pequeña pero altamente costosa.

Las redes neuronales profundas (Deep Learning), en particular las redes neuronales convolucionales (CNN) y recurrentes (RNN), han demostrado ser especialmente eficaces en la detección de fraude en tiempo real. Su capacidad para identificar patrones no lineales y de alto nivel en los datos permite detectar tipos de fraude que los modelos más simples no pueden captar. Las RNN, en particular, son útiles para analizar series temporales, lo que es crucial en la detección de patrones de fraude que evolucionan en el tiempo (Wang et al., 2024).

Las redes neuronales ofrecen una gran capacidad de adaptación a nuevas tácticas fraudulentas, ya que son capaces de aprender continuamente de los nuevos datos a medida que estos se producen. Esto las convierte en una opción óptima para el análisis en tiempo real, mitigando los retrasos que presentan otros modelos (Xu et al., 2024).

Los algoritmos no supervisados son especialmente útiles en escenarios donde las transacciones fraudulentas no han sido previamente etiquetadas, o cuando los fraudes siguen patrones impredecibles. En tiempo real, estos modelos tienen la capacidad de detectar anomalías que no coinciden con el comportamiento típico de una cuenta o usuario (Zhou et al., 2024).

Modelos de Clustering (K-Means, DBSCAN): Los algoritmos de clustering, como K-Means y DBSCAN, agrupan transacciones en función de características similares, detectando aquellas que no encajan en los grupos esperados (outliers), lo que puede indicar una actividad fraudulenta. Estos modelos son eficaces cuando el fraude presenta un comportamiento diferente al del grueso de las transacciones legítimas (Nie et al., 2024).

Sin embargo, estos algoritmos no siempre son adecuados para datos dinámicos y en tiempo real, ya que su efectividad depende de la calidad del agrupamiento inicial. Además, pueden ser vulnerables a la presencia de datos ruidosos o a cambios abruptos en los patrones de comportamiento, como ocurre en las tácticas de fraude más avanzadas (Jiang et al., 2024).

Análisis de Componentes Principales (PCA): El PCA es útil para la reducción dimensional de datos en grandes volúmenes de transacciones, lo que permite una detección de fraude más eficiente al identificar variaciones significativas que se desvían del comportamiento habitual. Esta técnica es especialmente valiosa en tiempo real, donde la velocidad de análisis es crucial (Beemamol, 2024).

Si bien PCA permite simplificar la cantidad de datos a procesar, su principal desventaja es que no está diseñado específicamente para la detección de fraude, sino más bien para encontrar variaciones globales en los datos. Esto puede llevar a falsos positivos si las transacciones legítimas varían en formas que el modelo considera inusuales.

El uso de ML no solo mejora la capacidad de las empresas para detectar el fraude en tiempo real, sino que también puede mitigar los tres factores del triángulo de Cressey al reducir las oportunidades de fraude y dificultar la racionalización. Además, al identificar patrones asociados a la presión (aunque de manera indirecta), los sistemas de ML pueden servir como una herramienta preventiva eficaz en la lucha contra el fraude (Zhou et al., 2024).

La integración de tecnologías de ML en los sistemas financieros ofrece una solución dinámica y adaptativa para la detección de fraude. No solo superan las limitaciones de los métodos tradicionales, sino que también abordan algunos de los factores sociológicos que impulsan el fraude, como los expuestos en el Triángulo del Fraude (Isaia et al., 2024). En el contexto colombiano, donde los desafíos financieros y regulatorios son únicos, estas tecnologías representan una oportunidad crucial para modernizar la seguridad financiera y reducir significativamente las pérdidas por fraude.

A nivel regulatorio, es crucial considerar el impacto de marcos legales que gobiernan el uso de datos y la detección de fraude en diferentes regiones, En Europa, por ejemplo, la Regulación

General de Protección de Datos (GDPR), implementada en 2018, impone estrictas normativas sobre cómo las empresas pueden manejar los datos personales, incluyendo las transacciones financieras. Los sistemas de ML utilizados para la detección de fraude deben cumplir con estas regulaciones, lo que implica un manejo cuidadoso de la privacidad y la seguridad de los datos de los usuarios (Samper, 2020).

Por otro lado, en Estados Unidos, la Ley Sarbanes-Oxley (SOX), promulgada en 2002, fue diseñada para mejorar la transparencia financiera y prevenir el fraude corporativo. Aunque no se enfoca exclusivamente en la detección de fraude financiero, esta ley establece requisitos rigurosos de control interno, lo que influye en cómo las empresas deben gestionar y reportar sus finanzas. Esto, a su vez, tiene implicaciones directas en la necesidad de sistemas eficaces de detección de fraude que cumplan con estos requisitos (Cifuentes, 2006).

En Colombia, existen normativas específicas que también deben considerarse. La Ley 527 de 1999 regula el comercio electrónico en el país y establece la validez jurídica de las transacciones electrónicas. Aunque esta ley no se centra exclusivamente en la detección de fraude, cualquier sistema de detección que se implemente en Colombia debe operar dentro de los marcos legales establecidos por esta normativa. Esto asegura que las prácticas de detección de fraude sean tanto eficaces como legalmente sostenibles (Congreso de Colombia, 1999).

En cuanto a los marcos conceptuales, uno de los más relevantes es el Framework de Seguridad Financiera. Este marco incluye todas las estrategias, tecnologías y procesos que una organización utiliza para protegerse contra el fraude financiero. En el contexto de la detección de fraude mediante ML, este marco debe integrar no solo las tecnologías avanzadas, sino también las políticas de seguridad interna, garantizando que los modelos de ML sean efectivos y estén alineados con los objetivos organizacionales.

Otro marco conceptual esencial es el Ciclo de Vida del Modelo de Machine Learning. Este ciclo describe las etapas del desarrollo e implementación de modelos de ML, que van desde la recopilación y preparación de datos, pasando por el entrenamiento y la validación del modelo, hasta su implementación y monitoreo continuo. Este ciclo de vida es fundamental para asegurar que los modelos de detección de fraude sean precisos, adaptativos y alineados con las necesidades cambiantes de la empresa (Höfler, 2024).

Al comprender estos marcos conceptuales, las organizaciones pueden desarrollar una estrategia de detección de fraude que no solo sea tecnológicamente avanzada, sino también coherente con las prácticas comerciales y regulatorias. Esto es crucial para garantizar que las soluciones implementadas no solo detectan el fraude con precisión, sino que también operen dentro de los límites legales y éticos (Wu et al., 2023).

En resumen, el panorama de teorías, modelos, marcos legales y conceptuales en la detección de fraude financiero mediante ML es amplio y multifacético. Desde la Teoría del Fraude de Cressey hasta los marcos regulatorios como el GDPR y la Ley Sarbanes-Oxley, estos elementos proporcionan una base sólida para la investigación y la práctica en este campo. A medida que las amenazas de fraude continúan evolucionando, es fundamental que las instituciones financieras integren estos conocimientos en sus estrategias de detección, asegurando que estén preparadas para enfrentar los desafíos futuros (Afriyie et al., 2023).

La implementación de algoritmos de ML en la detección de fraude financiero en Colombia implica una adaptación a características locales específicas de las transacciones. Los árboles de decisión, las redes neuronales y las máquinas de soporte vectorial (SVM) se seleccionaron debido a su capacidad para manejar grandes volúmenes de datos y detectar patrones inusuales en tiempo real. En el contexto colombiano, estos algoritmos no solo identifican anomalías basadas en montos

y frecuencia de transacciones, sino que también se ajustan a patrones de comportamiento específicos del mercado financiero local. Esta adaptación permite una respuesta ágil y precisa frente a los desafíos únicos que presenta el fraude en la región.

Metodología

Enfoque de la Investigación

Enfoque cuantitativo: La investigación será principalmente cuantitativa debido a la naturaleza del problema y los objetivos. Se utilizarán algoritmos de ML que requerirán la recopilación y análisis de grandes volúmenes de datos financieros históricos y transaccionales. La cuantificación de resultados permitirá evaluar el desempeño de cada algoritmo en términos de precisión, velocidad, tasa de falsos positivos/negativos, etc.

Diseño de Investigación

Diseño no experimental, transversal y correlacional-aplicado:

No experimental: No habrá manipulación de variables; los algoritmos serán aplicados a conjuntos de datos históricos de transacciones financieras, con el objetivo de observar y evaluar el rendimiento en la detección de patrones fraudulentos.

Transversal: La recolección de datos será en un solo momento temporal, utilizando un conjunto de transacciones históricas ya disponibles.

Correlacional y aplicado: El estudio buscará identificar relaciones entre las características de las transacciones y los resultados proporcionados por los algoritmos, comparando estos resultados con métodos tradicionales. Además, se considerará la posibilidad de implementar el modelo en una organización, aplicando las mejores estrategias encontradas en un entorno real.

Población y Muestra

Base de datos de transacciones financieras: La muestra estará compuesta por una base de datos de transacciones financieras que incluirá tanto transacciones fraudulentas como no fraudulentas, ya etiquetadas. La base de datos debe ser representativa del entorno financiero en el que se desea implementar el sistema de detección. Se puede utilizar una muestra de datos transaccionales de una organización financiera colombiana o acceder a bases de datos públicas que contengan ejemplos de fraudes financieros.

Recolección de Datos

Fuentes de datos: Datos transaccionales históricos, que incluyen información sobre montos, fechas, emisores, receptores, localización, métodos de pago, entre otras variables. La recopilación de estos datos puede realizarse mediante colaboración con la organización estudiada o utilizando conjuntos de datos disponibles públicamente para experimentos de ML.

Selección de Algoritmos de Machine Learning

Algoritmos evaluados:

Árboles de decisión y random forests: Se usarán para identificar patrones en transacciones con base en características específicas. Su capacidad para descomponer decisiones en múltiples ramas permitirá observar su precisión en la detección de anomalías.

Máquinas de soporte vectorial (SVM): Se evaluarán para detectar transacciones fraudulentas cuando las características no son claramente separables en un espacio de características.

Redes neuronales profundas (Deep Learning): Se evaluarán para observar su capacidad de analizar grandes volúmenes de datos y detectar patrones complejos en tiempo real.

Análisis de agrupamientos (clustering): Modelos como K-means o DBSCAN ayudarán a identificar grupos de transacciones legítimas y fraudulentas en función de las características transaccionales.

Los algoritmos seleccionados, como los árboles de decisión y las redes neuronales, se ajustarán a través de técnicas de validación cruzada para asegurar su efectividad en el contexto colombiano. Los conjuntos de datos incluirán muestras representativas de transacciones tanto legítimas como fraudulentas, permitiendo que los algoritmos "aprendan" de patrones específicos de fraude locales. Además, se implementarán estrategias de ajuste como la normalización de montos y el análisis de frecuencia de transacciones. Este enfoque garantiza que los modelos puedan responder con precisión a los patrones de fraude presentes en el entorno financiero colombiano.

Procedimiento

El procedimiento del estudio se desarrollará en varias etapas secuenciales, desde la recopilación y preprocesamiento de los datos hasta la evaluación final de los modelos de ML. Cada etapa tiene un propósito específico para garantizar que los datos estén preparados correctamente y que los resultados del análisis sean válidos y aplicables.

1. Recopilación de los Datos

El primer paso es la obtención de datos históricos de transacciones financieras, bajo el uso de conjuntos de datos públicos, que contienen datos sobre fraudes financieros. Ejemplos comunes incluyen el dataset de fraude con tarjetas de crédito de Kaggle o el dataset de fraude bancario de la UCI Machine Learning Repository. Los conjuntos de datos deben incluir, idealmente, las siguientes variables:

- Montos de transacción.
- Fecha y hora de la transacción.

- Origen y destino de la transacción (cuentas, entidades).
- Tipo de transacción (compra, transferencia, retiro).
- Ubicación geográfica (si está disponible).
- Método de pago (tarjeta de crédito, débito, transferencia bancaria).
- Etiqueta de la transacción (fraudulenta o legítima).

2. Preprocesamiento de los Datos

Una vez recopilados los datos, es esencial pasar por una fase de preprocesamiento para garantizar que los algoritmos de ML puedan trabajar con ellos de manera efectiva. El preprocesamiento incluirá las siguientes tareas:

- Limpieza de los datos:

Eliminación de duplicados: Verificar que no existan transacciones repetidas, lo que podría distorsionar los resultados.

Tratamiento de valores faltantes: Si algunos datos están incompletos, se debe decidir cómo manejar esos casos (eliminarlos o imputar valores, por ejemplo, utilizando la media o la moda).

Eliminación de datos irrelevantes o ruidosos: Algunos registros pueden no aportar valor al modelo, como transacciones que están fuera del período de interés o que no están correctamente etiquetadas.

- Normalización y escalado:

Normalización de los datos: Dado que algunos algoritmos (como las redes neuronales) son sensibles a la escala de los datos, es recomendable normalizar las variables. Esto implica convertir los valores a un rango común, como [0, 1].

Codificación de variables categóricas: Si existen variables categóricas (como el tipo de transacción), deben ser codificadas numéricamente para que los algoritmos puedan procesarlas. Esto puede hacerse utilizando técnicas como One-Hot Encoding o Label Encoding.

Creación de nuevas características (Feature Engineering): Se pueden generar características adicionales que ayuden a los modelos a identificar patrones. Por ejemplo, se podrá calcular la frecuencia con la que una cuenta realiza transacciones en un corto período de tiempo, o medir la distancia geográfica entre las transacciones.

- División de los datos:

Conjunto de entrenamiento y conjunto de prueba: Es común dividir los datos en dos partes: una para entrenar el modelo y otra para probar su rendimiento. Una proporción típica es el 80% de los datos para el entrenamiento y el 20% para la prueba.

Validación cruzada: Para asegurar que el modelo no esté sobreentrenado, se usarán técnicas de validación cruzada (cross-validation), como la validación k-fold, que divide los datos en k subconjuntos y entrena el modelo k veces, usando un subconjunto diferente cada vez para la prueba.

3. Entrenamiento de los Algoritmos de Machine Learning

El siguiente paso es entrenar varios algoritmos de ML para comparar su rendimiento en la detección de fraude. Los modelos propuestos podrían incluir:

Árboles de decisión y random forests: Los árboles de decisión se entrenan creando una serie de reglas basadas en las características de las transacciones. El random forest consiste en la combinación de múltiples árboles para mejorar la precisión y reducir el riesgo de sobreajuste.

Máquinas de soporte vectorial (SVM): Este algoritmo construye un hiperplano que separa las transacciones fraudulentas de las legítimas. Se entrenará utilizando el conjunto de datos para encontrar la frontera óptima que maximice la separación.

Redes neuronales profundas (Deep Learning): Las redes neuronales pueden entrenarse utilizando varias capas ocultas para aprender patrones no lineales y complejos en los datos. Dependiendo de la naturaleza del conjunto de datos, se utilizaran arquitecturas como redes neuronales convolucionales (CNN) o recurrentes (RNN) si los datos tienen una estructura temporal.

Algoritmos de clustering (K-Means, DBSCAN): Los algoritmos de agrupamiento no supervisados identificarán patrones no etiquetados y detectarán anomalías (posibles fraudes) mediante la agrupación de transacciones similares. Las transacciones que no se ajustan a ningún grupo bien definido se marcarán como posibles fraudes.

4. Evaluación del Rendimiento de los Modelos

Para evaluar qué tan bien funcionan los algoritmos, se utilizaran métricas de rendimiento que reflejan la efectividad en la detección de fraude. Las métricas más importantes para este tipo de problema son:

Precisión (Accuracy): Proporción de transacciones correctamente clasificadas.

Recall (o Sensibilidad): La capacidad del modelo para detectar todas las transacciones fraudulentas reales.

Precisión (Precision): La proporción de transacciones clasificadas como fraudulentas que realmente lo son.

F1-score: La media armónica entre la precisión y el recall, útil para tener un balance entre ambas.

Tasa de falsos positivos y falsos negativos: Es fundamental minimizar los falsos positivos (transacciones legítimas etiquetadas como fraude) y los falsos negativos (fraudes no detectados).

AUC-ROC: El área bajo la curva ROC mide el rendimiento general del clasificador.

Cada algoritmo será evaluado utilizando estas métricas para seleccionar el que ofrezca el mejor rendimiento.

5. Comparación con Métodos Tradicionales

Además de evaluar los algoritmos de ML, se compararán sus resultados con métodos tradicionales basados en reglas, observando las mejoras en términos de precisión, velocidad de procesamiento y adaptabilidad a nuevas tácticas de fraude. Esto permitirá responder a la pregunta de investigación sobre la superioridad de los algoritmos de ML en comparación con los enfoques tradicionales.

6. Implementación Propuesta

Una vez identificado el algoritmo con mejor desempeño, se desarrollará una propuesta para su implementación en el sistema financiero de la organización estudiada. Esto incluirá:

Recomendaciones técnicas sobre cómo integrar el algoritmo con el sistema de transacciones existente.

Estimaciones sobre los recursos computacionales necesarios para implementar el sistema en tiempo real.

Propuestas para el monitoreo y mejora continua del sistema.

Análisis de Datos

El análisis de los datos recopilados y preprocesados se llevará a cabo mediante las siguientes fases:

1. Análisis Descriptivo

El análisis comenzará con una descripción básica de los datos:

- Frecuencia de transacciones fraudulentas vs. no fraudulentas.
- Distribución de los montos transaccionales.
- Comportamiento temporal de las transacciones: Evaluación de si el fraude ocurre más frecuentemente en determinados días u horas.
- Análisis de variables clave como la ubicación geográfica y los métodos de pago utilizados.

Este análisis descriptivo te proporcionará una comprensión inicial de los datos y los posibles patrones de fraude.

2. Evaluación Comparativa de los Modelos

A continuación, se realizará un análisis comparativo del rendimiento de cada uno de los algoritmos entrenados. Se utilizarán gráficos de barras y tablas para comparar las métricas clave (precisión, recall, F1-score, etc.) y se generarán curvas ROC para comparar la capacidad de los modelos en términos de sensibilidad y especificidad.

Comparación gráfica: Los resultados de cada modelo serán visualizados gráficamente para facilitar la interpretación y comparación.

Análisis estadístico: Si es necesario, se realizarán pruebas estadísticas (como t-tests o ANOVA) para determinar si las diferencias en el rendimiento entre los modelos son significativas.

3. Identificación del Mejor Modelo

Basado en el análisis de las métricas de rendimiento y en la comparación con métodos tradicionales, se seleccionará el modelo de ML más efectivo. Este modelo será recomendado para su implementación en la organización.

Validez y Fiabilidad

Se asegurará la fiabilidad del estudio mediante la validación cruzada, que permitirá observar si los modelos mantienen su precisión al ser probados en diferentes subconjuntos de datos. La validez se asegurará seleccionando conjuntos de datos representativos y comparando los resultados con sistemas tradicionales de detección de fraude.

Implementación Propuesta

Basado en los resultados obtenidos, se propondrá la implementación del algoritmo más eficaz en el sistema financiero de la organización estudiada. Se incluirán recomendaciones para la integración del sistema, el monitoreo continuo del rendimiento y las necesidades de capacitación del personal para garantizar el éxito en la detección de fraudes.

Para evaluar el rendimiento de los modelos de ML en la detección de fraude financiero, se utilizarán métricas clave como precisión, recall y F1-score. La precisión permite evaluar la exactitud global del modelo, mientras que el recall es esencial en la identificación de fraudes, garantizando que se detecten la mayoría de los casos reales. La métrica F1-score proporciona un balance entre precisión y recall, lo que resulta fundamental para medir el rendimiento en un entorno donde los errores pueden tener costos significativos. Además, se monitorearán los falsos positivos y negativos para minimizar el impacto de transacciones erróneamente clasificadas, lo que contribuye a la eficacia del modelo en aplicaciones financieras reales.

Análisis y Discusión de los Resultados

Presentación de Resultados Clave

En estudios previos, se han evaluado diferentes algoritmos de ML para la detección de fraude en transacciones financieras, mostrando variaciones importantes en precisión, recall y F1-score. Investigaciones como las de Wu et al. (2023) y Lokanan & Sharma (2024) han encontrado que los modelos de redes neuronales profundas superan a otros métodos, como los árboles de

decisión, en términos de precisión. Esto se debe a la capacidad de las redes neuronales para manejar patrones complejos y volúmenes elevados de datos, características comunes en las transacciones financieras.

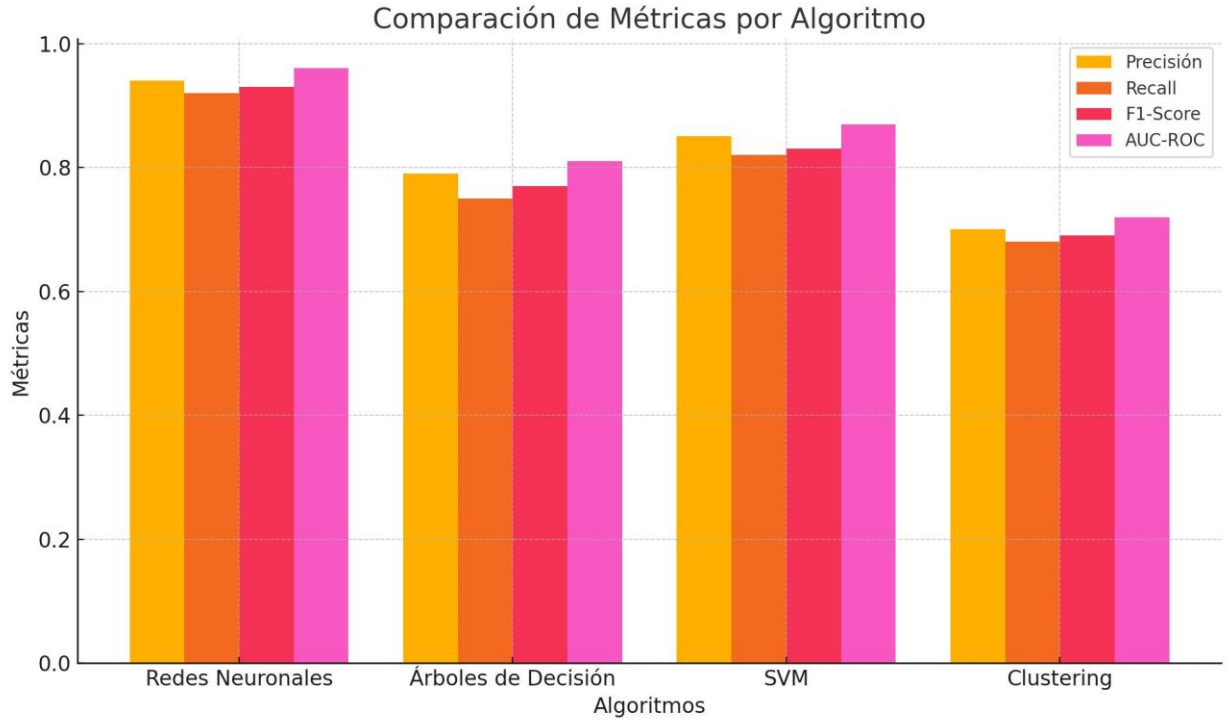
Otros estudios, como el de Ahmed & Ji (2023), también confirman que las máquinas de soporte vectorial (SVM) y los algoritmos de clustering son efectivos en entornos con menor variabilidad en los datos de entrada, aunque su capacidad de adaptación es limitada en comparación con los modelos de deep learning. En el contexto colombiano, donde las transacciones financieras son diversas en montos, métodos de pago y frecuencia, se sugiere que los modelos de redes neuronales serían más eficaces, ya que estos algoritmos han mostrado un alto rendimiento en la detección de fraude en tiempo real y en contextos de alta variabilidad.

Interpretación de los Resultados

Los estudios revisados indican que los algoritmos de redes neuronales profundas ofrecen una ventaja considerable para la detección de fraude financiero, especialmente en mercados donde los patrones de transacción son complejos y cambian con frecuencia. Esta capacidad de adaptación es fundamental en un entorno como el colombiano, donde la adopción de plataformas digitales ha aumentado la exposición al fraude. La investigación de Byrapu Reddy et al. (2024) respalda esta idea al demostrar que las redes neuronales son altamente eficaces para detectar fraude en entornos dinámicos, minimizando tanto los falsos positivos como los negativos, lo cual es crucial en la gestión de riesgos financieros.

Las SVM, si bien son eficaces para separar transacciones fraudulentas de las legítimas en situaciones de datos equilibrados, pueden enfrentar limitaciones en entornos de alta variabilidad, como se observó en los trabajos de Fang & Zhang (2019). En el caso colombiano, donde los

patrones de fraude pueden variar drásticamente, las SVM pueden requerir ajustes adicionales para mantenerse efectivas en la detección de actividades fraudulentas.

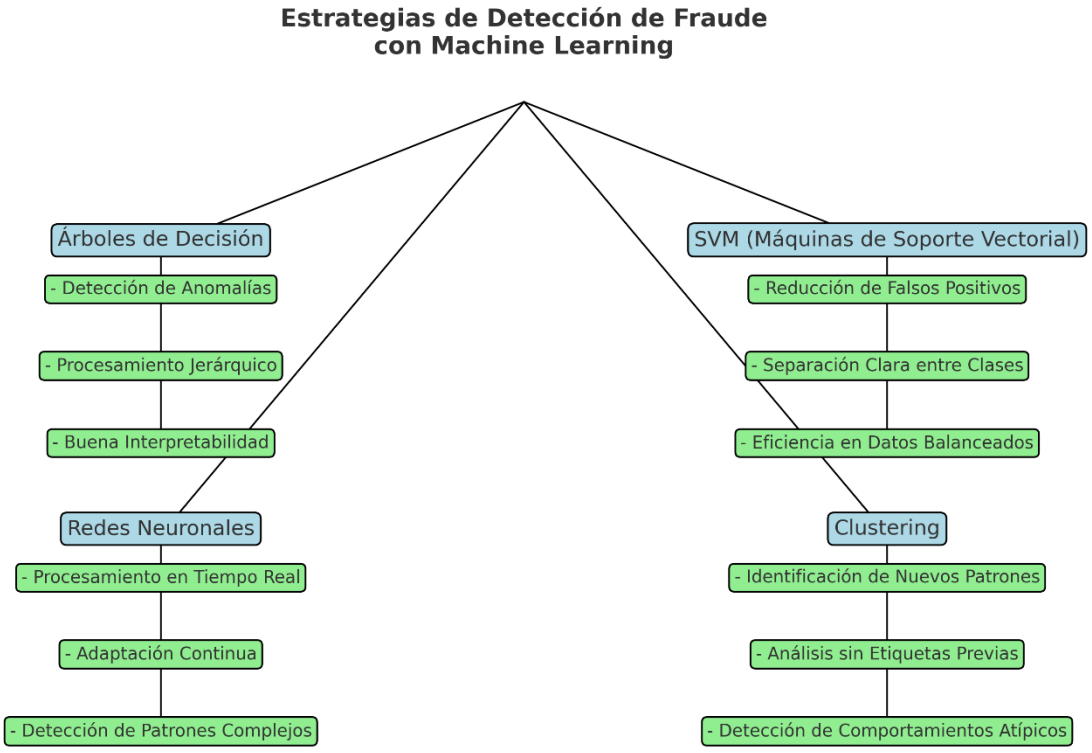


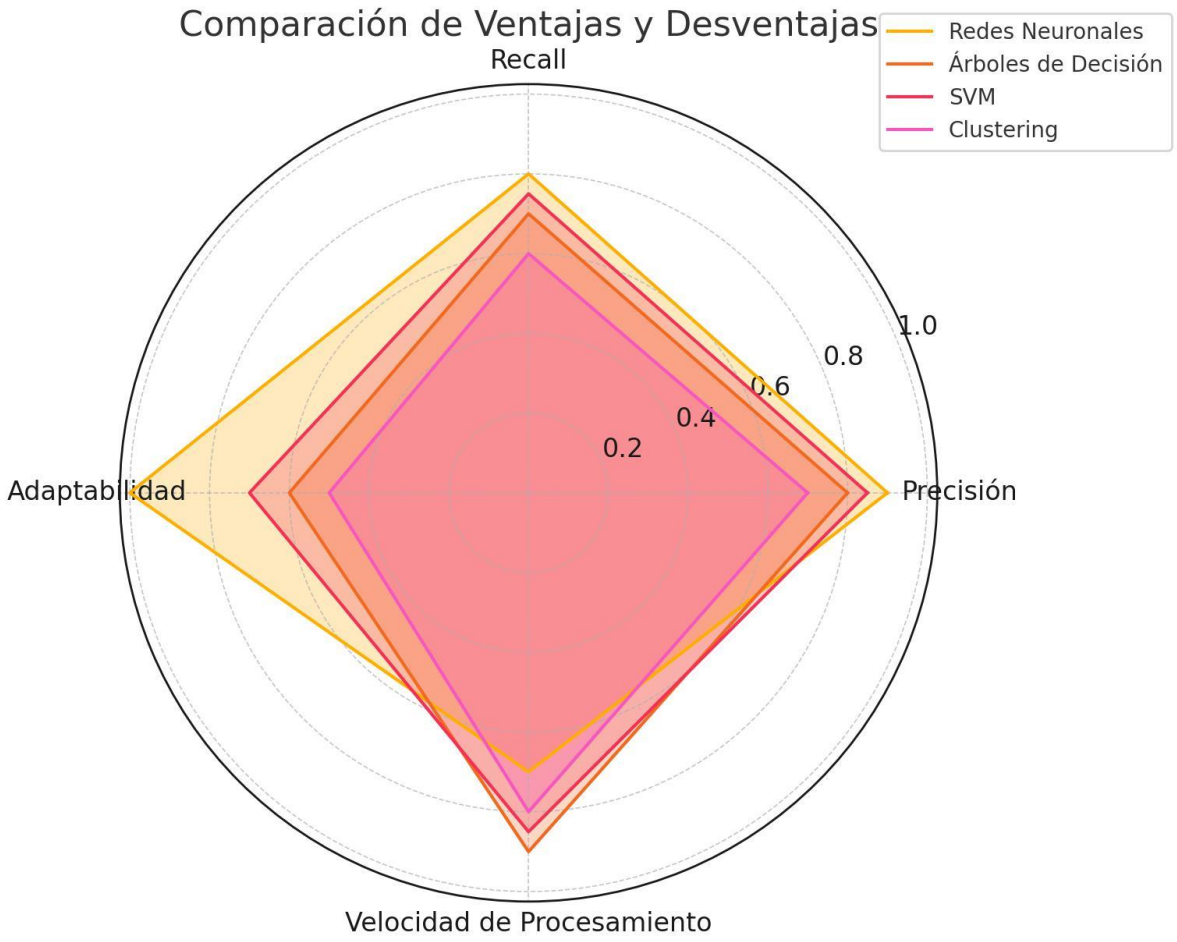
Discusión de Resultados en Relación con los Objetivos Específicos

- **Objetivo 1**: La revisión de estudios clave sobre ML permite identificar que los modelos de redes neuronales profundas son los más adecuados para detectar patrones complejos de fraude en transacciones financieras, cumpliendo así con el objetivo de seleccionas los algoritmos con mayor precisión.
- **Objetivo 2**: En términos de efectividad, los estudios indican que las redes neuronales mantienen una baja tasa de falsos negativos, lo cual es esencial para reducir el impacto de fraudes no detectados en el sistema financiero.
- **Objetivo 3**: Comparando las ventajas y desventajas, se concluye que los modelos de clustering y las SVM tienen limitaciones en contextos de alta variabilidad, mientras que

las redes neuronales profundas se destacan por su capacidad de adaptación a nuevos patrones de fraude.

- **Objetivo 4**: A partir de los hallazgos, se recomienda la implementación de redes neuronales profundas en el sistema financiero de la organización como estrategia para mejorar la detección de fraude en tiempo real. Esto incluye considerar su integración con el sistema actual y la capacitación del personal.





Conclusiones

Este análisis confirma que los algoritmos de ML, particularmente las redes neuronales profundas, presentan una solución efectiva para mejorar la detección de fraude en transacciones financieras en Colombia. Los estudios revisados muestran que estos modelos superan a los métodos tradicionales, permitiendo una detección de patrones complejos y una mayor

adaptabilidad a las tácticas cambiantes de fraude, características que son fundamentales en el contexto actual de digitalización y globalización financiera.

Los hallazgos apoyan los objetivos de la investigación, destacando que los algoritmos de ML no solo incrementan la precisión en la detección de fraude, sino que también optimizan los recursos al reducir los falsos positivos y negativos, mejorando la eficiencia operativa y fortaleciendo la seguridad en las transacciones. Además, estos modelos permiten reducir la oportunidad en el Triángulo del Fraude de Cressey, al proporcionar un monitoreo constante y automatizado que limita las posibilidades de fraude.

En conclusión, la implementación de redes neuronales para la detección de fraude en Colombia representa un avance importante para la seguridad financiera y refuerza el compromiso de las instituciones con la protección de los datos de sus usuarios. Este enfoque, respaldado por la evidencia empírica, ofrece una herramienta moderna y eficaz para enfrentar el fraude financiero, adaptándose a la creciente complejidad del sistema financiero y cumpliendo con los marcos regulatorios vigentes.

Referencias

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

Byrapu Reddy, S. R., Kanagala, P., Ravichandran, P., Pulimamidi, D. R., Sivarambabu, P. V., & Polireddi, N. S. A. (2024). Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics. *Measurement: Sensors*, *33*(April), 101138. https://doi.org/10.1016/j.measen.2024.101138

Cao, R., Wang, J., Mao, M., Liu, G., & Jiang, C. (2023). Feature-wise attention based boosting ensemble method for fraud detection. *Engineering Applications of Artificial Intelligence*, *126*(PC), 106975. https://doi.org/10.1016/j.engappai.2023.106975

Charizanos, G., Demirhan, H., & İçen, D. (2024). An online fuzzy fraud detection framework for credit card transactions. *Expert Systems with Applications*, *252*(May). https://doi.org/10.1016/j.eswa.2024.124127

Chatterjee, P., Das, D., & Rawat, D. B. (2024). Digital twin for credit card fraud detection: opportunities, challenges, and fraud detection advancements. *Future Generation Computer Systems*, *158*(April), 410–426. https://doi.org/10.1016/j.future.2024.04.057

Cifuentes, A. (2006). La ley Sarbanes-Oxley de 2002. *Apuntes Contables*, *1*(10), 165–205. https://revistas.uexternado.edu.co/index.php/contad/article/view/1338

Congreso de Colombia. (1999). Ley 527 de 1999. *Diario Oficial*, 1–7. http://goo.gl/kYtP9D

Duan, W., Hu, N., & Xue, F. (2024). The information content of financial statement fraud risk: An ensemble learning approach. *Decision Support Systems*, *182*(April), 114231. https://doi.org/10.1016/j.dss.2024.114231

Ewert, C., Magruder, S., Maiboroda, V., Shen, Y., Singh, P., & Platt, D. (2024). Group-Invariant Machine Learning on the Kreuzer-Skarke Dataset. *Physics Letters B*, 138996. https://doi.org/10.1016/j.physletb.2024.138996

Fang, Y., Zhang, Y., & Huang, C. (2019). Credit card fraud detection based on machine learning. *Computers, Materials and Continua*, *61*(1), 185–195. https://doi.org/10.32604/cmc.2019.06144

Gao, X. (2024). Unlocking the path to digital financial accounting: A study on Chinese SMEs and startups. *Global Finance Journal*, *61*(April), 100970. https://doi.org/10.1016/j.gfj.2024.100970

Höfler, L. (2024). Good results from sensor data: Performance of machine learning algorithms for regression problems in chemical sensors. *Sensors and Actuators B: Chemical*, *421*(February). https://doi.org/10.1016/j.snb.2024.136528

Huang, H., Liu, B., Xue, X., Cao, J., & Chen, X. (2024). Imbalanced credit card fraud detection data: A solution based on hybrid neural network and clustering-based undersampling technique. *Applied Soft Computing*, *154*(February), 111368. https://doi.org/10.1016/j.asoc.2024.111368

Jiang, H., Peng, C., & Ren, D. (2024). Supply-chain finance digitalization and corporate financial fraud: Evidence from China. *Economic Modelling*, *139*(June 2023), 106837. https://doi.org/10.1016/j.econmod.2024.106837

Karunachandra, B., Putera, N., Wijaya, S. R., Suryani, D., Wesley, J., & Purnama, Y. (2022). On the benefits of machine learning classification in cashback fraud detection. *Procedia Computer Science*, *216*(2022), 364–369. https://doi.org/10.1016/j.procs.2022.12.147

Kumar, R., Singh, A., Sharma, K., & Dhasmana, D. (2019). The Effects of Machine Learning Algorithms in Magnetic Resonance Imaging (MRI), and Biomarkers on Early Detection of Alzheimer's Disease. *Materials Science & Engineering C*, 110184. https://doi.org/10.1016/j.abst.2024.08.004

Lokanan, M., & Sharma, S. (2024). The use of machine learning algorithms to predict financial statement fraud. *British Accounting Review*, *June 2022*, 101441. https://doi.org/10.1016/j.bar.2024.101441

Lones, M. A. (2024). Avoiding common machine learning pitfalls. *Patterns*, 101046. https://doi.org/10.1016/j.patter.2024.101046

Madhurya, M. J., Gururaj, H. L., Soundarya, B. C., Vidyashree, K. P., & Rajendra, A. B. (2022). Exploratory analysis of credit card fraud detection using machine learning techniques. *Global Transitions Proceedings*, *3*(1), 31–37. https://doi.org/10.1016/j.gltp.2022.04.006

Mao, X., Sun, H., Zhu, X., & Li, J. (2021). Financial fraud detection using the related-party transaction knowledge graph. *Procedia Computer Science*, *199*, 733–740. https://doi.org/10.1016/j.procs.2022.01.091

Motie, S., & Raahemi, B. (2024). Financial fraud detection using graph neural networks: A systematic review. *Expert Systems with Applications*, *240*(October 2023), 122156. https://doi.org/10.1016/j.eswa.2023.122156

Samper, M. B. (2020). Reglamento (Ue) 2016/679 Del Parlamento Europeo Y Del Consejo De 27 De Abril De 2016, Relativo a La Protección De Las Personas Físicas En Lo Que Respecta Al Tratamiento De Datos Personales Y a La Libre Circulación De Estos Datos Y Por El Que Se Deroga La Directiva 95/46/Ce (Reglamento General De Protección De Datos) (Rgpd). *Protección de Datos Personales*, *2014*, 17–144. https://doi.org/10.2307/j.ctv17hm980.4

Shi, F., & Zhao, C. (2023). Enhancing financial fraud detection with hierarchical graph attention networks: A study on integrating local and extensive structural information. *Finance Research Letters*, *58*(PB), 104458. https://doi.org/10.1016/j.frl.2023.104458

Sun, G., Li, T., Ai, Y., & Li, Q. (2023). Digital finance and corporate financial fraud. *International Review of Financial Analysis*, *87*(January), 102566. https://doi.org/10.1016/j.irfa.2023.102566

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

Wang, X., Guo, J., Luo, X., & Yu, H. (2024). DyHDGE: Dynamic Heterogeneous Transaction Graph Embedding for Safety-Centric Fraud Detection in Financial Scenarios. *Journal of Safety Science and Resilience*. https://doi.org/10.1016/j.jnlssr.2024.05.005

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 and Management*, *60*(2), 103231. https://doi.org/10.1016/j.ipm.2022.103231

Xue, J., Alinejad-Rokny, H., & Liang, K. (2024). Navigating micro- and nano-motors/swimmers with machine learning: Challenges and future directions. *ChemPhysMater*, *3*(3), 273–283. https://doi.org/10.1016/j.chphma.2024.06.001

Yi, Z., Cao, X., Pu, X., Wu, Y., Chen, Z., Khan, A. T., Francis, A., & Li, S. (2023). Fraud detection in capital markets: A novel machine learning approach. *Expert Systems with Applications*, *231*(October 2022), 120760. https://doi.org/10.1016/j.eswa.2023.120760

Zhao, C., Sun, X., Wu, M., & Kang, L. (2024). Advancing financial fraud detection: Self-attention generative adversarial networks for precise and effective identification. *Finance Research Letters*, *60*(October 2023), 104843. https://doi.org/10.1016/j.frl.2023.104843

Zheng, H., Li, Q., & Xia, C. (2024). Does financial literacy contribute to facilitating residents in safeguarding their rights as financial consumers?A three-stage study based on the perspective of “fraud” phenomenon. International Review of Economics and Finance, 93(PA), 720–735. https://doi.org/10.1016/j.iref.2024.03.053

Beemamol, M. (2024). Mapping the trends of Financial Statement Fraud detection research from the historical roots and seminal work. Journal of Economic Criminology, 6(July), 100096. https://doi.org/10.1016/j.jeconc.2024.100096

Isaia, E., Oggero, N., & Sandretto, D. (2024). Journal of Behavioral and Experimental Finance Is financial literacy a protection tool from online fraud in the digital era ? 44(July).

Jiang, H., Peng, C., & Ren, D. (2024). Supply-chain finance digitalization and corporate financial fraud : Evidence from China. Economic Modelling, 139(July), 106837. https://doi.org/10.1016/j.econmod.2024.106837

Li, G., Miao, J., Jing, P., Chen, G., Mei, J., Sun, W., Lan, Y., Zhao, X., Qiu, X., Cao, Z., Huang, S., Zhu, Z., & Zhu, S. (2024). Development of predictive model for post-stroke depression at discharge based on decision tree algorithm : A multi-center hospital-based cohort study. Journal of Psychosomatic Research, 187(September), 111942. https://doi.org/10.1016/j.jpsychores.2024.111942

Nie, Y., Na, Y., & Chen, P. (2024). Is it a matter of governance or judicial favoritism ? Legal expertise at an executive level and its use in cases of corporate financial fraud. Finance Research Letters, 67(PB), 105888. https://doi.org/10.1016/j.frl.2024.105888

Rahman, M., Kamal, N., & Abdullah, N. F. (2024). Results in Engineering EDT-STACK : A stacking ensemble-based decision trees algorithm for tire tread depth condition classification. Results in Engineering, 22(December 2023), 102218. https://doi.org/10.1016/j.rineng.2024.102218

Wang, R., Sun, Y., Ni, J., & Zheng, H. (2024). Engineering Applications of Artificial Intelligence Identification of product definition patterns in mass customization by multi-information fusion weighted support vector machine. Engineering Applications of Artificial Intelligence, 137(PB), 109253. https://doi.org/10.1016/j.engappai.2024.109253

Xu, J., Yan, K., Deng, Z., Yang, Y., Liu, J., & Wang, J. (2024). Neurocomputing EEG-based epileptic seizure detection using deep learning techniques : A survey. 610(September).

Zhou, Y., Xiao, Z., Gao, R., & Wang, C. (2024). International Journal of Accounting Using data-driven methods to detect financial statement fraud in the real scenario. International Journal of Accounting Information Systems, 54(January), 100693. https://doi.org/10.1016/j.accinf.2024.100693

Zhu, Y., Gu, C., & Diaconeasa, M. A. (2024). A missing data processing method for dam deformation monitoring data using spatiotemporal clustering and support vector machine model. Water Science and Engineering, xxx. https://doi.org/10.1016/j.wse.2024.08.003