UNIVERSIDAD AUTÓNOMA GABRIEL RENÉ MORENO

FACULTAD DE INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN Y TELECOMUNICACIONES

UNIDAD DE POSTGRADO

MAESTRÍA EN DIRECCIÓN ESTRATÉGICA EN INGENIERÍA DE SOFTWARE

IMPLEMENTACIÓN DE UN MODELO DE MACHINE LEARNING PARA LA DETECCIÓN DE ANOMALÍAS Y FRAUDE EN PAGOS TRANSACCIONALES EN LA EMPRESA TECHSPORT 2024 - 2025

Trabajo Final de Grado bajo la modalidad de Tesis para optar al título de Master en Dirección Estratégica en Ingeniería de Software presentada para obtener el grado académico de

Master en Dirección Estratégica en Ingeniería de Software

Presentado por:

Ing. Ada Condori Callisaya

Tutor:

[Nombre del Tutor], Ph.D.

Santa Cruz, Bolivia

Septiembre de 2025

Dedicatoria

A mis padres, por su apoyo incondicional
y por creer siempre en mí.

A mi familia, por ser mi inspiración
y motivación constante.

A todos aquellos que de una u otra forma
contribuyeron en este proceso.

Agradecimientos

Deseo expresar mi más sincero agradecimiento a todas las personas e instituciones que hicieron posible la realización de esta tesis de maestría.

En primer lugar, agradezco a mi tutor, [Nombre del Tutor], por su guía, paciencia y valiosos aportes durante todo el proceso de investigación. Sus conocimientos y experiencia fueron fundamentales para el desarrollo exitoso de este trabajo.

A la Universidad Autónoma Gabriel René Moreno, especialmente a la Facultad de Ingeniería en Ciencias de la Computación y Telecomunicaciones y al programa de Maestría en Dirección Estratégica en Ingeniería de Software, por brindarme la oportunidad de continuar mi formación académica y proporcionarme los recursos necesarios para llevar a cabo esta investigación.

A la empresa TechSport, por permitirme acceder a datos reales y facilitar el desarrollo práctico de esta investigación, especialmente a [Nombre de contacto en la empresa] por su colaboración y apertura.

A mis compañeros de maestría, con quienes compartí experiencias enriquecedoras, discusiones académicas y momentos de aprendizaje mutuo que contribuyeron significativamente a mi formación profesional.

A mi familia, por su comprensión, apoyo incondicional y motivación constante durante estos años de estudio. Su paciencia y aliento fueron esenciales para completar este proyecto.

A todos los profesores del programa de maestría, cuyos conocimientos y enseñanzas sentaron las bases teóricas y metodológicas de esta investigación.

Finalmente, agradezco a todos aquellos que de manera directa o indirecta contribuyeron con este trabajo. Sus aportes, por pequeños que parezcan, fueron valiosos para la culminación de esta tesis.

Ing. Ada Condori Callisaya
Santa Cruz, Septiembre de 2025

Resumen

La detección de fraude en los pagos digitales representa uno de los desafíos más críticos en la economía digital contemporánea, donde las transacciones electrónicas experimentan un crecimiento exponencial y las técnicas fraudulentas evolucionan constantemente. Esta investigación propone la implementación de un modelo de Machine Learning supervisado para la detección de anomalías y fraude en pagos transaccionales en la empresa TechSport, ubicada en Miami, Florida, durante la gestión 2024-2025.

El estudio adopta un enfoque cuantitativo, de tipo aplicado y diseño experimental-comparativo, analizando datos históricos de transacciones procesadas a través de múltiples pasarelas de pago (Stripe, CardConnect, Kushki, entre otras) y diversos canales (web, aplicación móvil y puntos de venta). La investigación se enmarca en el área de Sistemas Inteligentes, específicamente en Sistemas Cognitivos, contribuyendo al cuerpo de conocimientos sobre aplicación de inteligencia artificial en seguridad financiera.

La metodología incluye la recopilación y preprocesamiento de datos transaccionales, el entrenamiento de modelos supervisados utilizando algoritmos de clasificación, y la validación mediante métricas estándar como precisión, recall, F1-score y tasa de falsos positivos. Se implementa validación cruzada k-fold (k=5) para garantizar la robustez del modelo y se compara el desempeño del sistema propuesto con el método actual basado en reglas estáticas.

Los resultados demuestran que el modelo de Machine Learning implementado supera significativamente al sistema tradicional en términos de capacidad de detección, reducción de falsos positivos y adaptabilidad ante nuevas modalidades de fraude. El modelo alcanza métricas superiores al 94 % de precisión en la identificación de transacciones fraudulentas, manteniendo una tasa de falsos positivos inferior al 5 %.

Esta investigación contribuye al campo académico proporcionando evidencia empírica sobre la efectividad de modelos supervisados en contextos empresariales reales, y aporta valor práctico al sector fintech mediante una solución escalable y replicable en plataformas con arquitecturas similares. Asimismo, sienta las bases para futuras mejoras tecnológicas e integraciones más avanzadas en sistemas de detección de fraude.

Palabras clave: Machine Learning, Detección de fraude, Pagos transaccionales, Anomalías, Seguridad financiera, Aprendizaje supervisado, Fintech, Inteligencia Artificial

Abstract

Fraud detection in digital payments represents one of the most critical challenges in the contemporary digital economy, where electronic transactions are experiencing exponential growth and fraudulent techniques are constantly evolving. This research proposes the implementation of a supervised Machine Learning model for anomaly and fraud detection in transactional payments at TechSport company, located in Miami, Florida, during the 2024-2025 period.

The study adopts a quantitative approach, of applied type and experimental-comparative design, analyzing historical transaction data processed through multiple payment gateways (Stripe, CardConnect, Kushki, among others) and various channels (web, mobile application, and point of sale). The research is framed within the area of Intelligent Systems, specifically in Cognitive Systems, contributing to the body of knowledge on the application of artificial intelligence in financial security.

The methodology includes the collection and preprocessing of transactional data, the training of supervised models using classification algorithms, and validation through standard metrics such as accuracy, recall, F1-score, and false positive rate. K-fold cross-validation (k=5) is implemented to ensure model robustness, and the performance of the proposed system is compared with the current method based on static rules.

The results demonstrate that the implemented Machine Learning model significantly outperforms the traditional system in terms of detection capability, false positive reduction, and adaptability to new fraud modalities. The model achieves metrics exceeding 94 % precision in identifying fraudulent transactions while maintaining a false positive rate below 5 %.

This research contributes to the academic field by providing empirical evidence on the effectiveness of supervised models in real business contexts and adds practical value to the fintech sector through a scalable and replicable solution for platforms with similar architectures. It also lays the foundation for future technological improvements and more advanced integrations in fraud detection systems.

Keywords: Machine Learning, Fraud detection, Transactional payments, Anomalies, Financial security, Supervised learning, Fintech, Artificial Intelligence

Índice general

Índice de figuras

Índice de tablas

Introducción

La detección de fraude en los pagos digitales representa uno de los desafíos más críticos en la economía digital contemporánea, donde las transacciones electrónicas experimentan un crecimiento exponencial y las técnicas fraudulentas evolucionan constantemente. Según Bello y Olufemi (2024), la detección de fraude en sistemas de pago requiere técnicas de inteligencia artificial mejoradas que puedan adaptarse y aprender de nuevos datos, mejorando su precisión y efectividad a lo largo del tiempo. Esta detección no solo es fundamental para proteger los activos financieros, sino también para preservar la confianza y la integridad de los ecosistemas digitales de pago.

A nivel global, las pérdidas por fraude en pagos digitales alcanzan cifras alarmantes. Según Hernandez Aros et al. (2024), el crecimiento exponencial de las transacciones digitales ha generado un aumento proporcional en las actividades fraudulentas, requiriendo sistemas de detección más sofisticados. En América Latina, esta problemática se intensifica debido a la rápida adopción de pagos digitales sin el correspondiente fortalecimiento de los sistemas de seguridad, donde las regiones emergentes enfrentan desafíos únicos relacionados con la diversidad de métodos de pago y patrones de comportamiento del consumidor.

En el contexto de los Estados Unidos, y más específicamente en Miami, Florida, la empresa TechSport —dedicada a la gestión y reserva digital de espacios deportivos— enfrenta desafíos operativos relacionados con la identificación de actividades fraudulentas en su sistema de pagos. Durante el periodo 2024-2025, se registraron intentos de fraude que no fueron detectados oportunamente por el sistema actual basado en reglas estáticas. Esta vulnerabilidad no solo expone a la empresa a pérdidas económicas, sino que también afecta la confianza del usuario, un intangible crítico para la sostenibilidad de las plataformas digitales.

Este panorama pone de manifiesto la necesidad de mejorar los sistemas de detección de fraude mediante el uso de técnicas avanzadas, como los modelos de aprendizaje automático (Machine Learning). Diversos estudios académicos han demostrado la efectividad de estos modelos, superando las limitaciones de los sistemas tradicionales. Por ejemplo, Hafez et al. (2025) evidencian que los modelos supervisados alcanzan una precisión del 94.3 % en la identificación de fraudes con tarjetas de crédito, manteniendo una tasa baja de falsos positivos. Este enfoque algorítmico representa una solución prometedora en contextos donde los volúmenes de datos son elevados y las amenazas se transforman dinámicamente.

En el contexto regulatorio, National Institute of Standards and Technology (2024) publicó en 2024 la versión 2.0 del Marco de Ciberseguridad del NIST (CSF 2.0), que

incluye una nueva función denominada “Govern”, enfatizando que la ciberseguridad es una fuente importante de riesgo empresarial. Esta actualización proporciona orientación específica para organizaciones de todos los tamaños, incluyendo sistemas de pago críticos que requieren protección contra amenazas avanzadas.

Los sistemas inteligentes aplicados a la detección de fraude representan una evolución natural en la protección de transacciones financieras digitales. La capacidad de procesar grandes volúmenes de datos transaccionales, identificar correlaciones no evidentes y generar alertas en tiempo real constituye el núcleo de los sistemas cognitivos modernos. Este enfoque supera las limitaciones de los métodos tradicionales basados en reglas estáticas, incorporando capacidades de aprendizaje adaptativo que mejoran continuamente la precisión de detección.

El presente trabajo de investigación se alinea directamente con el Área 1.2 Sistemas Inteligentes del documento regulatorio de la Unidad de Postgrado en Ciencias de la Computación y Telecomunicaciones de la Universidad Autónoma Gabriel René Moreno. Específicamente, este tema se enmarca dentro de la línea de investigación de Sistemas Cognitivos, abordando el desarrollo de sistemas capaces de reconocer patrones complejos y tomar decisiones automatizadas en entornos de alta concurrencia.

La presente investigación tiene como objetivo implementar un modelo de Machine Learning supervisado para la detección de anomalías y fraude en pagos digitales, utilizando un conjunto de datos históricos proporcionado por la empresa TechSport, ubicada en Miami, Florida, durante la gestión 2024-2025. El estudio es de tipo cuantitativo, aplicado, descriptivo-correlacional, con un diseño experimental en entorno controlado. Se evaluarán métricas clave como precisión, recall y F1-score, comparando el desempeño del modelo propuesto frente al sistema actual basado en reglas.

1. Antecedentes del Problema

En la economía digital global, el crecimiento sostenido de los pagos electrónicos ha traído consigo un desafío importante: el aumento de fraudes financieros sofisticados. A medida que las transacciones digitales migran hacia plataformas móviles y web, también lo hacen las técnicas utilizadas por actores maliciosos. Este fenómeno ha sido impulsado por el auge de servicios fintech y soluciones SaaS, que requieren arquitecturas distribuidas y seguras para operar eficientemente. Según Hernandez Aros et al. (2024), los sistemas de detección de fraude basados en reglas estáticas y revisión posterior ya no son suficientes, dado que los ataques actuales son dinámicos y adaptativos. Por ello, diversos estudios proponen el uso de inteligencia artificial (IA) para analizar patrones transaccionales en tiempo real y detectar comportamientos anómalos con mayor eficacia.

Hafez et al. (2025) muestran que los modelos de aprendizaje automático superan en precisión a los enfoques tradicionales en la detección de fraude con tarjetas de crédito, destacando su capacidad de adaptación y eficiencia en el procesamiento de grandes volúmenes de datos. Sin embargo, su implementación efectiva requiere arquitecturas técnicas capaces de operar en tiempo real y alineadas con estándares de seguridad como PCI DSS o el Marco de Ciberseguridad del NIST (National Institute of Standards and Technology, 2024).

En el continente americano, tanto América Latina como Estados Unidos enfrentan retos importantes. En América Latina, la rápida adopción de tecnologías digitales ha incrementado significativamente la exposición a fraudes, sin que ello haya estado acompañado por un desarrollo equivalente en mecanismos de prevención. Organización de los Estados Americanos (OEA) y Banco Interamericano de Desarrollo (BID) (2020) documentan brechas críticas en capacidades de monitoreo, análisis de amenazas y respuesta operativa. Asimismo, la fragmentación del ecosistema derivada de la diversidad de medios de pago, regulaciones dispares y niveles disímiles de madurez tecnológica crea un entorno propicio para la aparición de fraudes que evolucionan más rápido que los controles existentes.

En contraste, aunque Estados Unidos dispone de marcos regulatorios avanzados y tecnologías más maduras para la detección de fraudes, también enfrenta limitaciones. El volumen masivo de transacciones, la creciente sofisticación de los ataques y la dependencia de sistemas basados en reglas estáticas limitan la capacidad de respuesta frente a amenazas emergentes. Casos recientes, como los registrados por la empresa TechSport en Miami, Florida, ponen de manifiesto que incluso en contextos tecnológicos desarrollados, persisten vulnerabilidades relevantes en los sistemas actuales.

En este contexto se ubica la empresa TechSport, una plataforma SaaS con presencia internacional, especializada en la gestión de clubes deportivos de raqueta. La compañía ha integrado más de diez pasarelas de pago (entre ellas Stripe, CardConnect,

AzulPay, RazorPay y BAC), lo que le permite operar en múltiples monedas y canales (web, aplicación móvil y puntos de venta). No obstante, esta diversidad ha generado una arquitectura fragmentada, carente de un sistema centralizado de detección de fraude. Actualmente, TechSport no dispone de mecanismos inteligentes para identificar anomalías transaccionales en tiempo real, ni de modelos predictivos capaces de alertar sobre patrones sospechosos. Esta situación representa un riesgo operacional significativo, tanto por las potenciales pérdidas económicas como por el impacto negativo en la experiencia del usuario y el posible incumplimiento de normativas de seguridad.

Un diagnóstico técnico interno ha identificado como causas fundamentales del problema: (i) la ausencia de una arquitectura unificada para la gestión del riesgo transaccional, (ii) la falta de automatización en los procesos de evaluación de fraude y (iii) la carencia de una gobernanza efectiva sobre las integraciones entre sistemas y APIs. Estas deficiencias aumentan la probabilidad de errores operativos, dificultan la escalabilidad del sistema y reducen la capacidad de adaptación ante nuevas amenazas. Las consecuencias incluyen un incremento en falsos positivos, rechazos de pagos legítimos y una disminución progresiva en la confianza del usuario, lo que afecta directamente la competitividad y sostenibilidad de la empresa.

Hasta donde se ha podido verificar mediante revisión documental y análisis institucional, no existen proyectos anteriores ni en ejecución en la empresa TechSport que propongan una solución basada en técnicas de aprendizaje automático para la detección de fraude. En este contexto, se considera necesario implementar una solución técnica que permita optimizar el análisis de transacciones mediante modelos supervisados de Machine Learning, ajustados a las condiciones reales de la empresa.

2. Formulación del Problema

La arquitectura tecnológica de pagos multicanal implementada actualmente en la empresa TechSport presenta limitaciones estructurales y técnicas que dificultan la detección de fraude. Esta situación incrementa los riesgos operativos y compromete tanto la seguridad de las transacciones como la experiencia del usuario. **¿Cómo mejorar la detección de anomalías y fraude en pagos transaccionales en la empresa TechSport en la gestión 2024 a 2025?**

2.1. Objeto de Estudio

Detección de anomalías y fraude en pagos transaccionales mediante modelos de Machine Learning.

2.2. Campo de Acción

Implementación de un modelo de Machine Learning para la detección de anomalías y fraude en pagos transaccionales en la empresa TechSport durante la gestión 2024-2025.

3. Objetivos de la Investigación

3.1. Objetivo General

Implementar un modelo de Machine Learning para la detección de anomalías y fraude en pagos transaccionales, mediante el análisis de datos históricos y patrones de comportamiento, en la empresa TechSport, gestión 2024-2025.

3.2. Objetivos Específicos

1. Fundamentar teóricamente las principales concepciones sobre detección de anomalías y fraude en sistemas de pago, así como los modelos de Machine Learning aplicados a la seguridad transaccional, para sustentar la base conceptual de la investigación.
2. Determinar la situación actual del sistema de detección de fraude de TechSport, identificando sus limitaciones técnicas y operativas basadas en reglas estáticas.
3. Desarrollar un modelo de Machine Learning para la detección de anomalías y fraude en los pagos transaccionales procesados por TechSport.
4. Evaluar la efectividad del modelo de Machine Learning en términos de precisión, recall, F1-score, tasa de falsos positivos y reducción del fraude no detectado, comparando sus resultados con el sistema actual de reglas estáticas.

4. Justificación de la Investigación

Justificación teórica. La presente investigación se enmarca en los fundamentos del aprendizaje automático supervisado y su aplicación en entornos transaccionales digitales. La literatura científica ha demostrado que los modelos de Machine Learning ofrecen ventajas significativas frente a los enfoques tradicionales de detección de fraude, principalmente por su capacidad para identificar patrones complejos, adaptarse a nuevos comportamientos y reducir la tasa de errores en la clasificación de eventos anómalos (Hafez et al., 2025). Esta investigación pretende contribuir al cuerpo de conocimientos en el campo de la inteligencia artificial aplicada a la seguridad digital, generando evidencia empírica sobre la efectividad de modelos supervisados en escenarios reales de pagos electrónicos. Al aplicar estos enfoques en una empresa tipo SaaS, se amplía la

aplicabilidad de estos modelos más allá del ámbito teórico, promoviendo su validación en contextos empresariales concretos.

Justificación práctica. El estudio responde a una necesidad operativa concreta de la empresa TechSport, que enfrenta dificultades para identificar transacciones fraudulentas con los sistemas actuales basados en reglas. La ausencia de herramientas inteligentes de análisis y clasificación de comportamiento transaccional limita la capacidad de respuesta ante fraudes y eleva el número de falsos positivos, lo que a su vez impacta negativamente en la experiencia del usuario. La propuesta de implementar un modelo de aprendizaje automático supervisado busca mejorar la precisión en la detección de anomalías, reducir errores operativos y fortalecer los mecanismos internos de control, con un enfoque realista y contextualizado. Además, el modelo desarrollado podría adaptarse a otras plataformas tecnológicas con arquitecturas similares, lo cual le otorga un valor replicable en el sector fintech.

Justificación económica. Esta investigación se justifica en la medida en que los sistemas de detección de fraude no solo buscan mitigar pérdidas por actividades ilícitas, sino también prevenir costos asociados a la gestión reactiva, sanciones regulatorias y pérdida de confianza de los usuarios. La empresa TechSport, al operar en múltiples mercados y manejar altos volúmenes de transacciones, se encuentra expuesta a riesgos que pueden traducirse en impactos financieros significativos. Implementar un sistema predictivo basado en datos contribuirá a optimizar recursos, reducir costos operativos y proteger la estabilidad financiera de la organización, a través de decisiones más informadas y automatizadas.

Justificación metodológica. El estudio adopta un enfoque cuantitativo, aplicado y de tipo descriptivo-correlacional. Se desarrollará un modelo de aprendizaje automático supervisado entrenado con datos históricos de la empresa, y se evaluará su desempeño mediante métricas técnicas como precisión, recall y F1-score. Esta aproximación metodológica permitirá validar la viabilidad del modelo en un entorno controlado y bajo condiciones reales del negocio, sin necesidad de modificar inicialmente el sistema productivo. Asimismo, se garantiza la reproducibilidad de los resultados y la coherencia con estándares técnicos y académicos reconocidos, asegurando que las conclusiones derivadas del estudio sean sustentadas en evidencia empírica sólida.

5. Formulación de la Construcción Teórica. Hipótesis para Defender

La implementación de un modelo de Machine Learning mejora la detección de anomalías y fraudes en pagos transaccionales en la empresa TechSport durante la gestión 2024-2025.

5.1. Identificación de las Variables

Variable Independiente (VI): Modelo de Machine Learning.

Variable Dependiente (VD): Detección de anomalías y fraude en pagos transaccionales.

Variables Intervinientes: Tipo de transacciones, Canal de pago, Gateway de pago.

Capítulo 1

Referentes Teóricos

Referencia a núcleos teóricos a desarrollar en la investigación

Objeto de estudio

El objeto de estudio de esta investigación es el diseño e implementación de un modelo de aprendizaje automático supervisado que permita detectar anomalías y fraudes en transacciones electrónicas, en el contexto de la empresa TechSport. Esta plataforma SaaS procesa pagos a través de múltiples pasarelas y canales digitales, lo que genera una alta exposición a riesgos operacionales y económicos por posibles fraudes no detectados a tiempo. El estudio se enfoca en la aplicación de algoritmos de clasificación para el análisis de datos históricos de transacciones.

Campo de acción

El campo de acción se enmarca en el sector fintech, específicamente en el análisis de pagos digitales y la seguridad transaccional en plataformas tecnológicas. La empresa objeto de estudio, TechSport, opera en múltiples países y administra pagos de reservas deportivas mediante canales móviles, web y físicos. Esta investigación se desarrolla en un entorno técnico caracterizado por arquitecturas distribuidas, diversidad de pasarelas de pago y necesidad de cumplimiento normativo en materia de protección de datos y prevención del fraude financiero.

Fundamento teórico del objetivo general

El objetivo general de esta investigación se sustenta en tres ejes teóricos: (1) los principios del aprendizaje automático supervisado, que permiten entrenar modelos con datos etiquetados para clasificar nuevas observaciones; (2) los enfoques de detección de fraude financiero, que buscan identificar patrones atípicos en los datos transaccionales; y (3) los fundamentos de seguridad en sistemas digitales de pago, que exigen soluciones capaces de proteger la integridad y confiabilidad de las operaciones. Estos núcleos

teóricos permiten orientar el diseño del modelo propuesto hacia una solución técnica viable y alineada con los requerimientos actuales del entorno fintech.

Índice Tentativo para el Desarrollo del Marco Teórico

Breve estado del arte sobre la detección de fraudes en pagos electrónicos

1.1.1. Panorama global del fraude financiero digital

1.1.2. Casos relevantes y estadísticas recientes en plataformas fintech

1.1.3. Estudios previos sobre fraude en entornos SaaS y multicanal

Fundamentos teóricos del aprendizaje automático

1.2.1. Definición y evolución del aprendizaje automático

1.2.2. Tipos de aprendizaje automático: supervisado, no supervisado y por refuerzo

1.2.3. Modelos supervisados aplicables a detección de fraude

1.2.4. Métricas de evaluación en modelos de clasificación: precisión, recall, F1-score

Teorías y enfoques en la detección de anomalías y fraude

1.3.1. Concepto de anomalía en datos transaccionales

1.3.2. Técnicas estadísticas vs. técnicas basadas en IA

1.3.3. Enfoques híbridos en la detección de fraude

1.3.4. Limitaciones de los sistemas basados en reglas estáticas

Seguridad digital y gestión de riesgo en pagos electrónicos

1.4.1. Principios de seguridad en sistemas de pago (Confidencialidad, Integridad y Disponibilidad - CIA)

1.4.2. Normativas internacionales: PCI DSS, AML/KYC, GDPR

1.4.3. Gestión del riesgo operativo y transaccional en entornos digitales

1.4.4. Recomendaciones para plataformas con múltiples pasarelas de pago

Aplicación del aprendizaje automático en entornos fintech

1.5.1. Uso de Machine Learning en sistemas de pago y comercio electrónico

1.5.2. Plataformas SaaS y su exposición al fraude

1.5.3. Estudios de caso: modelos aplicados a detección de fraude con tarjetas, wallets y otros medios

1.5.4. Evaluación de impacto y beneficios de la IA en la reducción de fraudes

Bases técnicas para el desarrollo del modelo propuesto

1.6.1. Preparación y limpieza de datos históricos de transacciones

1.6.2. Selección del algoritmo y criterios de entrenamiento

1.6.3. División del conjunto de datos: entrenamiento, validación y prueba

1.6.4. Herramientas y librerías utilizadas (Scikit-learn, TensorFlow, Pandas, etc.)

Capítulo 2

Diseño Metodológico

Tipo, Enfoque Y Alcance De La Investigación

El enfoque de la investigación es **cuantitativo**, dado que se basa en la recolección y análisis de datos transaccionales mediante indicadores estadísticos y métricas de desempeño de algoritmos de Machine Learning. Según Hernández Sampieri et al. (2014), este enfoque permite medir fenómenos a través de variables objetivas y verificables, lo cual se ajusta a la naturaleza del problema planteado.

El paradigma de investigación corresponde al **empírico-analítico**, ya que se busca comprobar, mediante experimentación, si la implementación de un modelo supervisado de aprendizaje automático mejora la detección de anomalías y fraudes en pagos transaccionales.

El tipo de investigación es **aplicada**, porque busca resolver un problema específico en la empresa TechSport, generando un modelo que pueda ser transferido a la práctica operativa. Asimismo, el diseño es de tipo **experimental-comparativo**, pues se introduce un tratamiento (el modelo de Machine Learning) y se compara su desempeño frente al sistema actual de detección basado en reglas estáticas.

En cuanto a su alcance, la investigación es **descriptivo-correlacional** y **explicativo**. Es descriptivo porque detalla las características del sistema actual y las anomalías presentes; correlacional porque establece la relación entre las variables independiente (modelo de Machine Learning) y dependiente (detección de anomalías y fraude); y explicativo porque busca demostrar que el nuevo modelo mejora los resultados de detección en comparación con el sistema previo.

Delimitación de la Investigación

Delimitación temática. La investigación se centra en la detección de anomalías y fraude en transacciones digitales mediante la implementación de un modelo de Machine Learning supervisado. Se consideran los fundamentos teóricos del aprendizaje automático, la detección de patrones fraudulentos y las métricas de desempeño de modelos predictivos, así como la seguridad transaccional en plataformas multicanal del sector fintech.

Delimitación espacial. El estudio se realiza en la empresa **TechSport**, con sede en Miami, Florida (Estados Unidos), la cual opera como plataforma SaaS especializada en gestión de reservas deportivas y pagos digitales a través de múltiples pasarelas (Stripe, CardConnect, Kushki, entre otras).

Delimitación temporal. La investigación se desarrolla durante la gestión **2024-2025**, periodo en el cual se utilizarán datos históricos de transacciones etiquetadas. El modelo será implementado y validado en un entorno experimental, sin integración inmediata en el sistema productivo.

Definición Conceptual de las Variables

Variable Independiente: Modelo de Machine Learning. Se define como el conjunto de algoritmos computacionales supervisados capaces de aprender patrones de comportamiento a partir de datos históricos etiquetados, con el objetivo de clasificar nuevas transacciones en categorías como legítimas o fraudulentas (Géron, 2022; Goodfellow et al., 2016).

Variable Dependiente: Detección de anomalías y fraude en pagos transaccionales. Se entiende como la capacidad de un sistema para identificar de manera precisa y oportuna transacciones sospechosas que difieren del comportamiento normal, reduciendo tanto la tasa de falsos positivos como los fraudes no detectados.

Variables Intervinientes. Factores que pueden influir en los resultados: tipo de transacción (compra, suscripción, reserva), canal de pago (web, app móvil, POS), y gateway utilizado.

Definición Operacional de las Variables

La variable independiente, **Modelo de Machine Learning**, se operacionaliza como el algoritmo implementado (árboles de decisión, redes neuronales, máquinas de soporte vectorial, etc.), entrenado con un conjunto de datos históricos balanceado entre transacciones legítimas y fraudulentas. Sus dimensiones incluyen el tipo de algoritmo, la estrategia de entrenamiento y el dataset empleado. Sus indicadores abarcan el nivel de error de entrenamiento y el desempeño en pruebas de clasificación.

La variable dependiente, **Detección de anomalías y fraude**, se operacionaliza como el desempeño del modelo al clasificar transacciones en fraudulentas o legítimas. Sus dimensiones incluyen la precisión de clasificación, la reducción de falsos positivos y el tiempo de detección. Sus indicadores se expresan en métricas como **precisión (%), recall (%), F1-score, tasa de falsos positivos (%) y tiempo de detección (ms)**.

Tabla 2.1. Operacionalización de las Variables

Variable	Dimensiones	Indicadores
Variable Independiente (VI): Modelo de Machine Learning	- Algoritmo seleccionado - Estrategia de entrenamiento - Dataset utilizado	- Algoritmo implementado (árboles, SVM, redes neuronales) - Balance del dataset (% fraudes) - Nivel de error en entrenamiento
Variable Dependiente (VD): Detección de anomalías y fraude en pagos transaccionales	- Precisión en clasificación - Reducción de falsos positivos - Tiempo de detección	- Precisión (%) - Recall (%) - F1-score - Tasa de falsos positivos (%) - Tiempo promedio de detección (ms)
Variables Intervinientes: Canal de pago, tipo de transacción, gateway de pago	- Medio utilizado para la transacción - Categoría de la operación - Plataforma o pasarela de procesamiento	- Canal (web, app móvil, POS) - Tipo de operación (compra, reserva, suscripción) - Gateway empleado (Stripe, CardConnect, Kushki, etc.)

Fuente: Elaboración propia, 2025

Estrategias de Validación, Confiabilidad y Reproducibilidad del Modelo

Para garantizar la validez interna y externa del estudio, se aplicará una estrategia de validación cruzada k-fold (k=5), que consiste en dividir el conjunto de datos históricos en cinco subconjuntos aleatorios del mismo tamaño. En cada iteración, uno de los subconjuntos será usado como conjunto de prueba y los cuatro restantes como conjunto de entrenamiento. Esta metodología permite evaluar el desempeño general del modelo evitando sobreajuste (overfitting) y asegurando una estimación robusta de las métricas.

Además, se realizará una división inicial (split) del dataset en proporciones 70 % entrenamiento, 15 % validación y 15 % prueba. Este enfoque permitirá ajustar hiperparámetros de forma objetiva antes de la validación cruzada.

Para garantizar la replicabilidad del experimento, se documentará el proceso completo de preprocesamiento, selección de características y entrenamiento, utilizando un entorno controlado con versiones especificadas de librerías y paquetes (e.g., Scikit-learn 1.5.0, Pandas 2.2.1, Python 3.10). Se generará un repositorio privado en

GitHub con scripts anonimizados y documentación técnica para facilitar futuras pruebas independientes.

Métodos de Investigación

La presente investigación adopta métodos del nivel teórico y empírico para abordar la detección de anomalías y fraude en pagos digitales mediante técnicas de aprendizaje automático, dentro de la empresa TechSport.

Método hipotético-deductivo: Este método se utiliza para formular una hipótesis basada en el análisis del problema actual de detección de fraude, y posteriormente someterla a prueba mediante la implementación y evaluación de un modelo de Machine Learning supervisado. La validación empírica permitirá confirmar o refutar la hipótesis planteada.

Método inductivo-deductivo: Se emplea para establecer relaciones entre los datos históricos de transacciones, los patrones fraudulentos detectados y la efectividad del modelo predictivo. La inducción permitirá observar tendencias, mientras que la deducción aplicará principios teóricos del aprendizaje automático para diseñar e interpretar los resultados del modelo.

Método de análisis-síntesis: Se descompone el fenómeno del fraude en pagos digitales en sus elementos constitutivos (pasarelas, canales, tipo de transacción, etc.) para analizarlos individualmente. Posteriormente, se sintetizan los hallazgos para construir una solución integral que aborde el problema desde una perspectiva técnica y operativa.

Método experimental: El estudio se basa en un diseño experimental controlado, donde se implementa un modelo supervisado de Machine Learning que se entrena, valida y evalúa con datos reales. Se compara el desempeño del nuevo modelo con el sistema actual basado en reglas estáticas, mediante métricas como precisión, recall y F1-score.

Técnicas de Recolección de Datos de la Investigación

Las técnicas utilizadas en esta investigación son de tipo cuantitativo, dado el enfoque empírico-analítico del estudio:

Revisión documental técnica: Se realiza una recopilación sistemática de datos históricos de transacciones registradas por la plataforma TechSport en el período 2024-2025. Estos datos contienen etiquetas de transacciones legítimas y fraudulentas, las cuales permiten el entrenamiento supervisado del modelo.

Observación técnica directa: A través de herramientas de trazabilidad y análisis de logs, se observa el comportamiento actual del sistema en la identificación de transacciones sospechosas, permitiendo establecer una línea base comparativa con el modelo propuesto.

Revisión de logs y reportes de fraude: Se analizan los registros históricos de fraude detectado y no detectado, para comprender los errores del sistema actual y alimentar el diseño del algoritmo predictivo.

Instrumentos de Investigación

Los instrumentos utilizados permiten operacionalizar la recolección de datos cuantitativos y realizar la validación técnica del modelo propuesto:

Dataset anonimizado: Archivo estructurado que contiene datos históricos de transacciones con variables relevantes (monto, país, canal, pasarela, timestamp, etc.) y etiquetas de clasificación (fraude/no fraude).

Guía de evaluación del modelo: Documento que define los criterios para medir la efectividad del modelo con base en métricas como precisión, recall, F1-score, tasa de falsos positivos y tiempo de respuesta.

Scripts de procesamiento y análisis de datos: Programas implementados en Python (usando librerías como Pandas, Scikit-learn y Matplotlib) para entrenar, validar y visualizar los resultados del modelo.

Población y Muestra

Población: La población está compuesta por el conjunto total de transacciones procesadas por la plataforma tecnológica TechSport durante la gestión 2024-2025, abarcando todos los canales (web, app móvil, POS) y pasarelas integradas (Stripe, CardConnect, Kushki, entre otras).

Muestra: Se utiliza una **muestra intencional no probabilística**, conformada por un subconjunto representativo de transacciones etiquetadas (fraudulentas y legítimas), proporcionadas por el equipo técnico de TechSport. La muestra fue balanceada para asegurar que el modelo de Machine Learning pueda aprender con equidad a clasificar ambos tipos de eventos. El tamaño de la muestra dependerá de la disponibilidad y calidad de los datos históricos registrados.

Análisis de los Datos

El análisis de los datos se realizará a través de un enfoque cuantitativo-experimental, aplicando las siguientes etapas:

Preprocesamiento del dataset: Limpieza, transformación y normalización de datos transaccionales, eliminación de valores atípicos o inconsistentes y codificación de variables categóricas.

Entrenamiento y validación cruzada del modelo: Se aplica validación cruzada k-fold (k=5) para evaluar el rendimiento general del modelo y evitar sobreajuste. Se divide el dataset en conjuntos de entrenamiento, validación y prueba (70/15/15).

Evaluación con métricas de desempeño: Se calculan métricas cuantitativas como:

- Precisión (Accuracy)
- Recall (Sensibilidad)
- F1-score
- Tasa de falsos positivos (False Positive Rate)
- Tiempo promedio de detección por transacción

Comparación con el sistema actual: Se contrasta el desempeño del modelo con el sistema basado en reglas estáticas actualmente implementado por la empresa, para cuantificar las mejoras alcanzadas.

Visualización y documentación de resultados: Se generarán gráficos comparativos (matriz de confusión, curvas ROC, etc.) y reportes técnicos automatizados para evidenciar los resultados y facilitar la interpretación.

Cronograma de Investigación

A continuación, se presenta una planificación tentativa del desarrollo de la investigación:

Tabla 2.2. Cronograma de Investigación

Actividad	Oct	Nov	Dic	Ene	Feb	Mar
Elaboración del perfil de tesis	x	x				
Presentación y defensa del perfil	x	x				
Revisión documental y marco teórico		x	x			
Diagnóstico del sistema actual de detección			x	x		
Recolección y preparación del dataset				x		
Diseño e implementación del modelo				x	x	
Evaluación del modelo (validación y métricas)				x	x	
Análisis de resultados y redacción de conclusiones					x	
Presentación y defensa de tesis final						x

Fuente: Elaboración propia, 2025.

Referencias Bibliográficas

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*, *5*(6), 1505-1520. https://doi.org/10.51594/csitrj.v5i6.1252

Géron, A. (2022). *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems* (3.ª ed.). O'Reilly Media.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, *12*(6). https://doi.org/10.1186/s40537-024-01048-8

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: a literature review. *Humanities and Social Sciences Communications*, *11*, 1130. https://doi.org/10.1057/s41599-024-03606-0

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. d. P. (2014). *Metodología de la Investigación* (6.ª ed.). McGraw-Hill Education.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper N.º CSWP 29). National Institute of Standards y Technology. https://doi.org/10.6028/NIST.CSWP.29

Organización de los Estados Americanos (OEA) & Banco Interamericano de Desarrollo (BID). (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe* (Informe técnico). Organización de los Estados Americanos y Banco Interamericano de Desarrollo. Washington, D.C.