SELECCIÓN DE MÉTODOS DEL NIVEL TEÓRICO E ÍNDICE TENTATIVO DE LOS FUNDAMENTOS TEÓRICOS REFERENCIALES

Introducción

El presente documento tiene como propósito identificar y justificar los métodos del nivel teórico que proporcionan el sustento científico al proyecto de investigación *"Implementación de un Modelo de Machine Learning para la detección de Anomalías y fraude en pagos transaccionales en la empresa TechSport, gestión 2024–2025"*. Adicionalmente, se presenta la estructura preliminar del marco teórico referencial que orientará el análisis conceptual de la investigación.

Este trabajo contribuye al fortalecimiento del diseño metodológico del estudio, estableciendo vínculos coherentes entre el aparato teórico, los objetivos planteados y las variables definidas. Asimismo, asegura la solidez epistemológica y la relevancia operativa de la propuesta en el ámbito de la seguridad transaccional mediante algoritmos de aprendizaje automático.

1. Selección y fundamentación de los métodos del nivel teórico

El desarrollo de una investigación científica requiere la aplicación de métodos teóricos que organicen el razonamiento lógico y orienten la construcción del conocimiento. Para este estudio se han identificado cuatro métodos del nivel teórico que, de manera complementaria, facilitan el análisis crítico de las fuentes, la síntesis conceptual, el diseño del modelo computacional y la comprobación empírica de la hipótesis planteada en el contexto de la detección inteligente de fraude transaccional.

Método teórico	**Descripción**	**Fundamentación y pertinencia**
Analítico–Sintético	Posibilita la desagregación de los marcos conceptuales del aprendizaje automático, las metodologías de identificación de fraude y los estándares de protección transaccional (NIST CSF 2.0, PCI DSS) en sus componentes fundamentales, para posteriormente articular una propuesta coherente aplicable al entorno operativo de TechSport.	Se alinea con el **Objetivo Específico 1**, orientado a construir la base teórica sobre detección de anomalías y fraude en medios de pago digitales. Facilita la descomposición de conceptos complejos del Machine Learning y su posterior integración en un enfoque aplicado a la seguridad de transacciones.
Inductivo–Deductivo	Articula la observación de situaciones específicas en el contexto de TechSport (sistema vigente basado en reglas predefinidas) con teorías generales del aprendizaje supervisado y taxonomías de fraude respaldadas por evidencia científica, permitiendo transitar desde lo particular hacia lo universal y viceversa.	Respalda el **Objetivo Específico 2**, dirigido a caracterizar la situación actual de los mecanismos de detección de fraude en la empresa, revelando debilidades técnicas y funcionales, y derivando principios transferibles desde los fundamentos teóricos del Machine Learning hacia el caso concreto.

Método teórico	**Descripción**	**Fundamentación y pertinencia**
Modelación	Facilita la construcción de una abstracción formal y ejecutable del sistema inteligente de detección, incorporando algoritmos supervisados, atributos predictivos, indicadores de rendimiento y flujos de aprendizaje y prueba que representen la realidad operativa de manera simplificada pero rigurosa.	Da soporte al **Objetivo Específico 3**, enfocado en desarrollar el modelo de Machine Learning para detección de fraude. Permite diseñar una arquitectura conceptual sólida, con fundamento algorítmico y ajustada a las necesidades específicas del ecosistema transaccional de TechSport.
Hipotético–Deductivo	Permite someter a prueba la hipótesis formulada mediante diseño experimental, comparando el rendimiento del modelo inteligente propuesto versus el sistema tradicional mediante indicadores cuantitativos objetivos (precisión, exhaustividad, F1-score, ratio de falsos positivos).	Respalda el **Objetivo Específico 4**, centrado en evaluar la efectividad del modelo de Machine Learning. Garantiza la validación científica mediante contrastación empírica de los resultados obtenidos por ambos sistemas, aportando evidencia para confirmar o rechazar la hipótesis de superioridad del enfoque inteligente.

La selección conjunta de estos cuatro métodos responde a una estrategia metodológica integral que articula el trabajo teórico-conceptual con la validación experimental y el desarrollo aplicado. Su aplicación combinada fortalece la rigurosidad científica del estudio y asegura que el modelo de Machine Learning propuesto posea fundamento epistemológico sólido, relevancia práctica demostrable y capacidad de transferencia hacia otros contextos similares en el sector fintech.

2. Índice tentativo de los fundamentos teóricos referenciales

La construcción del marco teórico referencial se organiza mediante cinco ejes conceptuales que proporcionan los fundamentos epistemológicos, teóricos y metodológicos necesarios para el diseño, desarrollo y validación del modelo inteligente de detección de anomalías y fraude en transacciones digitales.

2.1. Estado del arte sobre la detección de fraude en pagos electrónicos

1. Panorama global del fraude financiero digital
    a) Evolución histórica del fraude en sistemas de pago
    b) Estadísticas recientes y tendencias globales
    c) Impacto económico del fraude en plataformas fintech
2. Estudios previos sobre fraude en entornos SaaS y multicanal
    a) Casos relevantes en plataformas de pago digital
    b) Vulnerabilidades en arquitecturas distribuidas
    c) Patrones de fraude en transacciones electrónicas
3. Marcos normativos y estándares de seguridad transaccional
    a) NIST Cybersecurity Framework (CSF) 2.0
    b) Payment Card Industry Data Security Standard (PCI DSS)
    c) Regulaciones AML/KYC y protección de datos (GDPR)

2.2. Fundamentos teóricos del aprendizaje automático

1. Definición y evolución del aprendizaje automático
    a) Conceptos fundamentales de Machine Learning
    b) Relación con la inteligencia artificial y ciencia de datos
    c) Desarrollo histórico y estado actual
2. Tipos de aprendizaje automático
    a) Aprendizaje supervisado
    b) Aprendizaje no supervisado

c) Aprendizaje por refuerzo

d) Aprendizaje semi-supervisado

3. Modelos supervisados aplicables a detección de fraude

a) Regresión logística

b) Árboles de decisión y Random Forest

c) Máquinas de vectores de soporte (SVM)

d) Redes neuronales artificiales

e) Gradient Boosting (XGBoost, LightGBM)

4. Métricas de evaluación en modelos de clasificación

a) Precisión (Precision), exhaustividad (Recall) y exactitud (Accuracy)

b) F1-score y curva ROC-AUC

c) Matriz de confusión

d) Manejo de clases desbalanceadas

2.3. Teorías y enfoques en la detección de anomalías y fraude

1. Concepto de anomalía en datos transaccionales

a) Definiciones y tipologías de anomalías

b) Diferencia entre anomalía, outlier y fraude

c) Características de transacciones fraudulentas

2. Técnicas estadísticas vs. técnicas basadas en IA

a) Métodos estadísticos tradicionales

b) Ventajas de los modelos de Machine Learning

c) Comparación de desempeño y escalabilidad

3. Enfoques híbridos en la detección de fraude

a) Combinación de reglas estáticas y modelos adaptativos

b) Sistemas de detección en tiempo real vs. batch

c) Análisis de comportamiento y perfiles de usuario

4. Limitaciones de los sistemas basados en reglas estáticas

a) Rigidez ante nuevos patrones de fraude

b) Altas tasas de falsos positivos

c) Dificultad de mantenimiento y escalabilidad

2.4. Seguridad digital y gestión de riesgo en pagos electrónicos

1. Principios de seguridad en sistemas de pago
    a) Triada CIA: Confidencialidad, Integridad y Disponibilidad
    b) Autenticación y autorización
    c) No repudio y trazabilidad
2. Gestión del riesgo operativo y transaccional
    a) Identificación y evaluación de riesgos
    b) Estrategias de mitigación
    c) Monitoreo continuo y respuesta a incidentes
3. Arquitecturas de seguridad en plataformas multicanal
    a) Integración segura de múltiples pasarelas de pago
    b) Tokenización y cifrado de datos sensibles
    c) Auditoría y logging de transacciones

2.5. Aplicación del aprendizaje automático en entornos fintech

1. Uso de Machine Learning en sistemas de pago y comercio electrónico
    a) Casos de éxito en la industria
    b) Modelos implementados por PayPal, Stripe y otras plataformas
    c) Beneficios operativos y económicos
2. Plataformas SaaS y su exposición al fraude
    a) Características de las plataformas SaaS multicanal
    b) Vectores de ataque específicos
    c) Estrategias de protección basadas en ML
3. Estudios de caso: modelos aplicados a detección de fraude
    a) Fraude con tarjetas de crédito
    b) Fraude en wallets digitales
    c) Fraude en transacciones móviles
4. Herramientas y tecnologías para el desarrollo del modelo
    a) Librerías de Python: Scikit-learn, TensorFlow, Keras

b) Frameworks para análisis de datos: Pandas, NumPy

c) Plataformas de visualización: Matplotlib, Seaborn

d) Entornos de experimentación: Jupyter Notebooks

La estructura presentada constituye la arquitectura conceptual preliminar del marco teórico, organizando de manera sistemática los principales ámbitos de conocimiento que sustentan la investigación: fundamentos del aprendizaje automático supervisado, teorías sobre detección de comportamientos anómalos, seguridad en medios de pago digitales y aplicaciones prácticas de inteligencia artificial en el sector fintech. Este ordenamiento facilita la construcción progresiva de un corpus teórico sólido, coherente y pertinente al objeto de estudio.