FUNDAMENTOS TEÓRICOS REFERENCIALES

Implementación de un Modelo de Machine Learning para la Detección de Anomalías y Fraude en Pagos Transaccionales en la Empresa TechSport, 2024–2025

Introducción

El presente documento expone los fundamentos teóricos y referenciales que sustentan la investigación titulada *Implementación de un modelo de Machine Learning para la detección de anomalías y fraude en pagos transaccionales en la empresa TechSport, 2024–2025*. Estos fundamentos permiten establecer la base conceptual, teórica, contextual y normativa del estudio, garantizando coherencia científica y rigurosidad metodológica.

La estructura de este documento integra cuatro marcos de estudio avanzados: el marco conceptual, que delimita los términos clave de la investigación; el marco teórico, que presenta las teorías y modelos científicos aplicables; el marco contextual, que describe el entorno específico de aplicación; y el marco legal-normativo, que identifica las regulaciones y estándares pertinentes al dominio de estudio.

1. Marco Conceptual

El marco conceptual define los constructos fundamentales que estructuran la investigación, proporcionando claridad terminológica y delimitación semántica de los conceptos centrales.

Machine Learning (Aprendizaje Automático). Disciplina de la inteligencia artificial que desarrolla algoritmos capaces de aprender patrones a partir de datos históricos sin ser explícitamente programados para cada tarea específica (Géron, 2022). En el contexto de esta investigación, se refiere específicamente a técnicas supervisadas de clasificación binaria aplicadas a la identificación de transacciones fraudulentas.

Fraude en pagos transaccionales. Acción deliberada destinada a obtener beneficios económicos ilícitos mediante el uso no autorizado de medios de pago, información financiera o identidades digitales, comprometiendo la integridad y confianza de los sistemas de comercio electrónico (Baesens et al., 2015). Hernandez Aros et al. (2024) señalan que el fraude transaccional ha evolucionado desde esquemas simples hacia operaciones sofisticadas que explotan vulnerabilidades tecnológicas y comportamentales.

Anomalía transaccional. Evento o patrón en los datos de transacciones que se desvía significativamente del comportamiento esperado, pudiendo indicar intentos de fraude,

errores operativos o comportamientos legítimos atípicos que requieren verificación adicional. Baesens et al. (2015) distinguen entre anomalías puntuales (transacciones individuales atípicas), anomalías contextuales (transacciones normales en circunstancias inusuales) y anomalías colectivas (secuencias coordinadas de transacciones sospechosas).

Modelo predictivo supervisado. Algoritmo de aprendizaje automático entrenado mediante ejemplos etiquetados, donde cada instancia del conjunto de entrenamiento incluye tanto las características descriptivas como la categoría de clasificación correspondiente (Bishop, 2006). En detección de fraude, estos modelos aprenden a distinguir transacciones legítimas de fraudulentas utilizando datos históricos previamente clasificados.

Métricas de evaluación. Indicadores cuantitativos que miden el desempeño de los modelos de clasificación. Géron (2022) enfatiza que en contextos desbalanceados como la detección de fraude, donde las transacciones fraudulentas son minoritarias, resulta imprescindible utilizar métricas como precisión (precision), exhaustividad (recall) y F1-score en lugar de la exactitud convencional, que puede resultar engañosa.

2. Marco Teórico

El marco teórico articula las teorías y modelos científicos que fundamentan el diseño e implementación del sistema de detección de fraude basado en aprendizaje automático.

Teoría del aprendizaje automático supervisado

El aprendizaje supervisado constituye un paradigma computacional donde los algoritmos aprenden funciones de mapeo entre variables de entrada y salida a partir de conjuntos de datos etiquetados (Bishop, 2006). Géron (2022) establece que estos modelos buscan aproximar una función desconocida minimizando el error de predicción mediante procesos iterativos de optimización. En el dominio de detección de fraude, esto implica entrenar algoritmos con transacciones históricas clasificadas, permitiendo al sistema aprender patrones distintivos de comportamiento fraudulento.

Goodfellow et al. (2016) amplían esta perspectiva mediante arquitecturas de aprendizaje profundo, que posibilitan la extracción automática de representaciones jerárquicas y la identificación de patrones complejos no lineales. Sin embargo, Hafez et al. (2025) advierten que la complejidad de estos modelos debe equilibrarse con requerimientos de interpretabilidad, especialmente en aplicaciones financieras donde la explicabilidad de las decisiones resulta crítica para el cumplimiento regulatorio.

Modelos de detección de anomalías

La detección de fraude puede conceptualizarse como un problema de identificación de anomalías, definidas como observaciones que se desvían significativamente de patro-

nes esperados (Baesens et al., 2015). Los autores distinguen entre enfoques estadísticos tradicionales (basados en umbrales y distribuciones probabilísticas) y técnicas contemporáneas de aprendizaje automático, que ofrecen mayor adaptabilidad y capacidad de generalización.

Hernandez Aros et al. (2024) documentan que los sistemas basados en reglas estáticas presentan limitaciones fundamentales ante la evolución dinámica de las técnicas fraudulentas, mientras que los modelos adaptativos de Machine Learning pueden actualizarse continuamente incorporando nuevos patrones de ataque. Feng y Kim (2024) desarrollan modelos novedosos que combinan múltiples algoritmos mediante técnicas de ensamblaje (ensemble learning), incrementando la robustez y reduciendo la sensibilidad a variaciones en los datos.

Teorías de evaluación en contextos desbalanceados

La evaluación de modelos de detección de fraude requiere consideraciones metodológicas especiales debido al desbalance inherente en los datos transaccionales (Murphy, 2022). El autor argumenta que métricas convencionales como la exactitud (accuracy) resultan inapropiadas cuando las clases presentan distribuciones asimétricas, recomendando el uso de precisión (minimiza falsos positivos), recall (maximiza detección de fraudes reales) y F1-score (equilibra ambos criterios).

3. Marco Contextual

El presente estudio se desarrolla en el contexto de TechSport, una plataforma SaaS especializada en gestión de reservas deportivas y procesamiento de pagos digitales, con sede principal en Miami, Florida, Estados Unidos, y operaciones en múltiples países de América Latina.

Caracterización de la empresa

TechSport opera como ecosistema tecnológico que integra más de diez pasarelas de pago (incluyendo Stripe, CardConnect, AzulPay, RazorPay y BAC), permitiendo procesar transacciones en múltiples monedas a través de canales web, aplicaciones móviles y puntos de venta físicos. Esta arquitectura distribuida multicanal, si bien facilita la escalabilidad operativa y cobertura geográfica, introduce complejidades significativas para la detección centralizada de fraude.

Problemática específica

Actualmente, TechSport no dispone de un sistema unificado de detección inteligente de fraude. La empresa opera con mecanismos fragmentados basados en reglas estáticas proporcionadas individualmente por cada pasarela de pago, lo que genera inconsistencias en los criterios de evaluación, altas tasas de falsos positivos (transacciones legítimas rechazadas incorrectamente) y fraudes no detectados que impactan la sostenibilidad financiera y la confianza del usuario.

El volumen transaccional procesado durante la gestión 2024-2025 y la diversidad de patrones de comportamiento entre diferentes mercados geográficos justifican la implementación de un sistema adaptativo basado en Machine Learning, capaz de aprender de los datos históricos de la plataforma y ajustarse dinámicamente a nuevos patrones de fraude emergentes.

4. Marco Legal y Normativo

La implementación de sistemas de detección de fraude debe alinearse con marcos regulatorios internacionales y nacionales que regulan la ciberseguridad, protección de datos y seguridad en medios de pago electrónicos.

Estándares internacionales de seguridad

PCI DSS (Payment Card Industry Data Security Standard). Estándar de seguridad establecido por las principales marcas de tarjetas de crédito que define requisitos obligatorios para organizaciones que almacenan, procesan o transmiten datos de tarjetas de pago. Incluye controles técnicos y organizacionales para prevenir fraude y proteger información financiera sensible.

ISO/IEC 27001. Norma internacional que especifica requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. Es aplicable a organizaciones que procesan datos financieros y transaccionales, proporcionando un marco estructurado para la gestión de riesgos de ciberseguridad.

NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology (2024) publicaron la versión actualizada del marco de ciberseguridad del NIST, incorporando la función “Govern” como eje transversal. Este marco proporciona orientación para organizaciones de todos los tamaños, incluyendo plataformas fintech, sobre cómo gestionar riesgos de ciberseguridad de manera integral, abarcando identificación, protección, detección, respuesta y recuperación ante incidentes.

Regulación de protección de datos

GDPR (General Data Protection Regulation). Reglamento europeo de protección de datos aplicable a organizaciones que procesan información de ciudadanos de la Unión Europea, independientemente de su ubicación geográfica. Establece principios de minimización de datos, limitación de finalidad, y derechos de los titulares de datos, incluyendo el derecho a la explicación de decisiones automatizadas (relevante para sistemas de ML).

Marco regulatorio boliviano

Ley 164 de Telecomunicaciones y Tecnologías de Información y Comunicación. Norma boliviana que regula el uso de tecnologías de información y comunicación, estableciendo obligaciones de seguridad, privacidad y protección de datos en servicios digitales. Aunque TechSport opera desde Estados Unidos, es pertinente considerar esta normativa si la empresa procesa transacciones de usuarios bolivianos.

Regulaciones de la Autoridad de Supervisión del Sistema Financiero (ASFI). En el contexto boliviano, las entidades que procesan pagos electrónicos deben cumplir con normativas emitidas por ASFI relacionadas con prevención de lavado de dinero, conocimiento del cliente (KYC) y seguridad en medios de pago electrónicos.

Conclusión

Los fundamentos teóricos referenciales presentados integran las dimensiones conceptual, teórica, contextual y normativa necesarias para sustentar científicamente la implementación de un modelo de Machine Learning en TechSport. La convergencia de teorías de aprendizaje automático, marcos normativos de ciberseguridad y el análisis del contexto operativo específico proporciona una base sólida para el diseño, desarrollo y validación del sistema propuesto, asegurando tanto rigor científico como viabilidad práctica y cumplimiento regulatorio.

Referencias Bibliográficas

Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection*. Wiley.

Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer-Verlag New York.

Feng, X., & Kim, S.-K. (2024). Novel Machine Learning Based Credit Card Fraud Detection Systems. *Mathematics*, *12*(12), 1869. https://doi.org/10.3390/math12121869

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

Murphy, K. P. (2022). *Probabilistic Machine Learning: An Introduction*. MIT Press.

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