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 desarrolla los fundamentos teóricos referenciales que sustentan la investigación sobre implementación de Machine Learning para detección de fraude en TechSport, 2024–2025. Siguiendo la metodología de Hernández Sampieri, se integran cuatro marcos que proporcionan solidez conceptual, empírica y normativa, respondiendo al **Objetivo Específico 1**: fundamentar teóricamente las concepciones sobre detección de anomalías, fraude en sistemas de pago y modelos de Machine Learning aplicados a seguridad transaccional.

1. Estado del Arte

El estado del arte constituye una revisión sistemática y crítica de las investigaciones previas desarrolladas sobre detección de fraude en pagos transaccionales mediante técnicas de inteligencia artificial y aprendizaje automático. Este análisis permite identificar los avances científicos, las metodologías empleadas, los vacíos de conocimiento existentes y el posicionamiento de la presente investigación en el contexto académico global.

1.1. Evolución histórica del campo de estudio

La detección automatizada de fraude transaccional ha experimentado una transformación sustancial durante las últimas dos décadas. Baesens et al. (2015) documentan que los primeros sistemas operaban mediante reglas estáticas basadas en umbrales predefinidos (montos máximos, frecuencia de transacciones, ubicaciones geográficas), lo cual resultaba efectivo ante esquemas de fraude simples pero demostraba rigidez ante tácticas fraudulentas evolutivas.

Lucas (2019) analiza la transición hacia enfoques adaptativos basados en aprendizaje automático, argumentando que la capacidad de los modelos para aprender patrones complejos a partir de datos históricos representa un salto cualitativo en la efectividad de detección. Esta evolución se aceleró durante la década de 2010–2020 con la disponibilidad de grandes volúmenes de datos transaccionales y el desarrollo de algoritmos de mayor poder computacional.

Estudios recientes de Hafez et al. (2025) y Hernandez Aros et al. (2024) confirman que la investigación contemporánea se centra en arquitecturas híbridas que combinan múltiples algoritmos (ensemble learning), incorporan procesamiento de lenguaje natural (Rodríguez et al., 2023) y utilizan redes neuronales de grafos para modelar relaciones complejas entre entidades (Cheng et al., 2025).

1.2. Matriz de referencias principales

La Tabla 1 sistematiza las veinte referencias científicas más relevantes que fundamentan esta investigación, clasificadas por tipo de fuente y aporte específico al estudio.

Tabla 1: Matriz de referencias principales sobre detección de fraude con Machine Learning

Referencia	**Aporte principal al estudio**	**Tipo**	**Año**
Géron (2022)	Fundamentos de algoritmos de ML supervisado y métricas de evaluación	Libro	2022
Bishop (2006)	Teoría estadística del aprendizaje y reconocimiento de patrones	Libro	2006
Baesens et al. (2015)	Metodologías específicas para analítica de fraude financiero	Libro	2015
Goodfellow et al. (2016)	Técnicas de deep learning aplicables a detección de anomalías	Libro	2016
Murphy (2022)	Enfoques probabilísticos y bayesianos en ML	Libro	2022
Hafez et al. (2025)	Revisión sistemática de técnicas de IA en fraude con tarjetas de crédito	Artículo	2025
Hernández Aros et al. (2024)	Literatura review sobre fraude financiero y ML	Artículo	2024
Feng & Kim (2024)	Modelos novedosos de ML para detección de fraude en tarjetas	Artículo	2024
Al-Khasawneh (2025)	Métodos híbridos de redes neuronales para fraude	Artículo	2025
Rodríguez et al. (2023)	Detección de fraude mediante procesamiento de lenguaje natural	Artículo	2023
Cheng et al. (2025)	Redes neuronales de grafos para detección de fraude financiero	Artículo	2025
Bello & Olufemi (2024)	IA en prevención de fraude: técnicas, aplicaciones y desafíos	Artículo	2024

Continúa en la página siguiente

Tabla 1 – Continuación de la página anterior

Referencia	Aporte principal al estudio	Tipo	Año
AlEmad (2022)	Detección de fraude con tarjetas usando KNN, SVM y regresión logística	Tesis	2022
Lucas (2019)	Fraude en tarjetas con integración de conocimiento contextual	Tesis PhD	2019
Chaquet (2022)	ML interpretable para detección de fraude crediticio	Tesis PhD	2022
Rayo (2020)	Prototipo de detección de fraude con IA en banco peruano	Tesis	2020
Pérez (2021)	Detección de transacciones fraudulentas con ML en Colombia	Tesis	2021
NIST (2024)	Framework de ciberseguridad CSF 2.0 con función "Govern"	Estándar	2024
OEA-BID (2020)	Ciberseguridad y fraude digital en América Latina	Reporte	2020
Dileep et al. (2023)	Detección de fraude financiero con técnicas de deep learning	Artículo	2023

1.3. Análisis de tesis doctorales y trabajos de maestría relacionados

El análisis de investigaciones previas revela diferentes enfoques metodológicos y contextos de aplicación que orientan el diseño del presente estudio.

Enfoque algorítmico supervisado. AlEmad (2022) desarrolló un modelo comparativo utilizando K-Nearest Neighbors (KNN), Support Vector Machines (SVM) y regresión logística aplicado a un dataset público de transacciones con tarjetas de crédito, concluyendo que los métodos de ensamblaje superan a algoritmos individuales. Esta investigación aporta antecedentes sobre selección y comparación de algoritmos supervisados.

Integración de conocimiento contextual. Lucas (2019) propone en su tesis doctoral la incorporación de información contextual secuencial (historial de transacciones del usuario, patrones temporales) además de características transaccionales individuales, logrando mejoras significativas en la tasa de detección. Este enfoque resulta relevante para el contexto de TechSport, donde los usuarios generan secuencias de transacciones a lo largo del tiempo.

Interpretabilidad y explicabilidad. Chaquet Ulldemolins (2022) enfatiza la necesidad de modelos interpretables en aplicaciones financieras, desarrollando técnicas de ML explicable (XAI) que permiten justificar las decisiones del sistema ante audi-

torías regulatorias. Este aspecto será considerado en la fase de evaluación del modelo propuesto.

Aplicaciones en contextos latinoamericanos. Las tesis de Rayo Mondragón (2020) en Perú y Pérez González (2021) en Colombia documentan implementaciones exitosas de modelos de Machine Learning en instituciones financieras de la región, validando la viabilidad técnica y operativa de estos sistemas en ecosistemas transaccionales similares al de TechSport.

1.4. Vacíos de conocimiento identificados

A pesar de los avances documentados, persisten áreas de oportunidad que justifican la presente investigación:

a) **Detección en arquitecturas multicanal distribuidas.** La mayoría de estudios analizan datos de una sola pasarela de pago, mientras que TechSport opera con más de diez pasarelas simultáneamente, requiriendo un enfoque unificado de detección.

b) **Contexto de plataformas SaaS deportivas.** Las investigaciones previas se concentran en banca tradicional y comercio electrónico general, existiendo escasa literatura sobre fraude en plataformas especializadas de reservas deportivas.

c) **Evaluación comparativa con sistemas basados en reglas.** Pocos estudios documentan comparaciones empíricas rigurosas entre el desempeño de sistemas tradicionales versus modelos inteligentes en entornos productivos reales.

1.5. Contextualización de la investigación

La presente investigación se desarrolla en TechSport, plataforma SaaS con sede en Miami, Florida, que opera en múltiples países de América Latina gestionando reservas deportivas y procesando pagos digitales. La empresa integra más de diez pasarelas de pago (Stripe, CardConnect, AzulPay, RazorPay, BAC, entre otras), procesando transacciones en múltiples monedas a través de canales web, móviles y puntos de venta físicos.

Actualmente, TechSport no dispone de un sistema centralizado de detección inteligente de fraude, operando con mecanismos fragmentados proporcionados individualmente por cada pasarela. Esta situación genera inconsistencias en criterios de evaluación, altas tasas de falsos positivos y fraudes no detectados que impactan la sostenibilidad financiera.

El volumen transaccional durante 2024-2025 y la diversidad de patrones de comportamiento entre mercados geográficos justifican la implementación de un modelo adaptativo basado en Machine Learning, alineado con los hallazgos de Hernandez Aros et al. (2024) sobre la superioridad de enfoques inteligentes frente a sistemas estáticos.

2. Marco Teórico Conceptual

El marco teórico conceptual articula los conceptos fundamentales y las teorías científicas que proporcionan sustento epistemológico a la investigación.

2.1. Definiciones conceptuales fundamentales

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 esta investigación se refiere 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 de los sistemas de comercio electrónico (Baesens et al., 2015).

Anomalía transaccional. Evento o patrón en los datos que se desvía significativamente del comportamiento esperado, pudiendo indicar intentos de fraude, errores operativos o comportamientos legítimos atípicos (Baesens et al., 2015). Se distinguen anomalías puntuales (transacciones individuales atípicas), contextuales (transacciones normales en circunstancias inusuales) y colectivas (secuencias coordinadas sospechosas).

Modelo predictivo supervisado. Algoritmo de aprendizaje automático entrenado mediante ejemplos etiquetados, donde cada instancia incluye características descriptivas y la categoría de clasificación (Bishop, 2006). En detección de fraude, estos modelos aprenden a distinguir transacciones legítimas de fraudulentas.

Métricas de evaluación. Indicadores cuantitativos que miden el desempeño de modelos de clasificación. Géron (2022) enfatiza que en contextos desbalanceados es imprescindible utilizar precisión (precision), exhaustividad (recall) y F1-score en lugar de exactitud convencional.

2.2. Definiciones operacionales de variables

Siguiendo los lineamientos metodológicos de Hernández Sampieri et al. (2014), se establecen las definiciones operacionales que especifican cómo se medirán las variables

de investigación en el contexto de TechSport.

Variable Dependiente: Detección de anomalías y fraude en pagos transaccionales. Se operacionaliza mediante indicadores cuantitativos de desempeño del modelo de clasificación:

- *Precisión (Precision):* Proporción de transacciones clasificadas como fraudulentas que efectivamente lo son. Medida: $Precision = \frac{VP}{VP+FP}$, donde VP = Verdaderos Positivos, FP = Falsos Positivos.
- *Exhaustividad (Recall):* Proporción de fraudes reales que el modelo detecta correctamente. Medida: $Recall = \frac{VP}{VP+FN}$, donde FN = Falsos Negativos.
- *F1-score:* Media armónica entre Precision y Recall. Medida: $F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$.
- *Tasa de Falsos Positivos:* Proporción de transacciones legítimas incorrectamente clasificadas como fraudulentas.
- *ROC-AUC:* Área bajo la curva ROC, evaluando capacidad discriminativa del modelo.

Variable Independiente: Modelo de Machine Learning. Se operacionaliza mediante:

- *Tipo de algoritmo:* Random Forest, Gradient Boosting o Regresión Logística.
- *Hiperparámetros:* Número de árboles, profundidad máxima, tasa de aprendizaje.
- *Características de entrada:* Variables numéricas y categóricas extraídas de transacciones.

Características transaccionales (features) consideradas:

- Monto de la transacción (continua)
- Hora del día (categórica: madrugada, mañana, tarde, noche)
- Día de la semana (categórica)
- Tipo de canal (categórica: web, móvil, punto de venta)
- Gateway de pago utilizado (categórica: Stripe, CardConnect, AzulPay, etc.)
- Moneda de la transacción (categórica)
- País de origen (categórica)

- Frecuencia de transacciones del usuario (continua)
- Tiempo transcurrido desde última transacción (continua)
- Monto promedio histórico del usuario (continua)

Estas definiciones operacionales fundamentan el **Objetivo Específico 1** (fundamentación teórica) y proporcionan criterios medibles para el **Objetivo Específico 4** (evaluación de efectividad).

2.3. 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 (fraudulentas/legítimas), permitiendo al sistema aprender patrones distintivos de comportamiento fraudulento. El proceso comprende tres fases: (1) entrenamiento, donde el modelo ajusta sus parámetros internos; (2) validación, que evalúa el desempeño en datos no vistos para prevenir sobreajuste; y (3) prueba, que mide la capacidad de generalización del modelo final.

2.4. Teoría 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 patrones 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.

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.

2.5. Teoría de evaluación en contextos desbalanceados

La evaluación de modelos de detección de fraude requiere consideraciones 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.

En contextos donde las transacciones fraudulentas representan menos del 1 % del total, un modelo trivial que clasifique todas las transacciones como legítimas alcanzaría 99 % de exactitud sin detectar ningún fraude. Por ello resulta imprescindible utilizar:

- **Precisión (Precision):** Minimiza falsos positivos, evitando el rechazo de transacciones legítimas.
- **Exhaustividad (Recall):** Maximiza la detección de fraudes reales, minimizando fraudes no detectados.
- **F1-score:** Equilibra ambos criterios mediante su media armónica.
- **ROC-AUC:** Evalúa el desempeño del modelo a través de diferentes umbrales de clasificación.

3. Marco Referencial

El marco referencial documenta aplicaciones prácticas, estudios de caso y herramientas tecnológicas que proporcionan evidencia empírica sobre la viabilidad y efectividad de sistemas de detección de fraude basados en Machine Learning.

3.1. Aplicaciones exitosas en la industria fintech

PayPal. Pionero en la implementación de sistemas inteligentes de detección de fraude, PayPal procesa cientos de millones de transacciones diarias utilizando modelos de aprendizaje profundo que analizan más de 1,000 características por transacción. Baesens et al. (2015) documentan que su sistema reduce las tasas de fraude por debajo del 0.32 % de las transacciones totales, superando significativamente a sistemas basados en reglas.

Análisis crítico: La experiencia de PayPal valida la superioridad de modelos inteligentes frente a sistemas estáticos. Sin embargo, su escala operativa (cientos de millones de transacciones) y recursos computacionales (análisis de 1,000+ características) difieren sustancialmente del contexto de TechSport. Para empresas de tamaño medio, resulta imprescindible adaptar el enfoque priorizando características discriminativas clave y arquitecturas eficientes que operen con volúmenes transaccionales moderados, sin comprometer la efectividad de detección.

Stripe. Esta pasarela de pago implementa modelos de ML adaptativos que aprenden continuamente de patrones de fraude emergentes. Bello y Olufemi (2024) destacan que Stripe actualiza sus modelos en tiempo real, incorporando retroalimentación de transacciones disputadas para mejorar progresivamente la precisión de detección.

Análisis crítico: El enfoque de aprendizaje continuo de Stripe representa un paradigma deseable pero técnicamente complejo. Su implementación requiere infraestructura de datos robusta, pipelines de reentrenamiento automatizados y mecanismos de validación en producción. Para TechSport, una estrategia realista consiste en implementar inicialmente un modelo estático validado, estableciendo posteriormente ciclos de reentrenamiento periódicos (mensuales o trimestrales) conforme se acumule suficiente retroalimentación etiquetada.

Mastercard Decision Intelligence. Utiliza redes neuronales recurrentes (RNN) y análisis de comportamiento histórico para evaluar cada transacción en milisegundos, reduciendo falsos positivos en un 50 % según reportes de la compañía citados por Feng y Kim (2024).

Análisis crítico: La reducción del 50 % en falsos positivos constituye un objetivo aspiracional para TechSport, considerando que los falsos positivos afectan directamente la experiencia del usuario legítimo. Arquitecturas RNN capturan secuencias temporales de comportamiento, pero requieren volúmenes históricos significativos por usuario. En el contexto de TechSport, donde usuarios nuevos generan transacciones sin historial previo, resulta preferible combinar modelos basados en características transaccionales individuales con análisis de comportamiento agregado cuando existan datos suficientes.

3.2. Estudios de caso específicos

Detección de fraude con tarjetas de crédito. Feng y Kim (2024) desarrollan un modelo híbrido que combina Random Forest y redes neuronales artificiales, logrando F1-score de 0.89 en un dataset público altamente desbalanceado (0.17 % de fraudes). Los autores identifican como características más predictivas: monto de la transacción, hora del día, distancia respecto a transacciones previas y frecuencia de uso.

Fraude en wallets digitales. Al-Khasawneh (2025) propone arquitecturas de redes neuronales híbridas (CNN-LSTM) que capturan tanto patrones espaciales como secuencias temporales de comportamiento, alcanzando 94 % de recall en la detección de fraudes en billeteras digitales.

Procesamiento de lenguaje natural en fraude. Rodríguez et al. (2023) demuestran que el análisis de descripciones textuales de transacciones (nombres de comercios, categorías de productos) mediante técnicas de NLP permite identificar esquemas fraudulentos que explotan nombres de comercios ficticios o categorías inusuales.

3.3. Modelos algorítmicos aplicables

Regresión logística. Algoritmo supervisado que estima la probabilidad de pertenencia a una clase mediante funciones logísticas. AlEmad (2022) documenta su efectividad en detección de fraude debido a su interpretabilidad y eficiencia compu-

tacional, siendo apropiado para entornos productivos que requieren predicciones en tiempo real.

Random Forest. Algoritmo de ensamblaje que combina múltiples árboles de decisión para mejorar robustez y reducir sobreajuste (Géron, 2022). Rayo Mondragón (2020) implementa este algoritmo en un banco peruano, logrando 91 % de precisión en detección de fraude con tarjetas.

Gradient Boosting (XGBoost, LightGBM). Técnicas de ensamblaje secuencial que construyen modelos iterativamente corrigiendo errores de modelos previos. Chaquet Ulldemolins (2022) demuestra que XGBoost alcanza desempeño superior en contextos desbalanceados mediante técnicas de ponderación de clases.

Redes neuronales artificiales. Modelos inspirados en estructuras biológicas capaces de aprender representaciones complejas no lineales (Goodfellow et al., 2016). Dileep et al. (2023) utilizan arquitecturas profundas (deep learning) que automatizan la extracción de características relevantes, eliminando la necesidad de ingeniería de atributos manual.

3.4. Análisis comparativo de modelos aplicables a TechSport

La selección de algoritmos apropiados para el contexto específico de TechSport requiere un análisis comparativo que considere las características operativas de la empresa: volumen transaccional moderado, arquitectura multicanal distribuida y necesidad de interpretabilidad ante auditorías. La Tabla 2 sistematiza ventajas, desventajas y aplicabilidad de cada enfoque algorítmico al contexto de TechSport.

Este análisis fundamenta la selección de Random Forest como modelo principal para el Objetivo Específico 3 (desarrollo del modelo), complementado con Regresión Logística como baseline y XGBoost para validación de desempeño superior. Las redes neuronales se reservan como línea futura de investigación cuando el volumen de datos históricos sea mayor.

3.5. Conexión con los objetivos de investigación

Los modelos algorítmicos, estudios de caso y aplicaciones documentadas en este Marco Referencial proporcionan sustento empírico para el **Objetivo Específico 3**: *Desarrollar un modelo de Machine Learning para la detección de anomalías y fraude en los pagos transaccionales procesados por TechSport.* La evidencia revisada demuestra que Random Forest y Gradient Boosting han sido implementados exitosamente en contextos similares (instituciones financieras latinoamericanas, plataformas de comercio electrónico), validando su viabilidad técnica y efectividad en entornos con características desbalanceadas y requerimientos de tiempo real.

Tabla 2: Comparación de algoritmos de Machine Learning para detección de fraude en TechSport

Algoritmo	**Ventajas**	**Desventajas**	**Aplicabilidad a TechSport**
Regresión Logística	Alta interpretabilidad; eficiencia computacional; predicciones en tiempo real	Limitada capacidad para capturar relaciones no lineales complejas	Alta. Apropiado para prototipo inicial y baseline de comparación. Facilita auditorías regulatorias.
Random Forest	Robusto ante sobreajuste; maneja datos desbalanceados; importancia de características	Mayor costo computacional; menor interpretabilidad que regresión logística	Alta. Balance óptimo entre desempeño y complejidad para volumen transaccional de TechSport.
Gradient Boosting (XGBoost)	Desempeño superior en datasets desbalanceados; ponderación de clases; regularización	Requiere ajuste fino de hiperparámetros; riesgo de sobreajuste	Media-Alta. Recomendado para fase de optimización posterior al modelo base.
Redes Neuronales	Captura patrones complejos; aprendizaje automático de características	Requiere grandes volúmenes de datos; baja interpretabilidad; alto costo computacional	Baja-Media. Volumen transaccional actual de TechSport puede ser insuficiente para entrenar arquitecturas profundas efectivamente.

Adicionalmente, los estudios de interpretabilidad y explicabilidad documentados fundamentan el **Objetivo Específico 4**: *Evaluar la efectividad del modelo*, proporcionando referencias metodológicas para seleccionar métricas apropiadas (Precision, Recall, F1-score, ROC-AUC) y establecer protocolos de validación rigurosos que permitan comparar el desempeño del modelo propuesto contra el sistema actual basado en reglas estáticas.

4. Marco Normativo

El marco normativo identifica las regulaciones, estándares y principios legales que enmarcan la implementación de sistemas de detección de fraude en medios de pago electrónicos, garantizando cumplimiento regulatorio y protección de derechos.

La construcción de este marco sigue los lineamientos metodológicos propuestos por Arias Odón (2016), quien establece que las bases legales o marco normativo constituyen el conjunto de normas, leyes, reglamentos y disposiciones jurídicas que regulan y fundamentan la investigación, proporcionando el sustento legal necesario para el desarrollo del proyecto. Complementariamente, Bernal Torres (2016) señala que el marco referencial debe incluir el sustento legal que enmarca el fenómeno de estudio, proporcionando legitimidad institucional y viabilidad jurídica a la propuesta de investigación.

Siguiendo los principios de Hernández Sampieri et al. (2014), este marco normativo se centra exclusivamente en la legislación **directamente pertinente** al contexto operativo de TechSport, empresa con sede en Miami, Florida, Estados Unidos. La pertinencia y coherencia entre el problema de investigación, los objetivos planteados y el sustento legal presentado constituyen criterios fundamentales para garantizar rigurosidad metodológica, evitando la inclusión de normativa no aplicable al objeto de estudio.

4.1. Marco regulatorio federal de Estados Unidos

Federal Trade Commission Act (FTC Act) - 15 U.S.C. § 41 et seq. Establece la autoridad de la FTC para prevenir prácticas comerciales desleales en transacciones electrónicas, requiriendo procedimientos de autorización y protección contra fraude en sistemas de pago digital.

Electronic Fund Transfer Act (EFTA) - 15 U.S.C. § 1693 et seq. Regula derechos y responsabilidades en transferencias electrónicas de fondos, estableciendo límites de responsabilidad por transacciones no autorizadas y requiriendo procedimientos específicos de contabilidad y resolución de errores.

Gramm-Leach-Bliley Act (GLBA) - 15 U.S.C. § 6801 et seq. Ley federal de 1999 que regula protección de información financiera de consumidores mediante

reglas de privacidad (notificación y limitación de divulgación), salvaguardas de seguridad (actualizada en 2023 con controles más estrictos) y prohibición de pretextos fraudulentos.

California Consumer Privacy Act (CCPA) - Cal. Civ. Code § 1798.100 et seq. Normativa de California (2018) aplicable a empresas que operan en el estado. Aunque exime datos cubiertos por GLBA, las instituciones financieras deben cumplir CCPA para datos de marketing, información de no clientes y obligaciones de seguridad ante violaciones de datos.

4.2. Estándares internacionales de seguridad

Payment Card Industry Data Security Standard (PCI DSS). Estándar de seguridad establecido por las principales marcas de tarjetas de crédito (Visa, Mastercard, American Express) que define doce requisitos obligatorios para organizaciones que almacenan, procesan o transmiten datos de tarjetas de pago. Incluye controles técnicos como cifrado, segmentación de red, monitoreo continuo y pruebas de penetración.

ISO/IEC 27001:2022. Norma internacional que especifica requisitos para establecer, implementar y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). Proporciona un marco estructurado para la gestión de riesgos de ciberseguridad aplicable a organizaciones que procesan datos financieros.

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 de gobernanza. Este marco proporciona orientación para organizaciones de todos los tamaños sobre gestión integral de riesgos de ciberseguridad, abarcando seis funciones: Govern, Identify, Protect, Detect, Respond y Recover.

La función "Detect" resulta particularmente relevante para sistemas de detección de fraude, estableciendo categorías para: monitoreo continuo de anomalías (DE.CM), procesos de detección de eventos adversos (DE.AE) y mejora continua de capacidades de detección (DE.DP).

4.3. Regulaciones transnacionales de protección de datos

General Data Protection Regulation (GDPR) - Reglamento (UE) 2016/679. Reglamento europeo de protección de datos aplicable a organizaciones que procesan información de ciudadanos de la Unión Europea, independientemente de su ubicación geográfica. Si TechSport procesa transacciones de usuarios residentes en la UE, debe cumplir con GDPR. Establece principios de minimización de datos, limitación de finalidad, transparencia en el procesamiento y derechos de los titulares, incluyendo el derecho a la explicación de decisiones automatizadas (Artículo 22), particularmen-

te relevante para sistemas de Machine Learning en aplicaciones financieras donde los modelos toman decisiones de clasificación de transacciones.

4.4. Regulaciones anti-lavado de dinero

Principios AML/KYC (Anti-Money Laundering / Know Your Customer). Estándares internacionales del Financial Action Task Force (FATF) que establecen obligaciones de identificación de clientes, monitoreo de transacciones sospechosas y reporte de actividades inusuales. Estas regulaciones complementan sistemas de detección de fraude, requiriendo análisis de patrones transaccionales para identificar operaciones potencialmente ilícitas.

4.5. Consideraciones para operaciones en América Latina

Marco regulatorio de países donde opera TechSport. Aunque TechSport tiene sede en Estados Unidos, procesa transacciones en múltiples países de América Latina. Cada jurisdicción donde opera establece requisitos específicos de protección de datos, prevención de fraude y cumplimiento financiero que deben considerarse en la implementación del sistema de detección.

Reporte OEA-BID (2020) sobre Ciberseguridad en América Latina y el Caribe. Organización de los Estados Americanos (OEA) y Banco Interamericano de Desarrollo (BID) (2020) documentan los riesgos de ciberseguridad específicos de la región, incluyendo fraude digital y vulnerabilidades en sistemas de pago electrónicos. El reporte identifica desafíos particulares de plataformas que operan en múltiples jurisdicciones latinoamericanas, recomendando implementación de controles técnicos avanzados, coordinación transnacional y capacitación continua en materia de prevención de fraude.

Conclusión

Los fundamentos teóricos referenciales desarrollados cumplen con el **Objetivo Específico 1**, proporcionando sustento científico robusto para la investigación mediante la integración de cuatro marcos complementarios.

El **Estado del Arte** identifica tres vacíos de conocimiento críticos que justifican la hipótesis de investigación: (1) escasa literatura sobre detección de fraude en arquitecturas multicanal distribuidas como la de TechSport, (2) ausencia de estudios en plataformas SaaS deportivas especializadas, y (3) limitadas comparaciones empíricas rigurosas entre sistemas tradicionales y modelos inteligentes. Estos hallazgos validan la necesidad de implementar un modelo adaptativo basado en Machine Learning, alinea-

do con la **hipótesis**: *La implementación de un modelo de Machine Learning mejora la detección de anomalías y fraudes en pagos transaccionales.*

El **Marco Teórico Conceptual** establece las definiciones operacionales de variables que permitirán medir la efectividad del modelo (**Objetivo Específico 4**): Precision, Recall, F1-score, tasa de falsos positivos y ROC-AUC. Además, delimita las características transaccionales discriminativas (monto, hora, canal, gateway, frecuencia) que fundamentarán el diseño del modelo (**Objetivo Específico 3**).

El **Marco Referencial** valida la viabilidad técnica mediante análisis crítico de aplicaciones exitosas (PayPal, Stripe, Mastercard) y proporciona evidencia empírica que orienta decisiones de diseño: selección de Random Forest como algoritmo principal por su balance entre desempeño y complejidad, estrategia de reentrenamiento periódico en lugar de tiempo real, y combinación de características transaccionales individuales con análisis de comportamiento agregado.

El **Marco Normativo** garantiza que el sistema propuesto operará dentro del marco legal aplicable a TechSport (normativa federal estadounidense, estándares PCI DSS, ISO 27001, NIST CSF 2.0), asegurando cumplimiento regulatorio y viabilidad institucional del proyecto.

La convergencia de estos fundamentos teóricos proporciona la base científica necesaria para abordar los objetivos específicos 2, 3 y 4, orientando el diseño metodológico, desarrollo del modelo y evaluación de resultados con criterios sólidos y validados en la literatura científica.

Referencias Bibliográficas

AlEmad, M. (2022). *Credit Card Fraud Detection Using Machine Learning* [Master's Project]. Rochester Institute of Technology.

Al-Khasawneh, M. (2025). Hybrid Neural Network Methods for the Detection of Credit Card Fraud. *Security and Privacy*. https://doi.org/10.1002/spy2.500

Arias Odón, F. G. (2016). *El Proyecto de Investigación: Introducción a la Metodología Científica* (7.ª ed.). Editorial Episteme.

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.

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

Bernal Torres, C. A. (2016). *Metodología de la Investigación: Administración, Economía, Humanidades y Ciencias Sociales* (4.ª ed.). Pearson Educación.

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

Chaquet Ulldemolins, J. (2022). *Machine learning interpretable para la detección del fraude crediticio* [Tesis doctoral, Universidad Rey Juan Carlos].

Cheng, D., Zou, Y., Xiang, S., & Jiang, C. (2025). Graph neural networks for financial fraud detection: a review. *Frontiers of Computer Science*. https://doi.org/10.1007/s11704-024-40474-y

Dileep, A., Karthik, A., Krishna, G., Ganesh, D., & Hariharan, S. (2023). Financial Fraud Detection Using Deep Learning Techniques. *2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*. https://doi.org/10.1109/ICDCECE57866.2023.10150467

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

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

Lucas, Y. (2019). *Credit card fraud detection using machine learning with integration of contextual knowledge* [Tesis doctoral, INSA de Lyon].

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

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.

Pérez González, G. A. (2021). *Detección de transacciones fraudulentas en tarjetas de crédito mediante el uso de modelos de Machine Learning* [Trabajo de grado]. Universidad de los Andes.

Rayo Mondragón, C. A. (2020). *Prototipo de detección de fraudes con tarjetas de crédito basado en inteligencia artificial aplicado a un banco peruano* [Trabajo de suficiencia profesional]. Universidad de Lima.

Rodríguez, J. F., Papale, M., Carminati, M., & Zanero, S. (2023). Fraud detection with natural language processing. *Machine Learning*. https://doi.org/10.1007/s10994-023-06354-5