

# **Verificación Metodológica del Proyecto de Investigación**

Detección de Fraude en Pagos Transaccionales usando Machine  
Learning

Según Metodología de Sampieri

Eidan Tarea Clase

17 de noviembre de 2025

# Índice

<b>Introducción</b>	<b>3</b>
<b>1. PARTE 1: APORTE TEÓRICO</b>	<b>4</b>
1.1. 1.1. Verificación del Objeto de Estudio . . . . .	4
1.1.1. 1.1.1. Definición del Objeto de Estudio . . . . .	4
1.1.2. 1.1.2. ¿Qué Estamos Investigando Realmente? . . . . .	4
1.1.3. 1.1.3. Parte Específica del Objeto . . . . .	5
1.1.4. 1.1.4. Área donde se Manifiesta el Problema . . . . .	5
1.2. 1.2. Pregunta de Investigación, Justificación Teórica y Práctica . . . . .	5
1.2.1. 1.2.1. Pregunta de Investigación . . . . .	5
1.2.2. 1.2.2. Justificación Teórica . . . . .	6
1.2.3. 1.2.3. Justificación Práctica . . . . .	7
1.3. 1.3. Aportes Teóricos . . . . .	8
1.3.1. 1.3.1. Elaboración de la Nueva Representación del Objeto (Representación Hipotética) . . . . .	8
1.3.2. 1.3.2. Búsqueda de Alternativas y Medios para la Implementación	9
1.3.3. 1.3.3. Diseño de la Nueva Representación y Expresión de Concepciones Teóricas . . . . .	11
<b>2. PARTE 2: APORTE DE LA SIGNIFICACIÓN PRÁCTICA</b>	<b>14</b>
2.1. 2.1. Estado Actual del Objeto (Diagnóstico Empírico) . . . . .	14
2.1.1. 2.1.1. Datos Empíricos Cuantitativos . . . . .	14
2.1.2. 2.1.2. Datos Empíricos Cualitativos . . . . .	15
2.1.3. 2.1.3. Diagnóstico del Estado Actual . . . . .	15
2.2. 2.2. Estado Ideal del Objeto (Cómo Debería Ser) . . . . .	16
2.2.1. 2.2.1. Características del Estado Ideal . . . . .	16
2.2.2. 2.2.2. Correspondencia con Marco Teórico . . . . .	18
2.3. 2.3. Interpretación Teórica de las Funciones del Objeto . . . . .	18
2.3.1. 2.3.1. ¿Qué Debe Hacer Exactamente el Objeto de Estudio? . . .	18
2.3.2. 2.3.2. ¿Qué Parte del Objeto Causa el Problema? . . . . .	20
2.3.3. 2.3.3. Relaciones Funcionales del Sistema Ideal . . . . .	21
2.3.4. 2.3.4. Síntesis de la Interpretación Funcional . . . . .	21
<b>Conclusiones</b>	<b>23</b>

# Introducción

El presente documento desarrolla la verificación metodológica del proyecto de investigación titulado “*Detección de Fraude en Pagos Transaccionales usando Machine Learning*”, siguiendo los lineamientos establecidos por Sampieri en su metodología de investigación científica.

El trabajo se estructura en dos grandes apartados: (1) el **Aporte Teórico**, que aborda la conceptualización y representación hipotética del objeto de estudio, y (2) el **Aporte de la Significación Práctica**, que vincula la teoría con la realidad empírica del contexto de aplicación en la empresa TechSport.

# 1 PARTE 1: APORTE TEÓRICO

Esta sección desarrolla la representación teórica del objeto de estudio, verificando su correcta definición y estableciendo las bases conceptuales que sustentan la investigación.

## 1.1. 1.1. Verificación del Objeto de Estudio

### 1.1.1. 1.1.1. Definición del Objeto de Estudio

El objeto de estudio de esta investigación es:

**“La detección de anomalías y fraude en pagos transaccionales mediante modelos de Machine Learning”**

Este objeto corresponde al campo científico de la inteligencia artificial aplicada a la seguridad financiera digital, específicamente en el dominio de sistemas de pago electrónico y prevención del fraude.

### 1.1.2. 1.1.2. ¿Qué Estamos Investigando Realmente?

Investigamos el **proceso de identificación automatizada de transacciones fraudulentas** en entornos de pago digital multicanal, utilizando técnicas de aprendizaje automático supervisado que permiten aprender patrones de comportamiento a partir de datos históricos.

Específicamente, nos enfocamos en:

- El análisis de datos transaccionales (montos, frecuencias, ubicaciones, dispositivos, pasarelas)
- La construcción de modelos predictivos capaces de clasificar transacciones como fraudulentas o legítimas
- La evaluación comparativa entre enfoques basados en reglas estáticas versus modelos de Machine Learning
- La integración de estos modelos en arquitecturas tecnológicas reales de plataformas SaaS

### **1.1.3. 1.1.3. Parte Específica del Objeto**

La investigación se concentra en la **fase de autorización y evaluación de riesgo de transacciones** dentro del flujo de procesamiento de pagos. Específicamente, el momento en que una transacción es enviada para aprobación y debe decidirse si proceder con ella o marcarla como sospechosa.

El área específica es: **el procesamiento de datos transaccionales y la aplicación de reglas/modelos ML para detección de fraude en tiempo real.**

### **1.1.4. 1.1.4. Área donde se Manifiesta el Problema**

El problema se manifiesta en las siguientes dimensiones del objeto de estudio:

- a) **Dimensión tecnológica:** Arquitectura fragmentada de pagos multicanal sin sistema centralizado de detección de fraude basado en IA. Los sistemas actuales dependen de reglas estáticas que no se adaptan a patrones emergentes.
- b) **Dimensión analítica:** Incapacidad para identificar patrones complejos y comportamientos anómalos en tiempo real a partir de datos históricos procesados por más de 10 pasarelas de pago en múltiples monedas y canales.
- c) **Dimensión operativa:** Ausencia de automatización en procesos de evaluación de riesgo transaccional, generando altas tasas de falsos positivos, rechazos de pagos legítimos y tiempos de respuesta inefficientes.
- d) **Dimensión de gestión del riesgo:** Deficiencias en gobernanza sobre integraciones entre sistemas y APIs, incrementando exposición al fraude y dificultando cumplimiento de normativas (PCI DSS, NIST).

**Síntesis del problema:** No existe un modelo/proceso efectivo basado en Machine Learning para identificar anomalías y fraudes en el contexto específico de TechSport, lo que resulta en pérdidas económicas, deterioro de la experiencia del usuario e ineficiencia operativa.

## **1.2. 1.2. Pregunta de Investigación, Justificación Teórica y Práctica**

### **1.2.1. 1.2.1. Pregunta de Investigación**

**Pregunta principal:**

¿Cómo mejorar la detección de anomalías y fraude en pagos transaccionales en la empresa TechSport durante la gestión 2024-2025?

**Preguntas derivadas:**

1. ¿Qué características transaccionales (features) son más relevantes para identificar patrones fraudulentos en pagos multicanal?
2. ¿Qué algoritmos de aprendizaje automático supervisado presentan mejor desempeño en la clasificación de transacciones fraudulentas versus legítimas en este contexto?
3. ¿Cómo se compara el rendimiento del modelo ML propuesto frente al sistema actual basado en reglas estáticas en términos de precisión, recall y F1-score?
4. ¿Qué arquitectura técnica es necesaria para integrar el modelo en el flujo operativo sin comprometer rendimiento del sistema?

**1.2.2. Justificación Teórica**

La investigación se fundamenta en tres cuerpos teóricos principales:

**a) Teoría del aprendizaje automático supervisado**

Los estudios de Hafez (2025) demuestran que los modelos de Machine Learning superan significativamente a enfoques tradicionales basados en reglas en la detección de fraude con tarjetas de crédito, principalmente por su capacidad de:

- Identificar patrones no lineales y relaciones complejas entre variables
- Adaptarse dinámicamente mediante reentrenamiento
- Reducir errores de clasificación (falsos positivos/negativos)
- Procesar grandes volúmenes de datos en tiempo real

**b) Teoría de detección de anomalías**

Los enfoques de detección de anomalías en datos transaccionales establecen que las desviaciones significativas respecto a patrones normales pueden indicar fraude, errores técnicos o cambios legítimos de comportamiento. Los modelos supervisados aprenden a distinguir estas situaciones mediante entrenamiento con casos etiquetados.

**c) Teoría de seguridad en sistemas de pago**

Los marcos normativos (PCI DSS, NIST Cybersecurity Framework) establecen que los sistemas de pago deben implementar mecanismos de prevención de fraude basados en múltiples capas de control, incluyendo análisis de comportamiento y detección de patrones.

#### **Contribución teórica de esta investigación:**

1. **Validación empírica:** Genera evidencia sobre aplicabilidad de modelos supervisados en arquitecturas multicanal con múltiples pasarelas, escenario poco explorado en literatura actual.
2. **Extensión conceptual:** Amplía marcos teóricos existentes al integrar variables específicas de plataformas SaaS deportivas (membresías, patrones de reserva).
3. **Metodología replicable:** Establece protocolo metodológico para implementación en empresas fintech con características similares.

#### **1.2.3. Justificación Práctica**

La necesidad práctica surge de problemas operacionales concretos en TechSport:

1. **Pérdidas económicas directas:** Transacciones fraudulentas no detectadas generan pérdidas y costos de devoluciones (chargebacks).
2. **Deterioro de experiencia del usuario:** Altas tasas de falsos positivos provocan rechazos de pagos legítimos, afectando satisfacción y conversión.
3. **Riesgos regulatorios:** Incumplimiento potencial de PCI DSS y estándares de seguridad, con consecuencias legales y reputacionales.
4. **Ineficiencia operativa:** Revisión manual de transacciones sospechosas consume recursos y retrasa confirmaciones.

#### **Beneficios esperados de la implementación:**

- Automatizar evaluación de riesgo en tiempo real
- Reducir costos operativos (menos revisión manual)
- Mejorar tasa de aprobación de pagos legítimos
- Fortalecer posición competitiva en mercado fintech
- Establecer bases para escalabilidad futura

#### **Coherencia entre pregunta, justificación teórica y práctica:**

La pregunta de investigación (¿cómo mejorar detección?) se responde mediante justificación teórica (estudios previos demuestran efectividad de ML) y se materializa en justificación práctica (reduce pérdidas económicas, mejora experiencia de usuario, optimiza operaciones).

### 1.3. 1.3. Aportes Teóricos

Según Sampieri, los aportes teóricos incluyen la elaboración de una nueva representación del objeto, identificación de alternativas de implementación, diseño de la nueva representación y expresión de concepciones teóricas.

#### 1.3.1. 1.3.1. Elaboración de la Nueva Representación del Objeto (Representación Hipotética)

La investigación propone una **nueva concepción teórica** del objeto de estudio:

*“Un sistema de detección de fraude basado en Machine Learning supervisado constituye un mecanismo adaptativo, inteligente y escalable que procesa datos transaccionales multicanal en tiempo real, identificando patrones fraudulentos mediante aprendizaje continuo a partir de ejemplos históricos, superando las limitaciones de sistemas basados en reglas estáticas al integrar capacidades de generalización, optimización automática y evolución ante nuevas amenazas.”*

**Características de la representación hipotética ideal:**

1. **Procesamiento en tiempo real:** El sistema debe evaluar cada transacción en milisegundos durante el flujo de autorización, sin generar latencia perceptible.
2. **Aprendizaje continuo:** El modelo debe actualizarse periódicamente incorporando nuevos patrones de fraude, sin requerir reprogramación manual.
3. **Análisis multidimensional:** Debe considerar simultáneamente variables técnicas (pasarela, canal, dispositivo), de negocio (membresía, historial) y contextuales (ubicación, hora, frecuencia).
4. **Equilibrio precision-recall:** Debe optimizar la detección de fraudes (recall alto) minimizando falsos positivos (precision alta), según umbrales definidos por el negocio.
5. **Explicabilidad:** Debe justificar cada clasificación identificando características más influyentes, facilitando auditoría y cumplimiento regulatorio.

### **Cómo debería funcionar idealmente según la teoría:**

- Recibir datos de transacción en tiempo real vía API
- Extraer y transformar características relevantes (feature engineering)
- Aplicar modelo entrenado para calcular probabilidad de fraude
- Clasificar transacción según umbral óptimo definido
- Generar explicación de la decisión (feature importance)
- Registrar resultado para reentrenamiento futuro
- Activar flujo de aprobación/rechazo según clasificación

#### **1.3.2. Búsqueda de Alternativas y Medios para la Implementación**

Para implementar la representación hipotética, la literatura identifica las siguientes alternativas:

##### **a) Alternativas de Modelado (qué herramientas/enfoques propone la literatura):**

###### **1. ML Supervisado - Modelos de Ensamble:**

- Random Forest: Robusto ante datos desbalanceados, permite interpretar importancia de características
- Gradient Boosting (XGBoost, LightGBM): Alta precisión, optimización de métricas específicas
- Ventaja: Mejor rendimiento documentado en literatura de fraude financiero

###### **2. ML Supervisado - Redes Neuronales:**

- Perceptrón Multicapa (MLP): Capacidad para patrones no lineales complejos
- Redes Profundas: Requieren mayor volumen de datos
- Limitación: Mayor costo computacional, menor explicabilidad

###### **3. Sistemas Híbridos:**

- Combinación de ML supervisado + detección de anomalías no supervisada
- Reglas de negocio + modelos ML para casos complejos

- Ventaja: Captura fraudes conocidos (reglas) y emergentes (ML)

#### 4. Modelos Lineales:

- Regresión Logística: Baseline simple, altamente explicable
- Limitación: Menor capacidad para patrones complejos

#### b) Medios Técnicos de Implementación:

- **Ingeniería de características:** Creación de features derivadas (agregaciones temporales, ratios, desviaciones respecto a comportamiento histórico del usuario)
- **Balanceo de clases:** Técnicas SMOTE, ajuste de pesos de clase para manejar desbalanceo transacciones legítimas vs. fraudulentas
- **Validación temporal:** División de datos respetando secuencia temporal para evitar data leakage
- **Optimización de hiperparámetros:** GridSearch, búsqueda bayesiana para configuraciones óptimas
- **Arquitectura de despliegue:** API REST integrada con flujo de autorización de pagos
- **Monitoreo de concept drift:** Detección de degradación del modelo en producción

#### c) Proceso de Implementación (Evaluación):

1. **Exploración y preparación de datos:** Análisis de calidad, tratamiento de valores faltantes, detección de outliers, codificación de variables categóricas
2. **Selección y entrenamiento de modelos:** Comparación empírica de algoritmos candidatos mediante validación cruzada temporal
3. **Optimización de hiperparámetros:** Búsqueda sistemática de configuraciones óptimas
4. **Evaluación comparativa:** Medición de desempeño frente al sistema actual usando precision, recall, F1-score, AUC-ROC
5. **Despliegue controlado:** Implementación inicial en modo observación (shadow mode) antes de activar decisiones automáticas
6. **Monitoreo y reentrenamiento:** Seguimiento de desempeño en producción y actualización periódica del modelo

### **1.3.3. 1.3.3. Diseño de la Nueva Representación y Expresión de Conceptos Teóricas**

Esta sección desarrolla la estructura teórica del objeto: definiciones, propiedades, clasificaciones y regularidades.

#### **a) Definiciones Fundamentales**

- **Fraude transaccional:** Uso no autorizado o manipulación intencional de información de pago con objetivo de obtener beneficios económicos ilícitos, caracterizado por patrones de comportamiento que se desvían significativamente de la normalidad estadística del usuario o del sistema.
- **Anomalía transaccional:** Transacción que presenta características atípicas respecto al perfil de comportamiento del usuario o patrones globales del sistema, pudiendo indicar fraude, error técnico o cambios legítimos en comportamiento.
- **Modelo supervisado de detección:** Sistema algorítmico que aprende a clasificar transacciones como fraudulentas o legítimas a partir de ejemplos históricos etiquetados, generalizando patrones para predecir el estado de nuevas observaciones.
- **Feature (característica):** Variable o atributo derivado de datos transaccionales utilizado como entrada del modelo (ej: monto, hora, ubicación geográfica, tiempo desde última transacción).
- **Falso positivo:** Transacción legítima incorrectamente clasificada como fraudulenta, genera fricción al usuario.
- **Falso negativo:** Transacción fraudulenta incorrectamente clasificada como legítima, genera pérdida económica.
- **Precision-Recall Trade-off:** Tensión entre maximizar detección de fraudes (recall) y minimizar rechazos incorrectos (precision).
- **Concept Drift:** Degradación temporal del modelo debido a cambios en patrones de fraude no reflejados en datos de entrenamiento.

#### **b) Propiedades del Objeto de Estudio**

Las propiedades fundamentales del sistema de detección de fraude mediante Machine Learning son:

1. **Adaptabilidad:** Capacidad del modelo para ajustar sus parámetros internos ante cambios en patrones de fraude mediante reentrenamiento periódico.

2. **Escalabilidad:** Habilidad para procesar volúmenes crecientes de transacciones sin degradación significativa del rendimiento temporal.
3. **Explicabilidad:** Posibilidad de interpretar decisiones del modelo identificando qué características contribuyen a clasificación como sospechosa.
4. **Robustez:** Resistencia ante datos ruidosos, valores atípicos o intentos de evasión mediante manipulación intencional de características.
5. **Generalización:** Capacidad de identificar fraudes con características similares pero no idénticas a ejemplos de entrenamiento.
6. **Eficiencia computacional:** Tiempo de inferencia compatible con requisitos de latencia del flujo de pagos (típicamente <100ms).

### c) Clasificación de Modelos Aplicables

Los modelos de Machine Learning para detección de fraude se clasifican según:

- **Tipo de aprendizaje:**
  - Supervisados: Requieren etiquetas (fraudulento/legítimo)
  - No supervisados: Detectan anomalías sin etiquetas previas
  - Semisupervisados: Combinan ambos enfoques
- **Complejidad algorítmica:**
  - Lineales: Regresión logística
  - Basados en árboles: Random Forest, XGBoost
  - Neuronales: Perceptrón multicapa, autoencoders
- **Momento de evaluación:**
  - Tiempo real: Decisión inmediata durante autorización
  - Batch: Revisión posterior de transacciones
- **Enfoque de detección:**
  - Basado en reglas: Umbrales fijos predefinidos
  - Basado en ML: Aprendizaje de patrones de datos
  - Híbrido: Combinación de reglas y ML

#### d) Regularidades Identificadas en la Literatura

El análisis teórico y empírico de detección de fraude revela las siguientes regularidades (patrones consistentes):

1. **Superioridad de ensambles:** Los modelos de ensamble basados en árboles (Random Forest, Gradient Boosting) consistentemente superan a modelos lineales en contextos de fraude financiero por su capacidad de capturar interacciones complejas entre variables.
2. **Desbalanceo de clases:** El desbalanceo inherente (pocas transacciones fraudulentas vs. muchas legítimas, típicamente 1:99 o menor) requiere técnicas específicas de balanceo o métricas alternativas a accuracy (precision, recall, F1-score).
3. **Importancia de feature engineering:** La ingeniería de características tiene mayor impacto en rendimiento que la selección del algoritmo, especialmente al incorporar conocimiento del dominio (ej: velocidad de transacciones, desviación respecto a comportamiento histórico).
4. **Degradación temporal:** Los modelos entrenados exclusivamente con datos históricos sufren degradación temporal (concept drift) debido a evolución de patrones de fraude, requiriendo actualización periódica (típicamente mensual o trimestral).
5. **Trade-off precision-recall:** No existe configuración óptima universal; el umbral de clasificación debe ajustarse según costos relativos de falsos positivos (fricción) vs. falsos negativos (pérdida económica).
6. **Necesidad de explicabilidad:** En contextos regulados, la capacidad de explicar decisiones del modelo (mediante SHAP values, feature importance) es tan importante como el rendimiento predictivo.

#### Síntesis del Aporte Teórico:

Se ha establecido una representación teórica completa del objeto de estudio, definiendo sus conceptos fundamentales, propiedades esenciales, clasificaciones relevantes y regularidades empíricas. Esta base conceptual, derivada de la literatura científica y alineada con Sampieri, fundamenta el diseño e implementación del modelo propuesto.

## 2 PARTE 2: APORTE DE LA SIGNIFICACIÓN PRÁCTICA

Esta sección vincula la teoría con la realidad empírica del objeto de estudio en el contexto específico de TechSport, siguiendo los tres componentes solicitados por Sampieri.

### 2.1. 2.1. Estado Actual del Objeto (Diagnóstico Empírico)

Descripción de lo que está pasando HOY con el objeto de estudio en TechSport, basada en datos empíricos recolectados.

#### 2.1.1. 2.1.1. Datos Empíricos Cuantitativos

- **Volumen transaccional:** La plataforma procesa transacciones a través de más de 10 pasarelas de pago diferentes (Stripe, CardConnect, AzulPay, RazorPay, BAC, entre otras) en múltiples monedas (USD, DOP, INR, CRC) y países.
- **Canales operativos:** Tres canales activos con comportamientos diferenciados:
  - Aplicación web
  - Aplicación móvil (iOS y Android)
  - Puntos de venta físicos (terminales)
- **Problema de fraude no detectado:** Actualmente existe fraude que pasa desapercibido porque no hay modelo ML que identifique patrones complejos.
- **Tasa de falsos positivos elevada:** El sistema actual basado en reglas genera rechazos injustificados que afectan experiencia del usuario y reducen tasa de conversión.
- **Tiempo de revisión manual:** Las transacciones marcadas como sospechosas requieren intervención humana, generando retrasos operativos y costos de personal.
- **Ausencia de registro formal:** No existe base de datos estructurada de transacciones marcadas como fraudulentas con etiquetas validadas que permita entrenamiento supervisado.

## 2.1.2. 2.1.2. Datos Empíricos Cualitativos

- **Ausencia total de ML:** No existe ningún modelo de aprendizaje automático implementado en el flujo de evaluación de transacciones.
- **Dependencia de reglas estáticas:** El sistema actual opera exclusivamente con reglas predefinidas basadas en umbrales fijos (ej: rechazar si monto > X”, “bloquear si más de Y transacciones en Z minutos”).
- **No hay aprendizaje del sistema:** Las reglas no evolucionan automáticamente; cualquier ajuste requiere modificación manual del código.
- **Fragmentación arquitectónica:** Cada pasarela de pago opera con sus propios mecanismos de control antifraude, sin consolidación ni análisis integrado de riesgo a nivel de plataforma TechSport.
- **Falta de gobernanza:** No existe proceso formal de gestión de integraciones, documentación de reglas de fraude ni responsables claros de la estrategia anti-fraude.
- **Pérdidas económicas por ”pagos fantasma”:** Se han identificado casos de pagos procesados que luego resultan ser fraudulentos (chargebacks), generando pérdidas directas más comisiones de devolución.
- **Fricción en experiencia de usuario:** Clientes legítimos ocasionalmente ven rechazados sus pagos por falsos positivos, lo que genera frustración, abandono de compra y tickets de soporte.

## 2.1.3. 2.1.3. Diagnóstico del Estado Actual

**Resumen: ¿Qué está pasando HOY con el objeto de estudio en TechSport?**

El sistema de detección de fraude en TechSport se encuentra en un **estado primitivo y reactivo**, caracterizado por:

1. **Arquitectura reactiva sin inteligencia:** El sistema solo responde a fraudes conocidos mediante reglas predefinidas, sin capacidad de anticipación, aprendizaje o identificación de nuevos patrones.
2. **Evaluación binaria simplista:** Las transacciones se evalúan mediante umbrales fijos (cantidad, frecuencia, ubicación geográfica) sin considerar contexto del usuario, historial de comportamiento ni relaciones complejas entre variables.

3. **Ausencia de capacidades predictivas:** No existe procesamiento de datos históricos para entrenar modelos, ni retroalimentación que permita mejorar el sistema con el tiempo.
4. **Gestión descentralizada y fragmentada:** Cada pasarela opera independientemente sin visión unificada del riesgo a nivel de usuario o transacción global.
5. **Ineficiencia operativa:** Alta carga de trabajo manual para revisión de alertas, tiempos de respuesta prolongados, imposibilidad de escalar proporcionalmente al crecimiento del negocio.
6. **Deficiencias en datos:** No hay registro sistemático de transacciones fraudulentas validadas (etiquetas de calidad) que permita entrenamiento supervisado futuro.

#### **Consecuencias observables del estado actual:**

- Pérdidas económicas por fraudes no detectados
- Pérdidas de conversión por falsos positivos
- Costos operativos elevados (revisión manual)
- Riesgos de incumplimiento regulatorio
- Limitada capacidad de crecimiento escalable

## **2.2. 2.2. Estado Ideal del Objeto (Cómo Debería Ser)**

Descripción del "deber ser" del objeto de estudio según el marco teórico revisado y en correspondencia con la situación problemática planteada.

### **2.2.1. 2.2.1. Características del Estado Ideal**

En correspondencia con la teoría de ML aplicado a detección de fraude y las necesidades de TechSport, el estado ideal debe alcanzar las siguientes características:

#### **1. Sistema con inteligencia predictiva en tiempo real:**

- Identifica transacciones potencialmente fraudulentas ANTES de autorización
- Evalúa probabilidad de fraude mediante modelo entrenado con patrones históricos

- Tiempo de respuesta  $\leq$  100ms compatible con flujo de pagos

## **2. Capacidad de aprendizaje y adaptación continua:**

- El modelo se actualiza periódicamente (mensual/trimestral) incorporando nuevos datos
- Se adapta automáticamente a cambios en patrones de fraude sin reprogramación manual
- Detecta concept drift y activa procesos de reentrenamiento

## **3. Equilibrio óptimo precision-recall:**

- Baja tasa de falsos positivos ( $\leq$  1-2 % de transacciones legítimas rechazadas)
- Alta tasa de detección de fraudes (recall  $\geq$  80-90 % de fraudes identificados)
- Umbral de clasificación ajustable según preferencias del negocio

## **4. Pipeline claro de entrenamiento y despliegue de ML:**

- Proceso documentado de extracción de datos, feature engineering, entrenamiento, evaluación
- Infraestructura automatizada (MLOps) para versionado de modelos y despliegue controlado
- Monitoreo continuo de desempeño en producción

## **5. Arquitectura centralizada e integrada:**

- Consolidación de datos de todas las pasarelas en sistema único de evaluación de riesgo
- Visión unificada del comportamiento transaccional del usuario across canales
- Integración mediante API REST con flujo de autorización de pagos

## **6. Automatización operativa con supervisión estratégica:**

- Reducción drástica de intervención manual (automatización  $\geq$  95 % de casos)
- Revisión humana limitada a casos de alta complejidad o ambigüedad predictiva
- Flujos de escalación claros para casos edge

## **7. Explicabilidad y cumplimiento regulatorio:**

- Capacidad de justificar cada clasificación (feature importance, SHAP values)
- Trazabilidad completa de decisiones para auditoría
- Cumplimiento de PCI DSS, protección de datos personales

#### **8. Registro sistemático de datos de calidad:**

- Base de datos estructurada de transacciones con etiquetas validadas (fraudulento/legítimo)
- Proceso de validación y corrección de etiquetas
- Disponibilidad de datos para reentrenamiento continuo

#### **2.2.2. 2.2.2. Correspondencia con Marco Teórico**

Este estado ideal se fundamenta en:

- **Teoría de ML supervisado:** Sistemas que aprenden de ejemplos etiquetados y generalizan a nuevos casos
- **Estudios empíricos** (Hafez 2025): Modelos ML superan reglas estáticas en precisión y adaptabilidad
- **Principios de seguridad en pagos:** Controles multicapa, monitoreo continuo, mejora iterativa
- **Buenas prácticas MLOps:** Automatización de pipeline, versionado de modelos, monitoreo de concept drift

#### **2.3. 2.3. Interpretación Teórica de las Funciones del Objeto**

Esta sección conecta el estado ideal con el estado actual, explicitando qué debe hacer el objeto según la teoría, qué funciones cumple, qué parte causa el problema y qué funciones deben mejorarse.

##### **2.3.1. 2.3.1. ¿Qué Debe Hacer Exactamente el Objeto de Estudio?**

Según el marco teórico de detección de fraude mediante ML, el objeto (sistema de detección) debe cumplir las siguientes funciones:

###### **Función 1: Clasificación de Transacciones en Riesgo**

- **Qué debe hacer:** Evaluar cada transacción en tiempo real y asignarle probabilidad de fraude
- **Cómo lo hace según teoría:** Aplicando modelo entrenado que procesa características transaccionales y genera score de riesgo
- **Estado actual:** NO LO HACE - solo aplica reglas binarias fijas
- **Qué debe mejorarse:** Implementar modelo ML supervisado que genere probabilidades continuas en lugar de decisiones binarias de reglas

#### **Función 2: Identificación de Patrones Complejos**

- **Qué debe hacer:** Detectar combinaciones no obvias de características que indican fraude (ej: monto bajo + velocidad alta + dispositivo nuevo + ubicación inusual)
- **Cómo lo hace según teoría:** Mediante algoritmos capaces de capturar interacciones entre variables (Random Forest, XGBoost)
- **Estado actual:** NO LO HACE - reglas estáticas solo evalúan variables individualmente
- **Qué debe mejorarse:** Desarrollar feature engineering que capture interacciones y entrenar modelos no lineales

#### **Función 3: Filtrado de Anomalías**

- **Qué debe hacer:** Distinguir entre anomalías fraudulentas, errores técnicos y cambios legítimos de comportamiento
- **Cómo lo hace según teoría:** Aprendiendo patrones de cada categoría a partir de datos históricos etiquetados
- **Estado actual:** NO LO HACE - toda anomalía se trata igual, generando falsos positivos
- **Qué debe mejorarse:** Crear dataset con etiquetas de calidad y entrenar modelo que discrimine tipos de anomalías

#### **Función 4: Escalación de Alertas**

- **Qué debe hacer:** Generar alertas priorizadas para revisión humana solo en casos de alta incertidumbre
- **Cómo lo hace según teoría:** Mediante umbrales de confianza que separan decisiones automáticas de casos que requieren supervisión

- **Estado actual:** PARCIALMENTE - genera alertas pero sin priorización inteligente
- **Qué debe mejorarse:** Calibrar umbrales de confianza y diseñar flujos de escalaución basados en scores de riesgo

#### **Función 5: Aprendizaje Continuo**

- **Qué debe hacer:** Mejorar su desempeño con el tiempo incorporando nuevos ejemplos de fraude
- **Cómo lo hace según teoría:** Mediante reentrenamiento periódico con datos actualizados
- **Estado actual:** NO LO HACE - las reglas permanecen estáticas
- **Qué debe mejorarse:** Establecer pipeline de reentrenamiento automatizado con nuevos datos validados

#### **Función 6: Optimización del Trade-off Negocio**

- **Qué debe hacer:** Balancear costos de falsos positivos (fricción) vs. falsos negativos (pérdida económica) según preferencias del negocio
- **Cómo lo hace según teoría:** Ajustando umbral de clasificación para maximizar métrica de negocio (ej: costo total esperado)
- **Estado actual:** NO LO HACE - umbrales de reglas son arbitrarios, no optimizados
- **Qué debe mejorarse:** Cuantificar costos de cada tipo de error y optimizar umbral mediante análisis de curva precision-recall

#### **2.3.2. 2.3.2. ¿Qué Parte del Objeto Causa el Problema?**

El problema no reside en una única parte, sino en **deficiencias estructurales del sistema actual:**

1. **Ausencia del componente de aprendizaje automático:** Es la deficiencia central. Sin modelo ML, el sistema carece de capacidad predictiva, adaptativa y de identificación de patrones complejos.
2. **Arquitectura de evaluación basada en reglas estáticas:** Este enfoque es inherentemente limitado para contextos dinámicos y complejos como el fraude financiero.

3. **Falta de datos estructurados de calidad:** Sin dataset de entrenamiento con etiquetas validadas, es imposible entrenar modelos supervisados efectivos.
4. **Fragmentación de pasarelas:** La desintegración impide análisis holístico del comportamiento del usuario y reduce capacidad de detección.
5. **Ausencia de gobernanza y procesos formales:** Sin responsables claros ni procesos documentados, el sistema no puede evolucionar sistemáticamente.

### **2.3.3. 2.3.3. Relaciones Funcionales del Sistema Ideal**

En el estado ideal, las funciones del objeto se relacionan sistémicamente:

- **Clasificación en tiempo real** (Función 1) → alimenta → **Escalación de alertas** (Función 4): Los scores de riesgo determinan qué casos requieren revisión humana.
- **Identificación de patrones** (Función 2) → mejora → **Clasificación** (Función 1): Feature engineering más sofisticado incrementa precisión predictiva.
- **Aprendizaje continuo** (Función 5) → mantiene → todas las funciones: Reentrenamiento periódico preserva efectividad ante evolución de fraudes.
- **Optimización del trade-off** (Función 6) → balancea → **Filtrado de anomalías** (Función 3): Ajuste de umbrales equilibra seguridad vs. fricción según objetivos de negocio.

### **2.3.4. 2.3.4. Síntesis de la Interpretación Funcional**

#### **Diagnóstico funcional:**

El sistema actual NO cumple adecuadamente las funciones primarias del objeto de estudio según la teoría:

- NO clasifica transacciones con probabilidades de riesgo
- NO identifica patrones complejos
- NO distingue tipos de anomalías
- NO aprende continuamente
- NO optimiza métricas de negocio

### **Intervención necesaria:**

Para transitar del estado actual al estado ideal, es necesario:

1. **Implementar componente de ML supervisado:** Núcleo de la solución, habilita funciones 1, 2, 3.
2. **Desarrollar dataset de calidad:** Prerequisito para entrenar modelos efectivos.
3. **Diseñar pipeline de reentrenamiento:** Habilita función 5 (aprendizaje continuo).
4. **Integrar arquitectura centralizada:** Consolida datos de todas las pasarelas.
5. **Calibrar umbrales de negocio:** Optimiza función 6 (trade-off).
6. **Establecer gobernanza formal:** Asegura sostenibilidad y evolución del sistema.

### **Vínculo con hipótesis de investigación:**

La hipótesis planteada ("La implementación de un modelo de Machine Learning mejora la detección de anomalías y fraudes...") se fundamenta precisamente en que el modelo ML habilitará las funciones actualmente ausentes o deficientes, permitiendo transitar del estado actual (primitivo, reactivo, estático) al estado ideal (inteligente, predictivo, adaptativo).

# Conclusiones

La verificación metodológica realizada confirma la solidez del proyecto de investigación en sus dimensiones teórica y práctica:

## Sobre el Aporte Teórico

1. El objeto de estudio está **correctamente definido**: "Detección de anomalías y fraude en pagos transaccionales mediante modelos de Machine Learning", con área específica claramente delimitada (procesamiento de datos transaccionales y aplicación de modelos ML).
2. El problema se manifiesta en **cuatro dimensiones identificables**: tecnológica, analítica, operativa y de gestión del riesgo.
3. Existe **coherencia entre pregunta de investigación, justificación teórica y práctica**: la pregunta (¿cómo mejorar detección?) se responde mediante teoría (estudios demuestran efectividad de ML) y se justifica prácticamente (reduce pérdidas, mejora experiencia).
4. Se ha desarrollado una **representación hipotética completa** del objeto de estudio, con alternativas de implementación (Random Forest, XGBoost, redes neuronales), medios técnicos (feature engineering, balanceo, validación temporal) y proceso de evaluación estructurado.
5. Se han establecido **concepciones teóricas fundamentales**: 8 definiciones clave, 6 propiedades del objeto, 4 clasificaciones y 6 regularidades empíricas derivadas de la literatura.

## Sobre la Significación Práctica

1. El diagnóstico empírico revela un **estado actual primitivo**: sistema reactivo basado en reglas estáticas, sin ML, sin aprendizaje, fragmentado, con pérdidas económicas por fraude no detectado y falsos positivos.
2. El **estado ideal está claramente definido** según marco teórico: sistema con inteligencia predictiva en tiempo real, aprendizaje continuo, equilibrio precision-recall optimizado, pipeline ML estructurado, arquitectura centralizada, alta automatización y explicabilidad.

3. La interpretación funcional identifica **6 funciones que el objeto debe cumplir**: clasificación de riesgo, identificación de patrones, filtrado de anomalías, escalación de alertas, aprendizaje continuo, optimización de trade-off negocio.
4. Se ha establecido claramente **qué parte del objeto causa el problema**: ausencia del componente ML (deficiencia central), arquitectura de reglas estáticas, falta de datos estructurados, fragmentación de pasarelas, ausencia de gobernanza.
5. La **brecha entre estado actual e ideal** justifica la intervención propuesta: implementar modelo ML supervisado que habilite las funciones actualmente ausentes o deficientes.

## Validación Metodológica General

El proyecto cumple los criterios de Sampieri para investigación científica aplicada:

- **Claridad del objeto:** Definición precisa y delimitada
- **Fundamentación teórica:** Sustentada en literatura científica relevante
- **Relevancia práctica:** Responde a necesidad operacional concreta
- **Coherencia metodológica:** Alineación entre problema, objetivos, teoría y solución propuesta
- **Viabilidad:** Condiciones técnicas, organizacionales y de datos permiten implementación
- **Aporte dual:** Contribución teórica (validación empírica de ML en contexto SaaS multicanal) y práctica (mejora operativa en TechSport)

La investigación está metodológicamente sólida y lista para proceder a las fases de desarrollo e implementación del modelo propuesto.