El uso de analytics para la prevención de fraudes en transacciones internacionales

Autor: Fadrique Álvarez De Toledo Abaitua

Tutor: Ignacio Ramos Villar

Grado en Relaciones Internacionales y Business Analytics

Universidad Pontificia Comillas

Fecha: 10/06/2025

Tabla de contenido

Relación de siglas

- **AI / IA:** Artificial Intelligence / Inteligencia Artificial.
- **AML:** Anti-Money Laundering (Prevención de Lavado de Dinero o Blanqueo de Capitales).
- **BSA:** Bank Secrecy Act (Ley de Secreto Bancario de EE. UU.).
- **CFT:** Combating the Financing of Terrorism (Lucha contra la Financiación del Terrorismo).
- **FATF / GAFI:** Financial Action Task Force / Grupo de Acción Financiera Internacional.
- **FCA:** Financial Conduct Authority (Autoridad de Conducta Financiera del Reino Unido).
- **FCPA:** Foreign Corrupt Practices Act (Ley de Prácticas Corruptas en el Extranjero de EE. UU.).
- **FinCEN:** Financial Crimes Enforcement Network (Red de Control de Delitos Financieros de EE. UU.).
- **GDPR / RGPD:** General Data Protection Regulation / Reglamento General de Protección de Datos.
- **KYC:** Know Your Customer (Procedimiento de "Conozca a su Cliente").
- **ML / AA:** Machine Learning / Aprendizaje Automático.
- **OFAC:** Office of Foreign Assets Control (Oficina de Control de Activos Extranjeros de EE. UU.).
- **OLAF:** European Anti-Fraud Office (Oficina Europea de Lucha contra el Fraude).
- **PEP:** Politically Exposed Person (Persona Políticamente Expuesta).
- **PSD2:** Payment Services Directive 2 (Segunda Directiva de Servicios de Pago de la UE).
- **ROC:** Receiver Operating Characteristic (Característica Operativa del Receptor, métrica de modelos de clasificación).
- **SAR:** Suspicious Activity Report (Reporte de Actividad Sospechosa).
- **SWIFT:** Society for Worldwide Interbank Financial Telecommunication (red global de mensajería financiera).
- **TBML:** Trade-Based Money Laundering (Blanqueo de capitales basado en el comercio).
- **UIF:** Unidad de Inteligencia Financiera.
- **VAA:** Visa Advanced Authorization (Sistema de autorización avanzada de Visa).
- **XAI:** Explainable AI (Inteligencia Artificial Explicable).

1. Introducción

El fraude en transacciones financieras internacionales se ha convertido en una verdadera amenaza en la economía global, una amenaza compleja y más presente a cada día que pasa. El avance de la tecnología digital ha facilitado la expansión del fraude a través de fronteras, resultando en pérdidas por miles de millones de dólares a nivel mundial cada año. Las empresas de todo el mundo se enfrentan a pérdidas importantes por fraude en pagos en línea, proyectándose que superarán los **$362.000 millones** entre 2023 y 2028. Esta situación plantea desafíos importantes para instituciones financieras, reguladores y autoridades, especialmente a medida que los defraudadores emplean tácticas cada vez más sofisticadas que **desbordan los métodos tradicionales de detección y prevención**. La creciente complejidad de los esquemas de fraude (como robos de identidad, fraudes en pagos y fraudes "sintéticos") pone de manifiesto que los enfoques convencionales (basados en reglas estáticas o controles manuales) resultan insuficientes para contener las amenazas emergentes. En consecuencia, existe una **necesidad urgente de enfoques más dinámicos** y con capacidad de adaptacion en la prevención de fraudes, donde las técnicas de *analytics* y análisis de datos juegan un papel crítico.

En este contexto, el término **analytics** se refiere al uso de la analítica de datos avanzada (incluyendo herramientas de *Big Data*, aprendizaje automático (*machine learning*) e inteligencia artificial) para sacar extraer patrones, monitorear transacciones en tiempo real e identificar actividades anómalas que puedan indicar fraude. El uso de analytics nos permite analizar **grandes volúmenes de datos transaccionales y de comportamiento** prácticamente al instante, lo que ofrece una detección más rapida de patrones sospechosos que los métodos tradicionales. Por ejemplo, mediante algoritmos de *machine learning* predictivo es posible supervisar en tiempo real las transacciones y señalar aquellas que se desvían de los comportamientos habituales, aportando a las empresas un enfoque más ágil para la prevención del fraude. Varios estudios han destacado que aprovechar la analítica de datos masivos puede mejorar significativamente la capacidad de descubrir patrones complejos de fraude y adaptarse a nuevas tácticas.

La importancia de investigar **el uso de analytics en la prevención del fraude internacional** es tanto práctica como académica. Prácticamente, las instituciones financieras y corporaciones multinacionales necesitan fortalecer sus sistemas anti-fraude para proteger sus activos y cumplir con las **normativas internacionales de cumplimiento** (por ejemplo, las relacionadas con anti-lavado de dinero y financiamiento del terrorismo). Académicamente, el área de la detección de fraudes se beneficia de una comprensión más profunda de cómo las técnicas analíticas modernas superan las limitaciones de enfoques tradicionales. Estudios previos han sentado las bases importantes: Bolton y Hand (2002) ofrecen una revisión fundamental de las técnicas estadísticas aplicadas a la detección de fraudes en diversos contextos, incluyendo transacciones internacionales. Phua et al. (2010) realizan un **análisis exhaustivo** de la aplicación de la minería de datos a la detección de fraudes,

demostrando los avances y desafíos en múltiples sectores, también en operaciones internacionales. Más recientemente, Zheng, Yuan y Wu (2018) proporcionaron una visión detallada de cómo los enfoques de análisis de datos pueden utilizarse específicamente para detectar fraudes financieros, mientras que Zhu et al. (2021) exploran nuevas herramientas y enfoques para analizar grandes volúmenes de datos con fines de detección de fraude. Islam et al. (2024), profundizan en el uso de la inteligencia artificial y su impacto en la identificación de patrones fraudulentos en el comercio internacional. Esta trayectoria bibliográfica señala la creciente importancia de integrar métodos analíticos avanzados en la lucha contra fraudes de alcance global.

Preguntas de investigación: A la luz de lo anterior, este trabajo busca responder preguntas como: **¿De qué manera las técnicas de analytics pueden mejorar la detección y prevención del fraude en transacciones internacionales?**; **¿Cuáles son las metodologías actuales más efectivas y cómo se comparan con los enfoques tradicionales?**; **¿Qué retos existen (técnicos, organizativos y regulatorios) para implementar analytics en programas antifraude internacionales?**; y **¿Cómo contribuye el uso de analytics al cumplimiento normativo global y qué implicaciones prácticas tiene para las empresas y reguladores?**.

Objetivos: El objetivo principal de este trabajo es **analizar cómo el uso de técnicas de análisis de datos (analytics) puede ser una herramienta eficaz para la prevención del fraude en transacciones internacionales**. Se pretende identificar patrones y caracteristicas de comportamiento fraudulento en el ámbito de las transacciones comerciales globales y examinar cómo estos patrones se relacionan con las políticas de **cumplimiento normativo** de las organizaciones, contribuyendo así a la reducción del riesgo. Un objetivo es explorar cómo los avances recientes en inteligencia artificial y *machine learning* pueden optimizar los procesos de monitoreo y detección temprana de fraudes internacionales, proporcionando a las empresas mecanismos más efectivos para identificar actividades sospechosas antes de que resulte en pérdidas importantes. Además, el trabajo busca **evaluar de forma crítica las fortalezas y limitaciones** de los enfoques basados en analytics frente a los métodos tradicionales, considerando tanto la literatura académica como ejemplos aplicados en la industria.

Hipótesis: Derivado de lo anterior, se plantea la hipótesis de que **la integración de técnicas avanzadas de analítica de datos en las estrategias de prevención de fraudes aumenta significativamente la capacidad de detección temprana de actividades fraudulentas en transacciones internacionales**, en comparación con los métodos convencionales basados en reglas estáticas. Esta hipótesis supone que la analítica avanzada (incluyendo algoritmos de *machine learning* e inteligencia artificial) mejora no solo la tasa de detección de fraudes, sino también la reducción de falsos positivos, y que complementa de manera efectiva las prácticas de cumplimiento normativo al proporcionar alertas más precisas. En otras palabras, se espera demostrar que un enfoque apoyado en analytics permite a las instituciones **anticiparse mejor a**

esquemas de fraude sofisticados y cumplir con las normativas internacionales de manera más eficiente, respeto a las aproximaciones tradicionales.

Para abordar la hipótesis y los objetivos planteados, la estructura del documento es la siguiente: en el **Marco teórico** realizamos una revisión bibliográfica que contextualiza el problema del fraude en transacciones internacionales, describiendo sus principales caracteristicas y las técnicas existentes para su detección, con el foco puesto en la evolución hacia métodos analíticos y su relación con las funciones de *compliance*. A continuación, en el **Marco normativo**, comparamos las legislaciones y estándares internacionales más relevantes en materia de prevención de fraudes y lavado de dinero, proporcionando el contexto legal en el cual operan las soluciones de analytics. La sección de **Metodología** describe el enfoque de investigación de tipo teórico y cualitativo empleado, basado en la revisión de fuentes académicas y de casos, justificando por qué este enfoque es adecuado para los objetivos del trabajo. Por otro lado, el **Análisis aplicado** presenta casos de estudio reales y tendencias de la industria donde se ha implementado (o podría implementar) analytics para combatir fraudes internacionales, ilustrando observaciones prácticas. En la **Discusión crítica**, planteamos las limitaciones actuales de los enfoques analíticos (como desafíos técnicos, consideraciones de privacidad, costes implementación) y analimaos las implicaciones tanto prácticas como regulatorias de adoptar estos métodos. Finalmente, en **Conclusiones y recomendaciones**, vamos a resumir los hallazgos principales, reflexiones sobre la validez de la hipótesis y recomendaciones tanto académicas (para futuras investigaciones) como profesionales (para empresas y reguladores) orientadas a fortalecer la prevención de fraudes en el ámbito internacional mediante el uso de analytics.

2. Marco teórico

En esta sección se van a presentar los fundamentos teóricos y hallazgos de investigaciones previas relacionados con el fraude en transacciones internacionales y las técnicas para su detección, con especial atención al rol de la analítica de datos (*analytics*) en dicho contexto. Se plantean cuatro aspectos principales: **(a)** la conceptualización del fraude en transacciones internacionales y sus tipologías más comunes; **(b)** las técnicas tradicionales de detección de fraude y sus limitaciones; **(c)** la evolución hacia técnicas basadas en analytics y *Big Data* para la detección de patrones anómalos; y **(d)** la integración de analytics en las funciones de cumplimiento (*compliance*) y gestión de riesgos de fraude.

2.1 Fraude en transacciones internacionales: naturaleza y tipologías

Llamamos **fraude en transacciones internacionales** a cualquier actividad ilícita deliberada que involucra transacciones financieras o comerciales entre diferentes países con el fin de obtener un beneficio indebido o causar perjuicio economico a terceros. Este concepto engloba diversos esquemas delictivos, desde el **fraude financiero clásico** (como transferencias bancarias fraudulentas o pagos con tarjetas robadas a nivel internacional) hasta formas más complejas como el **blanqueo de capitales transfronterizo**, el **fraude comercial** (manipulación de documentos de comercio exterior, facturación falsa, etc.) y las estafas apoyadas en la **cibercriminalidad global**.

En un entorno globalizado, las empresas (especialmente las que operan en comercio exterior) se enfrentan a múltiples formas de fraude cuando interactúan con contrapartes en otros países. En el caso de las pequeñas y medianas empresas exportadoras o importadoras, se han identificado varios **tipos de fraude en comercio internacional** frecuentes, entre los que destacan:

- **Fraude en pagos y cobros internacionales:** incluye transferencias bancarias fraudulentas, suplantación de identidad del beneficiario (por ejemplo, mediante *phishing* para desviar pagos) o el simple incumplimiento de pago por parte de clientes extranjeros. Un ejemplo típico es la estafa del *CEO falso* en la que un criminal, haciéndose pasar por un directivo, instruye una transferencia urgente a una cuenta en el exterior. También se incluyen aquí los casos en que se utilizan tarjetas de crédito robadas en transacciones *online* de alcance internacional.
- **Proveedores inexistentes o fraudulentos:** casos en los que una empresa paga por adelantado a un supuesto proveedor extranjero que en realidad no entrega la mercancía, o entrega productos de calidad o cantidad inferior a la acordada. Este tipo de fraude aprovecha la distancia geográfica y la dificultad de verificación para engañar a importadores. Por ejemplo, pueden presentarse *websites* fraudulentos de empresas fantasmas en otros países que atraen a compradores con ofertas atractivas, exigen pagos anticipados y luego desaparecen.
- **Phishing y ciberfraude transnacional:** los ciberdelincuentes emplean técnicas de ingeniería social (correos electrónicos falsificados, sitios web clonados, etc.) para obtener credenciales bancarias, contraseñas o información sensible de las empresas, con el objetivo de sustraer fondos o datos confidenciales. En el ámbito internacional, es común el *phishing* dirigido (spear phishing) donde se envían correos aparentando provenir de proveedores o bancos extranjeros legítimos, llevando a la realización de pagos a cuentas fraudulentas.
- **Falsificación de documentos comerciales:** implica la alteración o fabricación de documentos en operaciones internacionales (por ejemplo, certificados de origen, conocimientos de embarque, cartas de crédito, contratos) para obtener beneficios ilícitos. Un caso podría ser la presentación de documentos de embarque falsos para hacer creer que una mercancía fue enviada y así cobrar bajo una carta de crédito, cuando en realidad no existe tal envío. Esta categoría se relaciona estrechamente con prácticas de **fraude aduanero** y **fraude en garantías bancarias** en comercio exterior.
- **Intermediarios deshonestos:** en muchos países es habitual operar a través de agentes o distribuidores locales. Existe el riesgo de que estos intermediarios abusen de la confianza de la empresa extranjera, por ejemplo, desviando pagos de clientes hacia sus propias cuentas, inflando comisiones, o realizando acuerdos

paralelos que perjudican al proveedor. Este tipo de fraude suele apoyarse en la asimetría de información y la dificultad de supervisar directamente las actividades en el extranjero.

Estos ejemplos enseñan que el fraude internacional no es un fenómeno único, sino un **conjunto heterogéneo de amenazas** que abarcan desde delitos puramente financieros hasta combinaciones con delitos informáticos y maniobras comerciales. Un elemento común es la explotación de la **complejidad de las transacciones transfronterizas**, donde intervienen diferencias idiomáticas, legales y culturales, lo que dificulta la detección. Por ejemplo, el **blanqueo de capitales basado en el comercio (TBML)** aprovecha la apariencia de transacciones comerciales legítimas para lavar dinero: los criminales manipulan el valor, la cantidad o la calidad declarada de bienes en exportaciones/importaciones (mediante **sobrefacturación** o **subfacturación** de facturas, envíos fantasma, etc.) para mover valor ilícito entre países. Este tipo de fraude es especialmente engañoso porque implica documentación auténtica alterada y redes de empresas pantalla en distintos países, escapando a controles financieros tradicionales centrados solo en transferencias monetarias.

Otro punto que define al fraude en transacciones internacionales es su **escala y rapidez**. Las redes globales de pagos (como SWIFT para transferencias bancarias) y el comercio electrónico permiten mover fondos ilícitos por múltiples jurisdicciones en cuestión de minutos, desafiando la capacidad de respuesta de las entidades afectadas. Un ejemplo fue el *hack* al Banco Central de Bangladesh en 2016, donde ciberdelincuentes lograron ordenar transferencias por 81 millones de dólares a cuentas en Filipinas a través de SWIFT; la detección fue complicada debido a la coordinación internacional requerida y solo se recuperó una fracción de la cantidad tras la intervención de autoridades globales. Este caso evidenció la necesidad de **sistemas de alerta temprana** que consideren patrones inusuales en las transacciones internacionales (por ejemplo, cantidaes atípicas, destinos inusuales) para detener operaciones sospechosas antes de que se completen.

En resumen, el fraude en transacciones internacionales presenta **desafíos únicos** por su alcance geográfico y multi-disciplinario. Combinar tácticas tradicionales (ej. controles internos, verificación manual de documentos) con herramientas modernas de analytics es fundamental para abordar estas amenazas. Antes de profundizar en esas soluciones basadas en datos, es necesario repasar brevemente las técnicas clásicas de detección de fraude y entender por qué resultan insuficientes frente al panorama descrito.

2.2 Técnicas tradicionales de detección de fraude y sus limitaciones

Históricamente, la detección y prevención de fraudes financieros (tanto a nivel doméstico como internacional) se ha basado en **mecanismos tradicionales** basados en reglas de negocio, auditorías e intervención humana. Algunas de las técnicas convencionales más empleadas son:

- **Sistemas de reglas estáticas:** Las instituciones definen manualmente un conjunto de reglas o umbrales que, al ser excedidos, disparan alertas de posible fraude. Ejemplos: bloquear transacciones mayores a ciertas cantidades hacia ciertos países de alto riesgo, marcar transacciones si un cliente realiza más de X transferencias diarias, o denegar pagos si no coincide la dirección IP con el país de la tarjeta. Estas reglas se basan en la experiencia pasada de fraude y en criterios establecidos por analistas. Si bien son simples de entender y aplicar, tienen la desventaja de ser rígidas; los defraudadores pueden adaptarse rápidamente para evitar violar las reglas conocidas (por ejemplo, enviando cantidaes justo por debajo del umbral).
- **Listas negras y listas grises:** Otra técnica es mantener bases de datos de cuentas bancarias, IPs, nombres de personas o empresas que han sido identificadas previamente en fraudes (listas negras) o que presentan comportamientos inusuales (listas grises). Las transacciones involucrando entidades en estas listas se bloquean o se someten a revisión adicional. El problema es que las listas negras solo ayudan a detectar reincidencias, pero no nuevos defraudadores sin historial; además, pueden generar **falsos positivos** si no se depuran adecuadamente (por ejemplo, confundir a personas con nombres similares).
- **Segregación de funciones y controles internos:** En el ámbito corporativo, la prevención del fraude tradicional ha descansado en procesos como la doble verificación de transferencias (dos firmas requeridas), conciliaciones frecuentes, auditorías periódicas y revisión manual de transacciones de alto valor. Estas medidas operan bajo la suposición de que el fraude puede ser detectado por personal entrenado al revisar discrepancias o comportamientos sospechosos. Si bien son prácticas necesarias, su eficacia disminuye con el **volumen masivo de transacciones** y la **velocidad** de los flujos financieros actuales, donde es humanamente imposible revisar todo en tiempo real.
- **Modelos estadísticos simples:** Algunas instituciones han implementado puntuaciones de riesgo basadas en modelos estadísticos tradicionales (por ejemplo, algoritmos de regresión logística) usando un conjunto limitado de variables. Estos modelos se entrenan con datos históricos etiquetados (transacciones fraudulentas vs legítimas) para calcular la probabilidad de que una nueva transacción sea fraudulenta. En la literatura temprana, Bolton y Hand (2002) ya señalaban que tanto los métodos estadísticos como los de *machine learning* proveían tecnologías efectivas para detección de fraudes en áreas como blanqueo de capitales, fraude con tarjetas de crédito, etc.. Sin embargo, muchos de estos primeros modelos requerían supuestos fuertes (linealidad, distribuciones conocidas) y se enfrentaban a desafíos como el **desbalance de clases** (las transacciones fraudulentas son extremadamente escasas frente a las legítimas) y la rápida **desactualización** ante nuevas tácticas de fraude.

Un factor limitante general de los enfoques tradicionales es su carácter **reactivo y puntual**. Las reglas y controles suelen crearse *después* de haber experimentado un tipo

de fraude, es decir, responden a patrones ya conocidos. Esto deja expuesta a la organización frente a **nuevas modalidades** de fraude que no cumplen las reglas predefinidas. Además, los sistemas basados en reglas o listas generan a menudo un **volumen muy alto de alertas** (muchas de ellas falsos positivos) que deben ser analizadas manualmente, lo cual consume recursos de los equipos de cumplimiento o auditoría. Esta sobrecarga puede provocar que se pasen por alto verdaderas señales de fraude entre muchas alarmas irrelevantes.

Investigaciones en detección de fraudes señalan la importancia de técnicas no supervisadas para descubrir anormalidades sin depender de etiquetas de fraude conocidas. Por ejemplo, Bolton y Hand enfatizaron el rol de métodos **no supervisados** para identificar transacciones atípicas que podrían indicar fraudes desconocidos. Las técnicas no supervisadas (p.ej., agrupamiento –*clustering*– o detección de outliers) buscan patrones que se desvían de la norma, bajo la premisa de que los fraudes a menudo se manifiestan como **anomalías** en los datos. Sin embargo, aplicados en su forma más simple, estos métodos también tienden a marcar muchas anomalías que no son fraudulentas (por ejemplo, transacciones legítimas pero inusuales por razones comerciales).

En resumen, las metodologías tradicionales han proporcionado la primera línea de defensa contra el fraude y siguen siendo componentes necesarios de una estrategia íntegra. No obstante, por sí solas resultan insuficientes en el contexto actual de transacciones internacionales debido a: **(1)** la adaptabilidad de los delincuentes (que aprenden a eludir reglas fijas), **(2)** la escala y velocidad de las operaciones (que exceden la capacidad humana de monitoreo manual), y **(3)** la complejidad de los esquemas modernos de fraude (que involucran múltiples cuentas, países y métodos, haciendo difícil su detección mediante reglas simples). Estas brechas han motivado un cambio de paradigma hacia enfoques apoyados en la **analítica avanzada de datos**, los cuales se analizan a continuación.

2.3 Enfoques basados en analytics y Big Data para la detección de fraudes

La última década ha visto una transformación importante en las técnicas de detección de fraudes, impulsada por la disponibilidad de **grandes volúmenes de datos** (*Big Data*), mayores capacidades de cómputo y avances en algoritmos de inteligencia artificial. El término **fraud analytics** hace referencia a la aplicación de métodos de análisis de datos (incluyendo *machine learning*, minería de datos, análisis estadístico avanzado y herramientas de inteligencia artificial) para identificar patrones o irregularidades que sugieran actividad fraudulenta tanto *a priori* (prevención) como *a posteriori* (detección temprana). Estos enfoques se caracterizan por ser **proactivos, adaptativos y escalables**, superando muchas de las limitaciones de los métodos tradicionales.

Algunos componentes y técnicas clave de la analítica para detección de fraudes son:

- **Análisis predictivo mediante Machine Learning (ML):** Consiste en entrenar modelos con datos históricos para predecir la probabilidad de fraude en transacciones nuevas. A diferencia de los modelos estadísticos simples, el ML permite capturar relaciones no lineales complejas. Entre las técnicas más utilizadas en la literatura y la industria están los **árboles de decisión**, **bosques aleatorios**, **redes neuronales** (incluyendo *deep learning*), **modelos de ensamble** y **máquinas de vectores de soporte (SVM)**. Según revisiones académicas, los algoritmos más comunes aplicados a la detección de fraude financiero incluyen modelos logísticos, redes neuronales, redes bayesianas y árboles de decisión, todos los cuales han demostrado efectividad para clasificar transacciones como fraudulentas o legítimas. Estos modelos, una vez entrenados, pueden procesar enormes cantidades de transacciones en tiempo real, asignando a cada una un **puntuación de riesgo**. Un ejemplo notable es la red global de pagos VisaNet, donde Visa emplea algoritmos de aprendizaje automático (redes neuronales profundas) que analizan el **100% de las transacciones (más de 127 mil millones al año) en aproximadamente un milisegundo cada una**, permitiendo a las instituciones financieras identificar y bloquear transacciones fraudulentas casi instantáneamente. Gracias a estas técnicas, Visa consigue mantener las tasas de fraude global por debajo del 0,1% en su red, evitando aproximadamente 25.000 millones de dólares en fraudes anualmente mediante detección con IA.
- **Detección de anomalías (análisis no supervisado):** En escenarios donde no se cuenta con suficientes ejemplos etiquetados de fraude (lo cual es común, pues los fraudes conocidos son la "punta del iceberg"), se aplican métodos no supervisados para identificar patrones de transacción inusuales. Técnicas como **clústeres (clustering)** pueden agrupar transacciones o clientes por similitud; aquellos grupos o datos que no encajan en ningún clúster denso pueden señalar casos anómalos. Otras técnicas incluyen **métodos de vecinos cercanos**, **bosques de aislamiento** y análisis de outliers multivariado. Por ejemplo, en transacciones internacionales, una técnica no supervisada podría detectar si un cliente que normalmente opera solo localmente de repente envía transferencias a cuentas en múltiples países nuevos. Lo cual es un comportamiento anómalo que podría indicar que su cuenta fue comprometida. La eficacia de estos métodos radica en que pueden descubrir **"fraudes desconocidos"** (patrones nuevos) al enfocarse en la rareza estadística, aunque luego es necesaria la verificación humana para distinguir anormalidades legítimas de fraudes reales.
- **Minería de datos y herramientas de Big Data:** La detección moderna de fraudes aprovecha diversas fuentes de datos estructurados y no estructurados. Además de los datos transaccionales tradicionales (cantidades, fechas, contrapartes), se incorporan datos de comportamiento (por ejemplo, análisis de secuencias de eventos, hora y localización de transacciones), datos del dispositivo o canal (dirección IP, tipo de navegador, geolocalización GPS para pagos móviles) e incluso datos no estructurados como notas, correos electrónicos o mensajes relacionados con transacciones. La **minería de textos** puede utilizarse para, por ejemplo, analizar descripciones de pagos o comentarios buscando palabras clave que sugieran fraude. En contexto de Big

Data, se emplean plataformas de procesamiento distribuido (como Hadoop, Spark) para manejar *datasets* masivos en tiempo razonable. Zhu y col. (2021) ofrecen un panorama de cómo se explotan grandes volúmenes de datos en la detección de fraudes, discutiendo enfoques y herramientas para procesar información a escala masiva. Un beneficio de Big Data analytics es la posibilidad de **correlacionar información de múltiples fuentes**: por ejemplo, relacionar transacciones financieras con datos de redes sociales o bases de datos de sanciones internacionales para identificar conexiones ocultas entre actores sospechosos.

- **Sistemas basados en redes e inteligencia relacional:** Los fraudes internacionales a menudo involucran **redes de actores** (múltiples cuentas bancarias conectadas, empresas fachada relacionadas, etc.). Por ello, se han desarrollado técnicas de análisis de grafos o redes sociales aplicadas a datos financieros. Estas técnicas modelan las transacciones como grafos donde los nodos son personas/cuentas/entidades y las aristas son transacciones o relaciones. Luego se pueden aplicar algoritmos para detectar **comunidades sospechosas**, **estructuras circulares de movimientos de dinero** (indicativas de lavado en círculos), o nodos altamente conectados que puedan ser "concentradores" de fraude. Un ejemplo es identificar estructuras típicas de **esquemas de carrusel** (fraude de IVA intracomunitario) donde varias empresas en distintos países simulan ventas en cadena para defraudar impuestos: el análisis de grafos ayudaría a detectar el ciclo de facturación. Esta aproximación relacional complementa al análisis transaccional tradicional al mirar el "bosque" de interconexiones y no solo los "árboles" individuales.
- **Analítica en tiempo real y sistemas de alerta temprana:** Un avance fundamental es la capacidad de algunas instituciones para hacer análisis en **streaming** de datos de transacciones, es decir, procesarlos en el mismo momento en que ocurren. Sistemas de pagos y antifraude ahora utilizan modelos entrenados que evalúan cada transacción **antes de autorizarla**, devolviendo una decisión o alerta en fracciones de segundo. Como se mencionó, redes de pago como VisaNet aplican modelos de aprendizaje automático en milisegundos durante el proceso de autorización para decidir si aprobar o rechazar una transacción. Del mismo modo, los bancos implementan motores de reglas y modelos que funcionan 24/7 monitoreando transferencias (por ejemplo, a través de la red SWIFT). Esta analítica en tiempo real permite **prevenir el fraude antes de su consumación**, a diferencia de métodos tradicionales donde a veces el fraude se confirmaba una vez ocurrido (p.ej., cuando un cliente reclama un cargo fraudulento días después). Sin embargo, conlleva el reto de ser muy precisa para no frenar operaciones legítimas: la **tasa de falsos positivos** debe minimizarse para evitar fricción con usuarios. Visa, por ejemplo, ha debido equilibrar la seguridad con la experiencia del cliente, reduciendo falsos rechazos de transacciones legítimas al mismo tiempo que bloquea efectivamente el fraude.

El impacto de estos enfoques basados en analytics se ven en múltiples estudios de caso y aplicaciones. Por ejemplo, el estudio de Zheng, Yuan y Wu (2018) detalla casos donde la analítica de datos permitió detectar fraudes financieros específicos con mayor eficiencia. Asimismo, Baah et al. (2024) señalan que la analítica de *Big Data* combinada

con *machine learning* ha facilitado una **vigilancia más dinámica y adaptativa** de actividades fraudulentas, integrándose a menudo con sistemas existentes de las instituciones. Estos autores enfatizan que big data analytics habilita el monitoreo en tiempo real y puede analizar tanto datos transaccionales estructurados como datos de comportamiento del cliente para hallar patrones sospechosos. Sin embargo, también reconocen desafíos significativos para su implementación, tales como problemas de privacidad de datos, cumplimiento regulatorio y los altos costes tecnológicos.

En términos prácticos, la industria financiera ha adoptado herramientas especializadas de **Fraud Detection Systems** con capacidades de analytics. Muchas de estas soluciones comerciales incorporan modelos de ML actualizados continuamente y enriquecimiento de datos. Un ejemplo clave es la suite **Swift Compliance Analytics**, ofrecida por la red SWIFT a sus bancos miembros. Esta herramienta aprovecha los datos de mensajería SWIFT de cada banco para identificar patrones de riesgo y posible incumplimiento en pagos internacionales. Según información de SWIFT, Compliance Analytics provee a los bancos una **vista consolidada de su tráfico de pagos global**, alertando sobre picos inusuales, posibles brechas de políticas internas y permitiendo visualizar **tendencias gráficas** para investigaciones focalizadas. También facilita evaluaciones de relaciones de corresponsalía, ayudando a garantizar la debida diligencia en todas las transacciones. Es decir, combina analítica de fraude con analítica de cumplimiento (sanctions, KYC) en el contexto de transacciones transfronterizas.

Otro ejemplo industrial es el uso de **analítica avanzada por redes de tarjetas de pago**: Visa y MasterCard han desarrollado sus propios motores de AI (como *Visa Advanced Authorization*) que, como ya se indicó, analizan cientos de atributos en cada transacción y generan una puntuación de riesgo en tiempo real. Estas soluciones han revolucionado la capacidad de los emisores y compradores para **responder de inmediato** a actividades potencialmente fraudulentas a nivel global, marcando un contraste marcado con los enfoques tradicionales que detectaban fraude solo tras análisis manual días después.

En conclusión, los enfoques basados en analytics aportan **flexibilidad, velocidad y profundidad** al proceso de detección de fraudes internacionales. La **flexibilidad** proviene de la habilidad de los modelos de *machine learning* para recalibrarse con nuevos datos y captar patrones complejos (por ejemplo, detectando fraudes emergentes que no siguen patrones históricos exactos). La **velocidad** se logra con procesamiento en tiempo real y automatización de alertas, crucial para frenar transacciones fraudulentas mientras ocurren. Y la **profundidad** se refiere a la capacidad de analizar datos multifacéticos (transacciones, relaciones, comportamientos) encontrando conexiones sutiles que un humano no sería capaz de ver. Por estas razones, la literatura reciente sugiere que la analítica de datos se está consolidando como una **herramienta indispensable** en la lucha contra el fraude financiero, complementando (que no reemplazando completamente) a los sistemas tradicionales.

2.4 Analytics y funciones de compliance en la prevención de fraude

Un componente esencial para prevenir fraudes en transacciones internacionales es el **cumplimiento normativo** (*compliance*) de las instituciones financieras y corporaciones, especialmente respecto a regulaciones antilavado de dinero (AML) y contra financiamiento del terrorismo (CFT). Las áreas de compliance tradicionalmente se encargan de monitorear las operaciones para asegurarse de que cumplen con las leyes y regulaciones aplicables, reportando a las autoridades cualquier actividad sospechosa (por ejemplo, mediante **reportes de operación sospechosa** o SAR). En los últimos años, se ha vuelto evidente que las funciones de compliance pueden potenciarse de sobremanera mediante la incorporación de herramientas de analytics, lo cual permite una prevención del fraude más efectiva y al mismo tiempo un mejor cumplimiento de las obligaciones legales.

El **análisis de riesgo de transacciones (TRA)** es un buen ejemplo de la intersección entre analytics y compliance. Como describe Stripe (2024), el TRA implica analizar datos transaccionales en busca de patrones inusuales o riesgosos que puedan indicar fraude **o violaciones regulatorias**. Es decir, no solo se busca proteger contra pérdidas financieras, sino también **garantizar el cumplimiento de normativas** (por ejemplo, detectar posibles operaciones de lavado de dinero, transacciones que violen sanciones internacionales, etc.). Un sistema de TRA bien diseñado incorpora componentes como la recolección amplia de datos (historial transaccional, datos del cliente, datos externos económicos o geopolíticos), la identificación y evaluación de riesgos (fraude, crédito, mercado, etc.), la mitigación (acciones para reducir riesgos como límites o verificaciones adicionales), la supervisión continua y elaboración de informes para los interesados, y aún más importante, el **cumplimiento normativo y regulatorio** integrado en cada paso. Esto último implica asegurar que todos los procesos de transacción cumplan las leyes pertinentes, incluyendo estándares contra el blanqueo de capitales (AML), requisitos de KYC y otras normativas financieras.

La **analítica de datos** se ha convertido en un aliado de compliance al permitir cumplir más fácilmente con las normativas de monitoreo transaccional: mediante la vigilancia automatizada de las transacciones y la documentación/gestión inmediata de cualquier actividad sospechosa, las empresas pueden abordar las obligaciones regulatorias de forma más eficiente. Por ejemplo, los reguladores suelen exigir a los bancos que identifiquen patrones de posible lavado de dinero (como múltiples depósitos fraccionados (*smurfing*), movimientos en jurisdicciones de riesgo, clientes con actividades inusuales). Hacer esto manualmente sería inviable, pero con analytics se pueden crear perfiles de riesgo dinámicos y alertas automáticas que detecten estos escenarios en base a modelos.

Un claro indicador de la sinergia entre analytics y compliance es el auge del concepto **RegTech** (tecnología regulatoria). RegTech se refiere al uso de tecnologías innovadoras (Big Data, AI, blockchain, etc.) para mejorar la eficacia y eficiencia del cumplimiento regulatorio. En materia antifraude y AML, muchas soluciones RegTech analizan grandes conjuntos de datos de clientes y transacciones para identificar incumplimientos potenciales. Por ejemplo, soluciones que escanean todas las transacciones de un banco contra listas sancionatorias (OFAC, la UE, ONU) en tiempo real usando algoritmos rápidos; o herramientas que monitorean patrones inusuales de transacciones entre clientes para reportarlos oportunamente a la Unidad de Inteligencia Financiera (UIF) correspondiente.

Desde la perspectiva de la literatura y estándares internacionales, organizaciones como el **Grupo de Acción Financiera Internacional (GAFI)** han señalado la importancia de utilizar un enfoque basado en riesgo (Risk-Based Approach) en los programas AML/CFT. Esto implica que los recursos de monitoreo y prevención deben focalizarse donde el análisis indique mayores riesgos de lavado o fraude. La analítica avanzada es casi un requisito para implementar este enfoque de manera efectiva, ya que se necesita procesar información variada para asignar correctamente niveles de riesgo. Las **40 Recomendaciones del GAFI** (marco estándar internacional contra lavado de dinero) incitan a las instituciones a emplear sistemas de monitoreo que permitan detectar y reportar operaciones sospechosas. En la práctica, para cumplir con la recomendación sobre monitoreo continuo, los bancos han tenido que adoptar sistemas automatizados (basados en reglas y recientemente en ML) que revisan transacciones en busca de señales definidas de riesgo (muchas de las cuales son similares a señales de fraude).

Las leyes contra el lavado de dinero en distintas jurisdicciones imponen obligaciones específicas que son difíciles de gestionar sin analytics. Por ejemplo, la Ley de Secreto Bancario de EE.UU. (Bank Secrecy Act, BSA) y sus disposiciones posteriores (como la *USA PATRIOT Act*) requieren que los bancos reporten operaciones en efectivo mayores a $10,000 (CTR) y cualquier actividad sospechosa a través de SARs. Con miles de transacciones diarias, los bancos dependen de sistemas que filtren automáticamente aquellas que cumplen los criterios umbral (ej. CTR) y, más complejo aún, identifiquen actividades sospechosas que merezcan un SAR (por ejemplo, un cliente haciendo múltiples transacciones pequeñas que suman justo debajo de $10k para evadir el CTR, un patrón típico de structuring). Los sistemas de analytics pueden detectar ese *structuring* al correlacionar múltiples transacciones fragmentadas en un periodo. Asimismo, las regulaciones AML exigen hacer **diligencia debida del cliente (KYC)**, esto es, verificar identidad, entender el perfil transaccional esperado del cliente y monitorear desviaciones. Analytics ayuda a perfilar clientes usando datos históricos y comparar su comportamiento con pares para resaltar anomalías.

Un beneficio secundario de incorporar analytics en compliance es la **reducción de coste de cumplimiento** y la mejora en la reputación de la entidad. Tradicionalmente, los bancos han tenido que emplear grandes equipos de analistas para revisar alertas de

sistemas basados en reglas (con altos falsos positivos). Un sistema de *machine learning* bien calibrado puede reducir drásticamente las alertas irrelevantes al aprender patrones más refinados, lo que significa que los analistas dedican su tiempo solo a verdaderas sospechas. Además, un banco capaz de demostrar a sus reguladores que cuenta con sistemas avanzados de detección (por ejemplo, monitoreo en tiempo real, modelos adaptativos) puede tener un mejor diálogo durante inspecciones y reducir el riesgo de sanciones por fallas en prevención. No hay que olvidar que en los últimos años ha habido multas multimillonarias a bancos internacionales por no detectar a tiempo esquemas de lavado que pudieron haberse identificado con analítica más rigurosa (casos como HSBC en 2012, o Danske Bank en el escándalo de Estonia 2018, donde fluyeron miles de millones en transacciones sospechosas sin ser reportadas a tiempo).

En conclusión, la **integración de analytics en las funciones de compliance** representa una tendencia poderosa: por un lado, mejora la **capacidad preventiva** contra fraudes y delitos financieros al aprovechar la automatización y la inteligencia de datos; por otro, **asegura el cumplimiento regulatorio** al ayudar a las organizaciones a satisfacer las exigencias de monitoreo y reporte que imponen las leyes internacionales. Como resultado, muchas instituciones están evolucionando sus áreas de compliance hacia un enfoque de **"Compliance Analytics"**, donde el análisis de datos es central para la toma de decisiones de riesgo y la detección de conductas ilícitas antes de que causen un daño mayor.

3. Marco normativo

El **marco normativo** aplicable a la prevención de fraudes en transacciones internacionales abarca un amplio conjunto de leyes, regulaciones y estándares tanto a nivel supranacional como de países específicos. Estas normativas buscan proteger la integridad del sistema financiero global y del comercio internacional, estableciendo obligaciones para las instituciones en cuanto a la detección, prevención y reporte de actividades fraudulentas o de lavado de dinero. A continuación, se describen los principales componentes de este marco normativo, incluyendo iniciativas internacionales, legislación de referencia en distintas jurisdicciones y estándares de mejores prácticas.

3.1 Estándares internacionales y organismos clave

Grupo de Acción Financiera Internacional (GAFI/FATF): Fundado en 1989, el GAFI es el organismo intergubernamental líder en establecer estándares globales contra el lavado de dinero, financiamiento del terrorismo y, por extensión, otros delitos

financieros. Sus famosas **40 Recomendaciones** (revisadas más recientemente en 2012 y actualizadas periódicamente) constituyen un marco que los países deben seguir para desarrollar sus leyes nacionales. Entre estas recomendaciones figuran la obligación de las instituciones financieras de aplicar una **debida diligencia del cliente (KYC)**, llevar registros de transacciones, reportar operaciones sospechosas, y tener programas internos de prevención. Si bien el foco original del GAFI es AML/CFT, muchas de sus recomendaciones cubren prácticas que también sirven para prevenir fraudes (por ejemplo, la Recomendación 20 exige reportar sin retraso las operaciones sospechosas de lavado o de otro delito subyacente, lo que incluye fraude). El GAFI evalúa periódicamente a sus países miembros y publica "listas grises" y "listas negras" de jurisdicciones con deficiencias en sus regímenes ALD/CFT, influyendo en cómo se manejan las transacciones internacionales con esos países.

Naciones Unidas y convenios internacionales: En el plano multilateral, la **Convención de las Naciones Unidas contra la Corrupción (CNUCC)** y la **Convención de Palermo (contra la delincuencia organizada transnacional)** contienen disposiciones relacionadas con el lavado de activos y la cooperación internacional en materia de recuperación de activos y enjuiciamiento de fraudes masivos. La ONU también impulsa resoluciones de sanciones internacionales (por ejemplo, contra regímenes o grupos terroristas) que obligan a los países a congelar transacciones de ciertas personas o entidades listadas; esto se conecta con la prevención de que fondos ilícitos fluyan globalmente.

Basel Committee on Banking Supervision (BCBS): Aunque centrado en regulaciones prudenciales, el Comité de Basilea ha emitido apartados relevantes como el *Sound Management of Risks related to Money Laundering and Financing of Terrorism* (2014), que reforzó expectativas sobre los bancos para tener controles adecuados. También ha abordado el fraude en su documento *Fraud Risk Management* (2011), que si bien no es vinculante, establece principios para que los bancos gestionen el riesgo de fraude (por ejemplo, tener estrategias proactivas, marcos de control interno, etc.).

Organismos regionales similares al GAFI: Existen grupos estilo GAFI a nivel regional (conocidos como "FATF-Style Regional Bodies") que promueven estándares ALD/CFT. Por ejemplo, Moneyval (Europa), GAFILAT (América Latina), APG (Asia-Pacífico), entre otros. Estas entidades adaptan las recomendaciones globales a contextos regionales y evalúan a sus países miembros.

3.2 Legislación en los Estados Unidos

Debido al rol central de EE.UU. en las finanzas internacionales, sus leyes anti-fraude y anti-lavado tienen alcance global. Las más destacadas incluyen:

- **Bank Secrecy Act (BSA) de 1970:** Considerada la piedra angular de la regulación ALD en EE.UU. (también llamada Currency and Foreign Transactions Reporting Act). Fue la primera legislación que buscó prevenir y detectar el lavado de dinero a través de instituciones financieras. La BSA impone requerimientos de registro y reporte, como:
    - Presentar **Reportes de Transacciones Monetarias (CTR)** por transacciones en efectivo mayores a $10,000.
    - Mantener registros de compras de instrumentos monetarios (cheques de viajero, giros) arriba de $3,000.
    - Establecer programas de cumplimiento ALD en las instituciones (esto se reforzaría con leyes posteriores).

  La BSA sentó las bases para la cooperación de los bancos con las investigaciones gubernamentales, obligándolos a "seguir el rastro del dinero" y reportar movimientos significativos de fondos.

- **Money Laundering Control Act (1986):** Criminalizó el lavado de dinero como delito federal autónomo. Antes de esta ley, se perseguía el lavado indirectamente mediante delitos subyacentes; a partir de 1986, el acto de lavar dinero (ocultar el origen de fondos ilícitos) en sí mismo es un crimen. También permitió la confiscación de activos asociados sin necesidad de condena penal (forfeiture civil). Complementó a la BSA ampliando su alcance.
- **Annunzio-Wylie Anti-Money Laundering Act (1992):** Requirió a los bancos implementar **programas formales de prevención de lavado** y elevó penas. Introdujo la obligación de presentar **Reportes de Actividad Sospechosa (SAR)** por parte de las instituciones financieras. A partir de entonces, los bancos en EE.UU. deben reportar cualquier patrón o transacción que consideren sospechosa de involucrar fondos ilícitos o intento de encubrirlos, aun si la cantidad es inferior a $10k. Este mecanismo SAR es una herramienta crucial de compliance para detectar posibles fraudes también (un fraude financiero a menudo genera actividades sospechosas similares a las de lavado).
- **USA PATRIOT Act (2001):** Aprobada tras los atentados del 11-S, fortaleció de manera significativa el marco ALD/CFT. Extendió requisitos de *due diligence* a una gama más amplia de instituciones (como empresas de envío de dinero, casas de cambio), incrementó la cooperación internacional y estableció los **Customer Identification Programs (CIP)** o programas de identificación de cliente (lo que se conoce como KYC: "Know Your Customer"). Los bancos deben verificar la identidad de sus clientes y evaluarlos contra listas de sanciones y terrorismo. También prohibió relaciones de corresponsalía bancaria con *shell banks* (bancos fantasma sin presencia física real) y exigió *due diligence* mejorada en corresponsalías extranjeras y cuentas de personas políticamente expuestas (PEPs). La Patriot Act, al centrarse en la financiación terrorista, implícitamente reforzó todo el régimen antifraude, ya que redujo resquicios que podían ser explotados por redes ilícitas globales.
- **Financial Crimes Enforcement Network (FinCEN):** Si bien es una agencia (del Tesoro) más que una ley, FinCEN juega un papel normativo importante. Administra la BSA y sus reglamentos, emite guías interpretativas y recopila los

CTR, SAR y demás reportes. FinCEN ha implementado reglas estrictas para la diligencia debida del cliente y requerido, por ejemplo, la identificación del **beneficiario final** (beneficial owner) de cuentas corporativas –una medida clave para evitar uso de empresas fachada en fraudes.

Además de las leyes ALD, EE.UU. tiene normativa extensa contra fraudes específicos: por ejemplo, la **Foreign Corrupt Practices Act (FCPA)** de 1977, que prohíbe el soborno de funcionarios extranjeros por empresas estadounidenses. La FCPA no trata directamente transacciones financieras corrientes, pero es relevante porque muchos esquemas de corrupción internacional implican transferencias de dinero fraudulentas (sobornos) que luego se ocultan, a menudo catalogables como lavado de dinero. La FCPA ha obligado a empresas multinacionales a reforzar sus controles internos y programas de compliance para evitar pagos corruptos, y esto incluye monitoreo de pagos transfronterizos inusuales que podrían ser sobornos encubiertos (por ejemplo, a consultores o agentes en otros países).

También es importante mencionar las leyes de fraude bancario, electrónico y similares (ej. **Bank Fraud Act**, **Wire Fraud statutes**) que penalizan diversos fraudes. Cuando las transacciones internacionales usan medios electrónicos (lo que es lo usual), entran bajo la jurisdicción de fraude electrónico federal en EE.UU. si afectan instituciones estadounidenses. El Departamento de Justicia (DOJ) persigue estos casos apoyado en criterios como materialidad del daño, intencionalidad y jurisdicción, como señalan programas legales de whistleblower.

En suma, el marco de EE.UU. obliga a las instituciones a **monitorear y reportar transacciones sospechosas** rigurosamente. Sus leyes AML dificultan que criminales integren fondos ilícitos al sistema financiero, exigiendo a bancos y otras entidades mantener sistemas de control y detección robustos. Este marco normativo estadounidense ha servido de modelo para muchos otros países y, dado que el dólar es moneda principal de reserva, casi cualquier banco en el mundo que procese pagos en USD termina indirectamente sujeto a estas reglas (vía corresponsalías con bancos de EE.UU., etc.). Así, un fraude de alcance internacional podría implicar violaciones a varias de estas leyes si toca el sistema financiero estadounidense.

3.3 Normativa en la Unión Europea

La Unión Europea ha desarrollado un marco integral contra el lavado de dinero y fraude financiero que aplica a todos sus estados miembros, principalmente a través de Directivas comunitarias que luego se son traspuestas a las legislaciones nacionales:

- **Directivas Anti-Blanqueo de Capitales (AMLD):** La UE ha emitido sucesivas directivas ALD/CFT: la 4ª Directiva (2015/849), 5ª Directiva (2018/843) y 6ª Directiva (2018/1673), entre otras modificaciones. Estas directivas imponen obligaciones semejantes a las de EE.UU.:
    - Identificación formal de clientes y beneficiarios reales, con enfoque basado en riesgo (KYC).
    - Reporte de operaciones sospechosas a la *unidad de inteligencia financiera* nacional (en España, el SEPBLAC).
    - Conservación de registros y establecimiento de controles internos.

      La 5ª Directiva (AMLD5) en particular reforzó la transparencia sobre beneficiarios finales creando registros centrales en cada país para titulares reales de empresas (para evitar uso de empresas opacas), e incluyó a nuevas entidades como casas de cambio de criptomonedas dentro del ámbito de AML. También mejoró el acceso de autoridades a información financiera para investigar fraudes y esquemas de lavado a nivel europeo.

- **Reglamento de Transferencias de Fondos (EU 2015/847):** Impone que las transferencias de fondos incluyan datos completos sobre ordenante y beneficiario (nombre, cuenta, dirección o ID) para asegurar la trazabilidad. Esto es crucial para que los pagos transfronterizos puedan ser monitoreados y vinculados a personas concretas, dificultando el anonimato de transacciones fraudulentas. Los proveedores de pago deben rechazar transferencias que no vengan con la información requerida, ya que la norma busca prevenir que fondos ilícitos se muevan sin dejar rastro identificable.
- **Reglamento General de Protección de Datos (GDPR):** Si bien no es específico de fraude, GDPR (2016/679) afecta la prevención de fraude porque limita cómo se pueden tratar datos personales. Las instituciones deben equilibrar la analítica antifraude con la protección de datos. GDPR permite procesar datos personales para prevenir delitos (fraude incluido) bajo base de interés público o legítimo, pero impone garantías (por ejemplo, minimización de datos, derecho a explicación de decisiones automatizadas en ciertos casos). Esto significa que al implementar sistemas de detección automática basados en ML, los bancos europeos deben tener cuidado con la transparencia y posible no discriminación, temas que tocaremos en la discusión.
- **Otras normativas relevantes:** La UE también promulgó la **Directiva (UE) 2019/713** relativa a la lucha contra el fraude y falsificación de medios de pago distintos del efectivo, que actualiza definiciones y sanciones penales por fraudes con tarjetas, pagos electrónicos, etc., adaptándolos a la era digital. Igualmente, en el campo de mercados financieros, el Reglamento MAR sobre abuso de mercado tipifica sanciones por fraudes como el *insider trading* y la manipulación (importante para fraudes en transacciones bursátiles internacionales).

La aplicación de la normativa europea se apoya en instituciones nacionales (por ejemplo, el SEPBLAC en España, Tracfin en Francia, etc.) y en la cooperación coordinada de agencias europeas (Eurojust, Europol). Adicionalmente, la UE está

estableciendo una nueva **Autoridad Anti-Blanqueo** (AMLA) en los próximos años para supervisar de forma más uniforme el cumplimiento AML en el bloque.

En cuanto a **fraude comercial internacional**, la UE tiene regulaciones aduaneras y fiscales para combatir fraudes caros a los Estados (p.ej., fraude de IVA en comercio intracomunitario). La Oficina Europea de Lucha contra el Fraude (OLAF) se dedica a investigar fraudes que afectan al presupuesto de la UE, incluyendo fraude aduanero en importaciones, uso fraudulento de fondos europeos, etc. Un ejemplo es el fraude carrusel de IVA, un esquema intracomunitario donde se aprovecha la exención de IVA en exportaciones para hacer reclamaciones fraudulentas: la UE ha tenido que reforzar controles y mecanismos de intercambio de información entre países para detectarlo.

3.4 Marco normativo en otras jurisdicciones y convergencia global

Muchos otros países han alineado su legislación con los estándares GAFI. Por ejemplo:

- **Reino Unido:** Contaba con la *Money Laundering Regulations* (actualizada en 2017 acorde a AMLD4) y la *Proceeds of Crime Act* (POCA) 2002 que tipifica el lavado de dinero. Adicionalmente, el **UK Bribery Act 2010** es muy estricto respecto a sobornos internacionales (incluso más extraterritorial que FCPA), requiriendo procedimientos adecuados de prevención en empresas. La FCA (Financial Conduct Authority) supervisa a bancos en su cumplimiento AML y antifraude, imponiendo multas si fallan.
- **Latinoamérica:** Países como México (Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita), Colombia (normas de la UIAF), Argentina (Unidad de Información Financiera) han legislado fuertemente en AML siguiendo recomendaciones GAFI. Brasil, por ejemplo, tipifica lavado en Ley 12.683/2012. En general, en la región se exige a bancos reportar transacciones sospechosas y cumplir debida diligencia; además, hay esfuerzos para combatir la corrupción (que conlleva fraudes en transacciones públicas) mediante leyes inspiradas en la FCPA (como la Ley Anticorrupción brasileña de 2013).
- **Asia:** Hong Kong, Singapur, Australia tienen regímenes AML estrictos. Singapur, centro financiero internacional, posee la *Corruption, Drug Trafficking and Other Serious Crimes Act* y regula fuertemente las obligaciones de los bancos en AML/CFT. China ha fortalecido en años recientes su marco ALD y anti-fraude, aunque la aplicación práctica varía. India tiene la *Prevention of Money Laundering Act* (2002).
- **África y Oriente Medio:** Han mejorado marcos por pertenecer muchos países a FATF o grupos regionales. Por ejemplo, Sudáfrica (Financial Intelligence Centre Act), UAE (leyes AML 2018) que son cruciales en plazas emergentes de comercio.

Cabe destacar que independientemente de la jurisdicción local, las **instituciones financieras internacionales** suelen adoptar políticas globales internas que cumplen con los estándares más altos de entre sus jurisdicciones de operación. Un banco europeo operando en Latinoamérica, por ejemplo, aplicará sus políticas centrales de compliance que probablemente exceden requerimientos mínimos locales, para garantizar uniformidad y evitar sanciones en casa. Asimismo, la globalización ha dado paso a memorandos de entendimiento entre reguladores y **operativos internacionales conjuntos** para perseguir grandes esquemas de fraude y lavado. Organismos como Interpol y Egmont Group (red mundial de Unidades de Inteligencia Financiera) facilitan el intercambio de información que es vital para rastrear fraudes que cruzan fronteras.

Un área normativa emergente es la regulación sobre **tecnologías en finanzas** que puede incidir en el fraude: por ejemplo, reglas sobre criptomonedas (muchos países están empezando a regular casas de cambio cripto dentro del ámbito AML, ante casos de uso de criptodivisas para fraude o lavado), y regulaciones de servicios de pago digitales (como la **PSD2** en Europa, que introdujo requisitos de autenticación fuerte de cliente para reducir fraudes en pagos electrónicos).

En conclusión, el marco normativo internacional en materia de prevención de fraude y delitos financieros es complejo, pero converge en principios comunes: **conocer al cliente, monitorear activamente transacciones, reportar actividades inusuales, cooperar internacionalmente** y establecer **controles internos robustos**. Estas obligaciones legales, además de buscar castigar el fraude después de ocurrido, tienen un claro enfoque preventivo, empujando a las organizaciones a implementar sistemas de detección temprana – un rol que, como hemos visto, es potenciado en gran manera por la adopción de analytics y tecnologías avanzadas. De hecho, se puede afirmar que **el cumplimiento normativo efectivo hoy demanda el uso de herramientas analíticas**, ya que es la única vía para manejar el volumen y complejidad de datos necesarios para detectar irregularidades en un mundo financiero interconectado.

4. Metodología

El trabajo se desarrolla con un enfoque metodológico de carácter **cualitativo y exploratorio**, basado principalmente en una **revisión sistemática de la literatura** y el análisis conceptual de casos documentados. A diferencia de una investigación empírica con recolección de datos primarios, este estudio se basa en la integración y análisis crítico de fuentes secundarias (artículos académicos, informes técnicos, normativas y estudios de caso), con el objetivo de **sintetizar conocimiento** y extraer patrones relevantes sobre el uso de analytics en la prevención de fraude internacional. A continuación, se detallan los aspectos metodológicos específicos:

4.1 Revisión bibliográfica sistemática

Se lleva a cabo un proceso estructurado de búsqueda y selección de literatura relevante. Para ello, se definen palabras clave en español e inglés (por ejemplo, “fraude transacciones internacionales”, “fraud detection analytics”, “AML compliance analytics”, “fraud case study international”) que se utilizan en bases de datos académicas (IEEE Xplore, ACM Digital Library, Scopus) y motores de búsqueda especializados. Se establecen criterios de inclusión, dando prioridad a estudios:

- Publicados en los últimos ~10 años (2015-2025) para asegurar un cierto grado de actualidad, complementando con trabajos clásicos fundamentales (como Bolton & Hand 2002, Zhu et al. 2021) para fundamentos teóricos.
- Relevantes al **tema central**: se incluyeron artículos sobre detección de fraude con data analytics, big data en fraude financiero, machine learning para AML, etc., así como publicaciones sobre casos de fraude internacional y marcos regulatorios.
- Respaldados por revisión por pares (en el caso de fuentes académicas) o emitidos por organizaciones reconocidas (p. ej., informes de corporaciones financieras, guías de reguladores, blogs de instituciones financieras reconocidas).

Se revisó una amplia base de literatura académica y técnica para construir el marco teórico, normativo y de análisis de casos, seleccionando aproximadamente 40 fuentes clave a partir de un conjunto inicial más amplio. Las referencias incluyen artículos académicos, normativa legal, white papers y documentación relevante del sector.

Durante la revisión, se extrae de cada fuente los hallazgos clave relacionados con:

- Técnicas de detección de fraude (p. ej., qué algoritmos se usan, qué efectividad reportan, desafíos mencionados).
- Tendencias en la industria (ej., inversión en IA por parte de empresas de pagos, uso de analytics en bancos).
- Aspectos regulatorios y de cumplimiento (ej., qué obligaciones existen y cómo la tecnología las aborda).
- Casos concretos de fraude o iniciativas anti-fraude.

Los hallazgos de distintas fuentes se usan para identificar **coincidencias y divergencias**. Por ejemplo, si múltiples estudios coincidían en la importancia de la detección en tiempo real o en la necesidad de reducir falsos positivos, esto se resalta como tendencia clave. Si había opiniones diferentes (por ejemplo, visiones críticas sobre limitaciones de AI en compliance), también se recogen para asegurar una visión equilibrada.

4.2 Análisis conceptual y crítico

Más allá de recopilar información, se lleva a cabo un análisis crítico de los contenidos. Esto implica situar los hallazgos en el contexto de las preguntas de investigación y evaluar la **validez y aplicabilidad** de las afirmaciones. Por ejemplo, al considerar un estudio que reporta éxito de cierto algoritmo para detectar fraude con datos públicos, se discute si ese enfoque sería viable en transacciones internacionales reales con restricciones de datos. Del mismo modo, se contrasta las ventajas teóricas de analytics (reportadas en la literatura) con las **barreras prácticas** (reportadas en casos de la industria o en la normativa).

El enfoque investigativo adoptado es predominantemente **descriptivo-analítico**: se describe el estado del arte (qué se hace, qué se conoce) y se analiza cómo encajan las piezas (tecnología, procesos, normativas) para responder a los objetivos planteados. No se realiza experimentación ni se construyen modelos propios, dado que el alcance es teórico y aplicado "en papel".

4.3 Fuentes de casos y datos aplicados

En la sección de *Análisis aplicado*, se recogen casos ilustrativos. La metodología para esa sección implica identificar **ejemplos documentados** de uso de analytics en prevención de fraude o bien casos clave de fraude donde su análisis retrospectivo sugiere el valor de analytics. Estas fuentes incluyen:

- Notas de prensa (p. ej., comunicado de Visa sobre sus sistemas de IA y el fraude prevenido, informes de bancos sobre implementaciones de IA).
- Blogs y reportes de proveedores de soluciones (*industry reports* de consultoras como Deloitte, LexisNexis, etc., cuando disponibles en español o inglés).
- Estudios de organismos internacionales (algún reporte de FATF con casos, informes de Europol u OLAF).
- Documentación de casos judiciales relevantes (p. ej., el caso Bangladesh Bank) y análisis forenses disponibles públicamente.

A partir de estas, se elaboran **resúmenes de caso** tratando de resaltar: contexto, qué sucedió, cómo se detectó o no el fraude, y qué papel jugó o pudo jugar la analítica de datos en ello.

4.4 Alcances y delimitaciones

Es importante señalar que si bien el trabajo cubre un amplio espectro (teórico, normativo, metodológico, aplicado), existen ciertas delimitaciones metodológicas. Por un lado, la **falta de datos transaccionales reales** (por motivos de confidencialidad y alcance del TFG) impide realizar una prueba empírica de las técnicas descritas. La validación de supuestos se basa en estudios de terceros y no en experimentación propia.

Esto limita el trabajo a un plano conceptual; sin embargo, se busca mitigar esto aportando múltiples referencias empíricas de la literatura para respaldar las afirmaciones.

Por otro lado, la **rapidez de cambios en el entorno** fraude-analytics implica que cualquier revisión es una foto temporal. Para abordar esto, se incluyen las fuentes más recientes disponibles (hasta 2024-2025) y se enfatizan tendencias en desarrollo, como la adopción de IA generativa o la futura autoridad AML europea, aunque aún no hayan madurado completamente.

4.5 Estructura de análisis

La metodología define que la estructura del documento sigue un orden lógico derivado de las preguntas de investigación: inicio con conceptos, luego marco legal, luego enfoque metodológico y finalmente análisis de casos y discusión. Esto responde también a un **método analítico-deductivo**: tras exponer los principios generales (teoría, leyes), se deduce su aplicación en ejemplos prácticos y se reflexiona críticamente sobre ellos.

En síntesis, la metodología del TFG se centra en la **síntesis rigurosa y crítica** de información existente, con la meta de construir un argumento sólido sobre la hipótesis planteada. La revisión sistemática de literatura asegura la **base académica**, mientras que el análisis de casos aporta la **dimensión aplicada**. La combinación de ambos, sumada a la discusión crítica, permite generar conclusiones informadas y ofrecer recomendaciones con sustento tanto teórico como práctico.

5. Análisis aplicado

En esta sección se examinan aplicaciones prácticas y casos reales que ilustran cómo la analítica de datos se utiliza (o puede utilizarse) para prevenir y detectar fraudes en transacciones internacionales. Se presentan **estudios de caso** y **tendencias metodológicas** observadas en la industria financiera, con el fin de conectar la teoría y la normativa discutidas con situaciones concretas. Los casos abarcan tanto éxitos en la detección de fraudes gracias a analytics, como lecciones aprendidas de incidentes donde la falta o insuficiencia de análisis de datos contribuyó al problema.

5.1 Caso 1: Detección proactiva de fraude en pagos globales – Visa Advanced Authorization

Uno de los ejemplos representativos del uso de analytics a escala global es el sistema **Visa Advanced Authorization (VAA)**, parte de la red VisaNet que conecta instituciones financieras en todo el mundo. Visa procesa miles de millones de transacciones de pago internacionalmente, lo que la convierte en blanco de fraudes con tarjetas robadas, clonadas u otras formas de estafa en compras digitales transfronterizas. Para mitigar esto, Visa implementó desde los años 90 un sistema basado en **redes neuronales** que evalúa el riesgo de cada transacción en tiempo real. En la actualidad, VAA utiliza **modelos de aprendizaje automático de última generación** que analizan más de **500 atributos de riesgo en aproximadamente un milisegundo por transacción**, incluyendo: historial del titular, ubicación geográfica del comprador, patrón de compra, dispositivo utilizado, entre otros.

El sistema genera un **puntuación de riesgo** instantáneo que se envía al banco emisor de la tarjeta, el cual decide aprobar, denegar o marcar la transacción para verificación adicional. Gracias a esta capa de inteligencia, Visa reportó en 2019 que su plataforma ayudaba a prevenir alrededor de **USD 25 mil millones en fraudes al año** a nivel global. Además, Visa logró mantener la tasa de fraude en su red en **menos del 0,1%** de las transacciones totales, un mínimo histórico. Esto es considerable considerando que Juniper Research estimó el fraude en comercio electrónico mundial en $44 mil millones para 2024, lo cual implica que sistemas como el de Visa son cruciales para contener esas pérdidas.

Un elemento interesante de este caso es cómo Visa mantiene un equilibrio entre **seguridad y experiencia de usuario**. Los modelos de IA detectan no solo transacciones potencialmente malas sino también reconocen transacciones legítimas, aunque inusuales, reduciendo los **falsos positivos** (rechazos indebidos que molestan al cliente). Por ejemplo, si un tarjetahabiente realiza una compra grande fuera de su país, el sistema puede identificar si ese comportamiento, aunque raro, encaja con un perfil de viaje (quizás por geolocalización de compras previas), evitando un bloqueo innecesario. En cambio, si un estafador intenta múltiples compras pequeñas en diferentes países en corto tiempo, las correlaciones descubiertas por la IA (imposibles de ver con reglas simples) permiten bloquear esas transacciones rápidamente.

El éxito de Visa Advanced Authorization demuestra el poder de **combinar big data y aprendizaje automático en un entorno transaccional global**. Es probable que, sin este nivel de analítica, los fraudes con tarjetas especialmente en transacciones internacionales se hubieran disparado, pues los delincuentes apuntan a operaciones transfronterizas esperando menos controles. Hoy en día, redes similares (Mastercard con sistemas como Decision Intelligence, o AmEx) han adoptado enfoques comparables,

generando un estándar industrial donde la analítica en tiempo real es indispensable para cualquier procesador de pagos global.

5.2 Caso 2: Uso de Compliance Analytics en la banca internacional – Herramienta SWIFT

La red **SWIFT** (Society for Worldwide Interbank Financial Telecommunication) conecta a más de 11.000 instituciones financieras en 200 países, facilitando mensajería estandarizada para pagos internacionales interbancarios. Históricamente, SWIFT proveía solo el canal de mensajería, mientras cada banco gestionaba sus propios controles de fraude/AML. Sin embargo, en respuesta a incidentes de alto perfil (como el ciberfraude al Banco de Bangladesh en 2016, donde hackers enviaron mensajes SWIFT fraudulentos para sustraer fondos) y ante las crecientes exigencias regulatorias, SWIFT desarrolló la solución **Compliance Analytics**.

Lanzada en la segunda mitad de la década de 2010, **SWIFT Compliance Analytics** permite a los bancos miembros **analizar sus propios datos de tráfico SWIFT** con fines de detección de riesgo. En esencia, SWIFT toma todos los mensajes de pago enviados/recibidos por un banco y los consolida en una plataforma analítica segura donde el banco puede aplicar filtros, visualizaciones y comparativas. Según la descripción de SWIFT, esta herramienta ofrece una vista clara del tráfico de pagos, ayudando con funciones de KYC, AML y cumplimiento de sanciones.

Algunos casos de uso del sistema:

- Detectar **picos inusuales** en volúmenes de transferencias a ciertos países o contrapartes, lo que podría indicar actividad sospechosa (por ejemplo, si un banco observa repentinamente muchos envíos hacia un país con el que normalmente no transacciona, podría ser señal de un esquema de fraude o lavado usando ese banco como paso).
- Identificar **brechas potenciales de política interna**, como transferencias que violan límites o pasan por corresponsales no deseados. La herramienta alerta sobre “posibles incumplimientos de políticas”.
- Evaluar **tendencias y patrones** mediante gráficos: por ejemplo, tendencias mensuales de pagos relacionados con ciertas regiones. Esto ayuda a los oficiales de cumplimiento a focalizar investigaciones en tendencias atípicas.
- Facilitar la **diligencia debida en corresponsalía**: SWIFT Compliance Analytics tiene un módulo de *Correspondent Monitoring* que genera reportes globales para revisar la actividad de los bancos corresponsales. Esto es esencial porque un banco puede ser utilizado inadvertidamente por un corresponsal para mover fondos ilícitos; con la herramienta, un banco puede ver si ciertos corresponsales suyos envían mucho volumen hacia paraísos fiscales o reciben pagos de

entidades sancionadas, etc., y así tomar medidas (pedir aclaraciones, restringir relaciones).

Un ejemplo práctico: Supongamos que el Banco X observa mediante Compliance Analytics que en el último trimestre hubo un aumento del 300% en pagos procedentes de ciertos bancos pequeños de otro país, todos con destino final a cuentas en un tercer país distinto. Este patrón inusual podría sugerir una **estructura de "multi-hop" para ocultar origen de fondos**, típica de lavado. Con esa información, el Banco X puede investigar internamente esas transacciones, potencialmente elevar un reporte SAR a su regulador, o contactar a sus corresponsales para mayor información. Antes, detectar esto manualmente era improbable porque los datos estaban dispersos en miles de mensajes diarios.

Otro aspecto del caso SWIFT es que demuestra colaboración en la industria para combatir fraude: SWIFT, como cooperativa de bancos, desarrolló esta herramienta reconociendo que **la lucha contra el fraude/AML es un esfuerzo común**. Si un banco sufre un fraude como el de Bangladesh, es malo para la reputación y confianza en toda la red. Por ello, hay también iniciativas como **KYC Registry** de SWIFT donde los bancos comparten información de sus políticas AML y reciben alertas de contrapartes riesgosas.

Los resultados de implementar Compliance Analytics han sido positivos según reportes anecdóticos: varios bancos lograron identificar **transacciones sancionadas** que inicialmente pasaron (p.ej., pagos que involucraban personas que luego fueron añadidas a listas OFAC), permitiendo bloquear fondos a tiempo; otros detectaron **ineficiencias operativas** (como datos faltantes en mensajes) y las corrigieron. Aunque SWIFT no publica estadísticas agregadas de fraudes prevenidos, la percepción es que la herramienta **eleva el estándar de control** en pagos internacionales, complementando los sistemas internos de cada banco.

En resumen, el caso de SWIFT Compliance Analytics ilustra una **tendencia metodológica**: el uso de **plataformas compartidas de datos y analytics en la industria financiera** para afrontar amenazas comunes de fraude. Al centralizar ciertos análisis (respetando la confidencialidad de datos individuales de cada banco), se logran sinergias y se dota a incluso bancos medianos/pequeños de capacidades analíticas que quizás no podrían desarrollar solos. Esta democratización de la analítica antifraude en la red global es crucial para que los eslabones más débiles no sean explotados por delincuentes.

5.3 Caso 3: Escándalo de lavado en banca privada – Danske Bank Estonia (2014-2015)

Un contraejemplo a los anteriores (donde la analítica ayudó a prevenir) es el caso del **Danske Bank** en Estonia, considerado uno de los mayores escándalos de lavado de dinero en Europa. Si bien se trata principalmente de lavado de capitales, el esquema involucró transacciones internacionales fraudulentas de miles de millones de euros entre 2007 y 2015, y es ilustrativo por las lecciones sobre fallos de detección.

Danske Bank, el banco más grande de Dinamarca, operaba una filial en Estonia que manejaba cuentas de **no-residentes** (principalmente clientes de Rusia y ex URSS). Entre estos clientes había numerosas empresas fachada a través de las cuales se movieron fondos de posible origen ilícito (evasión fiscal, corrupción, fraudes diversos en Rusia). Investigaciones ulteriores revelaron que más de **€200.000 millones** en pagos sospechosos fluyeron por esa filial en pocos años sin ser reportados adecuadamente.

¿Qué falló desde el punto de vista analítico/compliance? Entre otros puntos:

- **Sistemas de monitoreo ineficaces:** Danske Estonia disponía de software básico de detección, pero aparentemente con **configuraciones muy laxas** (umbrales altos, reglas limitadas) que omitieron patrones obvios. Por ejemplo, no se detectó que empleados locales ayudaban a clientes a crear múltiples transferencias justas por debajo de los umbrales de reporte, o la creación de múltiples cuentas interconectadas moviendo fondos circularmente.
- **Alertas ignoradas:** Hubo reportes de la casa matriz y auditores internos señalando volúmenes inusuales de pagos de no residentes, pero la filial no actuó. Esto indica un fallo no solo tecnológico sino de **gobernanza de datos**: tener analytics no sirve si la cultura organizacional no le da seguimiento.
- **Falta de incorporación de datos externos:** Muchas de las empresas implicadas figuraban en listas de riesgo (por ejemplo, informes de prensa o bases de datos de empresas sin actividad real). Un sistema de analytics robusto podría haber incorporado una puntuación de riesgo externa por cliente. No se hizo, y algunas entidades claramente sospechosas (direcciones repetidas, nombres similares a empresas offshore) pasaron por alto.
- **Volumen no contextualizado:** Lo más sorprendente es el simple volumen: €200bn es gigantesco comparado con la economía estonia. Un simple análisis comparativo (analytics descriptivo) habría mostrado que la filial manejaba flujos decenas de veces superiores a su tamaño de negocio normal, una **anomalía macro** que debería haber saltado a la vista de un dashboard de riesgos.

Tras estallar el caso (2018), Danske Bank enfrentó investigaciones y multas. Desde entonces, han invertido mucho en mejorar sus sistemas AML y analítica, pero el daño ya estaba hecho. Este caso sirve para resaltar:

- La importancia de **parámetros adecuados** en los sistemas de detección (no sirve el mejor software si se configura para generar cero alertas).
- La necesidad de **supervisión central**: la matriz debió consolidar datos de filiales y aplicar analytics global para ver patrones de riesgo (similar a lo que hace hoy SWIFT con Compliance Analytics).
- Cómo **fraudes masivos** pueden ocurrir cuando los delincuentes explotan un nodo con controles débiles: en este caso, toda Europa del Este canalizó fondos sucios por Estonia. Este "eslabón débil" demuestra que la analítica preventiva debe ser adoptada universalmente, no solo por unos cuantos bancos grandes.

El aprendizaje para la industria fue drástico: a raíz de esto, muchos bancos nórdicos y europeos revisaron sus modelos de risk scoring, cerraron servicios a clientes no-residentes de alto riesgo y adoptaron herramientas de **network analytics** para detectar redes de cuentas asociadas. Por ejemplo, algunos incorporaron soluciones de inteligencia artificial que evalúan la **estructura de las relaciones de cuentas** (grafo) para ver si muchas cuentas aparentemente separadas comparten IPs, dispositivos o patrones (lo cual suele indicar un mismo beneficiario oculto manejándolas). Estas herramientas de análisis relacional podrían haber identificado que muchas empresas en Danske Estonia tenían administradores comunes o se transferían fondos entre sí en círculo, revelando la red fraudulenta.

Resumiendo, el caso Danske subraya que la **ausencia o mal uso de analytics** puede facilitar que se materialicen fraudes gigantescos. Es un llamado de atención a que la implementación de analytics debe ir acompañada de una cultura de cumplimiento activa y de actualizaciones constantes (pues los defraudadores cambiarán de táctica cuando detecten controles).

5.4 Caso 4: Prevención de fraude en comercio electrónico internacional – Plataforma Stripe

Las plataformas *fintech* y de pagos en línea enfrentan un panorama de fraude especialmente dinámico, pues conectan comercios de todo el mundo con consumidores y diversos métodos de pago. **Stripe**, una compañía global de procesamiento de pagos, ha destacado por integrar analytics y machine learning en su oferta de seguridad transaccional. Dado que muchos de sus clientes son comerciantes que venden internacionalmente, Stripe debe detectar fraudes con tarjetas robadas, *chargebacks* fraudulentos, y otras estafas que pueden provenir de cualquier lugar del globo.

Stripe desarrolló un sistema llamado **Radar**, que utiliza machine learning entrenado en **billones de datos** recopilados de su red de pagos global. Radar evalúa cada pago procesado con miles de etiquetas (features) y genera decisiones de aprobar/declinar. Un atributo valioso es que Stripe observa datos a través de múltiples comercios: por ejemplo, si una tarjeta presentó fraude en un comercio A, Radar lo aprende y puede declinar intentos con esa tarjeta en comercios B, C, etc., antes de que ocurra otro cargo fraudulento (esto es una ventaja de tener un **dataset compartido global**). Stripe menciona que Radar bloquea a priori una gran proporción de transacciones fraudulentas y reduce en más de un 25% los *chargebacks* para los comerciantes, comparado con no usarlo.

Un ejemplo de fraude internacional que Radar ayudaría a frenar: un estafador en país X prueba números de tarjeta robados comprando productos digitales pequeños en distintos sitios web globales (técnica de *card testing*). Tradicionalmente, hasta que cada comercio detectara el fraude habrían pasado varios intentos. Con analytics centralizado, Stripe identifica un patrón: la misma IP u ordenador haciendo compras fallidas en varios comercios, tarjetas declinadas por fondos insuficientes repetidamente, etc. La IA de Radar rápidamente *"aprende"* que esa firma digital es maliciosa y comienza a rechazar todos los pagos de ese origen para todos los comercios, cortando de raíz la operación. Esto ilustra la eficiencia de la **inteligencia colectiva** potenciada por analytics en la prevención de fraude distribuido.

Adicionalmente, Stripe combina su ML con **herramientas para que los usuarios comerciante definan reglas personalizadas**. Esto es importante porque cada negocio tiene tolerancia al riesgo distinta. Por ejemplo, un comerciante puede instruir que Radar rechace automáticamente pedidos internacionales de valor muy alto si el correo del cliente es recién creado (indicador de posible fraude). Stripe mezcla la **automatización** con la **personalización**, guiando a los usuarios con recomendaciones basadas en datos ("80% de comerciantes como tú rechazan pedidos con estas características…").

El resultado es un sistema robusto y flexible. Cabe notar que Stripe también educa a sus clientes sobre **análisis de riesgo de transacciones (TRA)**, como vimos en el recurso de Stripe en español, destacando componentes de análisis y cumplimiento. Esto muestra que más allá de la tecnología, hay una capa de **metodología y mejores prácticas** que se difunde.

La eficacia de plataformas como Radar se refleja en la confianza de grandes compañías globales (Amazon, Booking.com, etc. usan Stripe en parte de sus flujos). Para la temática de nuestro trabajo, este caso subraya:

- La importancia de **compartir datos y señales** para combatir fraude: analytics es más potente cuando se nutre de un ecosistema amplio (así los defraudadores no pueden aprovechar fragmentación de información).
- El valor de combinar **modelos ML globales con configuraciones locales**: equilibra la inteligencia general con el conocimiento específico de cada empresa.
- Cómo un enfoque analytics bien diseñado logra mitigar fraude manteniendo baja la fricción para usuarios legítimos, lo cual es crítico en comercio electrónico internacional donde la experiencia del cliente es muy sensible.

5.5 Tendencias metodológicas en la industria

Además de los casos puntuales, es útil resumir algunas **tendencias generales** observadas en cómo la industria está aplicando analytics en prevención de fraude internacional:

- **Adopción de la Inteligencia Artificial y Aprendizaje profundo:** Muchas instituciones están pasando de modelos basados en reglas o ML básico a incorporar **deep learning** (redes neuronales profundas) y técnicas avanzadas. Por ejemplo, algunos bancos emplean **modelos de redes recurrentes o LSTM** para detectar patrones secuenciales complejos en series de transacciones (útil para ver cómo evoluciona el comportamiento de una cuenta en el tiempo). Otros experimentan con **modelos generativos o de anomaly detection sofisticados** para encontrar aberraciones que escapaban a métodos anteriores. Si bien la IA ofrece mayor poder predictivo, también trae desafíos como la interpretabilidad (los reguladores comienzan a preguntar cómo explica un banco su modelo de fraude).
- **Herramientas de visualización y análisis para analistas:** Dado que no todo puede ni debe automatizarse, ha crecido la oferta de plataformas que presentan datos integrados (de múltiples sistemas) en **dashboards inteligentes** para los equipos de riesgo. Estas herramientas usan analytics para priorizar qué alertas revisar primero (ranking basado en riesgo), agrupar alertas relacionadas (p. ej. varias cuentas que apuntan al mismo beneficiario final) y proporcionar información contextual (dossiers del cliente, vínculos conocidos, etc.). De esta forma, un analista de compliance puede trabajar con eficacia multiplicada por la analítica. Esta tendencia reconoce que la **intervención humana sigue siendo crucial** en la toma de decisiones finales, pero empodera a las personas con mejor análisis.
- **Énfasis en prevención más que en reacción:** Tradicionalmente muchas instituciones "cazaban" fraude después de ocurrido, indemnizando al cliente pero asumiendo la pérdida. Ahora, impulsadas por normativas y por evitar pérdidas reputacionales, la tendencia es invertir en **sistemas preventivos** que reduzcan la incidencia del fraude antes de que suceda. Esto se logra con análisis en tiempo real y **colaboración interbancaria** (como compartiendo indicadores de fraude, listas de dispositivos sospechosos, etc.). Un ejemplo emergente es el uso de **consorcios de datos**: en algunos países, bancos comparten en tiempo real

ciertas alertas para frenar cadenas de fraude (por ej., si el Banco A detecta una transferencia fraudulenta y ve que va al Banco B, alerta al B para congelarla).

- **Analítica de nuevas fuentes de datos:** Además de los datos financieros tradicionales, se están incorporando fuentes como:
    - **Datos de dispositivos y biometría:** huella digital del dispositivo, comportamientos de tecleo, reconocimiento facial en autenticaciones, etc., todo analizado con ML para detectar posibles impostores.
    - **Redes sociales y web:** Algunas fintech analizan la presencia en línea de solicitantes de préstamos o participantes de transacciones para evaluar credibilidad (aunque esto choca con consideraciones éticas y de privacidad).
    - **Blockchain analytics:** Con el auge de las criptomonedas, han surgido empresas (Chainalysis, Elliptic) que emplean analytics para rastrear transacciones en cadenas de bloques públicas e identificar fondos asociados a hacks, ransomware, u otros ilícitos. Bancos y reguladores empiezan a usar estos servicios para complementariamente monitorear si fondos cripto que pasan a fiat vienen de fuentes dudosas.
- **Uso de técnicas híbridas y enfoques holísticos:** No existe una única bala de plata. La industria combina **múltiples métodos analíticos**: por ejemplo, primero un filtro de reglas sencillas para descartar casos obvios, luego un modelo ML supervisado para puntuar riesgo general, luego un modelo no supervisado para detectar outliers residuales. Este formato reduce la carga y mejora precisión. Además, se integran consideraciones de **ciberseguridad**: muchos fraudes se inician con brechas de seguridad (malware robando credenciales, phishing). Por ello, los equipos de fraude y ciberseguridad colaboran más, compartiendo data (intentos de intrusión, IPs maliciosas conocidas) que se integra en el análisis de riesgo transaccional.

El fraude actual es complejo y global, por lo que solo una respuesta igual de compleja (basada en análisis de datos inteligentes) puede combatirlo eficazmente.

6. Discusión crítica

En función del marco teórico, normativo y los casos analizados, en esta sección se aborda una discusión crítica sobre los hallazgos, enfatizando **limitaciones, desafíos y consideraciones prácticas** de los enfoques actuales para prevenir fraudes internacionales mediante analytics. Asimismo, se exploran las **implicaciones regulatorias y éticas** de estas prácticas, dado que la adopción de técnicas avanzadas no está exenta de fricciones con marcos normativos o con principios de equidad y transparencia. La discusión se organiza en torno a varios ejes principales: eficacia vs. falsos positivos, adaptabilidad vs. adversarios adaptativos, privacidad y cumplimiento normativo, costes e implementación, y alcance de la cooperación internacional.

6.1 Eficacia de la analítica vs. falsos positivos y fricción con el cliente

Uno de los dilemas centrales al implementar sistemas analíticos de detección de fraude es encontrar el **equilibrio entre detectar la mayor cantidad de fraudes posible (sensibilidad)** y minimizar las alertas incorrectas o **falsos positivos** (especificidad). Un sistema demasiado estricto puede bloquear o marcar transacciones legítimas, generando fricción con clientes y costes operativos de investigación; uno muy laxo dejará pasar fraudes. Este **trade-off** ha sido ampliamente reconocido por la industria. Como señaló una ejecutiva de Visa, "uno de los desafíos más difíciles en los pagos es separar las transacciones buenas de las malas sin añadir fricción al proceso". Visa logró avances importantes aplicando IA desde 1993, reduciendo el fraude drásticamente sin incrementar rechazos legítimos, pero alcanzar ese punto de equilibrio implicó décadas de ajuste y aprendizaje.

Incluso con machine learning avanzado, los **falsos positivos** siguen siendo un problema. Modelos complejos pueden identificar patrones sutiles de fraude, pero a veces marcan conductas atípicas pero legítimas. Por ejemplo, una persona que normalmente opera localmente y de repente envía dinero al extranjero por una emergencia familiar podría ser señalada por un sistema analítico como anómala (y potencial fraude) simplemente porque sale de su patrón histórico. Si el sistema bloquea esa transacción legítima, hay un impacto negativo en la experiencia del cliente y posiblemente en la confianza hacia la institución.

Para mitigar esto, han surgido prácticas como:

- **Modelos de dos fases:** primero un modelo amplio detecta posibles fraudes; luego un modelo específico filtra los casos de mayor puntuación de riesgo reduciendo falsos positivos. Por ejemplo, en credit scoring se usan modelos que predicen también la probabilidad de falsos positivos para calibrar la decisión final.
- **Segmentación de clientes y contexto:** los sistemas modernos tratan de entender el contexto de la transacción. No es lo mismo un pago internacional de un cliente corporativo (como es de esperar) que de un jubilado que nunca antes ha hecho transferencias al extranjero. La segmentación analítica permite aplicar criterios distintos para diferentes perfiles, disminuyendo alertas innecesarias.
- **Revisión humana de alertas de cierto nivel:** muchas instituciones establecen que, por encima de cierto umbral de puntuación de riesgo, una alerta sea revisada manualmente antes de bloquear definitivo. Esto introduce un control de calidad, pero, claro, a costa de tiempo y recursos. Por eso los esfuerzos se han volcado a bajar la cantidad de alertas totales.

Otra táctica es invitar al **cliente a validar** ciertas operaciones. Por ejemplo, ante una transacción internacional inusual, algunas aplicaciones bancarias ahora mandan notificaciones al cliente ("¿Usted está haciendo esta transacción?") antes de procesarla completamente. Esto, si bien añade fricción, la traslada en parte al usuario y puede resultar en una experiencia más controlada (el usuario confirma y aprende que el banco vela por su seguridad).

La discusión de falsos positivos también tiene una dimensión financiera: altos falsos positivos implican costes en atención al cliente, investigaciones e incluso pérdida de ventas (en comercio electrónico, falsos rechazos significan ventas no realizadas). Según un informe de la NRF/Forrester, más de la mitad de minoristas consideraban el **fraude como su principal desafío de pagos**, pero a la vez reconocían que debían evitar rechazar clientes legítimos al combatirlo. Esto ha llevado a soluciones híbridas donde **analytics y reglas se afinan constantemente** usando feedback. Muchas empresas monitorizan métricas de rendimiento del sistema antifraude: tasa de fraude real (fraudes que pasaron), tasa de falsos positivos (clientes legítimos bloqueados) y utilizan técnicas de optimización para moverse en la curva ROC a un punto ideal.

En resumen, aunque la evidencia sugiere que analytics ha **mejorado sustancialmente la eficacia** (reduciendo fraude a niveles históricos bajos en ciertos ámbitos), la problemática de falsos positivos persiste como reto operativo. La solución parece residir en **analíticas más contextuales e inteligentes**, que entiendan la "normalidad" de cada cliente mejor, y en **UX de seguridad** que integre al cliente en la validación. De lo contrario, existe riesgo de perder apoyo del público o de staff interno que se ve abrumado por alertas.

6.2 Adaptabilidad de los modelos vs. adaptabilidad de los defraudadores

Un principio fundamental es que la **amenaza del fraude es evolutiva**. Los defraudadores constantemente prueban nuevas técnicas para eludir controles, en lo que se describe a menudo como una "carrera armamentista" entre los delincuentes y las entidades antifraude. La introducción de analytics avanzados ha elevado la vara para los estafadores, pero estos a su vez se **vuelven más sofisticados**. Algunas consideraciones críticas:

- Los defraudadores pueden emplear también **herramientas de AI** para probar y evadir sistemas de detección. Por ejemplo, se han documentado casos de *fraud rings* que usan simulaciones de comportamientos típicos (usando bots que generan tráfico "normal") para confundir a los modelos de fraude. Incluso se habla de **ataques adversariales**: intentar introducir datos diseñados para engañar al modelo ML (similar a cómo imágenes adulteradas pueden engañar a un clasificador de visión).

- Existe el riesgo de que modelos ML entrenados con historiales pasados no detecten un **fraude de tipo completamente nuevo**, ya que por definición no habría patrones similares en los datos históricos. Esto es especialmente relevante en fraudes internacionales complejos, que pueden involucrar esquemas inéditos combinando vulnerabilidades tecnológicas y legales. Si bien las técnicas de detección de anomalías pueden atrapar cosas nunca vistas, a menudo se requiere cierta "imaginación" humana para anticipar nuevas formas de fraude (por ejemplo, la aparición de fraudes usando deepfakes de voz/imágenes para suplantar identidades en procesos remotos).
- Un punto frágil es la **dependencia de los modelos en los datos de entrenamiento**. Si los defraudadores identifican que un sistema presta mucha atención a cierto indicador (feature), pueden modificar su comportamiento para que ese indicador pase desapercibido. Por ejemplo, si saben que transferir justo $9,999 para evitar CTR es obvio y levantará sospecha, pueden transferir números extraños (p.ej., $9,231) para tratar de parecer aleatorios. Los modelos deben entonces evolucionar para no depender demasiado de reglas fijas sino de correlaciones contextuales.

En la literatura de seguridad informática se discute el concepto de **adversarial machine learning**, que es justamente el estudio de cómo un adversario puede engañar a un modelo de ML y cómo robustecer este contra ello. Esto aplica igualmente al fraude: investigadores han demostrado que pueden manipular ligeramente atributos de transacciones para moverlas de "fraudulenta" a "legítima" según los criterios de un modelo (lo que indica que un defraudador sofisticado podría hacer lo mismo si lograra sondear el modelo suficientemente). Biggio et al. (2013), por ejemplo, mostraron la viabilidad de ataques de envenenamiento y evasión en clasificadores de seguridad. En consecuencia, los sistemas antifraude deben incorporar *hardening*, es decir, entrenamiento robusto incluyendo posibles intentos de adversarios de engañar al modelo.

Desde una perspectiva estratégica, las instituciones deben mantener un **ciclo de mejora continua**: monitorizar sus indicadores de fraude, aprender de cada incidente (cómo esquivó los controles) e incorporar esos aprendizajes al sistema. Un peligro identificado es la **excesiva confianza en la automatización**. Si un banco delega completamente en el algoritmo, puede volverse ciego a señales cualitativas. Un ejemplo: algunos bancos que usan solamente puntuaciones automáticas para aprobar préstamos en línea sufrieron estafas donde grupos coordinados pasaban los procesos iniciales al replicar características de buen perfil, algo que un analista humano con contexto habría sospechado (por ejemplo, notando que 50 solicitantes distintos usan la misma dirección IP, incluso si el modelo no lo penalizaba mucho).

En la lucha adaptativa, la **colaboración y compartir inteligencia** es vital. Un banco aislado puede tardar en darse cuenta de un nuevo modus operandi que ya ha afectado a otra entidad. Por eso, esquemas de **fraud information sharing** a través de asociaciones

(e.g., SWIFT has its Information Sharing and Analysis Centre) o mediante vendors comunes (como vimos con Stripe Radar o consorcios) son armas para reaccionar más rápido colectivamente.

En resumen, la analítica otorga adaptabilidad a las defensas (los modelos aprenden y se actualizan), pero los defraudadores también se adaptan, explotando cualquier punto ciego del sistema. La implicación práctica es que no es posible un sistema "set and forget"; se requiere **supervisión experta continua** de los modelos, reentrenamiento frecuente con datos recientes, validaciones cruzadas, y asumir un enfoque de ciberriesgo: planificar para cuándo (no si) un control será superado. En otras palabras, la resiliencia antifraude moderna se basa tanto en la **tecnología adaptativa** como en la **vigilancia activa y proactividad humana**.

6.3 Consideraciones de privacidad, ética y cumplimiento al usar analytics

La implementación de analytics en la detección de fraude conlleva manejar grandes cantidades de datos personales sensibles y aplicar decisiones automatizadas que afectan a individuos (bloquear una transacción, cerrar una cuenta, etc.). Esto genera varias preocupaciones de **privacidad y ética**:

Cumplimiento con leyes de protección de datos: En jurisdicciones con GDPR u otras leyes de privacidad, las instituciones deben justificar legalmente el procesamiento masivo de datos para fines de prevención de delitos. Afortunadamente, la mayoría de legislaciones permite excepciones para procesar datos con el fin de prevenir fraudes o lavado (considerado interés público o legítimo). Sin embargo, deben seguirse principios de **minimización** (usar solo datos necesarios) y **limitación de propósito** (no reutilizar datos recopilados para fraude en marketing, por ejemplo, sin consentimiento). Un punto de roce podría ser la retención de datos: los sistemas de analytics a veces quieren conservar históricos largos para entrenar modelos, pero las leyes pueden exigir borrar datos de clientes tras X años de no ser necesarios. Las instituciones deben entonces encontrar equilibrios y, en ocasiones, **anonimizar** datos para conservarlos con fines de mejora de modelos sin violar privacidad.

Transparencia y derecho a explicación: GDPR introdujo de manera indirecta (y algunos reguladores reafirman) el derecho de una persona a recibir una explicación si una decisión significativa fue tomada de forma automatizada. En contexto de fraude, esto es complejo: si un banco revela exactamente por qué su sistema bloqueó a un cliente ("porque su transacción era inusual en horario y país"), podría dar pistas a defraudadores. Muchas instituciones manejan esto proporcionando explicaciones genéricas ("su transacción se marcó por nuestros controles de seguridad") y revisiones

manuales bajo solicitud. Existe un debate ético sobre cuánta **"caja negra"** es aceptable en pro de la seguridad. Algunos argumentan que la opacidad de los modelos ML, si bien justificada en antifraude, puede terminar afectando desproporcionadamente a ciertos grupos (posibles sesgos).

Posibles sesgos y discriminación algorítmica: Si los datos históricos tienen sesgos (por ejemplo, más fraude detectado en ciertos países, o en cierto segmento demográfico), un modelo ML podría perpetuar un trato discriminatorio. Imagínese que un sistema marque como más riesgosas transacciones provenientes de determinados países solo porque históricamente hubo más reportes (lo cual puede reflejar más vigilancia ahí que incidencia real). Esto podría llevar a **exclusión financiera** de personas legítimas de esas regiones. Es un tema delicado: por un lado, el riesgo país es un factor real incorporado incluso en normativas (listas de países de alto riesgo GAFI); por otro, debe cuidarse de no sobre-generalizar y bloquear actividades lícitas. Las instituciones deben auditar sus modelos en busca de bias inadvertidos y calibrarlos para evitar daños colaterales indebidos.

Compatibilidad con regulaciones financieras y responsabilidad legal: Otra arista es cómo los reguladores supervisan los sistemas analíticos. Tradicionalmente, en auditorías AML, se revisaban las reglas y su efectividad. Ahora, con ML, muchos supervisores (ej. la FCA en Reino Unido) están desarrollando guías para la **validación de modelos AI**. Quieren asegurarse de que los bancos entiendan su propio modelo, puedan explicar altas omisiones o falsas alarmas, y no dependan ciegamente en un proveedor externo. En caso de que un gran fraude pase desapercibido, un banco podría enfrentar la pregunta: "¿por qué su modelo no lo detectó?, ¿lo habían calibrado correctamente?". La **responsabilidad** recae en la institución, no en la IA en sí misma, por lo que se insiste en mantener *"human-in-the-loop"* y gobierno sobre los modelos.

Un ejemplo concreto: si un cliente sufre repetidamente bloqueos que él considera injustificados y el banco no justifica bien el criterio, podría incluso emprender acciones legales por daño o discriminación. No es común, pero a medida que la sociedad entienda más el rol de algoritmos, podría ocurrir. Las entidades deberán entonces poder defender sus sistemas con documentación (e.g., pruebas de que su modelo pasó tests, que cumple estándares industriales, etc.).

Confidencialidad e intercambio de datos entre instituciones: Mientras que compartir información de fraude es beneficioso, también choca con leyes de confidencialidad bancaria y privacidad. Se han tenido que crear **marcos legales específicos** para compartir ciertos datos a efectos de prevención de delitos. Por ejemplo, en EE.UU. la Patriot Act Sección 314(b) permite a instituciones compartir información de clientes sospechosos de lavado bajo protección legal, pero deben registrarse en FinCEN y solo usarlo para ese fin. En la UE, propuestas para que bancos compartan más datos chocan

con GDPR y secretos bancarios nacionales. Algunas soluciones han sido usar **terceros centralizadores** (como SWIFT KYC Registry) donde los datos se dan con consentimiento limitado. También se investiga usar **técnicas de privacidad avanzada**, como aprendizaje federado: bancos entrenan un modelo compartido sin revelar sus datos entre sí, solo compartiendo parámetros agregados (esto mantiene privacidad pero permite aprovechar inteligencia colectiva). Tales enfoques podrían ser el futuro para conjugar eficacia antifraude con protección de datos.

Resumiendo, el despliegue de analytics debe navegar un terreno normativo/ético complejo. Las implicaciones son que las instituciones necesitan **multidisciplinariedad**: involucrar a sus equipos legales y de cumplimiento de privacidad en el diseño de sistemas antifraude. Y a nivel regulatorio, se requerirá actualizar marcos para dar espacio al uso de IA manteniendo salvaguardias. Probablemente veremos más guías de "AI ética" de parte de reguladores financieros, y auditorías específicas a los algoritmos en grandes bancos.

6.4 Costes, recursos e implementación: una brecha entre líderes y rezagados

No todos los actores del sistema financiero global cuentan con los mismos medios para implementar soluciones analíticas de punta. Un gran banco internacional puede invertir cientos de millones en sistemas de AI, contratar científicos de datos y comprar herramientas de vanguardia; en cambio, una cooperativa pequeña o un banco en un país en desarrollo puede apenas sostener un equipo básico de compliance. Esta **brecha de capacidades** genera riesgos, porque los defraudadores tienden a enfocarse en los eslabones débiles.

Por ejemplo, un banco minorista pequeño podría no detectar un esquema de fraude pasando por él, sirviendo involuntariamente como "puente" para defraudadores que luego sacan dinero en efectivo o lo mueven offshore. Esto sugiere que, si bien los líderes en analytics elevan la barra, el sistema en su conjunto es tan fuerte como su participante más débil. Normativas internacionales presionan a todos a subir estándares, pero en la práctica hay rezagos.

Una limitante importante son los **costes e infraestructura**. La implementación de big data analytics requiere:

- Sistemas de TI robustos capaces de manejar y almacenar grandes volúmenes de datos, con baja latencia (especialmente para monitoreo en tiempo real).

- Software especializado (algunos bancos grandes desarrollan in-house, otros deben adquirir soluciones de mercado).
- Talento humano: científicos de datos, analistas de fraude, ingenieros de ML, etc., perfiles escasos y caros.
- Procedimientos y capacitación: incorporar la herramienta significa reentrenar personal, redefinir flujos de trabajo.

Para entidades medianas/pequeñas, una solución ha sido recurrir a proveedores terceros o consorcios. Por ejemplo, muchos bancos contratan servicios de compañías especializadas (Feedzai, FICO Falcon, SAS, etc.) que proveen plataformas de fraude con modelos preconstruidos. Esto puede ser más efectivo en términos de precios que desarrollar desde cero. Sin embargo, la efectividad dependerá de customizar bien la herramienta al perfil del banco y de alimentar con datos de calidad.

Otra opción emergente es el uso de **servicios en la nube**. Bancos que no pueden montar su big data center internamente están utilizando cloud (AWS, Azure, Google) que ofrecen entornos seguros con herramientas de ML integradas. Esto reduce barreras de entrada, aunque plantea consideraciones de seguridad (¿poner datos de transacciones en la nube es aceptable? Muchos bancos antes se oponían, ahora con cifrado y acuerdos adecuados se está adoptando).

Los reguladores también juegan un rol: por ejemplo, algunos bancos se quejan de que la **incertidumbre regulatoria** (falta de guías claras sobre el uso de AI) los vuelve reacios a invertir mucho por miedo a hacerlo mal. Si los supervisores dan luz verde o incluso incentivos para adoptar analytics (como considerar atenuantes de sanciones si demuestran tener sistemas avanzados, aun si ocurrió un incidente), más instituciones se sumarán.

Además, existe un **coste de falsa percepción**: algunas directivas creen que comprar la herramienta milagrosa resolverá todo, sin darse cuenta que es un proceso continuo. Esto lleva a implementaciones a medias o decepción ("compramos X y seguimos teniendo alertas manuales"). Aquí la limitación es conceptual: es necesario un cambio cultural hacia la **innovación constante** y a integrar los equipos de data science con los de negocio y compliance.

En conclusión, la brecha entre entidades en capacidades analíticas es un desafío. Es imperativo buscar soluciones colaborativas (como utilidades compartidas de prevención de fraude) y que los gobiernos/organismos internacionales apoyen a instituciones de países con menos recursos para ponerse al día (quizá vía entrenamientos, fondos,

plataformas regionales). De lo contrario, los defraudadores explotarán jurisdicciones o bancos con menor vigilancia, minando el esfuerzo global.

6.5 Cooperación internacional: implicaciones prácticas y regulatorias

Dado que el fraude en transacciones internacionales, por definición, involucra múltiples jurisdicciones, su prevención y persecución eficaz requieren una **cooperación internacional estrecha**. Esto tiene varias dimensiones:

- **Intercambio de información entre autoridades:** Ya se mencionó la importancia de Egmont Group (UIFs compartiendo inteligencia). También, en casos grandes, equipos conjuntos de investigación (JITs) bajo Europol o convenios bilaterales han sido cruciales. Normativamente, tratados de asistencia legal mutua (MLATs) y, en la UE, instrumentos como Eurojust facilitan compartir pruebas y congelar activos transfronterizos. Sin embargo, estos procesos suelen ser lentos comparado a la velocidad del dinero digital. Se está discutiendo implementar **mecanismos más rápidos** (por ejemplo, EU está creando un HUB para intercambio inmediato de información financiera entre países miembros).
- **Harmonización de normativas:** Cuando las leyes difieren mucho, los delincuentes arbitrarán hacia la más débil. Se ha avanzado en AML con estándares GAFI, pero en fraude cibernético o protección al usuario hay divergencias. Un ejemplo: hasta hace poco, transferir dinero a cuentas de mulas en ciertos países tenía pocas consecuencias porque ese país no tipificaba claramente el delito. Ahora se ve tendencia a leyes unificadas (como la Convención de Budapest para ciberdelitos). La UE con su directiva antifraude de medios de pago de 2019 busca que todos penalicen similar los fraudes online.
- **Responsabilidad compartida de empresas internacionales:** Muchas compañías involucradas (ej. redes de pago, fintechs) operan globalmente. Un problema era que un estafador bloqueado en un país simplemente usaba el mismo servicio en otro país con menos filtros. Ahora, empresas como Visa, MasterCard, PayPal tienen políticas globales: si detectan un defraudador, lo vetan a nivel global. Pero para ello necesitan base legal para compartir datos de incidentes entre sus filiales en distintos países (lo cual de nuevo entra a chocar con privacidad en algunos casos).
- **Implicaciones regulatorias de tecnologías globales:** Por ejemplo, las **criptomonedas** permiten mover valor internacionalmente fuera del sistema bancario tradicional. Los reguladores están apresurándose a someterlas a normas AML (como la “regla de viaje” que obligará a exchanges a enviar información del remitente y receptor junto con la transacción, análogo al sistema bancario). Esto es vital porque de lo contrario, las cripto serían la ruta de escape perfecta de análisis (donde no hay SWIFT Compliance que valga). Países del GAFI han comenzado a implementar esta Travel Rule, pero se necesita adopción global coordinada para ser eficaz.
- **Desbalance en aplicación de sanciones:** Un punto complicado: a veces los marcos antifraude colisionan con intereses geopolíticos. Por ejemplo, cuando un

> gran banco global detecta un esquema de lavado ligado a políticos de un país, idealmente debe reportar a ese país. Pero, ¿qué si ese país carece de estado de derecho? ¿Se arriesga a represalias? Ha habido casos donde cooperación se dificulta por desconfianza entre autoridades. Las soluciones pasan por canales discretos y presión diplomática, pero no siempre se logra. En estos casos, las instituciones financieras hacen su parte bloqueando o cerrando cuentas, pero la red criminal puede seguir operando vía otras regiones.

Impulsar la cooperación requiere **voluntad política** y marcos legales actualizados. La creación de la nueva **Autoridad Antilavado de la UE** (AMLA) para 2024-25 busca centralizar supervisión de riesgos transfronterizos significativos en Europa, lo que podría servir de modelo a otros bloques. También, a nivel de Naciones Unidas, se discute un tratado global sobre cibercrimen que incluiría fraude digital.

Finalmente, la **normalización de estándares técnicos** ayuda: por ejemplo, promover formatos comunes para reportes de fraude entre bancos a nivel internacional permitiría comparabilidad y más fácil consolidación. Iniciativas ISO o consorcios (como ACFE, Association of Certified Fraud Examiners, que difunde guías) también contribuyen.

En resumen, si bien cada institución y país mejora su arsenal analítico, **ninguno puede luchar solo contra el fraude internacional**. Las implicaciones prácticas son que deben invertirse esfuerzos en **mecanismos colectivos**, alineamiento de políticas y confianza mutua. De lo contrario, los defraudadores explotarán grietas jurisdiccionales, ya sea moviendo operaciones a países con menor control o fragmentando sus transacciones entre muchas áreas para diluir señales (lo que complica a analytics en silos nacionales). Un sistema global más interconectado de prevención es posiblemente el ideal a perseguir, aunque su consecución enfrenta retos de soberanía, legales y de recursos.

Reflexión final de la discusión: La prevención de fraudes en transacciones internacionales mediante analytics se revela como un campo con un progreso acelerado pero con obstáculos importantes. Los avances en detección temprana y reducción de fraude son tangibles (como tasas históricamente bajas en ciertos dominios) sin embargo, este éxito parcial coexiste con amenazas cambiantes y desafíos de implementación. A medida que avanzamos, será crucial mantener una **visión crítica y equilibrada**: aprovechar la tecnología de datos masivos e inteligencia artificial al máximo, sin perder de vista los factores humanos, éticos y colaborativos que finalmente determinarán el éxito sostenido de estas iniciativas.

7. Conclusiones y recomendaciones

La investigación ha explorado en profundidad el uso de analytics para la prevención de fraudes en transacciones internacionales, abarcando perspectivas teóricas, normativas, metodológicas y aplicadas. A la luz de los hallazgos, es posible extraer **conclusiones generales** sobre la efectividad y el rol de la analítica de datos en este ámbito, así como formular **recomendaciones** tanto para el ámbito académico (futuras investigaciones) como para el profesional (instituciones financieras, reguladores y empresas) con el fin de fortalecer la lucha contra el fraude internacional.

Conclusiones principales:

- La adopción de técnicas avanzadas de análisis de datos (incluyendo machine learning, Big Data y herramientas de inteligencia artificial) se han consolidado como un **componente indispensable** en los sistemas modernos de detección y prevención de fraude financiero internacional. Los enfoques tradicionales basados exclusivamente en reglas, listas y controles manuales ya no bastan ante la escala y sofisticación de los fraudes contemporáneos. La analítica proporciona la capacidad de **monitoreo en tiempo real**, detección de **patrones complejos** y adaptación continua a nuevas amenazas, lo cual representa una ventaja fundamental para reducir pérdidas y riesgos operativos.
- La integración de analytics en la prevención de fraude no solo mejora la eficacia en la detección, sino que también **fortalece el cumplimiento normativo** de las instituciones. Las normativas internacionales (FATF, BSA/AML, Directivas UE, etc.) exigen monitoreo proactivo y reporte oportuno de actividades sospechosas; en la práctica, solo mediante sistemas analíticos automatizados es factible cumplir con estas obligaciones de manera consistente, especialmente para instituciones con gran volumen de transacciones. En consecuencia, existe una sinergia: los programas de compliance que incorporan analytics muestran mejores resultados en la identificación de operaciones inusuales y por ende en la prevención del delito financiero, reforzando la integridad del sistema financiero global.
- Se confirma la hipótesis planteada: **la integración de técnicas avanzadas de analítica de datos en estrategias antifraude eleva significativamente la capacidad de detección temprana de fraudes en transacciones internacionales y contribuye al cumplimiento regulatorio**. La evidencia recopilada muestra múltiples casos de éxito (Visa, Stripe, SWIFT, etc.) donde la analítica ha permitido interceptar esquemas fraudulentos en el momento o incluso antes de materializarse, reduciendo drásticamente las pérdidas frente a escenarios sin dichas herramientas. Asimismo, se ha observado cómo la analítica ayuda a identificar brechas de cumplimiento (por ejemplo, transacciones no reportadas que debían serlo) y a focalizar recursos en las áreas de mayor riesgo, haciendo los programas de prevención más efectivos y eficientes.
- No obstante, se identifican **limitaciones y desafíos** clave: (a) Los sistemas analíticos deben lidiar con el equilibrio entre sensibilidad y especificidad para no generar falsos positivos excesivos que afecten a clientes legítimos ; (b) Los defraudadores aprenden y evolucionan, surgiendo un juego adversarial que obliga a actualizar constantemente los modelos y a mantener intervención

humana experta; (c) Existen tensiones con aspectos de privacidad y ética, requiriendo que las soluciones sean transparentes, justas y respetuosas de los derechos individuales en la medida de lo posible; y (d) Persiste una brecha de capacidades entre distintas organizaciones, lo que puede dejar puntos débiles a nivel sistémico. Esto implica que la efectividad global de la analítica antifraude depende también de **factores organizacionales, legales y cooperativos**, no solo tecnológicos.

- El marco normativo internacional se está adaptando gradualmente para fomentar la innovación en prevención de fraude mediante tecnología, pero aún tiene terreno por recorrer. Regulaciones emergentes sobre inteligencia artificial, normas de supervisores para validación de modelos, y acuerdos internacionales para compartir información serán determinantes para crear un entorno donde las instituciones puedan aprovechar plenamente la analítica sin temor a incoherencias legales. La estandarización y coordinación global en esta materia reforzará aún más el impacto positivo de la analítica en la lucha contra el fraude.

Recomendaciones:

Para instituciones financieras y empresas:

1. **Invertir en infraestructura analítica y talento especializado:** Los bancos y empresas involucradas en transacciones internacionales deben priorizar la implementación (o actualización) de plataformas de análisis de fraude. Esto incluye no solo adquirir herramientas de software modernas, sino también formar equipos multidisciplinarios con científicos de datos, analistas de fraude y expertos en cumplimiento que trabajen en conjunto. La inversión debe verse no como un gasto, sino como un mecanismo de ahorro de pérdidas futuras y de cumplimiento regulatorio. Se recomienda también aprovechar soluciones en la nube y servicios externos donde sea apropiado, especialmente para actores más pequeños, a fin de reducir la brecha tecnológica.
2. **Adoptar un enfoque de mejora continua y gestión del ciclo de vida de los modelos:** Un modelo de detección de fraude no puede implementarse de manera estática. Se recomienda establecer procedimientos de **reentrenamiento periódico** (por ejemplo, mensual o trimestral) de los algoritmos con datos recientes, y validaciones constantes de su desempeño (tasa de detección, falsos positivos, etc.). Igualmente, probar los modelos ante potenciales ataques adversariales y escenarios hipotéticos de nuevos fraudes (ejercicios de *red teaming*) ayudará a robustecerlos. Cada incidente de fraude que ocurra debe analizarse post-mortem para ajustar las reglas o modelos y evitar repeticiones.
3. **Mantener al cliente en el centro de la estrategia antifraude:** A pesar de la automatización, es importante diseñar las soluciones pensando en minimizar la fricción para clientes legítimos. Se recomienda implementar **mecanismos de autenticación y verificación escalonada** (por capas) donde a mayor riesgo detectado, se solicite información o confirmación adicional al cliente en lugar de simplemente rechazar la transacción. Asimismo, comunicar de manera clara a los usuarios las medidas de seguridad y ofrecer canales rápidos de resolución

cuando una transacción es bloqueada por sospecha (ej. confirmarla vía banca móvil) mejorará la confianza y colaboración del público en los esfuerzos antifraude.

4. **Fortalecer la gobernanza de datos y la ética en AI:** Las instituciones deben desarrollar políticas internas que aseguren el uso responsable de la analítica. Esto implica auditar los modelos para detectar posibles sesgos discriminatorios, limitar el acceso a datos sensibles solo para los fines de fraude/compliance, y mantener documentación de la lógica de los sistemas para poder explicarlos ante auditorías o reclamaciones. La figura de un "Chief Data Officer" o "AI Ethics Officer" puede ser valiosa en grandes organizaciones para supervisar estos aspectos. Asimismo, adherirse a principios como los propuestos por autoridades (por ejemplo, los principios éticos de la UE para IA) mostrará diligencia y previsión en la aplicación de estas tecnologías.
5. **Participar activamente en redes de cooperación e intercambio de inteligencia anti-fraude:** Se recomienda que las empresas se sumen a foros de la industria, asociaciones y acuerdos bilaterales de intercambio de señales de fraude. Esto puede ser a través de organismos nacionales (asociaciones bancarias locales con listas compartidas de estafadores conocidos), internacionales (Certificados compartidos de ciberamenazas, grupos de trabajo de Interpol, etc.) o mediante plataformas centralizadas (como registrarse en programas de información compartida de SWIFT, FinCEN 314(b) en EE.UU., etc.). La colaboración no debe verse solo como altruismo, sino como una estrategia de defensa colectiva: cada entidad que mejora su detección fortalece el ecosistema completo.

Para reguladores y formuladores de políticas:

1. **Desarrollar directrices claras sobre el uso de IA/analytics en servicios financieros:** Las agencias supervisoras deberían emitir guías o regulaciones específicas que indiquen expectativas sobre explicabilidad de modelos, validación, gobierno y auditoría de los mismos. Esto daría certidumbre a las instituciones para innovar sin temer incumplir normas implícitas. Un equilibrio regulatorio recomendable es exigir a las entidades que demuestren control sobre sus sistemas (por ejemplo, validar periódicamente que no haya sesgos prohibidos, que las tasas de falso positivo/falso negativo están dentro de ciertos rangos) en lugar de coartar qué técnicas pueden usar. Iniciativas como *"sandboxes regulatorios"* para probar nuevas soluciones antifraude con supervisión flexible podrían acelerar la adopción.
2. **Impulsar la estandarización y la interoperabilidad internacional:** Los organismos internacionales (FMI, Banco Mundial, FATF, UE, etc.) deberían promover estándares comunes de datos para reportes de transacciones sospechosas y para indicadores clave de fraude. Asimismo, actualizar los marcos legales (tratados, MLATs) para facilitar el intercambio rápido de información entre países en casos de fraude transnacional. Se sugiere evaluar la creación de **centros regionales de inteligencia financiera** que integren analytics a nivel supranacional, para apoyar a países con menos recursos en la detección de patrones que cruzan fronteras. Por ejemplo, un centro europeo que reciba y

analice datos agregados de transacciones transfronterizas podría identificar esquemas de fraude carrusel que ningún país vería completo por sí solo.

3. **Fomentar programas de capacitación y apoyo técnico:** Especialmente en economías emergentes, los reguladores junto con organismos multilaterales pueden lanzar programas para dotar de capacidades a bancos locales en el uso de herramientas analíticas y proveer asistencia técnica o fondos para su implementación. Esto podría tomar forma de talleres, intercambios de mejores prácticas, o incluso dotación de software básico de monitoreo a quienes no lo posean. Cerrar la brecha de capacidades ayudará a que los defraudadores tengan menos "refugios fáciles" en el sistema global.
4. **Considerar incentivos para la colaboración de empresas tecnológicas:** Muchas innovaciones en analytics vienen del sector privado (fintechs, startups de AI). Reguladores pueden facilitar esquemas para que bancos tradicionales colaboren con fintechs en prevención de fraude sin incurrir en problemas de responsabilidad o compliance. Por ejemplo, aprobar acuerdos de *outsourcing* o de intercambio de data anonimizados con startups especializadas. Incluso se podrían dar **incentivos regulatorios** (como puntuaciones mejoradas en evaluaciones de riesgo) a las instituciones que demuestren adopción efectiva de analytics en su marco de control interno.

Para la academia y futuras investigaciones:

1. **Investigación en algoritmos explicables y robustos:** Sería valioso profundizar en técnicas de **Explainable AI (XAI)** aplicadas a la detección de fraudes, para lograr modelos que mantengan alto rendimeinto pero cuyos resultados puedan interpretarse fácilmente (p. ej., usando metodologías SHAP, LIME adaptadas a transacciones financieras). Esto aliviaría la tensión con la transparencia. Asimismo, continuar investigando métodos para hacer **modelos resistentes a ataques adversariales** y a adaptaciones de defraudadores, tal como se hace en ciberseguridad, podría anticipar la próxima generación de fraudes antes de que ocurran.
2. **Estudios de impacto y coste-beneficio:** Sería útil contar con estudios empíricos que cuantifiquen el beneficio económico y operativo de implementar analytics vs. métodos tradicionales en la prevención de fraude. Por ejemplo, análisis en bancos similares con y sin AI para medir reducción de pérdidas, o modelar el ROI de la inversión en tecnología antifraude. Esto ayudaría a convencer a tomadores de decisión más reticentes y a optimizar la asignación de recursos (saber hasta qué punto un modelo más complejo brinda retornos marginales).
3. **Fraude en nuevas plataformas y entornos descentralizados:** La academia puede explorar más el tema emergente de fraude en contextos como finanzas descentralizadas (DeFi), criptomonedas, y plataformas P2P. Desarrollar frameworks analíticos para detectar manipulación o fraude en blockchain, por ejemplo, es un campo incipiente. Dado que es probable que los defraudadores migren parcialmente a estos ecosistemas, adelantarse con investigación podría dotar a reguladores y empresas de conocimiento para abordarlos.
4. **Dimensión humana y de comportamiento:** Complementar la visión técnica con estudios en ciencias sociales: comprender las motivaciones y patrones de comportamiento de los defraudadores internacionales (perfil criminológico), o

investigar cómo reacciona el personal de un banco ante la integración de AI (aceptación, confianza en el sistema, etc.), permitirá diseñar sistemas más efectivos en la práctica. Por ejemplo, un hallazgo sociológico podría ser que ciertos fraudes prosperan por complicidad interna – entonces la prevención debe incluir analytics no solo en transacciones sino en detectar conductas inusuales de empleados (*insider threats*).

En conclusión, el **uso de analytics en la prevención de fraudes en transacciones internacionales** representa un cambio de paradigma en la gestión del riesgo financiero, alineado con la transformación digital de la industria. Los resultados logrados hasta ahora validan su potencial: se han reducido índices de fraude, se han destapado esquemas antes indetectables y se ha fortalecido la resiliencia del sistema financiero. Sin embargo, también ha quedado claro que no es una solución mágica libre de desafíos; es más bien una nueva **capacidad** que debe integrarse estratégica y responsablemente en las organizaciones.

El camino a seguir requiere una visión global donde tecnología, procesos, personas y regulaciones evolucionen de la mano. Solo así se podrá mantener la ventaja frente a adversarios cada vez más creativos y resguardar la confianza en las transacciones internacionales, que son un pilar del comercio y la economía global. Al adoptar las recomendaciones aquí propuestas, tanto el sector público como el privado estarán mejor posicionados para **anticipar, prevenir y mitigar** el fraude internacional, avanzando hacia un ecosistema financiero más seguro, transparente y confiable.

8. Bibliografía

Baah, S. S., Adu-Twum, H. T., Adjei, S. O., Ampadu, G., & Awofadeju, M. O. (2024). Leveraging big data analytics to combat emerging financial fraud schemes in the USA: A literature review and practical implications. World Journal of Advanced Research and Reviews, 24(1), 17–43. https://doi.org/10.30574/wjarr.2024.24.1.2999

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. John Wiley & Sons.

Banco Sabadell. (2025, 7 de abril). El fraude en el comercio internacional: qué es y cómo prevenirlo. Blog Banco Sabadell.

Basel Committee on Banking Supervision. (2020). Sound management of risks related to money laundering and financing of terrorism. Bank for International Settlements. https://www.bis.org/bcbs/publ/d505.pdf

Bolton, R. J., & Hand, D. J. (2002). Statistical Fraud Detection: A Review. Statistical Science, 17(3), 235–255. https://doi.org/10.1214/ss/1042727940

Booth, W. C., Colomb, G. G., & Williams, J. M. (2016). The craft of research (4th ed.). University of Chicago Press.

De la Torre, A. (2023, 31 de octubre). Blanqueo de dinero a través del comercio exterior. Investigación Criminal. https://investigacioncriminal.es/blanqueo-de-dinero-a-traves-del-comercio-exterior/

Danske Bank. (2018). Report on the Non-Resident Portfolio at Danske Bank's Estonian branch. https://danskebank.com/-/media/danske-bank-com/file-cloud/2018/9/report-on-the-non-resident-portfolio-at-danske-banks-estonian-branch.pdf

Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

European Commission. (2015). Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006. Official Journal of the European Union, L 141/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847

FATF (2012-2025), International Standards on Combating Money Laundering and the Financing of
Terrorism & Proliferation, FATF, Paris, France,
www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Financial Action Task Force. (2025, 31 de enero). FATF Annual Report 2023–2024 (Singapore Presidency) [Informe anual]. FATF. https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-Annual-report-2023-2024.html

Friling Law Firm. (s.f.). Anti-Money Laundering (AML). Recuperado el 10 de junio de 2025, de https://frilinglaw.com/es/servicios/whistleblower-services-es/international-fraud-violations-es/anti-money-laundering-aml-es

Friling Law Firm. (s.f.). Government programs and laws – International. Recuperado el 10 de junio de 2025, de https://frilinglaw.com/es/servicios/whistleblower-services-es/international-fraud-violations-es/government-programs-and-laws-international-es

Gottschalk, Petter. (2010). Categories of financial crime. Journal of Financial Crime. 17. 441-458. 10.1108/13590791011082797.

Gough, D., Oliver, S., & Thomas, J. (2017). An introduction to systematic reviews (2nd ed.). Sage Publications.

International Business Machines Corporation [IBM]. (s.f.). ¿Qué es la lucha contra el blanqueo de capitales? Recuperado el 11 de junio de 2025, de https://www.ibm.com/es-es/topics/anti-money-laundering

International Organization for Standardization. (2021). ISO 37301: Compliance management systems — Requirements with guidance for use. ISO.

Institute of International Finance & Deloitte. (2021, noviembre). The effectiveness of financial crime risk management reform and next steps on a global basis [White paper]. Institute of International Finance & Deloitte. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-iif-the-effectiveness-of-financial-crime.pdf

Islam, T., Islam, S. A. M., Sarkar, A., Obaidur Rahman Khan, A. J. M., Paul, R., & Bari, M. S. (2024). Artificial intelligence in fraud detection and financial risk mitigation: Future directions and business applications. International Journal for Multidisciplinary Research, 6(5), 1–23. https://doi.org/10.36948/ijfmr.2024.v06i05.28496

KPMG. (2019). Global Banking Fraud Survey. KPMG International. https://kpmg.com/xx/en/home/insights/2022/05/global-banking-fraud-survey.html

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Mihus, O., & Laptiev, M. (2025). INSIDE THE MIND OF THE MODERN FRAUDSTER: A TEN-YEAR COMPARATIVE ANALYSIS (2014–2024). Public Administration and Law Review, (1(21), 75–86. https://doi.org/10.36690/2674-5216-2025-1-75-86

Harris, L. (2024, noviembre). Fraud detection in the financial sector using advanced data analysis techniques [Informe técnico]. Stanford University. https://www.researchgate.net/publication/386111741_Fraud_Detection_in_the_Financial_Sector_Using_Advanced_Data_Analysis_Techniques

Parlamento Europeo y Consejo de la Unión Europea. (2018). Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo, de 30 de mayo de 2018, por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. Diario Oficial de la Unión Europea, L 156/43. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32018L0843

Phua, Clifton & Lee, Vincent & Smith-Miles, Kate & Gayler, Ross. (2010). A Comprehensive Survey of Data Mining-based Fraud Detection Research. CoRR. abs/1009.6119.

PricewaterhouseCoopers. (2020). PwC's Global Economic Crime and Fraud Survey 2020. PwC. https://www.global-screeningsolutions.com/industries/global-economic-crime-and-fraud-survey-2020-1.pdf

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Stripe. (2024, 9 de octubre). ¿Qué es el análisis de riesgo de las transacciones? En qué consiste y cómo trabajar con él. Stripe. https://stripe.com/es-us/resources/more/what-is-transaction-risk-analysis-what-it-involves-and-how-to-work-with-it

SWIFT. (2021). Compliance Analytics – Powerful data, world-class analytics. [White paper]. SWIFT. https://www.swift.com/risk-and-compliance/compliance-analytics-solutions

U.S. Congress. (1970). Currency and Foreign Transactions Reporting Act (Bank Secrecy Act), Pub. L. 91-508.

U.S. Congress. (2001). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272. https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

U.S. Congress. (2002). Sarbanes-Oxley Act of 2002, Pub. L. No. 107–204, 116 Stat. 745. https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf
Parliament of the United Kingdom. (2010). Bribery Act 2010: Chapter 23. https://www.legislation.gov.uk/ukpga/2010/23/contents

Visa Inc. (2019, 19 de junio). Visa previene aproximadamente US$25.000 millones en fraude usando inteligencia artificial. [Nota de prensa]. https://www.visa.com.mx/acerca-de-visa/sala-de-noticias/notas-de-prensa/inteligencia-artificial.html

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47–66. https://www.sciencedirect.com/science/article/abs/pii/S0167404815001261

Zheng, P., Yuan, S. & Wu, X. (2018). *SAFE: A Neural Survival Analysis Model for Fraud Early Detection*. arXiv preprint.

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. (2021). Intelligent financial fraud detection practices in post-pandemic era. Innovation (Cambridge (Mass.)), 2(4), 100176. https://doi.org/10.1016/j.xinn.2021.100176

de IAG de código sólo en el contexto de las actividades descritas a continuación [el alumno debe mantener solo aquellas en las que se ha usado ChatGPT o similares y borrar el resto. Si no se ha usado ninguna, borrar todas y escribir “no he usado ninguna”]:
1. Brainstorming de ideas de investigación: Utilizado para idear y esbozar posibles áreas de investigación.
2. 3. Crítico: Para encontrar contra-argumentos a una tesis específica que pretendo defender.
Referencias: Usado conjuntamente con otras herramientas, como Science, para identificar referencias preliminares que luego he contrastado y validado.
4. 5. Metodólogo: Para descubrir métodos aplicables a problemas específicos de investigación.
Interpretador de código: Para realizar análisis de datos preliminares.
6. Estudios multidisciplinares: Para comprender perspectivas de otras comunidades sobre temas de naturaleza multidisciplinar.
7. 8. Constructor de plantillas: Para diseñar formatos específicos para secciones del trabajo.
Corrector de estilo literario y de lenguaje: Para mejorar la calidad lingüística y estilística del texto.
9. Generador previo de diagramas de flujo y contenido: Para esbozar diagramas iniciales.
10. Sintetizador y divulgador de libros complicados: Para resumir y comprender literatura compleja.
11. Generador de datos sintéticos de prueba: Para la creación de conjuntos de datos ficticios.
12. Generador de problemas de ejemplo: Para ilustrar conceptos y técnicas.
13. Revisor: Para recibir sugerencias sobre cómo mejorar y perfeccionar el trabajo con diferentes niveles de exigencia.
14. Generador de encuestas: Para diseñar cuestionarios preliminares.
15. Traductor: Para traducir textos de un lenguaje a otro.
Afirmo que toda la información y contenido presentados en este trabajo son producto de mi investigación y esfuerzo individual, excepto donde se ha indicado lo contrario y se han dado los créditos correspondientes (he incluido las referencias adecuadas en el TFG y he explicitado para que se ha usado ChatGPT u otras herramientas similares). Soy consciente de las implicaciones académicas y éticas de presentar un trabajo no original y acepto las consecuencias de cualquier violación a esta declaración.
Fecha: 14/06/2025
Firma: Fadrique Álvarez De Toledo Abaitua