



Inteligencia Artificial en la Prevención del Lavado de Activos:
Una Perspectiva Técnica y Pragmática
Retos y oportunidades

*Juan Pablo Rodríguez C.

**René M. Castro V.

***Camilo A. Rueda B.

La incorporación de tecnologías avanzadas de inteligencia artificial (IA) en los programas de prevención del lavado de activos (AML) y financiación del terrorismo (CFT) ha captado la atención de reguladores, profesionales del cumplimiento y equipos de analítica de firmas financieras en todo el mundo. Según el informe técnico del Bank for International Settlements (BIS) titulado *Regulating AI in the financial sector: recent developments and main challenges*¹, la IA tiene el potencial de transformar la gestión del riesgo financiero al mejorar la eficiencia operativa, fortalecer la experiencia cliente y optimizar el modelado de riesgo. En ese mismo sentido, el documento subraya que muchas de las problemáticas tradicionales del sector (como el riesgo de modelo, la privacidad de datos o la gobernanza) persisten y deben atenderse con rigor.

De acuerdo con esta fuente, uno de los beneficios más tangibles es que los modelos de machine learning pueden “encontrar agujas en el pajar” — es decir, detectar patrones de transacciones o comportamientos que los sistemas basados en reglas no capturan fácilmente. Esto cobra relevancia en el contexto de grandes volúmenes de datos, múltiples jurisdicciones y actores que operan de forma distribuida. Al mismo tiempo, BIS señala que la implementación de IA no está exenta de retos, en particular en lo que respecta a la gobernanza del dato y la infraestructura tecnológica.

Asimismo, otras publicaciones especializadas refuerzan esta visión. Por ejemplo, el informe de ACAMS *Global AFC Threats Report 2025*² identifica entre sus conclusiones que el uso de IA generativa por parte de actores delictivos (como deepfakes, fraude automatizado, redes sociales) representa una de las principales amenazas externas de los próximos dos años, con el 75 % de los encuestados calificándolo como “alto o muy alto”. En consecuencia, los profesionales del AML deben considerar que la IA no solo ofrece oportunidades para la defensa, sino que también amplía el campo de acción del adversario.

Por tanto, desde una perspectiva práctica, la IA aplicada al AML presenta **pros** claros: mejora de la detección de tipologías emergentes, eficiencia operativa mediante menor carga de alertas y optimización de recursos humanos. Por ejemplo, la literatura técnica sobre grafos y aprendizaje automático³ muestra que representaciones avanzadas (como grafos de clientes-transacciones) pueden superar los sistemas tradicionales en términos de AUC (área bajo curva) o detección de anomalías. Al mismo tiempo, se evidencian **contras**: la necesidad de datos de alta calidad, la gestión del riesgo del modelo (model risk management), los sesgos inherentes a los algoritmos y los desafíos de explicabilidad frente al regulador.

De modo coherente con lo anterior, el GAFI aborda en su informe *Digital Transformation of AML/CFT*⁴ que la tecnología (incluida la IA) puede facilitar el cumplimiento normativo mediante métodos como data-pooling, análisis colaborativo y analítica avanzada, pero hace hincapié en que el simple uso de tecnología no garantiza

¹ Ver documento completo en <https://www.bis.org/fsi/publ/insights63.htm>

² Ver documento completo en <https://www.acams.org/en/global-afc-threats-report-2025>

³ Ver documento completo en <https://arxiv.org/abs/2210.14360>

⁴ Ver documento completo en <https://www.fatf-gafi.org/en/publications/Digitaltransformation/Digital-transformation.html>





el éxito, las nuevas tecnologías AML/CFT en cuanto a habilidades, métodos y procesos innovadores deben integrarse dentro de un marco de gestión de riesgo y normativa. Así, el GAFI plantea que la adopción tecnológica debe ir acompañada de una gobernanza adecuada, y que la tecnología por sí sola no sustituye el juicio humano ni la necesidad de un enfoque basado en riesgo.

Igualmente, la encuesta mencionada por ACAMS sobre adopción de IA y ML en AML indica que ya más de la mitad de las instituciones (57 %) han desplegado o están pilotando soluciones de IA/ML, y que los principales motivadores son la mejora de la calidad de las investigaciones (40 %) y la reducción de falsos positivos (38 %)⁵. A su vez, este dato evidencia que la industria ya avanza hacia un uso más maduro de la IA, aunque aún con retos operacionales para su puesta en producción.

Dado lo anterior, el panorama regulatorio emerge como un factor crítico. Según el reporte del BIS de diciembre de 2024, los reguladores no han emitido todavía marcos específicos para IA en instituciones financieras, pues muchos de los riesgos que plantea la IA ya están cubiertos por la normativa existente. Sin embargo, se identifican siete áreas que requieren mayor atención: gobernanza, experiencia y habilidades, gestión del modelo, datos, participantes no tradicionales, nuevos modelos de negocio y proveedores externos de IA. Esto implica que las entidades deben anticipar (y no reaccionar tarde) a la evolución normativa, con mecanismos de auditabilidad, explicabilidad y trazabilidad.

En este contexto, para profesionales en AML/CFT, el mensaje es claro: adoptarse de forma responsable. Un programa de IA exitoso debe partir de una infraestructura de datos sólida — que incluya calidad, integración y disponibilidad transfronteriza cuando aplique —, incorporar un equipo híbrido que combine conocimiento AML con ciencia de datos, y establecer un ciclo continuo de validación y retraining del modelo. Al mismo tiempo, debe contemplar mitigaciones para riesgos adversarios, dado que los delincuentes también están utilizando IA generativa para escalar su ofensiva.

En conclusión, la IA representa un potencial transformador para la prevención del lavado de activos: puede elevar la capacidad de detección, racionalizar procesos y permitir investigar con mayor profundidad. No obstante, su verdadero valor dependerá del entorno organizacional, de la calidad del dato, de la capacidad de gobernanza del modelo y de la colaboración sectorial. Como advierten tanto BIS como ACAMS y GAFI, la tecnología por sí sola no es la panacea, y debe incorporarse dentro de una estrategia de riesgo basada en principios sólidos.

***Juan Pablo Rodríguez C.**

Abogado Penalista

Escritor, conferencista y consultor internacional.

Certificado en Blockchain y Disrupción Tecnológica del MIT.

Certificado en Compliance CESCO® de la Asociación Española de Compliance, ASCOM, 2020.

Certified Lead Auditor, Lead Implementer y Trainer en ISO 37001 Gestión Antisoborno, PECB, 2020.

Certified Professional in Anti-Money Laundering - CPAML de FIBA (Florida International Bankers Association).

Certified on Governance, Risk Management and Compliance Professional (GRCP) y GRC Fundamentals of Open Compliance and Ethics Group (OCEG), 2016

Presidente y Socio de RICS Management.

jrodriguez@ricsmanagement.com

⁵ Ver documento completo en <https://i-aml.com/news/third-of-finance-firms-accelerate-use-of-artificial-intelligence-to-detect-money-laundering/>





riesgo • inteligencia • cumplimiento • seguridad

rics
management

****René M. Castro V.**

Contador Público con Magister en Contabilidad y Auditoría de Gestión de la Universidad de Santiago de Chile.
Escritor, conferencista y consultor internacional.

Certified Trainer y Lead Compliance Manager en ISO 19600 Gestión de Cumplimiento, PECB, 2020

Certified on Financial Services and Market Regulation, London School of Economics, (LSE), 2016

Certified on Corporate Compliance and Ethics, New York University, 2015.

Vicepresidente & Socio RICS Management

rcastro@ricsmanagement.com

*****Camilo A. Rueda B.**

Profesional en Finanzas y Relaciones Internacionales de la Universidad Externado de Colombia con estudios de Maestría en Seguridad y Defensa Nacional de la Escuela Superior de Guerra.

Anti-Money Laundering Certified Associate (AMLCA) por Florida International Bankers Association - FIBA

Certificado en Compliance CESCO® de la Asociación Española de Compliance, ASCOM, 2020.

Escritor, conferencista y consultor internacional.

Socio y Director RICS Management Guatemala

crueda@ricsmanagement.com



Edificio Tierra Firme Santa Bárbara • Cra 9. No. 115 - 06 Piso 17, Bogotá

Teléfono +57 1 639-8456 • Celular +57 311 5140915

consultor@ricsmanagement.com • info@ricsmanagement.com

www.ricsmanagement.com

