

Monografía

Gobernanza y RegTech en el nuevo orden financiero: El papel de la IA
y Blockchain en la arquitectura de cumplimiento PLAFT 2026

Autor

Héctor Del Rosario Rodríguez, República Dominicana

Trabajo presentado al XV Concurso Latinoamericano de Monografías
en materia de Prevención del Lavado de Activos y el Financiamiento
del Terrorismo organizado por FELABAN y COPLAFT.

Santo Domingo, D. N., República Dominicana

Julio 17, 2026

Índice

Resumen Ejecutivo	4
Introducción.....	5
Título: Gobernanza y RegTech en el nuevo orden financiero: El papel de la IA y Blockchain en la arquitectura de cumplimiento PLAFT 2026.....	7
1. Evolución del Riesgo LA/FT y el Ecosistema RegTech en América Latina	7
1.1. De la revisión manual al cumplimiento automatizado	8
1.2. Inteligencia Artificial y Machine Learning en la reducción de falsos positivos 10	
1.3. Blockchain y criptoactivos: Riesgos emergentes y oportunidades de trazabilidad.....	13
2. El Dilema de la "Caja Negra" y la Teoría de Agencia en la Banca.....	14
2.1. Opacidad algorítmica y la pérdida de explicabilidad en el cumplimiento.....	14
2.2. La Teoría de Agencia frente a la disrupción tecnológica y la asimetría de información	18
2.3. Implicaciones ético-legales, sesgos y la responsabilidad penal corporativa	20
3. Sinergia Tecnológica: Inteligencia Artificial Explicable (XAI) y Blockchain como Herramientas de Cumplimiento	21
3.1. La Inteligencia Artificial Explicable (XAI) como puente hacia la transparencia regulatoria	22
3.2. Inmutabilidad descentralizada: El rol del Blockchain en la Debida Diligencia (KYC)	23
3.3. Convergencia tecnológica: La IA mitigando las vulnerabilidades del Blockchain.....	24
4. Desafíos Regulatorios: El Contexto Latinoamericano y la Inercia Normativa en República Dominicana.....	25
4.1. La arquitectura regulatoria: Entre los principios de Basilea y la era algorítmica.....	26
4.2. El dinamismo del sector privado frente al rezago institucional	27
4.3. Riesgos estratégicos y el camino hacia la soberanía digital regional	28
5. Propuesta: Hacia un Modelo de Gobernanza Híbrida.....	29
5.1. Pilares del Modelo de Gobernanza Híbrida.....	29
5.2. Operacionalización del Modelo en la Banca Múltiple	30
5.3. Estandarización regional y soberanía digital.....	31
5.4. Dimensión Regional: Escalabilidad y Armonización en América Latina	32
6. Perspectivas y recomendaciones	34

6.1.	La carrera contra lo inalcanzable	35
6.2.	Lo imperativo de la transparencia algorítmica	36
6.3.	Mi perspectiva: el usuario frente a la máquina.....	37
6.4.	Recomendaciones.....	37
6.5.	Cambio cultural	39
	Conclusión	41
	Referencias bibliográficas.....	43

Resumen Ejecutivo

La digitalización financiera ha reconfigurado el riesgo de Lavado de Activos y Financiamiento del Terrorismo (LA/FT), exigiendo una respuesta tecnológica superior. Esta monografía analiza la tensión estructural entre la adopción de Regulatory Technology (RegTech) Inteligencia Artificial (IA) y Blockchain y la necesidad de una gobernanza corporativa auditable. El problema central es la desincronización entre la innovación algorítmica y los marcos normativos actuales, creando un "dilema de caja negra" donde la opacidad en las decisiones automatizadas expone a las entidades financieras a riesgos penales, regulatorios y reputacionales.

Esta investigación propone un Modelo de Gobernanza Híbrida para la banca múltiple, aplicable al contexto de República Dominicana y América Latina. Este modelo articula tres pilares estratégicos: 1) Inteligencia Artificial Explicable (XAI), que garantiza la trazabilidad y justificación de cada decisión algorítmica ante los reguladores; 2) Tecnología Blockchain, que asegura la inmutabilidad y procedencia de los datos, eliminando la manipulación; y 3) Supervisión Humana Activa, que formaliza el juicio crítico directivo mediante auditorías algorítmicas, evitando la delegación absoluta a sistemas autónomos.

El aporte consiste en una hoja de ruta operativa para que los Consejos de Administración auditen la lógica algorítmica y alineen la innovación con estándares internacionales (GAFI). Se concluye que la resiliencia financiera no reside en la automatización total, sino en integrar la eficiencia tecnológica con la ética, el criterio y la rendición de cuentas humana.

Introducción

Vivimos en una era donde la frontera entre la innovación financiera y el riesgo sistémico se ha vuelto casi imperceptible. La digitalización acelerada no solo ha optimizado la experiencia del cliente, sino que ha desatado una carrera armamentista tecnológica: mientras las instituciones financieras buscan agilidad, las redes criminales han mutado sus métodos, aprovechando la velocidad y el anonimato de la economía digital para sofisticar sus esquemas de lavado de activos y financiamiento del terrorismo. Ante esta amenaza asimétrica, la adopción de soluciones de *Regulatory Technology* (RegTech), como la Inteligencia Artificial (IA) y el Blockchain, ha dejado de ser una ventaja competitiva para convertirse en un imperativo de supervivencia. Sin embargo, este trabajo parte de una premisa ineludible: la tecnología, por sí sola, no es un remedio. Su efectividad es ilusoria si no está contenida en un marco de gobernanza que garantice, ante todo, explicabilidad, trazabilidad y responsabilidad corporativa.

América Latina, y en particular la República Dominicana, transita un momento crítico. La presión por alinearse con los estándares internacionales plasmada localmente en la Ley 155-17 ha forzado a la banca múltiple a modernizar sus controles. No obstante, existe un espejismo en la automatización: muchas entidades han implementado sistemas predictivos sin cuestionar la "caja negra" algorítmica, delegando decisiones de alto impacto a modelos cuyo razonamiento interno es inaccesible. Este fenómeno no es solo técnico, sino profundamente político y ético. La desincronización entre la velocidad del código y la capacidad de los Consejos de Administración para auditar sus propias decisiones ha redefinido

el problema de agencia: ¿cómo puede un directivo asumir la responsabilidad fiduciaria de controles tecnológicos que no comprende?

El problema central que aborda esta monografía es la erosión de la gobernanza corporativa ante la disrupción algorítmica. No basta con automatizar; es vital responsabilizar. Ante este vacío, se propone un Modelo de Gobernanza Híbrida, una estructura diseñada para armonizar la eficiencia predictiva de la Inteligencia Artificial Explicable (XAI) y la inmutabilidad del Blockchain con mecanismos de supervisión humana activa y auditoría tecnológica permanente. Este enfoque no pretende frenar la innovación, sino dotarla de un andamiaje legal y ético que permita a las instituciones financieras reducir su exposición jurídica mientras blindan su integridad operativa.

El estudio articula evidencia global con la experiencia local, examinando el ecosistema RegTech latinoamericano, los dilemas éticos de la opacidad algorítmica y la sinergia técnica entre la XAI y la descentralización. A través de este análisis, se ofrecen recomendaciones prácticas para la banca múltiple dominicana y regional, buscando transformar la modernización tecnológica de un riesgo latente en el pilar fundamental de una defensa financiera robusta, transparente y, sobre todo, soberana.

Título: Gobernanza y RegTech en el nuevo orden financiero: El papel de la IA y Blockchain en la arquitectura de cumplimiento PLAFT 2026

1. Evolución del Riesgo LA/FT y el Ecosistema RegTech en América Latina

La globalización de los mercados y la aceleración de la economía digital han desdibujado las fronteras tradicionales del sector financiero, permitiendo que el flujo de capitales se mueva en milisegundos y que las estructuras criminales operen ya no de forma aislada sino como redes transnacionales altamente tecnológicas. Según el Grupo de Acción Financiera Internacional (GAFI, 2021), la sofisticación de los esquemas de lavado de activos ha alcanzado niveles en los que la detección humana, sin herramientas tecnológicas avanzadas, resulta insuficiente. En este contexto, la transformación digital del sistema financiero ha reconfigurado de manera irreversible la tipología y la velocidad de los delitos económicos; en América Latina, región de economías emergentes y marcos institucionales en proceso de maduración, las organizaciones criminales han aprovechado la interconexión tecnológica para sofisticar sus esquemas de Lavado de Activos y Financiamiento del Terrorismo (LA/FT). Frente a esta amenaza asimétrica, la sostenibilidad empresarial y la seguridad del sector dependen cada vez más de la adopción de tecnologías financieras (FinTech) y de regulación (RegTech), que han dejado de ser meras herramientas de eficiencia para consolidarse como pilares estratégicos de defensa corporativa (Grupo de Acción Financiera Internacional [GAFI], 2021).

1.1. De la revisión manual al cumplimiento automatizado

Históricamente, la mitigación de los riesgos LA/FT en las instituciones financieras latinoamericanas se apoyó en sistemas transaccionales basados en reglas estáticas y umbrales rígidos (p. ej., reportes automáticos por transacciones superiores a montos fijos). Estos modelos heredados operaban bajo una lógica binaria si ocurre X, entonces marcar Y y dependían de manera abrumadora de la intervención humana para la revisión manual de alertas, así como de la estandarización de prácticas como Conozca a su Cliente (KYC) y la Debida Diligencia del Cliente (CDD). La explosión exponencial del volumen de datos financieros y la inmediatez de los pagos transfronterizos desbordaron rápidamente las capacidades del análisis humano, generando un ecosistema de cumplimiento reactivo y altamente propenso al error.

Ese enfoque produjo dos problemas estructurales que se retroalimentan. Primero, un cuello de botella cognitivo: los oficiales de cumplimiento se vieron saturados por una avalancha de alertas, muchas de ellas irrelevantes, lo que redujo la capacidad de investigar con profundidad los casos complejos y elevó el riesgo de omisión de señales verdaderamente críticas. Segundo, una rigidez procedimental que los delincuentes financieros explotaron mediante técnicas de fragmentación de operaciones, diseño de transacciones estructuradas y uso de instrumentos financieros intermedios para mantenerse por debajo de umbrales predefinidos. En la práctica, estas limitaciones tradujeron la eficiencia aparente de los sistemas basados en reglas en una falsa sensación de control.

Frente a esta vulnerabilidad, la adopción de ecosistemas RegTech seguros e inteligentes ha marcado un cambio de paradigma operativo. La incorporación de analíticas de Big Data, modelos de Machine Learning y procesamiento en tiempo real permite ahora priorizar alertas por riesgo contextual, correlacionar señales entre múltiples fuentes y generar perfiles dinámicos de comportamiento transaccional. Esto transforma la función del Oficial de Cumplimiento: de revisor masivo de alertas a supervisor de sistemas predictivos, encargado de validar, interpretar y auditar decisiones automatizadas. Además, la automatización inteligente facilita la creación de rastro de auditoría y evidencia explicable que respalda los Reportes de Operación Sospechosa (ROS), mejorando la trazabilidad y la defensabilidad jurídica de las decisiones de cumplimiento.

En el contexto latinoamericano y de manera particular en la República Dominicana tras la promulgación de la Ley 155-17 esta transición tecnológica no es solo una mejora operativa, sino un imperativo regulatorio y de integridad institucional. La modernización exige inversiones en infraestructura de datos, gobernanza de modelos, controles de calidad de la información y capacitación especializada para los equipos de cumplimiento. También requiere protocolos de validación continua de los modelos, mecanismos de gestión de falsos positivos y procesos formales de intervención humana en decisiones de alto impacto. Solo mediante la combinación de capacidades tecnológicas avanzadas y un marco de gobernanza robusto las instituciones podrán reducir la carga operativa, mejorar la detección de tipologías complejas y cumplir con los estándares internacionales de transparencia y reportabilidad. (El Khoury et al., 2024; El Harras & Salahddine, 2024).

1.2. Inteligencia Artificial y Machine Learning en la reducción de falsos positivos

El mayor desafío de los sistemas antilavado tradicionales es la generación masiva de falsos positivos, donde transacciones legítimas son marcadas como sospechosas por reglas estáticas que carecen de contexto histórico y comportamental. Un sistema basado únicamente en reglas responde al monto o a una condición puntual, pero no modela la trayectoria ni la variabilidad del comportamiento del cliente, lo que produce un alto ruido estadístico y un desgaste operativo en los equipos de cumplimiento. (Anik, 2026).

Capacidades técnicas de ML aplicadas

- **Perfilado dinámico:** los modelos de aprendizaje supervisado y no supervisado construyen perfiles transaccionales por cliente que incorporan variables temporales, geográficas y de contrapartes. Estos perfiles permiten identificar desviaciones significativas respecto a la línea base individual en lugar de comparar la conducta con umbrales universales. (Anik, 2026).
- **Reducción del ruido estadístico:** mediante entrenamiento con conjuntos históricos etiquetados (fraude vs. legítimo), los clasificadores aprenden patrones complejos secuencias, frecuencias, relaciones entre atributos que distinguen señales relevantes del ruido, reduciendo la tasa de falsos positivos y priorizando alertas de mayor probabilidad. (Anik, 2026).
- **Detección de anomalías y clustering:** técnicas no supervisadas (clustering, autoencoders, isolation forest) detectan comportamientos

atípicos sin depender de etiquetas previas, lo que es útil para tipologías emergentes que no están representadas en los datos históricos. (Anik, 2026).

- **Modelos de scoring y calibración probabilística:** los sistemas modernos generan una puntuación de riesgo continuo por evento o por cliente, que puede calibrarse para distintos niveles de tolerancia al riesgo y ajustarse dinámicamente según la carga operativa y el apetito institucional. (Anik, 2026).

Arquitectura operativa recomendada

- **Pipeline de datos robusto:** ingesta en tiempo real, normalización, enriquecimiento con fuentes externas y control de calidad; los modelos solo son tan buenos como los datos que consumen.
- **Módulo de priorización:** combinar score ML con reglas de negocio y señales heurísticas para producir una lista priorizada de alertas con explicaciones asociadas.
- **Supervisión humana:** mantener intervención humana en validación de alertas críticas y en la retroalimentación que alimenta el reentrenamiento continuo del modelo.
- **Testeo y monitoreo:** pruebas periódicas de desempeño y monitoreo de deriva de datos para detectar degradación del modelo y necesidad de recalibración. (Anik, 2026).

IA Generativa y LLMs: valor añadido y límites La incorporación de IA generativa y grandes modelos de lenguaje permite enriquecer el contexto de una alerta mediante la síntesis de información no estructurada (mensajes, descripciones de transacciones, noticias) y la generación de explicaciones en lenguaje natural que facilitan la revisión humana y la trazabilidad regulatoria (World Compliance Association, 2024). No obstante, estos modelos requieren controles estrictos de veracidad y mecanismos de verificación, pues pueden introducir sesgos o producir salidas no verificables si no se integran con fuentes confiables.

Evidencia práctica y condiciones de efectividad

La experiencia gremial en la banca dominicana muestra reducciones operativas significativas en falsos positivos cuando los modelos se implementan con gobernanza adecuada, datos de calidad y procesos de validación continua (Asociación de Bancos Múltiples de la República Dominicana, 2025). Sin embargo, el impacto real depende del entorno institucional: en marcos regulatorios y de gobernanza débiles, la IA puede ser mal parametrizada o explotada, lo que subraya la necesidad de políticas de gobernanza de datos, auditorías algorítmicas y transparencia en los criterios de decisión automatizada (Al Qudah & Alwaked, 2025).

La transición de reglas estáticas a modelos predictivos no elimina la necesidad del juicio humano ni las obligaciones regulatorias; las tecnologías IA/ML deben implementarse como sistemas híbridos que combinen perfilado dinámico, priorización probabilística, explicabilidad y supervisión humana continua para maximizar la reducción de falsos positivos sin sacrificar la defensabilidad jurídica ni

la equidad en el trato al cliente. (Anik, 2026; World Compliance Association, 2024; Asociación de Bancos Múltiples de la República Dominicana, 2025; Al Qudah & Alwaked, 2025).

1.3. Blockchain y criptoactivos: Riesgos emergentes y oportunidades de trazabilidad

En paralelo al avance de la IA, el surgimiento de la tecnología de contabilidad distribuida (Blockchain) y los criptoactivos ha introducido un escenario dual para los reguladores en América Latina. Por un lado, la descentralización financiera facilita esquemas complejos de anonimato. La ciberseguridad se erige entonces como un elemento crítico; sin protocolos robustos de protección de la información, el combate al financiamiento del terrorismo y el lavado de dinero en entornos descentralizados resulta insostenible.

Por otro lado, el Blockchain en sí mismo constituye una de las herramientas RegTech más potentes para la mitigación del riesgo operativo. Su arquitectura resuelve de forma directa los problemas de asimetría de la información y la credibilidad de los datos en los sistemas de prevención financiera (Sun et al., 2025). Cuando el Blockchain se integra con la Inteligencia Artificial, se genera un mecanismo de control superior: la IA aporta la capacidad predictiva para identificar el fraude, mientras que el Blockchain garantiza la seguridad y la inmutabilidad de los datos analizados, creando mecanismos de detección robustos e integrales (Guere Castellanos, 2023).

Para América Latina, el reto consiste en adoptar esta sinergia tecnológica asegurando la soberanía digital y la protección de la privacidad de los usuarios, mediante enfoques colaborativos que armonicen las normativas locales con la cooperación financiera global frente a un fenómeno que no reconoce fronteras.

2. El Dilema de la "Caja Negra" y la Teoría de Agencia en la Banca

La transición hacia ecosistemas de cumplimiento automatizados no es un proceso exento de profundas fricciones organizacionales. A medida que las instituciones financieras de América Latina adoptan soluciones RegTech de última generación, emerge una severa tensión estructural en los niveles directivos. Esta fricción se origina en el choque inherente entre la complejidad matemática y computacional de las nuevas herramientas predictivas y los principios jurídicos ineludibles de responsabilidad corporativa que rigen la banca múltiple. No se trata de un simple problema de implementación de *software*, sino de un cambio de paradigma que desafía las bases mismas de la gobernanza corporativa.

2.1. Opacidad algorítmica y la pérdida de explicabilidad en el cumplimiento

La incorporación sistemática de la Inteligencia Artificial (IA) en los procesos de prevención ha generado la opacidad algorítmica o “caja negra”, fenómeno en el que modelos complejos especialmente redes neuronales profundas alcanzan niveles de autonomía que dificultan rastrear la lógica exacta detrás de una decisión automatizada. Esta opacidad crea una tensión práctica: los modelos más precisos para detectar fraudes complejos suelen ser los menos interpretables, lo que en el

ámbito del cumplimiento bancario constituye una vulnerabilidad operativa crítica (Iguodala & Oyiborhoro, 2025; Dobbe et al., 2021).

Profundización técnica: tipos de explicabilidad y técnicas aplicables

- **Modelos interpretables:** priorizar, cuando sea posible, modelos intrínsecamente explicables (árboles de decisión, regresiones penalizadas, reglas extraíbles) para casos donde la trazabilidad jurídica es prioritaria.
- **Técnicas de revisión continua:** aplicar métodos que expliquen cualquier modelo sin alterar su estructura, por ejemplo, SHAP (valores de Shapley) y LIME para atribuir importancia a características en decisiones puntuales; estas técnicas ofrecen explicaciones locales y globales que facilitan la defensa técnica de un ROS.
- **Técnicas de modelos específicos:** Para auditorías técnicas de alta precisión, es indispensable emplear técnicas de modelos específicos que, a diferencia de los métodos agnósticos, explotan la arquitectura interna del algoritmo para revelar el procesamiento de datos. En el caso de las redes neuronales, el uso de mapas de relevancia, gradientes integrados y la atribución de características permite cuantificar con exactitud el peso de variables críticas como montos o jurisdicciones en la predicción final, ofreciendo una justificación auditable de la alerta. Por otro lado, en modelos secuenciales orientados a detectar patrones en series temporales, la implementación de mecanismos de atención y el análisis de contribución temporal facilitan la reconstrucción de la cronología del riesgo, permitiendo

al oficial de cumplimiento aislar los eventos específicos dentro de una serie transaccional que motivaron la clasificación de actividad sospechosa, validando así la lógica evolutiva del modelo de forma intrínseca.

- **Contrafactuales y explicaciones contrastivas:** generar escenarios mínimos alternativos que cambien la decisión qué habría que modificar para que la alerta no se dispare para facilitar la comprensión humana y la argumentación jurídica.
- **Modelos subrogados:** constituye una técnica fundamental para la explicabilidad. Este enfoque consiste en entrenar modelos intrínsecamente interpretables como árboles de decisión o regresiones lineales diseñados para aproximar el comportamiento del modelo complejo en regiones relevantes del espacio de características. Al simplificar la lógica de predicción en entornos locales específicos, los modelos subrogados permiten a los oficiales de cumplimiento comprender las decisiones del sistema ante alertas de riesgo determinadas, obteniendo una interpretación comprensible y auditable sin necesidad de reducir la complejidad ni sacrificar la capacidad predictiva del algoritmo original.

Gobernanza técnica y operativa para la explicabilidad

- **XAI-by-design:** incorporar requisitos de explicabilidad desde la adquisición y contratación de soluciones documentación de variables, límites de imputación, pruebas de robustez.

- **Rastro de auditoría y metadatos:** registrar versiones de modelos, datos de entrenamiento, parámetros, métricas de desempeño y decisiones de reentrenamiento; asegurar inmutabilidad y accesibilidad para auditorías internas y regulatorias.
- **Validación continua y revisión:** establecer pruebas periódicas de desempeño y métricas de explicabilidad consistencia de atribuciones, estabilidad local para detectar deriva y degradación.
- **Gestión de incertidumbre:** reportar scores probabilísticos y márgenes de confianza; cuando la incertidumbre supere umbrales definidos, forzar intervención humana antes de emitir un ROS.

Requisitos para defensabilidad jurídica

- **Documentación técnica accesible:** además de la explicación técnica, producir resúmenes ejecutivos y justificaciones en lenguaje jurídico que vinculen variables del modelo con criterios regulatorios.
- **Trazabilidad de decisiones: cada ROS debe incluir:** (1) la explicación del modelo, (2) la versión del modelo y datos usados, (3) la intervención humana realizada y (4) el razonamiento final del Oficial de Cumplimiento.
- **Pruebas de equidad y sesgo:** ejecutar auditorías de sesgo y equidad sobre subgrupos relevantes; documentar mitigaciones aplicadas para evitar discriminación y proteger la inclusión financiera.

Riesgos residuales y mitigaciones

- **Sobreconfianza tecnológica:** evitar delegar la responsabilidad fiduciaria; la Alta Dirección debe exigir evidencia de explicabilidad y controles.
- **Manipulación adversaria:** implementar pruebas adversariales y detección de envenenamiento de datos; combinar XAI con controles de integridad de datos.
- **Limitaciones de XAI:** reconocer que ninguna técnica garantiza explicaciones perfectas; las explicaciones deben evaluarse por su utilidad práctica, estabilidad y verificabilidad, no solo por su apariencia interpretativa (Dobbe et al., 2021; Barredo Arrieta et al., 2020).

La adopción de XAI no es un lujo técnico sino un requisito funcional para cualquier estrategia RegTech viable: permite reconciliar la eficacia predictiva de modelos avanzados con la exigencia de trazabilidad, justificabilidad y responsabilidad corporativa en el cumplimiento financiero. Implementada mediante una combinación de técnicas interpretables, gobernanza de modelos, auditoría continua y participación humana, la XAI transforma la “caja negra” en un sistema auditable y defendible ante reguladores y tribunales (Barredo Arrieta et al., 2020; Dobbe et al., 2021; Iguodala & Oyiborhoro, 2025).

2.2. La Teoría de Agencia frente a la disrupción tecnológica y la asimetría de información

Desde la perspectiva del Gobierno Corporativo, la opacidad algorítmica desestabiliza y reconfigura los fundamentos clásicos de la Teoría de Agencia

(Jensen & Meckling, 1976). En su concepción original, este marco conceptual postula que los directivos (agentes) actúan en representación de los accionistas y grupos de interés (principales), asumiendo la responsabilidad fiduciaria indelegable de proteger a la entidad contra riesgos operacionales, reputacionales y legales. Sin embargo, al integrar la Inteligencia Artificial en el monitoreo de transacciones, emerge un "doble problema de agencia": la Alta Dirección (agente del accionista) delega ahora funciones críticas de control a un ente no humano (el algoritmo), sobre el cual no posee una comprensión técnica absoluta.

Esta delegación genera una brecha masiva de asimetría de la información en los mecanismos de control de riesgos financieros (Sun et al., 2025). La evidencia empírica contemporánea demuestra que el despliegue tecnológico sin un andamiaje institucional robusto que cierre esta brecha es contraproducente. En economías con gobernanza corporativa débil o inmadura, la Inteligencia Artificial no solo fracasa en la mitigación del riesgo, sino que sus vulnerabilidades pueden ser explotadas de manera adversaria para facilitar el flujo de capitales ilícitos en la economía en la sombra (Al Qudah & Alwaked, 2025).

Esta pérdida de control directivo se agudiza en jurisdicciones altamente reguladas como la República Dominicana. La normativa local, a través del *Reglamento de Gobierno Corporativo*, obliga expresa e inexcusablemente a la Alta Gerencia y a los miembros del Consejo de Administración a "comprender la naturaleza de los riesgos asumidos" por la entidad (Junta Monetaria de la República Dominicana, 2007). Argumentar desconocimiento técnico sobre cómo opera el *software* de cumplimiento no exime de responsabilidad al directorio. Para cumplir con este

mandato jurídico y restaurar el equilibrio de la agencia, la industria financiera debe transitar desde enfoques centrados puramente en la automatización hacia una inteligencia artificial "simbiótica", donde el juicio crítico humano y la capacidad predictiva del algoritmo interactúen de forma colaborativa, transparente y auditable en la toma de decisiones (Calvano et al., 2025).

2.3. Implicaciones ético-legales, sesgos y la responsabilidad penal corporativa

El impacto del dilema de la caja negra trasciende la ineficiencia procedimental para adentrarse peligrosamente en el terreno del derecho y la responsabilidad penal de las personas jurídicas. Delegar decisiones sensibles de cumplimiento normativo a la Inteligencia Artificial sin un marco de supervisión humana estricto y documentado expone a las instituciones a graves riesgos jurídicos, haciendo mandatorio la implementación de un "modelo de gobierno híbrido" que integre la innovación tecnológica con la ineludible rendición de cuentas (Manfrin, 2025). Si un algoritmo clasifica erróneamente operaciones lícitas o aprueba transacciones vinculadas al financiamiento del terrorismo debido a un diseño deficiente, la responsabilidad ante la ley, y las multas multimillonarias asociadas, recaen exclusivamente sobre la corporación financiera y sus directivos (Aksenova, 2024).

Asimismo, la toma de decisiones algorítmicas de alto impacto exige abordar de manera frontal el problema de los sesgos en los datos de entrenamiento (Mehrabi et al., 2021). La inducción de clasificadores automatizados en la prevención de lavado de dinero requiere mecanismos estadísticos y de auditoría que garanticen la equidad y la justicia en el trato al cliente, evitando que la IA discrimine perfiles

financieros de manera injustificada o afecte negativamente la inclusión financiera de sectores vulnerables (Arguelles Toache, 2026). Cualquier vulneración sistemática a estos principios éticos no solo acarrea sanciones regulatorias severas, sino un daño reputacional a menudo irreversible.

Finalmente, este dilema directivo se entrelaza estrechamente con las crecientes preocupaciones globales sobre la privacidad de la información bancaria. La rápida digitalización exige la adopción de protocolos criptográficos que protejan la información personal sensible, fortaleciendo la soberanía digital de los estados para evitar que las amplias exigencias del monitoreo financiero y el intercambio de datos transfronterizos vulneren los derechos individuales de los ciudadanos (Abdullahi et al., 2025). En consecuencia, la adquisición y parametrización de herramientas RegTech debe elevarse, sin excepciones, a una decisión estratégica del más alto nivel del Gobierno Corporativo, garantizando que los sistemas blinden a la institución frente a la incertidumbre regulatoria y el riesgo penal, operando siempre bajo un escrutinio ético y legal inquebrantable.

3. Sinergia Tecnológica: Inteligencia Artificial Explicable (XAI) y Blockchain como Herramientas de Cumplimiento

Frente a la tensión estructural generada por la opacidad algorítmica y los riesgos de responsabilidad corporativa, la respuesta institucional no puede consistir en un retroceso tecnológico. Por el contrario, la solución reside en la integración de una arquitectura RegTech superior que elimine las asimetrías de información. Es en este punto donde la convergencia entre la Inteligencia Artificial Explicable (XAI) y la tecnología de contabilidad distribuida (*Blockchain*) se erige como el ecosistema

definitivo para el cumplimiento normativo. Ambas tecnologías, al operar en sinergia, resuelven sus debilidades intrínsecas y proporcionan a la Alta Dirección el andamiaje auditable necesario para una gobernanza corporativa efectiva.

3.1. La Inteligencia Artificial Explicable (XAI) como puente hacia la transparencia regulatoria

La Inteligencia Artificial Explicable (XAI) representa el avance técnico y conceptual más significativo para restaurar la confianza y la rendición de cuentas en los procesos de cumplimiento financiero. Frente a la inescrutabilidad de los algoritmos de "caja negra", la XAI surge como una subdisciplina de la ciencia de datos orientada específicamente a estructurar modelos de aprendizaje automático cuyos procesos internos, variables de ponderación y decisiones predictivas puedan ser completamente auditados e interpretados por el juicio humano (Barredo Arrieta et al., 2020).

En los sistemas de prevención del Lavado de Activos y Financiamiento del Terrorismo (LA/FT), la XAI altera radicalmente el paradigma de evaluación de riesgos. Esta tecnología garantiza que cada alerta generada ya sea el bloqueo de una transacción transfronteriza o la clasificación de alto riesgo de un cliente corporativo posea justificaciones lógicas, matemáticas y, sobre todo, trazables en lenguaje natural (Iguodala & Oyiborhoro, 2025). Esto permite que los Oficiales de Cumplimiento puedan presentar evidencias claras, fundamentadas y verificables ante los reguladores financieros u organismos como la Unidad de Análisis Financiero (UAF), eliminando de raíz la incertidumbre jurídica asociada a las decisiones automatizadas.

La implementación de XAI requiere adoptar un enfoque de "explicabilidad por diseño", en el cual el modelo no solo es evaluado por su precisión predictiva (*accuracy*), sino por su capacidad de generar un rastro de auditoría transparente que respalde el proceso cognitivo de la máquina. Como señalan Iguodala y Oyiborhoro (2025), este nivel de transparencia fomenta una confianza institucional inquebrantable en las operaciones de seguridad financiera, permitiendo que la Alta Dirección asuma la responsabilidad de las decisiones tecnológicas sin exponerse a la negligencia fiduciaria.

3.2. Inmutabilidad descentralizada: El rol del Blockchain en la Debida Diligencia (KYC)

Mientras la XAI aporta claridad interpretativa a la toma de decisiones, la tecnología *Blockchain* garantiza la integridad absoluta y la procedencia de los datos que alimentan dichos modelos predictivos. En la actualidad, los procesos de Conozca a su Cliente (KYC) y Debida Diligencia (CDD) sufren de una severa fragmentación, caracterizándose por bases de datos en silos, redundancia de esfuerzos interbancarios y una vulnerabilidad latente a la manipulación de información.

La arquitectura del Blockchain aborda de frente los problemas de asimetría de la información y falta de credibilidad de los datos en la gestión de riesgos corporativos (Sun et al., 2025). Su aplicación en los protocolos de prevención LA/FT permite la creación de registros descentralizados e inmutables. Esta inmutabilidad criptográfica asegura que una vez que la identidad de un cliente o el origen de los fondos han sido verificados y registrados en la cadena de bloques, dicha

información no puede ser alterada, falsificada ni eliminada retrospectivamente sin el consenso de la red.

Esta característica descentralizada facilita una trazabilidad interbancaria sin precedentes, reduciendo drásticamente la fricción y los costos operativos en el intercambio de información entre instituciones financieras, respetando simultáneamente las normativas de privacidad mediante el uso de encriptación avanzada y contratos inteligentes. Al utilizar Blockchain, los bancos pueden auditar el historial completo y cronológico de una transacción, garantizando a los sistemas de Inteligencia Artificial una fuente de datos veraz, limpia y libre de manipulaciones adversarias (Guere Castellanos, 2023).

3.3. Convergencia tecnológica: La IA mitigando las vulnerabilidades del Blockchain

El ecosistema RegTech alcanza su máxima eficacia cuando se comprende que el *Blockchain* y la IA son tecnologías simbióticas. Aunque el *Blockchain* es inherentemente seguro contra la alteración de datos, la literatura académica documenta ampliamente que no está exento de riesgos operacionales; vulnerabilidades en el código de los contratos inteligentes, problemas de escalabilidad, incertidumbres regulatorias e ineficiencias operativas han sido identificadas como barreras críticas para su adopción masiva en la industria bancaria (Malik et al., 2025).

Es precisamente en estas vulnerabilidades donde la Inteligencia Artificial actúa como un mecanismo de resiliencia y optimización. Los sistemas impulsados por IA,

mediante métodos de análisis predictivo y detección de anomalías en tiempo real, son capaces de monitorear de forma continua el tráfico de la red *Blockchain* para identificar intentos de intrusión o patrones de transacciones colusorias que intenten explotar vulnerabilidades de escalabilidad (Malik et al., 2025). Además, el procesamiento de lenguaje natural y el aprendizaje profundo permiten realizar auditorías automatizadas y verificación inteligente de los contratos, asegurando que la lógica programada cumpla estrictamente con las normativas vigentes y no contenga puertas traseras explotables por criminales financieros (Malik et al., 2025).

Esta interacción bidireccional consolida una arquitectura de defensa impenetrable: la IA supervisa la eficiencia, la seguridad operativa y la lógica del *Blockchain*, mientras que el *Blockchain* garantiza la inmutabilidad y la pureza de los datos de entrenamiento que utiliza la IA, previniendo ataques de envenenamiento de datos (Guere Castellanos, 2023). Al integrar ambas tecnologías, la banca múltiple latinoamericana puede construir un ecosistema de cumplimiento robusto y altamente automatizado que no solo cumple con los rigurosos estándares del Grupo de Acción Financiera Internacional (GAFI), sino que proporciona a la Alta Dirección la tranquilidad jurídica de operar bajo un marco totalmente auditable.

4. Desafíos Regulatorios: El Contexto Latinoamericano y la Inercia Normativa en República Dominicana

La implementación de herramientas *Regulatory Technology* (RegTech), tales como la Inteligencia Artificial (IA) y el *Blockchain*, no ocurre en un vacío geográfico, sino dentro de un complejo entramado institucional caracterizado por economías

emergentes y marcos regulatorios que presentan diversos niveles de madurez. En América Latina, la brecha entre la capacidad técnica de los sistemas y la obsolescencia normativa no es un fenómeno aislado de la República Dominicana; es un desafío regional. Mientras la industria financiera latinoamericana lidera esfuerzos hacia la digitalización, los marcos regulatorios a menudo operan bajo una inercia que dificulta la plena adopción de estas innovaciones.

4.1. La arquitectura regulatoria: Entre los principios de Basilea y la era algorítmica

Históricamente, los sistemas financieros de la región, incluyendo el dominicano, han construido sus estructuras de gobierno corporativo bajo la influencia de los principios internacionales de Basilea y lineamientos de la OCDE. En República Dominicana, el *Reglamento de Gobierno Corporativo* (Junta Monetaria de la República Dominicana, 2007) constituye la base legal que impone a la Alta Dirección la responsabilidad de supervisar la gestión de riesgos. Si bien este modelo es robusto, su aplicación en la actualidad enfrenta un desafío dialéctico: la norma es principista y estática, mientras que la tecnología es dinámica y algorítmica.

Esta desconexión es una constante en América Latina. A diferencia de jurisdicciones con marcos de regulación ágil, los países latinoamericanos suelen carecer de guías específicas sobre la responsabilidad algorítmica o la explicabilidad técnica de los modelos predictivos. La Alta Dirección se enfrenta así a una paradoja fiduciaria: tiene la obligación legal de comprender los riesgos asumidos, pero opera bajo normativas que no definen estándares de auditabilidad para los sistemas de

"caja negra" que el mercado ya está utilizando. Esta asimetría cognitiva entre lo que la ley exige y lo que la tecnología hace es el nudo gordiano que la gobernanza híbrida debe desatar.

4.2. El dinamismo del sector privado frente al rezago institucional

En la región, se observa un patrón claro: el sector bancario, movido por la necesidad de eficiencia y la presión competitiva, suele anticiparse a la regulación. En República Dominicana, la Asociación de Bancos Múltiples (ABA, 2025) ha validado que el sector bancario mantiene una transición activa hacia modelos predictivos, reconociendo que la tecnología es una aliada vital para cumplir eficazmente con la Ley 155-17. Esta postura proactiva es un denominador común en la banca múltiple latinoamericana, donde las instituciones están invirtiendo en IA para reducir falsos positivos y mejorar el escaneo transaccional, a menudo sin que exista una norma nacional que valide explícitamente estas metodologías.

Sin embargo, esta proactividad industrial encuentra límites severos cuando se trata de tecnologías disruptivas como el *Blockchain*. Al igual que en otras economías regionales, el ecosistema dominicano muestra una infraestructura tecnológica en desarrollo, pero con una falta de robustez normativa para soportar operaciones descentralizadas (Melo & Díaz, 2024). La incertidumbre jurídica derivada de esta falta de regulación específica para activos virtuales y tecnología de registro distribuido obliga a las entidades a una prudencia paralizante, limitando el potencial de innovaciones que, en mercados con mayor seguridad jurídica, ya están siendo integradas para prevenir el fraude mediante la inmutabilidad de datos.

4.3. Riesgos estratégicos y el camino hacia la soberanía digital regional

La literatura internacional sobre riesgos en mercados emergentes advierte que una adopción tecnológica sin un marco legal que la respalde crea vulnerabilidades sistémicas. Al Qudah y Alwaked (2025) han demostrado que, en entornos de gobernanza débil, los sistemas de IA pueden ser ineficaces o incluso explotados por actores ilícitos si no existe un control normativo estricto que obligue a la transparencia. Este es un riesgo compartido por toda América Latina; cuando el regulador no establece guías claras de debida diligencia tecnológica, la responsabilidad penal corporativa recae íntegramente sobre los directivos, convirtiendo la innovación en un riesgo legal inaceptable.

Para superar esta etapa de inercia, la región necesita un nuevo contrato entre el sector público y privado. Siguiendo las directrices de Abdullahi et al. (2025), el camino debe orientarse hacia el fortalecimiento de la soberanía digital, donde los estados no se aíslan, sino que colaboren para establecer estándares regionales de transparencia algorítmica. La solución no reside en frenar la tecnología, sino en evolucionar hacia normativas adaptables que reconozcan explícitamente protocolos de Inteligencia Artificial Explicable (XAI). Solo mediante una armonización que transforme al regulador de un actor sancionador a un facilitador de estándares tecnológicos, la banca dominicana y latinoamericana podrá alinear su capacidad técnica con la seguridad jurídica, convirtiendo sus controles de cumplimiento en verdaderos escudos de integridad financiera global.

5. Propuesta: Hacia un Modelo de Gobernanza Híbrida

La investigación realizada en los capítulos precedentes demuestra que la tecnología, por sí sola, es insuficiente para mitigar los riesgos LA/FT/PADM. La brecha entre la capacidad técnica de los sistemas RegTech y la rigidez de los modelos tradicionales de Gobierno Corporativo constituye el mayor desafío para la banca moderna. Ante este escenario, la presente monografía propone un Modelo de Gobernanza Híbrida, diseñado para fusionar la velocidad predictiva de la Inteligencia Artificial con la supervisión crítica y ética del juicio humano, permitiendo así una transición segura hacia la banca digital.

5.1. Pilares del Modelo de Gobernanza Híbrida

El Modelo de Gobernanza Híbrida se fundamenta en la premisa de que la responsabilidad fiduciaria es indelegable. Este enfoque estructural propone tres pilares operativos que deben ser integrados en las políticas de cumplimiento de toda institución financiera:

- a) **Transparencia Algorítmica y Explicabilidad (XAI):** Las instituciones deben abandonar la adquisición de soluciones de "caja negra". Cualquier herramienta RegTech de IA implementada debe cumplir con el criterio de *XAI-by-design*, asegurando que el Oficial de Cumplimiento pueda interpretar las variables que motivaron una alerta de riesgo (Barredo Arrieta et al., 2020). La explicabilidad es, en última instancia, el mecanismo que permite transformar el veredicto de una máquina en un argumento jurídico válido ante los entes reguladores.

b) Validación de Datos mediante Inmutabilidad (Blockchain): Para que un modelo de IA sea confiable, debe alimentarse de datos íntegros. El modelo híbrido propone el uso de tecnología *Blockchain* para certificar la procedencia y la inalterabilidad de la información utilizada en los procesos de debida diligencia (Sun et al., 2025). Esto garantiza que la IA no tome decisiones basadas en información manipulada o sesgada, blindando la integridad del proceso de toma de decisiones.

c) Supervisión Humana Activa (Human-in-the-loop): El modelo rechaza la automatización total en decisiones críticas. La Alta Dirección debe establecer comités interdisciplinarios integrados por expertos en tecnología, cumplimiento y legal encargados de realizar auditorías periódicas sobre la lógica algorítmica, validando que esta se mantenga alineada con los parámetros de riesgo aceptados por la institución (Manfrin, 2025).

5.2. Operacionalización del Modelo en la Banca Múltiple

Para que este modelo sea funcional, debe superar la fase conceptual e integrarse en los procesos operativos diarios. Basándonos en la experiencia del sector bancario dominicano, que ya ha iniciado una transición hacia modelos predictivos para reducir los falsos positivos (ABA, 2025), el Modelo de Gobernanza Híbrida propone una hoja de ruta para las Juntas Directivas:

- **Comités de Supervisión Tecnológica:** Es necesario elevar la supervisión tecnológica al nivel del Comité de Riesgos. Este órgano debe ser responsable de evaluar no solo la eficiencia operativa de las herramientas,

sino su alineación con el *Reglamento de Gobierno Corporativo* (Junta Monetaria de la República Dominicana, 2007). La responsabilidad de "comprender los riesgos" debe interpretarse ahora como la capacidad de auditar la lógica del sistema.

- **Protocolos de Auditoría Algorítmica:** Las instituciones deben adoptar protocolos de testeo continuo que detecten sesgos en los algoritmos de detección de fraudes (Arguelles Toache, 2026). Esto requiere una capacitación constante del personal humano para que, al gestionar estas nuevas herramientas, mantengan un escepticismo profesional que permita detectar cuando el sistema automatizado está operando fuera de sus parámetros de seguridad (ABA, 2025).

5.3. Estandarización regional y soberanía digital

La propuesta de este modelo no es solo una solución corporativa aislada, sino una estructura escalable para el sistema financiero latinoamericano. La fragmentación regulatoria que impide la cooperación regional (Melo & Díaz, 2024) puede ser superada mediante la adopción de estándares comunes de gobernanza tecnológica.

Si las instituciones de la región adoptan este modelo híbrido, se sientan las bases para una "gobernanza de datos compartida" que facilita la cooperación transfronteriza sin vulnerar la soberanía digital de cada nación. Como señalan Abdullahi et al. (2025), el fortalecimiento de la soberanía digital a través de

tecnologías que preservan la privacidad permite que la cooperación financiera global no sea un riesgo, sino una ventaja competitiva.

Este modelo de gobernanza híbrida permite, además, armonizar la autonomía nacional con los estándares internacionales del GAFI. Al implementar una arquitectura donde la IA actúa bajo supervisión humana auditable y los datos se protegen mediante la inmutabilidad del *Blockchain*, la banca múltiple puede enfrentar la sofisticación del crimen financiero con soluciones que sean, ante todo, auditables, seguras y responsables. La banca, en última instancia, no solo protege sus activos, sino que protege la integridad del sistema financiero nacional frente a amenazas transnacionales, cumpliendo así con su mandato ético y legal en la sociedad digital (El Harras & Salahddine, 2024).

5.4. Dimensión Regional: Escalabilidad y Armonización en América Latina

El Modelo de Gobernanza Híbrida propuesto no está concebido como una solución aislada para la banca múltiple dominicana, sino como un estándar escalable capaz de adaptarse a la heterogeneidad regulatoria de América Latina. La región se caracteriza por una marcada diversidad en la madurez de sus ecosistemas digitales, lo que demanda una arquitectura de gobernanza flexible, pero alineada con estándares globales de integridad financiera.

La realidad latinoamericana presenta un desafío compartido: la disparidad entre países que han implementado entornos de prueba regulatorios y aquellos que, como República Dominicana, operan bajo marcos normativos principistas que requieren de una interpretación proactiva por parte de la Alta Dirección (Junta

Monetaria de la República Dominicana, 2007). Esta fragmentación crea una asimetría de información que los actores ilícitos aprovechan para mover fondos a través de jurisdicciones con controles más laxos o tecnológicamente desactualizados. La investigación empírica regional sugiere que la adopción de IA en entornos de gobernanza débil resulta ineficaz, siendo susceptible de explotación por redes criminales (Al Qudah & Alwaked, 2025).

Ante este panorama, la propuesta de gobernanza híbrida se convierte en un mecanismo de defensa regional mediante los siguientes ejes:

- **Interoperabilidad regulatoria:** La adopción de estándares comunes de explicabilidad (XAI) permitiría que las instituciones financieras de la región hablen un "lenguaje técnico común" frente a los reguladores. Esto facilitaría la cooperación transfronteriza, transformando el cumplimiento normativo en una red colaborativa en lugar de un conjunto de silos aislados (El Harras & Salahddine, 2024).
- **Soberanía digital cooperativa:** América Latina debe transitar hacia un modelo donde la soberanía digital no implique aislamiento, sino la capacidad estratégica de gestionar datos financieros bajo estándares compartidos de privacidad. La integración de *Blockchain* y tecnologías que preservan la confidencialidad permite equilibrar la autonomía nacional con la cooperación global, asegurando que la información sensible no sea expuesta durante el intercambio transfronterizo (Abdullahi et al., 2025).

- **Armonización de estándares de auditoría:** El modelo sugiere que los países miembros de FELABAN adopten una "Matriz de Madurez RegTech". Esta matriz, basada en el Modelo de Gobernanza Híbrida, permitiría a las entidades autoevaluar su nivel de explicabilidad algorítmica y seguridad operativa, creando una hoja de ruta regional para reducir las brechas de cumplimiento técnico (Manfrin, 2025).

Por consiguiente, la adopción regional de este modelo permite que el sector bancario latinoamericano deje de reaccionar ante la inercia regulatoria para liderar la agenda de seguridad financiera. Al alinear los mandatos de gobernanza corporativa que son comunes a toda la región con protocolos técnicos de auditoría híbrida, América Latina puede posicionarse como un referente mundial en la prevención del lavado de activos, demostrando que la innovación tecnológica, cuando es supervisada responsablemente, es el mayor activo de integridad que puede poseer una nación (Aksenova, 2024).

6. Perspectivas y recomendaciones

Al concluir este recorrido, es importante apartar el análisis teórico para ofrecer una perspectiva pragmática, nacida de mi experiencia como consultor y usuario cotidiano de sistemas de vanguardia. La tecnología no es un evento futuro; es nuestra realidad operativa presente, y mi conclusión más firme es que, si bien la tecnología ha alcanzado una velocidad exponencial, la capacidad regulatoria de nuestros países se mantiene en una escala lineal, creando una brecha que, de no cerrarse, nos dejará indefensos. Esta asimetría es técnica, institucional y cultural: la innovación se autoconstruye en ciclos cortos mientras que los marcos

normativos, las capacidades directivas y las prácticas organizacionales evolucionan con lentitud. Si no actuamos con decisión para alinear gobernanza, capacidades y marcos regulatorios, la innovación terminará por amplificar riesgos en lugar de mitigarlos.

6.1. La carrera contra lo inalcanzable

Como profesional que interactúa diariamente con la arquitectura de datos, el análisis de tipologías y la implementación de soluciones RegTech, observo un fenómeno inquietante: el ritmo al que avanza la inteligencia artificial y el procesamiento descentralizado es, sencillamente, demasiado veloz. La innovación tecnológica hoy no espera permisos ni marcos legales; se autoconstruye sobre la marcha, optimizándose en ciclos de días, mientras que nuestras normativas tardan años en ser discutidas, redactadas y aprobadas. Debemos aceptar una realidad incómoda: ninguna norma, por exhaustiva que sea, logrará adaptarse con la agilidad necesaria al futuro tecnológico. La pretensión de legislar sobre “cómo” debe funcionar cada algoritmo es una batalla perdida de antemano. La regulación tradicional prescriptiva y rígida está diseñada para un mundo analógico donde las reglas cambiaban cada década; hoy, las reglas del juego financiero cambian cada trimestre. Intentar encorsetar la tecnología en marcos estáticos no solo es inútil, sino contraproducente: solo logra que las instituciones financieras más conservadoras se queden atrás, mientras que los actores ilícitos, que no tienen que cumplir con ninguna norma, nos llevan una ventaja tecnológica abismal. Por ello, la respuesta debe orientarse a principios, resultados y mecanismos de

experimentación supervisada que permitan aprender y ajustar sin paralizar la innovación legítima.

6.2. Lo imperativo de la transparencia algorítmica

La premisa central de esta investigación confirma que, aunque las tecnologías RegTech (IA y Blockchain) poseen un potencial disruptivo sin igual, su valor real es nulo si se implementan bajo esquemas de “caja negra”. La automatización, por sí misma, no garantiza integridad; solo amplifica la eficiencia de los procesos subyacentes, sean estos correctos o erróneos. El dilema fundamental radica en la explicabilidad: la eficacia de las herramientas antilavado modernas depende de la capacidad técnica de los sistemas para justificar sus alertas ante la autoridad competente. La IA Explicable (XAI) no es un lujo académico, es una condición operativa y legal que permite traducir decisiones algorítmicas en criterios auditables. Asimismo, la integración del Blockchain no solo aporta inmutabilidad, sino que actúa como ancla de veracidad para que la IA opere sobre datos confiables, mitigando el riesgo de sesgos y ataques adversarios. En definitiva, la tecnología no debe ser un sustituto de la responsabilidad humana, sino el catalizador que permite a los Oficiales de Cumplimiento concentrarse en el análisis de alto valor, delegando en la máquina la detección de anomalías y reservando la intervención humana para la interpretación, la validación y la decisión final.

6.3. Mi perspectiva: el usuario frente a la máquina

Desde mi práctica profesional y académica, el principal obstáculo para la adopción masiva no es la falta de presupuesto ni de acceso a herramientas, sino la “parálisis por miedo” al riesgo reputacional y penal. He constatado que muchas entidades prefieren procesos ineficientes y manuales antes que enfrentar una auditoría externa donde deban explicar la lógica interna de un algoritmo que nadie en la institución domina. Esa resistencia es racional cuando la responsabilidad penal y administrativa está en juego. La respuesta práctica es la adopción de XAI: cuando los modelos entregan explicaciones comprensibles y reproducibles, los oficiales de cumplimiento pueden auditar criterios, cuestionar resultados y tomar decisiones informadas. La soberanía digital control, trazabilidad y capacidad de cuestionar resultados algorítmicos debe convertirse en una competencia central del oficial moderno. La automatización sin transparencia es una vulnerabilidad; la automatización con explicabilidad es, en cambio, nuestra mayor fortaleza contra el crimen financiero. La formación técnica, la cultura de escepticismo profesional y la capacidad de ejecutar pruebas adversariales básicas son requisitos indispensables para que la tecnología cumpla su promesa.

6.4. Recomendaciones

Para cerrar la brecha entre la innovación y el marco normativo propongo recomendaciones concretas y priorizadas:

- **Para los reguladores.** Evolucionar el Reglamento de Gobierno Corporativo para incluir una “Guía de Devida Diligencia Tecnológica”

que transite de un enfoque meramente principista a estándares de auditabilidad técnica. Adoptar marcos de apertura supervisada que permitan pruebas controladas de XAI y Blockchain con métricas de salida, requisitos de reporte y protocolos de mitigación. Migrar hacia regulación basada en principios y resultados auditabilidad, trazabilidad, protección de datos y continuidad operativa en lugar de prescribir métodos técnicos.

- **Para la Alta Dirección y Juntas.** Elevar la supervisión tecnológica al nivel estratégico: integrar perfiles técnicos en comités de riesgo y auditoría, formalizar protocolos de intervención humana, definir umbrales de tolerancia y responsabilidades documentadas frente a decisiones automatizadas. Exigir XAI en adquisiciones y cláusulas contractuales que obliguen a proveedores a entregar documentación reproducible, pruebas de robustez y mecanismos de explicación.
- **Para las áreas operativas (Cumplimiento, TI, Riesgos).** Implementar programas de capacitación intergeneracional que formen a oficiales y auditores en fundamentos de modelos predictivos, identificación de sesgos, interpretación de salidas y pruebas adversariales. Fortalecer controles de calidad de datos y políticas de soberanía digital que permitan compartir inteligencia de forma segura y conforme a la protección de datos.
- **Para la cooperación regional.** Promover, a través de organismos como FELABAN, la creación de una “Matriz de Madurez RegTech”

regional que estandarice niveles mínimos de explicabilidad, seguridad y gobernanza, facilite interoperabilidad y reduzca el arbitraje regulatorio entre países. Fomentar protocolos comunes de intercambio de inteligencia con salvaguardas de privacidad.

6.5. Cambio cultural

La transformación tecnológica descrita es inútil sin una transformación cultural paralela. La "parálisis por miedo" que he constatado en el sector no se cura solo con más normativa, sino con una redefinición del perfil del oficial de cumplimiento. La lucha contra el lavado de activos en la era digital no se ganará con más burocracia manual, sino con la capacidad de desafiar al algoritmo, entender sus limitaciones y garantizar que la tecnología actúe siempre bajo una ética humana.

El profesional del futuro debe desarrollar una "mente crítica digital". Esto implica no aceptar el output de un software como una verdad absoluta, sino como una hipótesis que requiere validación. La gobernanza de la IA es, en última instancia, una gobernanza de la responsabilidad humana. Tenemos en nuestras manos el poder de blindar nuestros sistemas financieros con una eficiencia sin precedentes, pero ese poder exige un regulador audaz, una alta dirección comprometida y un sector privado que entienda que la burocracia técnica es el enemigo de la eficacia. La tecnología nos brinda la velocidad; la gobernanza, guiada por este plan de acción, debe brindarnos la dirección y la certeza jurídica necesarias para proteger el sistema financiero regional.

En definitiva, mi propuesta no es una rendición ante la máquina, sino una redefinición de nuestro rol: debemos dejar de ser operativos de reglas estáticas para convertirnos en auditores de criterios. El profesional del futuro en PLAFT debe tener la capacidad de desafiar al algoritmo, entender sus sesgos y garantizar que la tecnología actúe siempre bajo una ética humana. La lucha contra el lavado de activos y el financiamiento del terrorismo en América Latina no se ganará con más burocracia manual, sino con más inteligencia humana y artificial bien gobernada. La tecnología nos da la velocidad; la gobernanza debe dar la dirección. Tenemos en nuestras manos el poder de blindar nuestros sistemas financieros con una eficiencia que antes solo podíamos imaginar, pero ese poder exige un regulador audaz, una alta dirección comprometida y un sector privado que entienda que la burocracia técnica es el enemigo de la eficacia.

Conclusión

La revolución digital ha transformado de forma irreversible la naturaleza y la velocidad del delito financiero; en este nuevo escenario, la adopción de soluciones RegTech particularmente la Inteligencia Artificial y el Blockchain deja de ser una mejora opcional para convertirse en una condición de supervivencia institucional. La monografía demuestra que, aunque estas tecnologías ofrecen capacidades predictivas y de trazabilidad que reducen falsos positivos y mejoran la detección, su eficacia real depende de la capacidad institucional para gobernarlas. La sofisticación algorítmica progresa a ritmos exponenciales mientras que la gobernanza, la regulación y la comprensión directiva avanzan de forma lineal; esa desincronización genera una brecha crítica donde la opacidad de los modelos automatizados la “caja negra” puede transformar la innovación en una fuente de riesgo jurídico y reputacional si no se acompaña de exigencias de explicabilidad, trazabilidad y control humano.

Frente a este desafío, la monografía propone un Modelo de Gobernanza Híbrida que articula tres pilares inseparables: XAI para que las decisiones algorítmicas sean auditables y justificables; Blockchain como garante de la integridad y procedencia de los datos; y supervisión humana activa mediante comités interdisciplinarios, protocolos de auditoría algorítmica y pruebas adversariales periódicas. Este enfoque no pretende frenar la automatización, sino dotarla de un andamiaje institucional que permita a la Alta Dirección cumplir su mandato fiduciario de “comprender los riesgos asumidos” y presentar ante reguladores evidencias sólidas y reproducibles. La sinergia XAI+Blockchain, gobernada por reglas claras, métricas

operativas y responsabilidades definidas, convierte la tecnología en una herramienta jurídicamente defendible y operativamente eficaz.

A nivel regional, la prioridad es avanzar hacia una agilidad regulatoria y una cooperación público-privada que permitan experimentar y validar soluciones sin sacrificar la seguridad jurídica. Las jurisdicciones deben transitar desde marcos estáticos hacia entornos de experimentación supervisada, exigir cláusulas de explicabilidad en las adquisiciones tecnológicas, y promover una Matriz de Madurez RegTech que armonice estándares de explicabilidad, soberanía digital y protección de datos. Si bien algunos países de la región ya muestran avances, el desafío es colectivo: gobernar la innovación, y no resistirla, es la vía para transformar la tecnología en un escudo de integridad financiera que preserve la confianza, la transparencia y la resiliencia del sistema en una era de incertidumbre tecnológica.

Referencias bibliográficas

- Abdullahi, M. B., Jiya, M., & Shehu, I. S. (2025). *Strengthening Digital Sovereignty in the Fight Against Money Laundering and Terrorism Financing*. 193–220. <https://doi.org/10.4018/979-8-3693-9137-2.ch008>
- Arguelles Toache, E. (2026). Sesgos algorítmicos en los sistemas de inteligencia artificial implementados en administración pública: Un análisis de casos sobre modelos de predicción de riesgo. *Revista CTS*, 229–255.
- Aksenova, M. (2024). Legal Support of Artificial Intelligence in Countering Anti-Money Laundering and Terrorism Financing Regimes in the BRICS Plus Countries. *BRICS Law Journal*, 11(3), 92–116. <https://doi.org/10.21684/2412-2343-2024-11-3-92-116>
- Al Qudah, A., & Alwaked, A. (2025). *Artificial Intelligence in the Shadow Economy: Detecting and Enabling Financial Crime*. <https://doi.org/10.20944/preprints202506.2156.v1>
- Anik, Md Monir Hasan, Machine Learning Algorithms for Money Laundering Detection: A Comparative Performance Analysis (2026). Available at SSRN: <http://dx.doi.org/10.2139/ssrn.6575820>
- Asociación de Bancos Múltiples de la República Dominicana. (2025, 24 de abril). *La tecnología es una aliada vital para la prevención de lavado de activos en entidades bancarias*. ABA Sala de Prensa. <https://aba.org.do/sala-de-prensa/2025/04/24/noticias/tecnologia-prevencion-lavado-activos-plaft-entidades-bancarias/>
- Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82–115. <https://doi.org/10.1016/j.inffus.2019.12.012>

- Calvano, M., Curci, A., Desolda, G., et al. (2025). Construyendo inteligencia artificial simbiótica: Revisión de la ley de IA para un marco basado en principios y centrado en el ser humano. *Minds & Machines*, 36(1). <https://doi.org/10.1007/s11023-025-09753-w>
- Dobbe, R. I. J., Gilbert, T., & Mintz, Y. D. (2021). Hard choices in artificial intelligence. *Artificial Intelligence*, 298, 103555. <https://doi.org/10.1016/j.artint.2021.103555>
- El Harras, M., & Salahddine, M. A. (2025). Tracking financial crime through code and law: A review of RegTech applications in anti-money laundering and terrorism financing. *Corporate Law & Governance Review*, 7(3), 73–85. <https://doi.org/10.22495/clgrv7i3p7>
- El Khoury, R. M., Alshater, M. M., & Joshipura, M. (2024). Avances en RegTech: una revisión exhaustiva de su evolución, desafíos e implicaciones para la regulación y el cumplimiento financiero. *Journal of Financial Regulation and Compliance*. <https://doi.org/10.1108/JFRA-05-2024-0286>
- Guere Castellanos, N. (2023). Revolutionizing management with AI and blockchain for smarter anomaly detection and fraud prevention. *Computing Innovations and Applications*, 10–18. <https://doi.org/10.63575/CIA.2023.10102>
- Grupo de Acción Financiera Internacional “GAFI”. (2024). *Estándares internacionales para la lucha contra el lavado de activos y el financiamiento del terrorismo* <https://biblioteca.gafilat.org/wp-content/uploads/2024/07/Recomendaciones-metodologia-actDIC2023.pdf>
- Grupo de Acción Financiera Internacional “GAFI”. (2021). *Oportunidades y desafíos de las nuevas tecnologías para la lucha contra el lavado de activos y el financiamiento del terrorismo*. <https://www.fatf-gafi.org/es/publicaciones/Metodosy-tendencias/Nuevas-tecnologias-aml-cft.html>

- Iguodala, O. D., & Oyiborhoro, A. (2025). AI-Powered Anti-Money Laundering (AML) and fraud detection - enhancing financial security through intelligent fraud detection. *World Journal Of Advanced Research and Reviews*, 26(2), 3702–3714. <https://doi.org/10.30574/wjarr.2025.26.2.0637>
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360.
- Malik, M. Z., Khan, H. U., & Nazir, S. (2025). Exploring blockchain risks and AI solutions in the financial industry: A systematic literature review. *2025 IEEE International Conference on Real-time Computing and Robotics (RCAR)*, 216–221. <https://doi.org/10.1109/RCAR65431.2025.11139589>
- Manfrin, F. S. M. (2025). *Prevenção à lavagem de dinheiro com ferramentas de IA: potencial, limites e compliance regulatório*. IIScientific. <https://doi.org/10.63391/421F89>
- Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys*, 54(6), Artículo 115, 1–35. <https://doi.org/10.1145/3457607>
- Melo, J., & Díaz, A. (2024). *Análisis de las monedas digitales de bancos centrales (MDBC) y sus desafíos en el sistema financiero dominicano* [Tesis de maestría, Pontificia Universidad Católica Madre y Maestra]. Repositorio Institucional PUCMM. <https://repositorio.pucmm.edu.do/>
- Sun, Y., Yin, Z., & Zhang, Z. (2025). Research on enterprise financial risk prevention and control system combining artificial intelligence and blockchain technology. *Advances in Economics, Management and Political Sciences*, 210(1), 112–117. <https://doi.org/10.54254/2754-1169/2025.BL26429>
- World Compliance Association. (2024). *El impacto de la inteligencia artificial en el cumplimiento de las normas regulatorias – Cristina Vargas*.

<https://www.worldcomplianceassociation.com/3286/articulo-el-impacto-de-la-inteligencia-artificial-en-el-cumplimiento-de-las-normas-regulatorias.html>

Normativa y documentos oficiales

Junta Monetaria de la República Dominicana. (2007). *Reglamento de Gobierno Corporativo*.

República Dominicana. (2017). Ley No. 155-17 sobre prevención del lavado de activos y financiamiento del terrorismo. Gaceta Oficial.
<https://www.gacetaoficial.gob.do>

República Dominicana. (2013). Ley No. 172-13 sobre protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes (G. O. No. 10737, 15 de diciembre de 2013). Gaceta Oficial.
<https://www.gacetaoficial.gob.do>