República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

NUEVAS TECNOLOGÍAS Y DELINCUENCIA ORGANIZADA: RETOS Y TRANSFORMACIONES DEL SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS DE LC/FT/FPADM

Facilitadora: MSc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

Prólogo

El siglo XXI ha transformado de manera irreversible el ecosistema financiero global y, con ello, la naturaleza misma de las amenazas que atentan contra su integridad. La delincuencia organizada transnacional ha demostrado una capacidad de adaptación rizomática, adoptando tecnologías de vanguardia para perfeccionar sus esquemas de ocultamiento y movilidad de capitales.

Frente a esta realidad, el cumplimiento normativo ya no puede sostenerse sobre modelos estáticos ni reaccionar con la lentitud de los métodos analógicos; exige una anticipación predictiva y una comprensión profunda de los nuevos entornos digitales. Esta compilación de ensayos nace como una respuesta académica y operativa a dicha exigencia.

Reúne la rigurosa investigación de catorce profesionales, quienes, desde la vanguardia de la enseñanza de tipologías en materia de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM), y el desempeño desde diversos escenarios de prevención y represión de dichos delitos, desentrañan las complejidades de la revolución digital.

A lo largo de estas páginas, el lector encontrará un análisis exhaustivo de cómo la ciberresiliencia y la ciberseguridad deben integrarse imperativamente como pilares estratégicos en el Buen Gobierno Corporativo y en los Sistemas Integrales de Administración de Riesgos (SIAR). Las investigaciones abordan el punto de inflexión que atraviesa el Oficial de Cumplimiento ante la irrupción de la Inteligencia Artificial.

Se plantea un debate crucial sobre la supervivencia y metamorfosis de este profesional frente al nacimiento de agentes de inteligencia artificial autónomos, advirtiendo simultáneamente sobre los peligros procesales y operativos de fundamentar Reportes de Actividades Sospechosas (RAS) en modelos de "caja negra" o IA no explicable que contaminan la inteligencia financiera.

Asimismo, la obra profundiza en las mutaciones de los mecanismos de transferencia de valor, explorando cómo sistemas ancestrales como la Hawala y el Fei Chien se han hibridado con la mensajería encriptada y las *stablecoins* para eludir los controles tradicionales. Se traza la ruta hacia una "Inteligencia Financiera 4.0", donde el Big Data y la analítica prescriptiva permiten desarticular estructuras criminales antes de que el riesgo se materialice.

El contexto venezolano no escapa a este análisis. La compilación examina los desafíos específicos de la digitalización del mercado bursátil nacional, destacando las vulnerabilidades frente a identidades sintéticas y *deepfakes* en procesos de *onboarding digital*. Además, se detalla el impacto de la tokenización de activos como innovación financiera y se desnudan las tácticas de la delincuencia organizada mediante el uso de criptoactivos, puentes cross-chain y monedas de privacidad como Monero.

Este documento no es solo una revisión teórica; es un instrumento de trabajo y reflexión crítica. Constituye un llamado a desaprender paradigmas obsoletos y a forjar una nueva generación de hermeneutas organizacionales capaces de gobernar la tecnología.

Los ensayos aquí presentados demuestran que, si bien las herramientas de la delincuencia han evolucionado, la capacidad de análisis, la ética y el rigor de quienes defienden la integridad del sistema financiero siguen siendo nuestra principal ventaja competitiva.

ÌNDICE

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

CIBERRESILIENCIA EN EL BUEN GOBIERNO CORPORATIVO: INTEGRACIÓN DE LA CIBERSEGURIDAD COMO PILAR ESTRATÉGICO DEL SIAR DE LC/FT/FPADM

Autor: Abg. Yabandra N. Lorca Cabeza
Facilitadora: Msc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

Ciberresiliencia en el Buen Gobierno Corporativo: Integración de la ciberseguridad como pilar estratégico del SIAR de LC/FT/FPADM

Autor: Abg. Yabandra N. Lorca Cabeza
Código ORCID: 0009-0003-5803-3825
Correo electrónico: yabandralorca@gmail.com

Resumen

La transformación digital ha revolucionado la vida cotidiana y las operaciones de las organizaciones, convirtiéndose en una fuente clave de riqueza y ventaja competitiva. Esta riqueza se genera a través de la transferencia digital de activos informativos, lo que ha cambiado la naturaleza de los conflictos; hoy en día, un ciberataque a los sistemas informáticos puede desestabilizar gobiernos y organizaciones. En este contexto, la ciberresiliencia se vuelve vital. A medida que los ciberataques aumentan en frecuencia y sofisticación, es crucial que las organizaciones implementen políticas de ciberseguridad para proteger sus operaciones y los datos de sus clientes. Este ensayo pretende analizar cómo la ciberresiliencia debe integrarse en el Buen Gobierno Corporativo para mitigar riesgos y asegurar la sostenibilidad frente a ciberamenazas, toda vez que las tecnologías de la información (TIC) han transformado la delincuencia organizada, permitiendo a los grupos delictivos operar en un entorno digital, colaborando con expertos en cibercriminalidad para realizar actividades ilícitas sin necesidad de encuentros físicos. En este contexto, es esencial que las juntas directivas, como máximas instancias de administración en el entorno empresarial, incorporen la ciberseguridad en su Sistema Integral de Administración de Riesgos (SIAR), garantizando una cultura de protección de datos. Las estrategias de mitigación y respuesta, junto con auditorías internas, deben fortalecer la resiliencia institucional, convirtiendo la gestión de riesgos en una ventaja competitiva y promoviendo un entorno de confianza en el mercado.

Descriptores clave: (Ciberresiliencia, Ciberseguridad, Gobierno Corporativo, SIAR, TIC).

Abstract

Digital transformation has revolutionized daily life and organizational operations, becoming a key source of wealth and competitive advantage. This wealth is generated through the digital transfer of information assets, which has changed the nature of conflicts; today, a cyberattack on computer systems can destabilize governments and organizations. In this context, cyber resilience becomes vital. As cyberattacks increase in frequency and sophistication, it is crucial that organizations implement cybersecurity policies to protect their operations and customer data. This essay aims to analyze how cyber resilience should be integrated into good corporate governance to mitigate risks and ensure sustainability in the face of cyber threats, given that information and communication technologies (ICTs) have transformed organized crime, allowing criminal groups to operate in a digital environment, collaborating with cybercrime experts to carry out illicit activities without the need for physical encounters. In this context, it is essential that boards of directors, as the highest governing bodies in the business environment, incorporate cybersecurity into their Integrated Risk Management System (IRMS), ensuring a culture of data protection. Mitigation and response strategies, along with internal audits, should strengthen institutional resilience, transforming risk management into a competitive advantage and fostering a trusting environment in the market.
Keywords: (Cyber resilience, Cybersecurity, Corporate Governance, SIAR, ICT).

Introducción

La transformación digital impacta significativamente la vida cotidiana y el funcionamiento de las organizaciones, por lo que, en la actualidad se ha convertido en la principal fuente de riqueza para las empresas y en un factor clave de la ventaja competitiva entre los países. Obtener esta riqueza ya no depende de conflictos armados, sino de una “sencilla” transferencia digital de los activos informativos.

Con solo una “ciberbatalla” dirigida a los sistemas informáticos esenciales, es posible acceder a la información necesaria para derrocar un gobierno, atacar a una organización y quitarles su ventaja competitiva.

En este contexto ser resiliente es una necesidad fundamental para las organizaciones, entendiendo la resiliencia como “la habilidad innata de un organismo, entidad, empresa o estado para enfrentar una crisis sin que sus

operaciones se vean comprometidas", ya que no se trata únicamente de recuperarse, sino de renacer y fortalecerse después de atravesar una circunstancia adversa.

El presente ensayo pretende analizar el papel determinante de la "ciberresiliencia", vista no como proceso técnico aislado, sino un componente vital del Buen Gobierno Corporativo (BGC) para mitigar el riesgo reputacional y asegurar la sostenibilidad del negocio frente a amenazas disruptivas, haciéndose necesaria, la participación del Gobierno Corporativo, como garante de la integridad institucional, integrando la ciberseguridad dentro del Sistema Integral de Administración de Riesgos (SIAR) de LC/FT/FPADM.

I. Nuevas Tecnologías y sus retos frente a la Delincuencia Organizada.

Las tecnologías de la información y las comunicaciones (TIC) han cambiado profundamente cómo entendemos la delincuencia organizada. No solo han alterado el tipo de delitos que se cometen y las maneras en que los grupos criminales actúan, sino que también han ampliado el perfil de las personas que pueden estar involucradas.

Los grupos delictivos tradicionales han comenzado a trasladar parte de sus actividades al mundo digital, aunque no han hecho una transición completa hacia la ciberdelincuencia. Lo que sí ocurre es que ahora realizan algunas operaciones ilícitas en línea y buscan cada vez más colaborar con expertos en delitos cibernéticos, como programadores que crean software malicioso o hackers que aprovechan vulnerabilidades en sistemas para cometer fraudes o ataques.

Las TIC han transformado la forma en que estos grupos delictivos se organizan, por lo que ya no es necesario que sus miembros se reúnan cara a cara; pudiendo trabajar de manera conjunta y coordinada desde cualquier lugar del mundo, sin haberse visto nunca, utilizando seudónimos para proteger su verdadera identidad y ubicación, lo que les permite reducir el riesgo de ser descubiertos dentro del grupo mientras llevan a cabo sus actividades ilegales.

Los nuevos desafíos derivados de la materialización de amenazas en el ciberespacio, han originado un incremento notable de los ciberataques, tanto en volumen como en frecuencia y sofisticación. Es por ello, que hacer frente a los nuevos retos de ciberseguridad requiere de políticas de revisión y mejora continuada, así como de la optimización de los controles y medidas de ciberseguridad, aplicadas tanto a la protección del valor y funcionamiento de las organizaciones, como a la protección de los datos de los ciudadanos en poder de aquellas.

Según UNODC (2022): La ciberdelincuencia es un concepto complejo que engloba una variedad de actividades ilícitas que tienen como blanco las TIC o que las utilizan para cometer los delitos. Los ilícitos considerados ciberdelitos son aquellos facilitados por la cibernética o basados en ella.

En el caso de los delitos facilitados por la cibernética, las TIC desempeñan un papel fundamental en el método de operación (el modus operandi) del delincuente o los delincuentes. Por el contrario, en los delitos basados en la cibernética, que incluyen aquellos que solo se pueden cometer utilizando computadoras, redes informáticas u otras formas de tecnología de comunicación de la información, el blanco de ese tipo de delitos son las TIC.

Así pues, los grupos de ciberdelincuencia organizada son grupos delictivos organizados que cometen delitos cibernéticos en el entendido, que en estos casos tanto la estructura, organización y los tipos de grupos de ciberdelincuencia organizada varían, al igual que las funciones desempeñadas dentro de ellos. También varían la ubicación geográfica o la concentración o distribución de los miembros de los grupos, y también de las víctimas de ese tipo de delitos.

En conjunción con lo antes señalado resulta importante significar, que existen dos tipos de ciberdelincuencia organizada: la delincuencia organizada basada en la cibernética y la delincuencia organizada facilitada por la cibernética.

En el primer supuesto, los delitos basados en la cibernética, tienen como objetivo las TIC y no sería posible cometerlos sin el uso de esta tecnología.

Estos delitos apuntan a la confidencialidad (el acceso está restringido a los usuarios autorizados), la integridad (los datos son correctos, fidedignos y válidos) y la disponibilidad (los sistemas y los datos son accesibles a quienes los soliciten) de los sistemas y los datos informáticos.

Los actos ilícitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informáticos incluyen el acceso ilegal a un sistema informático o a datos informáticos; la interceptación ilegal de datos informáticos o adquisición ilegal de datos informáticos; interferencias ilegales en los datos y en los sistemas; y la producción, distribución, utilización y posesión ilegales de herramientas para el uso indebido de computadoras.

Por su parte, en el caso de los delitos facilitados por la cibernética, son aquellos en que las TIC desempeñan un papel fundamental en los métodos utilizados para cometerlos y facilitarlos.

En los tipos de delitos facilitados por la cibernética se incluyen, entre otros: el fraude o la falsificación relacionados con la informática (el fraude bancario, la suplantación de identidad o phishing); los delitos informáticos relacionados con la identidad; los delitos relacionados con la falsificación de productos médicos; los delitos de abusos y explotación sexual de niños; la trata de personas; el tráfico de migrantes; el tráfico de drogas; el tráfico de armas de fuego; el tráfico de especies de fauna y flora silvestres; el tráfico de bienes culturales; el blanqueo de dinero, y los juegos de azar por Internet.

Así pues, la Evaluación Global de la Amenaza del Fraude Financiero de INTERPOL de 2026 advierte que, con el aumento de la colaboración criminal a nivel mundial, el fraude ya no es una amenaza periférica, sino que se encuentra en el centro de la policriminalidad, entrecruzándose con el crimen organizado, la trata de personas y el cibercrimen.

Entre los principales hallazgos de esta evaluación se incluyen, entre otros: el fraude potenciado por IA es 4,5 veces más rentable que los métodos tradicionales. Los sistemas de "IA génica" pueden planificar y ejecutar de

forma autónoma campañas de fraude completas, desde el reconocimiento hasta las demandas de rescate.

En este sentido, como bien lo señala Granadillo (2025): “Los ciberdelitos representan una amenaza real y creciente en el mundo. Los grupos de delincuencia organizada utilizan cada vez más tecnologías para obtener grandes ganancias producto de actividades ilegales y, además emplean estructuras complejas con las cuales materializan rápidamente grandes movimientos de lavado de dinero o legitimación de capitales.”

Para la referida autora las medidas preventivas de gestión de riesgos, asociadas a Ciberseguridad, pueden reducir significativamente los impactos negativos del ciber crimen, que van desde daños económicos hasta reputacionales.

II. Ciberseguridad, ciberresiliencia y gobernanza.

Desde nuestros inicios como oficiales de cumplimiento, preventólogos o gestores de riesgos de legitimación de capitales, financiamiento al terrorismo, financiamiento de la proliferación de armas de destrucción masiva, nuestra labor estaba centrada en el análisis de normas, la revisión de manuales, documentos y la gestión de expedientes físicos o digitales básicas. En los actuales momentos la irrupción de la Inteligencia Artificial (IA), está redefiniendo la toma de decisiones, la gestión de riesgos y los procesos de supervisión institucional.

Este punto de inflexión histórico, implica que el profesional moderno ya no solo trabaja con leyes, sino que debe aprender a gestionar ecosistemas completos de información. Los riesgos actuales para una organización no provienen únicamente de transgredir la normativa; ahora surgen de decisiones automatizadas deficientes, errores en algoritmos, sesgos en modelos de datos, exposición reputacional en redes y vulnerabilidades de ciberseguridad.

Por tanto, la labor de cumplimiento ahora requiere una comprensión integral donde convergen el derecho, la tecnología, la reputación y la estrategia corporativa. En este mismo orden, según Panda Security Summit (2018): “Asistimos a una transformación de las relaciones sociales, del tejido empresarial y de las gestiones de los gobiernos. Una transformación que basa su potencial en la tecnología, en los datos y en la inteligencia artificial que recoge, filtra, clasifica y correlaciona datos a gran escala para aprender de ellos y ser capaz de predecir.”

Desde otra perspectiva, al referirse a la inteligencia artificial (IA), en su Carta Encíclica Magnifica Humanitas (2026), el Santo Padre, LEÓN XIV, toca un aspecto importante que tiene que ver con la “Responsabilidad, transparencia y gobernanza de la IA”.

En este sentido, la carta señala: “El uso de la IA nunca es un hecho puramente técnico: cuando entra en procesos que inciden en la vida de las personas, afecta a sus derechos, oportunidades, reputación y libertad. Las decisiones delicadas que repercuten en el trabajo, el acceso a créditos y a otros servicios, y la reputación de las personas, corren el riesgo de ser confiadas completamente a sistemas automatizados que no conocen «la compasión, la misericordia, el perdón y, sobre todo, la apertura a la esperanza de cambio en el individuo», pudiendo así producir nuevas formas de descarte.

Puede haber usos evidentemente antihumanos, como la manipulación de la información o la violación de la privacidad, pero puede haber también un engaño menos evidente, cuando los sistemas de IA, presentándose como neutrales y objetivos, reflejan y refuerzan estereotipos o posiciones ideológicas de quienes los han diseñado y programado.

Resalta en Santo Padre en su encíclica que: “Para que la IA respete la dignidad humana y sirva realmente al bien común, es esencial que las responsabilidades estén claras en todas las etapas: desde quienes diseñan y programan los sistemas hasta quienes los utilizan y quienes resuelven confiarles las decisiones concretas. En muchos casos, sin embargo, los

procesos internos que conducen a un resultado pueden ser poco transparentes, y eso hace más difícil atribuir responsabilidades y corregir los errores.

Es aquí donde se vuelve decisivo lo que llamamos “responsabilidad” (accountability): la posibilidad de identificar quién debe “rendir cuentas” de las decisiones, motivarlas, controlarlas y, cuando es necesario, cuestionarlas y remediar los daños que derivan de ellas.”

Partiendo de lo anterior, considera quien escribe, que tal como lo señala Granadillo, supra mencionada: “Desde la perspectiva internacional, la naturaleza transfronteriza de la inteligencia artificial requiere mecanismos de cooperación internacional para combatir su uso criminal. Para ello, los Estados y las Organizaciones Internacionales deben intercambiar información e inteligencia, compartir mejores prácticas y coordinar esfuerzos para detectar y prevenir delitos relacionados con el uso de la inteligencia artificial.”

Por lo que, desde estas perspectivas, necesariamente al hablar de IA también debemos referirnos a la gobernanza de IA, que no es más que el marco normativo y las herramientas técnicas que utilizan las entidades (financieras, de seguros etc.) para mitigar el sesgo, cumplir con las regulaciones y auditar los sistemas automáticos, previniendo así penalizaciones operacionales. La ausencia de este control expone a las organizaciones a penalizaciones económicas (sanción), daño reputacional, vulnerabilidades de ciberseguridad (filtración de información confidencial, ineficiencia y altos costos.

En este sentido, según Chinchilla (2026): “La Inteligencia Artificial no representa únicamente una innovación tecnológica. Representa una transformación profunda en la forma en que las Organizaciones gestionan información, riesgos y decisiones.

Para el referido autor: “Quienes comprendan esta evolución podrán utilizar la IA para fortalecer su gobernanza, mejorar su cumplimiento y aumentar su capacidad de anticipación. Quienes no lo hagan, podrían enfrentar riesgos que todavía no logran visualizar. Porque en la nueva economía del conocimiento,

la ventaja competitiva ya no depende únicamente de tener información. Depende de saber interpretarla inteligentemente, y precisamente allí es donde convergen el derecho, el compliance, la tecnología y la estrategia."

III. Integración de la ciberseguridad como pilar del SIAR de LC/FT/FPADM y del Gobierno Corporativo.

Hasta hace poco, las empresas financieras y los gobiernos eran los principales objetivos de los ciberataques, hoy en día, el desarrollo de los negocios de las empresas de cualquier tamaño y sector depende en mayor o menor medida de Internet y, por lo que ahora la amenaza se ha convertido en universal. Partiendo de esta visión, en el ámbito de la seguridad, la ciberresiliencia está referida a la capacidad o destreza de una organización para mantener su misión principal y su integridad ante la constante amenaza de ataques cibernéticos.

Una empresa que es ciberresiliente es capaz de prevenir, identificar, contener y recuperarse de estos incidentes, reduciendo al mínimo tanto el tiempo de vulnerabilidad como el impacto que pueden tener en el negocio diversas amenazas significativas dirigidas a datos, aplicaciones e infraestructura tecnológica.

Esto es especialmente importante en los equipos, donde se almacenan los activos más valiosos para la organización, dado que comprometerlos implica también poner en riesgo la integridad de las identidades y usuarios.

En este sentido, las distintas normativas en materia de prevención o administración de riesgos de legitimación de capitales, financiamiento al terrorismo, financiamiento de la proliferación de armas de destrucción masiva, en el país, contemplan la obligación ineludible de la junta directiva o el órgano que haga sus veces, de proporcionar la infraestructura organizativa y presupuestaria para que el Sistema Integral de Administración de Riesgos

(SIAR), sea eficiente y capaz de mitigar los riesgos de que la organización sea objeto de amenazas delictivas, entre ellas ataques cibernéticos.

Por lo que, existiría a criterio de quien escribe, una responsabilidad vinculante, que implica el "deber de cuidado y diligencia" de los directores o administradores, de asumir la responsabilidad última por las fallas en el control interno.

Tal es el caso, verbi gracia, de la regulación contenida en la Providencia Administrativa N° SAA-01-0530-2024, publicada el 3 de septiembre de 2024 en la Gaceta Oficial de Venezuela, que contempla las normas sobre Buen Gobierno Corporativo para las empresas del sector asegurador, conforme a la cual, la junta directiva o administradora tiene la responsabilidad de fomentar la creación y aplicación de políticas, normas y procedimientos enfocados en la ciberseguridad y la ciberresiliencia.

El objetivo de la norma está enfocado en proteger la información tanto de la empresa como la de sus clientes, asegurados, beneficiarios y demás usuarios vinculados. De esta manera, se busca garantizar la integridad y seguridad de los datos frente a posibles amenazas digitales.

Así pues, conforme al artículo 11 ejusdem, la junta directiva como máxima instancia de administración de una empresa debe contribuir con la sostenibilidad de la organización a través de buenas prácticas que permitan fomentar una cultura corporativa donde la protección de la data sea una prioridad ética, anteponiendo la seguridad institucional al lucro comercial inmediato.

Aunado a los anterior, desde el gobierno corporativo, existe la obligación ineludible de proporcionar la infraestructura organizativa, funcional y presupuestaria idónea para que el SIAR sea eficiente.

Esto incluye, por un lado la asignación de recursos financieros específicos para adquirir soluciones informáticas y herramientas de ciberseguridad, tal es el caso, por ejemplo de la obligación contenida en el artículo 80 de providencia administrativa 536, en materia de administración de riesgos de legitimación de

capitales, financiamiento al terrorismo, financiamiento de la proliferación de ramas de destrucción masiva y otros ilícitos en el sector seguros, que prevé la obligación para los sujetos obligados de ese sector de implementar herramientas tecnológicas.

En este mismo orden se establece el deber de supervisar que la gestión de riesgos se adapte a la economía digital para mitigar el riesgo reputacional derivado de posibles brechas de seguridad.

Siguiendo este orden, para Granadillo, supra mencionada: "Desde la perspectiva empresarial o corporativa, incrementar o reforzar las medidas de ciberseguridad es fundamental para protegerse contra los ciberataques, el acceso no autorizado de datos o información sensible. Esto implica invertir en tecnologías de ciberseguridad avanzadas, realizar auditorías de seguridad con regularidad y educar a las personas y organizaciones sobre las mejores prácticas de ciberseguridad."

Ahora bien, bajo la visión de quien escribe, estas políticas, procedimientos, mejores prácticas supra mencionados, deben incluirse o ser incorporados en el Sistema Integral de Administración de Riesgo de Legitimación de Capitales, Financiamiento al Terrorismo, Financiamiento de la Proliferación de Armas de Destrucción Masiva, (SIAR LC/FT/FPADM), el cual constituye un escudo de protección, institucional, que debe diseñar, implementar y mantener activo el sujeto obligado a los efectos de la mitigación de los riesgos.

En este sentido, para Negrón y Chang (2021): "El Sistema Integral de Administración de Riesgos (SIAR) es el conjunto de programas, políticas, manuales, normas, procedimientos, estructuras, planes, estrategias y controles, tanto internos como externos, adoptados por los sujetos obligados. Su propósito fundamental es reducir la posibilidad de que los productos, servicios, canales de distribución o clientes de una institución sean utilizados para ocultar el origen de capitales ilícitos o para desviar fondos hacia el terrorismo y la proliferación de armas de destrucción masiva."

A criterio de los referidos autores, el SIAR constituye el eje central de la "malla de protección institucional" y debe estar estrictamente alineado con las mejores prácticas de un buen Gobierno Corporativo Antilavado. Así pues, las "herramientas tecnológicas" constituyen uno de los seis pilares antilavado esenciales que sostienen la malla de protección institucional. Un programa de cumplimiento exitoso requiere obligatoriamente de una herramienta tecnológica de primera línea que sea capaz de interactuar con la base de datos de los clientes en tiempo real para detectar operaciones inusuales.

Ahora bien, cuando se hace referencia a la ciberseguridad, en el contexto de la organización necesariamente debe verse como un componente transversal de la administración de riesgos, lo que nos llevaría a darle un tratamiento similar a las políticas de "conozca a su cliente" (KYC) y "conozca su riesgo" (KYR), etc.

Así pues, partiendo de la posición de los mencionados autores, consideramos, que el cumplimiento contemporáneo ha dejado de ser una simple verificación de requisitos para convertirse en una disciplina dinámica y multidimensional. La inteligencia artificial (IA) potencia este nuevo enfoque al permitir un monitoreo de riesgos mucho más ágil que los sistemas tradicionales, detectando señales tempranas de comportamientos atípicos.

La IA contribuye en facilitar la gestión documental y el fortalecimiento de los procesos de conocimiento del cliente (KYC), del empleado (KYE), de proveedores (KYS) y de cualquier contraparte, mediante el análisis de datos públicos y corporativos.

No obstante, como administradores de riesgos, debemos reconocer que la IA introduce sus propios desafíos. Entre los más críticos se encuentran los sesgos algorítmicos, que pueden replicar errores presentes en los datos; la falta de transparencia de los sistemas denominados "cajas negras", que dificultan entender cómo se llega a una conclusión; y los riesgos operativos y de protección de datos. Estos elementos pueden impactar severamente la reputación de la organización ante reguladores e inversionistas

Debido a estas implicaciones, la supervisión de la IA no es una tarea exclusiva del departamento de tecnología, sino una responsabilidad directa del Gobierno Corporativo. Las Juntas Directivas deben involucrarse activamente, cuestionando cómo se utiliza la tecnología, qué controles existen para evitar sesgos y quién asume la responsabilidad por las decisiones apoyadas en modelos automatizados.

En esa línea se pronunció Germán Sánchez, (2026) de Inforges, en la edición N° 38 de la revista IT Digital Magazine, quien recordó que la ciberseguridad ya no puede tratarse como una partida aislada. “La ciberseguridad ya no es una cuestión técnica, es una cuestión de negocio”, indicó. Cuando una fábrica se detiene, cuando un ERP queda bloqueado o cuando una operación logística se interrumpe, el problema deja de pertenecer al área tecnológica y pasa a la cuenta de resultados”.

En igual sentido, Negrón y Chang, supra citados, consideran que la ciberseguridad no es un área aislada, sino que está directamente vinculada a la prevención de la legitimación de capitales por dos razones: la primera razón relacionada con el origen del dinero, toda vez que los delitos informáticos (como el phishing, el fraude electrónico y el sabotaje de sistemas) generan recursos ilícitos que los delincuentes deben "blanquear" posteriormente a través del sistema financiero.

La segunda razón tiene que ver con el hecho de que, el uso de nuevas tecnologías permite a los criminales operar con mayor rapidez y anonimato, lo que exige que el SIAR incluya controles específicos sobre la banca virtual y canales electrónicos, bien sean estos utilizados como pasarelas de pago o medios para la vinculación de contrapartes, especialmente si se trata de clientes, constituyéndose así en canales para el lavado o la legitimación de capitales.

Los autores enfatizan que, según la recomendación 15 del GAFI, las instituciones financieras deben realizar una evaluación de riesgos de LC/FT/FPADM antes del lanzamiento de cualquier nuevo producto o práctica

comercial que utilice nuevas tecnologías. Esto implica que la ciberseguridad debe ser parte del análisis estratégico del Plan Operativo Anual (POA) de los sujetos obligados, incluyendo el perfeccionamiento de sistemas informáticos de detección.

Ciberresiliencia y continuidad del negocio.

El término "ciberresiliencia" abordado conceptualmente bajo la Administración Integral de Riesgos, implica la capacidad de una organización para resistir y recuperarse de eventos negativos (incluyendo ciberataques), siendo vital para mantener la disciplina de mercado y la confianza de los accionistas y reguladores.

Así pues, un SIAR que ignore las amenazas digitales constituye una vulnerabilidad crítica en la evaluación de riesgos de las organizaciones, toda vez que a gestión de riesgos ha dejado de ser un proceso reactivo para convertirse en el núcleo de la estabilidad institucional, ya que no basta con prevenir ataques; sino que la capacidad de resistir y recuperarse de éstos es lo que garantiza la disciplina de mercado y la confianza de accionistas, reguladores y grupos de interés.

En este orden a manera de reflexión final, consideramos que un Sistema de Administración Integral de Riesgos (SIAR) que ignore las amenazas digitales no solo es incompleto, sino que representa una vulnerabilidad crítica en la evaluación de la continuidad del negocio. Ya que la verdadera sinergia entre la gobernanza y la seguridad, viene dada por la supervivencia en la era tecnológica, la cual exige una interdependencia necesaria entre el gobierno corporativo, la prevención de ilícitos financieros y la seguridad digital.

Siendo esta tríada la que garantiza que la organización no solo cumpla con la normativa en preventiva o de gestión de riesgos antilavado (LC), sino que sea capaz de blindar sus canales ante la intrusión de capitales ilícitos que viajan a través de vulnerabilidades informáticas. Es por ello que la ciberseguridad debe verse como parte de ese escudo estratégico, que es el SIAR, el cual ante la

"aceleración tecnológica" que la delincuencia organizada utiliza para infiltrar estructuras financieras, se erige como una estrategia defensiva vital y no como un gasto.

Finalmente, consideramos que convertir la gestión de riesgos en una ventaja competitiva implica proyectar una imagen de solidez y resiliencia al mercado. De este modo, la ciberresiliencia se erige como el pilar fundamental del cumplimiento, orientada a garantizar una infraestructura operativa para la prevención de LC/FT/FPADM tan robusta como su propio marco regulatorio y metodológico, toda vez que la verdadera ventaja competitiva reside en la combinación de la potencia tecnológica con la experiencia humana, transitando de una gestión de riesgos reactiva a un modelo inteligente. Ya que como bien lo sostiene Chinchilla, supra citado: “El futuro no pertenece a quienes simplemente adopten Inteligencia Artificial. Pertenece a quienes aprendan a gobernarla.”

Siglas y acrónimos utilizados:

IA (Inteligencia Artificia).

BGC (Buen Gobierno Corporativo).

ERP (Enterprise Resource Planning, que en español se traduce como Planificación de Recursos Empresariales).

GAFI (Grupo de Acción Financiera Internacional).

KYC (Conozca a su Cliente)

KYE (Conozca a su Empleado)

KYR (Conozca a su Riesgo)

KYS (Conozca a s Proveedor)

LC/FT/FPADM (Legitimación de capitales, financiamiento al terrorismo, financiamiento de la proliferación de armas de destrucción masiva).

SIAR (Sistema Integral de Administración de Riesgos).

TIC (Tecnologías de la Información y la Comunicación).

UNODC (United Nations Office on Drugs and Crime) Oficina de las Naciones Unidas contra la Droga y el Delito.

Referencias

Chinchilla Sánchez, William. (2026, junio 9). Cómo la Inteligencia Artificial está transformando el trabajo legal y de compliance. [Artículo]. LinkedIn https://www.linkedin.com/pulse/c%C3%B3mo-la-inteligencia-artificial-est%C3%A1-transformando-el-william-abbqe/

E.Negron/K.Chang (2021). Manual Antilavado y Gobierno Corporativo Centro de Estudios Financieros Avanzados (CEF) Caracas. Venezuela.

Granadillo Colmenares, Nancy Carolina. (2025). Compliance y Prevención de la Criminalidad Empresarial.3ra Edición. Caracas.

IT. Digital Magazine N° 38 (2026).

Interpol. (2026). GLOBAL FINANCIAL FRAUD THREAT ASSESSMENT SECOND EDITION, en https://www.interpol.int/content/download/24291/file/INTERPOL%20Global%20Financial%20Fraud%20Threat%20Assessment%202026.pdf .

Oficina de las Naciones Unidas contra la Droga y el Delito. (2022) Compendio de Ciberdelincuencia Organizada. Viena.

Panda Security Summit (2018). Ciber resiliencia: la clave de la seguridad. https://www.pandasecurity.com/es/mediacenter/src/uploads/2018/05/Informe-Ciber-resiliencia-ES.pdf

Santo Padre, León XIV (2026). Magnifica Humanitas. Dicasterio para la Comunicación - Libreria Editrice Vaticana- en https://share.google/3RtDE1n8AG6RJK1fm.

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

EL OFICIAL DE CUMPLIMIENTO ANTE LA INTELIGENCIA ARTIFICIAL E INCERTIDUMBRE TECNOLÓGICA EN LAS ORGANIZACIONES

Autor: Dr. Oscar Perdomo
Facilitadora: Msc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

El Oficial de Cumplimiento ante la Inteligencia Artificial e Incertidumbre Tecnológica en las organizaciones

Autor: Dr. Oscar Perdomo
Código ORCID: 0009-0003-9026-9184
Correo electrónico: oscarperdomovielma@gmail.com

Resumen

Este estudio analiza el punto de inflexión del rol que ejerce el Oficial de Cumplimiento frente a la Inteligencia Artificial (IA) y la incertidumbre tecnológica en las organizaciones, bajo el paradigma de la transcomplejidad. El problema central radica en la brecha entre la velocidad analítica "cableada" de los algoritmos y la multidimensionalidad humana, indispensable para la intuición y la ética. El anclaje Epistemológico, se fundamenta en la racionalidad limitada de Herbert Simon, justificando el uso de la IA para superar los límites cognitivos humanos al procesar datos masivos. Simultáneamente, se integra la teoría de Frank Knight para reconfigurar el beneficio empresarial como un "beneficio preventivo" contra la legitimación de capitales. En materia de gobernanza, se proponen los conceptos de Hermenéutica Algorítmica y Transpedagogía Tecnocientífica, los cuales fomentan una metacognición aumentada y un proceso dinámico de aprender y desaprender. Sosteniendo que la eficacia del sistema no reside en una automatización opaca, sino en una justicia algorítmica alineada con la ética de la información. Se concluye que la IA no desplaza al factor humano, sino que redefine al Oficial de Cumplimiento como un hermeneuta organizacional encargado de dotar de sentido ético y contextual a los patrones tecnológicos, garantizando la autonomía intelectual humana.

Palabras claves: Inteligencia Artificial, Oficial de Cumplimiento, Transcomplejidad, Incertidumbre Tecnológica, Legitimación de Capitales.

Abstract

This study analyzes the turning point in the role of the Compliance Officer in the face of Artificial Intelligence (AI) and technological uncertainty in organizations, under the paradigm of transcomplexity. The central problem lies in the gap between the "hardwired" analytical speed of algorithms and human multidimensionality, essential for intuition and ethics. The epistemological framework is based on Herbert Simon's bounded rationality, justifying the use of AI to overcome human cognitive limitations in processing massive amounts of data. Simultaneously, Frank Knight's theory is integrated to reconfigure corporate profit as a "preventive benefit" against money laundering. In terms of governance, the concepts of Algorithmic Hermeneutics and Technoscientific Transpedagogy are proposed, which foster enhanced metacognition and a dynamic process of learning and unlearning. It argues that the system's effectiveness does not reside in opaque automation, but rather in algorithmic justice aligned with information ethics. It is concluded that AI does not displace the human factor, but rather redefines the Compliance Officer as an organizational interpreter responsible for providing ethical and contextual meaning to technological patterns, thus guaranteeing human intellectual autonomy.

Keywords: Artificial Intelligence, Compliance Officer, Transcomplexity, Technological Uncertainty, Money Laundering.

Introducción

En la actualidad resulta evidente que los modelos tradicionales de cumplimiento, basados en normas lineales y estáticas, son insuficientes ante la capacidad de creatividad de la delincuencia organizada, la cual opera de forma rizomática y digital. Por lo tanto, resulta pertinente desarrollar un contenido que considere el paradigma de la transcomplejidad para abordar el planteamiento. Así mismo, se considera en el contenido la Paradoja de la Prótesis Cognitiva, la cual plantea explícitamente la tensión entre la IA, que surge como una necesidad para superar la racionalidad limitada del ser humano, pero a su vez genera una incertidumbre tecnológica que el ser humano aún no sabe gestionar plenamente. Bajo este escenario, el propósito epistémico decanta en proponer una redefinición ontológica del Oficial de Cumplimiento, de ser un vigilante de procesos a un "hermeneuta organizacional".

El abordaje de la Inteligencia Artificial (IA) e Incertidumbre Tecnológica, transita por la irrupción de la IA y se analiza, no solo como una herramienta técnica, sino como un desafío para la autonomía intelectual y la ética. En este escenario, se hace evidente una brecha fundamental, donde la IA posee velocidad "cableada" pero carece de la multidimensionalidad humana que da origen a la intuición y propicia la justicia algorítmica. Ante este límite, emergen dos conceptos clave para el debate contemporáneo: La *Hermenéutica Algorítmica*, resultante de la combinación de la reflexión humana profunda con la capacidad analítica de los algoritmos; y la *Transpedagogía Tecnocientífica* entendida como un modelo de aprendizaje rizomático que une el conocimiento tradicional con las "galaxias digitales", promoviendo una metacognición aumentada.

Esta praxis, vista desde la denominada justicia algorítmica, y la adaptación de la ética de la información, plantea cómo la IA debe alinearse con la gobernanza institucional humana, y sostiene que en la "infosfera" actual, debe centrarse en la protección de la autonomía humana frente a los sistemas digitales, fortaleciendo la tesis sobre el desafío a la autonomía intelectual planteado por la IA.

Todo lo anterior ocurre de manera dinámica dentro y fuera de las organizaciones. Para otorgar forma a la dimensión interna, se adopta el enfoque del *Comportamiento Administrativo* (Simón, 1972), el cual centra sus hipótesis de trabajo y supuestos en el desempeño individual del trabajador, lo cual permite estudiar las prácticas en la gerencia estratégica del riesgo contra la legitimación de capitales desde este ángulo en las organizaciones. El gerenciamiento es sinónimo de toma de decisiones en la realidad organizacional y cómo pueden estas llegar a ser más efectivas.

De igual forma se considera al enfoque antes referido, como la mirada más pertinente para examinar las prácticas que envuelve la gestión de riesgos en las organizaciones, para poder emitir conclusiones que resulten un aporte para las diligencias conducentes en aumentar la eficacia y eficiencia de la acción

estratégica contra la legitimación de capitales, todo ello realizado bajo el paradigma de la transcomplejidad.

La Dimensión del Comportamiento Administrativo

Para Herbert Simón, uno de los principales representantes del Comportamiento Administrativo, el gerenciamiento es sinónimo de toma de decisiones en la realidad organizacional y cómo pueden estas llegar a ser más efectivas.

Sugiere entonces, con relación a este proceso, la existencia de tres etapas principales:

- Encontrando ocasiones o escenarios en las cuales exista una decisión a tomar.
- Analizando y optando ante posibles cursos de acción.
- Eligiendo un curso particular de acción de todas las opciones posibles, representando una actividad “de opción / elección” u “optativa”.

Esto explica, los argumentos expuestos por algunos analistas cuando hacen hincapié en la personalidad del decisor y justifica desde el punto de vista de la racionalidad limitada[1] y de la contingencia organizacional[2] sostenida por Herbert Simon, la decisión puede ser interpretada como parte de un proceso de ensayo - error o de una relación fortuita entre oportunidades, problemas y soluciones ya establecidas, con las consecuencias hasta ahora conocidas en el avance de este tipo de delito.

En el contexto de las organizaciones, gerenciar ejerciendo el rol como oficial de cumplimiento, se ha convertido en una tarea fundamental dada la situación

[1] La idea de racionalidad limitada está basada en que, a la hora de decidir, es prácticamente imposible tomar la opción perfecta, pues usualmente esta, se verá influenciada por los conocimientos, hábitos, destrezas y pensamientos inconsciente de quién toma la decisión.

[2] Proposición cuya verdad o falsedad solamente puede conocerse por la experiencia o la evidencia y no por la razón. El enfoque situacional o contingente destaca la dificultad de alcanzar la eficacia, siguiendo un modelo organizacional único y exclusivo, por lo cual pondera en alto grado la contextualización de las prácticas gerenciales frente a la homogenización o estandarización de las decisiones.

política y económica global, regional y local. La gerencia se enfrenta a un desafío importante en la prevención y control de la legitimación de capitales. Es por ello que es crucial estudiar los factores clave del éxito que los gerentes necesitan para dirigir en este contexto complejo.

Todo ello implica la toma de decisiones en condiciones de incertidumbre, caos, orden y desorden. Por lo tanto, es fundamental que los gerentes cuenten con las características necesarias para abordar esta problemática de manera efectiva y alcanzar los objetivos establecidos.

En suma, la gerencia en las organizaciones ejecuta una labor que requiere habilidades especiales y un profundo entendimiento del entorno en las que se desenvuelven. Los gerentes deben estar preparados para enfrentar los desafíos que presenta combatir la legitimación de capitales y tomar decisiones acertadas en situaciones difíciles.

La gerencia entonces desempeña un papel fundamental en un entorno organizacional complejo. Es la encargada de garantizar el cumplimiento de normativas, implementar una gestión eficaz y proteger a las organizaciones, fortaleciendo su reputación y contribuyendo a un sistema más seguro y transparente.

En este sentido, la gerencia debe estar necesariamente al tanto de los avances tecnológicos, como la inteligencia artificial, que permite analizar grandes cantidades de información en busca de actividades sospechosas. Asimismo, por el ejemplo la tecnología *Blockchain*[3] que puede optimizar la identificación y trazabilidad de las transacciones, aumentando elementos para la verificación, la seguridad y transparencia en las actividades.

Por lo tanto, en este contexto, es fundamental que la gerencia esté comprometida a enfrentar desafíos importantes al implementar medidas de prevención y control de la legitimación de capitales. Estas medidas incluyen la inversión en tecnología, capacitación y personal de manera significativa, así

[3] Tecnológica caracterizada por su capacidad de trazabilidad e inmutabilidad, fundamental para garantizar la integridad y transparencia en la administración de riesgos financieros.

como la necesidad de actualizar y armonizar las políticas, procesos y mejores prácticas relacionadas. También es crucial abordar la resistencia al cambio y la falta de conocimiento y experiencia para identificar y reportar actividades cada vez más complejas.

Ante esta situación, la gerencia debe considerar nuevos modelos de gestión que fomenten la cultura de innovación, estimulen la creatividad y la búsqueda de soluciones nuevas, y adopten un enfoque basado en riesgos que priorice las áreas de mayor vulnerabilidad.

Por lo tanto, los Oficiales de Cumplimiento deben asumir un papel de liderazgo activo en la lucha contra la legitimación de capitales, demostrando un compromiso proactivo con la ética y el cumplimiento. Los nuevos enfoques de gestión ya no son solo una tendencia, sino una necesidad imperativa para que las organizaciones puedan prosperar en un entorno dinámico y competitivo. La gerencia del futuro, especialmente la del Oficial de Cumplimiento, debe estar preparada para liderar el cambio, adaptarse a las nuevas tendencias y construir un futuro sostenible tanto para la organización como para la sociedad.

Es fundamental resaltar la importancia del desarrollo de competencias técnicas y profesionales en el equipo directivo, ya que estas competencias influyen directamente en los resultados de la gestión contra la legitimación de capitales. Es crucial fortalecer de manera continua una cultura ética[4] dentro de la organización, así como tener la capacidad de identificar y gestionar de forma eficaz los riesgos asociados con este delito. Además, es esencial cumplir con las leyes y regulaciones pertinentes, enfrentar la cultura del privilegio y proteger la reputación de la organización para evitar posibles multas y sanciones.

Finalmente, desde el horizonte Ontoepistémico la Gerencia es un proceso clave para garantizar la eficiencia y la eficacia contra la legitimación de

[4] Compromiso real de la alta dirección, que ha sido aceptado y asumido por todos los empleados, para hacer lo correcto, respetar la ley y los derechos de los demás.

capitales, en contextos complejos y autodeterminados, en el cual la codependencia de hábitos y comportamientos inconscientes obstaculizan el desaprendizaje y no favorecen el reaprendizaje de prácticas conscientes en materia de gestión de riesgos contra la legitimación de capitales ante la evolución de la delincuencia organizada.

En este punto, se puede indicar que el Oficial de Cumplimiento toma decisiones basadas en hábitos, sesgos e información incompleta ante un entorno de caos y orden en las organizaciones, no obstante la Inteligencia Artificial emerge no como un accesorio técnico, sino como una herramienta que altera radicalmente los límites de esa racionalidad, expandiendo la capacidad analítica, pero introduciendo una nueva forma de incertidumbre.

En el mismo orden de ideas, desde la perspectiva del Comportamiento Administrativo de Herbert Simón, el gerenciamiento se define esencialmente como un proceso continuo de toma de decisiones que inicia con la identificación de escenarios, el análisis de cursos de acción y finalmente con la elección. En el complejo contexto socioeconómico de las organizaciones, la praxis del Oficial de Cumplimiento en la prevención de la legitimación de capitales se ejerce bajo las condiciones de una racionalidad limitada y una contingencia situacional, donde las decisiones fluctúan entre el orden, el desorden y el ensayo-error frente a las mutaciones de la delincuencia organizada.

Rescatando lo antes comentado, desde un horizonte ontoepistémico, esta gestión se ve desafiada por hábitos organizacionales e impulsos inconscientes que obstaculizan el desaprendizaje y el reaprendizaje de prácticas conscientes de riesgo. Sin embargo, para superar las fronteras de esta racionalidad humana e impulsar la eficiencia sistémica, la gerencia se ve obligada a adoptar nuevos modelos de gestión basados en la innovación y el liderazgo ético. Es precisamente en la necesidad de procesar la complejidad de este entorno y neutralizar las vulnerabilidades donde el Comportamiento Administrativo se intercepta con la irrupción de la Inteligencia Artificial, optimizando las

capacidades e introduciendo al Oficial de Cumplimiento en una nueva dimensión de asimetría cognitiva e incertidumbre tecnológica.

Inteligencia Artificial (IA) e Incertidumbre Tecnológica

El marco analítico antes desarrollado e instituido por Herbert Simon, nos ha permitido comprender la gerencia del riesgo como un ejercicio intrínsecamente ligado a la toma de decisiones bajo condiciones de orden y desorden. Sobre esta base, el presente capítulo avanza hacia la dimensión de la Inteligencia Artificial y la Incertidumbre Tecnológica, entendiendo que las herramientas de automatización masiva representan un catalizador del Comportamiento Administrativo. La presente sección se plantea con el propósito de conectar la gestión del Oficial de Cumplimiento con las galaxias digitales de la modernidad, examinando cómo la velocidad de procesamiento de los algoritmos y la inmutabilidad de tecnologías, abren ventanas de oportunidad para optimizar el rendimiento de las organizaciones, pero también configuran un estado de versatilidad e incertidumbre radical que redefine éticamente la lucha contra la delincuencia organizada transnacional.

Resulta en este punto nuevamente pertinente, destacar de manera breve el análisis precedente en torno al Comportamiento Administrativo, el cual demuestra que la eficiencia y eficacia contra la legitimación de capitales dependen del desempeño individual del trabajador y de su capacidad para aprender y desaprender en entornos complejos. Sin embargo, la realidad organizacional del siglo XXI se encuentra signada por una paradoja tecnológica: la necesidad de delegar la detección de patrones delictivos en arquitecturas de Inteligencia Artificial para superar la racionalidad limitada humana. Al iniciar este apartado, se propone explorar la transición desde la toma de decisiones convencional hacia un neoparadigma dominado por la incertidumbre tecnológica. El abordaje de la IA se asume aquí no como una mera adopción de herramientas analíticas de alta velocidad, sino como un desafío directo a la autonomía intelectual y la ética de la información, donde la

estructura automatizada carece de la intuición y la justicia algorítmica inherentes al ser humano, forzando la emergencia de una hermenéutica capaz de conciliar la técnica con la gobernanza institucional.

En consonancia con lo anterior, el transitar la conexión entre la Transcomplejidad e Inteligencia Artificial (IA) se inicia enfatizando una brecha fundamental, la IA aunque procesa datos a velocidades "cableadas", carece de la multidimensionalidad transcompleja, es decir carece de intuición, ética y espiritualidad. En este escenario el gerente, reconfigurado bajo el paradigma de la transcomplejidad como Oficial de Cumplimiento, asume una nueva praxis organizacional enfocada en la prevención de la legitimación de capitales. Este actor es quien aporta la dimensión interpretativa y el sentido crítico que las redes neuronales artificiales son incapaces de generar.

Desde un enfoque integrador, es necesario vincular el rol de la Inteligencia Artificial (IA) considerando el efecto en la autonomía, creatividad y pensamiento crítico. Con base en los planteamientos de Schavino, Colavolpe (2025) la irrupción de la IA está transformando profundamente el desarrollo cognitivo y tiene el potencial de personalizar el aprendizaje y ampliar el acceso a recursos, lo que representa una oportunidad para el desarrollo de nuevas competencias y habilidades del gerente, sin embargo, las referidas autoras también advierten sobre riesgos significativos si su uso no es acompañado por reflexión crítica, ética y estrategias pedagógicas adecuadas. Por lo tanto, indican que la autonomía intelectual puede resultar igualmente impactada por la facilidad del acceso automatizado a soluciones inmediatas, lo que puede inhibir la perseverancia, el esfuerzo y el aprendizaje del gerente.

Enfoque desde la Hermenéutica Algorítmica

Frente a la asimetría entre la velocidad analítica de la máquina y la multidimensionalidad humana, surge la Hermenéutica Algorítmica. En ese sentido Peña Peinado (2025) introduce constructos claves en lo que denomina el "mar de la transcomplejidad" presentando la denominada Hermenéutica

Algorítmica, la cual señala, define la interpretación de la realidad mediante la combinación de la reflexión profunda humana y las capacidades analíticas de los algoritmos, así como la Transpedagogía Tecnocientífica como un modelo rizomático que teje puentes entre el conocimiento tradicional y las "galaxias digitales" del aprendizaje, promoviendo una metacognición aumentada. Esta interpretación no puede ser meramente técnica; requiere de la transdisciplinariedad[5] propuesta por Basarab Nicolescu (1996) para integrar niveles de realidad que la máquina ignora, como la intuición y la espiritualidad. La transdisciplinariedad, por lo tanto, es un camino para que emerja un nuevo tipo de ser humano, el Homo sui transcendentalis. Este no es un "hombre nuevo" creado por ideologías, sino un ser que nace de nuevo al autotranscederse, y encontrar su lugar único en la unidad abierta del mundo[6].

Enfoque desde la justicia algorítmica

Asimismo, para asegurar que esta praxis derive en una verdadera justicia algorítmica, es imperativo adoptar la ética de la información de Luciano Floridi (2013) y cómo la IA debe alinearse con la gobernanza institucional humana, sostiene que en la "infosfera" actual, debe centrarse en la protección de la autonomía humana frente a los sistemas digitales, fortaleciendo la tesis sobre el desafío a la autonomía intelectual planteado por la IA.

Lo anterior permite plantear la posibilidad de neutralizar los sesgos inherentes a los modelos matemáticos opacos descritos por Cathy O'Neil (2016), la cual fundamenta técnicamente por qué es necesaria la justicia algorítmica para evitar sesgos que afecten la efectividad del Oficial de cumplimiento en la sociedad planetaria. En este ecosistema de cambio, la transparencia en el análisis del conocimiento es clave para contener las repercusiones técnicas,

[5] Basarab Nicolescu es un físico teórico rumano y una figura central en el pensamiento contemporáneo, reconocido principalmente como el arquitecto y promotor de la metodología de la transdisciplinariedad.

[6] El pensamiento de Nicolescu trasciende lo técnico para proponer una reforma de la existencia.

sociales y políticas en la administración de riesgos (Schavino y Colavolpe, 2025).

Esta dinámica de transformación exige un proceso simultáneo de "aprender y desaprender" como señala Shulman (1999) destacando el dinámico y simultáneo proceso cuando indica que “Ahora entendemos el aprendizaje como un proceso dual en el cual, inicialmente, las creencias y los entendimientos interiores deben salir y solamente entonces algo que está afuera puede entrar” la capacidad inherente en la gestión del riesgo para el gerente requiere precisamente en un constante aprendizaje de entender el comportamiento y tendencias de la Delincuencia Organizada, las tipologías entre otros aspectos técnicos, de esa manera el programa de prevención estará fortalecido.

Para el Oficial de Cumplimiento, el desaprendizaje gerencial es una ventaja metodológica que le obliga a evaluar críticamente lo aprendido, obligando permanentemente plantearse la renovación de los conocimientos obsoletos para comprender las mutaciones de la delincuencia organizada y sus tipologías financieras. En suma, partiendo del razonamiento lógico de nuestros conocimientos, y a la habilidad de recordar y aplicar aquellos que sigan siendo adecuados a los nuevos tiempos, pero renovar aquellos que se hayan quedado obsoletos, esto es fundamental ya que de lo contrario nos limita en nuestras posibilidades de futuro.

Trascender hacia este neoparadigma implica evitar lo que Perdomo (2026) define en su obra Tecno-Therian como el procesamiento automatizado del mundo sin interpretación; el gerente del siglo XXI no puede operar como una red neuronal desprovista de hermenéutica, sino que debe compasar sus acciones con la complejidad del entorno. Para el gerente resolver los problemas sobre la materia se determinan por acciones, que logren acompasar con las realidades del entorno, su compresión y acciones deben responder a la naturaleza del siglo XXI.

Análisis desde la teoría de la incertidumbre de Frank Knight

Finalmente, este enfoque se encuentra profundamente vinculado con la teoría de la incertidumbre de Frank Knight el autor examina el mecanismo del valor bajo escenarios de competencia perfecta donde el conocimiento perfecto excluye el riesgo y la incertidumbre, para el caso de la competencia imperfecta, la incertidumbre radical da origen al beneficio puro. Al trasladar esta tesis al marco de la transcomplejidad, el "beneficio" del Oficial de Cumplimiento no es financiero, sino preventivo. Consiste en la neutralización de los esquemas operativos de la delincuencia organizada. La gerencia del riesgo, por lo tanto, reconfigura las incertidumbres de la conducta humana en probabilidades medibles mediante el enjuiciamiento de las capacidades organizacionales, consolidando un sistema robusto y dinámico contra la legitimación de capitales.

En este punto se puede indicar la importancia de todo lo antes expresado, justificando redefiniendo el enfoque de riesgos, para impulsar el camino a lo convencional, en donde podamos adecuar la Gestión de Riesgo asociándola con la Legitimación de Capitales, incorporando al Gerente de manera inherente una gestión fundamental que tribute en el fortalecimiento del Sistema Contra la Legitimación de Capitales.

Considerando lo antes señalado, la gerencia del riesgo implica una redefinición con una propuesta alternativa que permita desarrollar una gestión efectiva, en este punto se puede señalar lo establecido por Knight en el Capítulo X cuando introduce el caso del Gerente asalariado, afirmando que “el único riesgo que conduce a un beneficio es una incertidumbre única que resulta de un ejercicio de la responsabilidad final, que en su misma naturaleza no puede ser ni asegurada, ni capitalizada, ni asalariada. El beneficio surge de la inherente imposibilidad absoluta de pronosticar las cosas, que proviene del hecho escueto de que los resultados de la actividad humana no pueden ser previstos y solamente en tanto que aun entonces sea imposible y carezca de sentido un cálculo de probabilidad respecto a aquéllos” en este caso el beneficio se

encuentra asociado con evitar que la delincuencia organizada logre desarrollar y operar esquemas para Legitimar Capitales.

La IA como instrumento de investigación: Tensiones éticas y científicas

Resulta necesario incorporar las tensiones éticas y científicas que emergen cuando la IA se convierte en herramienta, un instrumento de investigación, para las actividades del Gerente como Oficial de cumplimiento gestionando un cambio de paradigma en la praxis individual y organizacional, dado que el hecho social, impulsa una realidad dinámica nos encausa para indicar algunos asuntos de énfasis sobre el referido asunto.

Interpretando la publicación de Schavino, Colavolpe (2025) la transparencia y responsabilidad en el análisis de conocimiento mediante IA es fundamental, dado las consecuencias en la gestión y administración de riesgo y sus posibles colaterales señalados como problemas técnicos y sus efectos en los ámbitos social y político.

Desde una perspectiva de "incertidumbre tecnológica" la IA integra al sistema financiero un multinivel de permanente consideración, a la luz de oportunidades para potenciar competencias gerenciales, la inteligencia artificial se incorpora en las estructuras financieras para transformar la toma de decisiones. La tecnología introduce un estado de versatilidad ante la incertidumbre tecnológica que obliga a las organizaciones a adaptarse constantemente. La integración de la IA en las empresas le permiten un encuentro con nuevas vías para fortalecer las capacidades directivas y mejorar el rendimiento institucional. De este modo, la IA no solo actúa como una herramienta técnica, sino como un motor para potenciar el liderazgo en entornos económicos complejos, para combatir la delincuencia organizada. Todo ello, resulta en oportunidades permiten a los gerentes, actuando desde las luces, navegar con mayor eficacia en un mercado globalizado, desmaterializado por lo tanto digital.

El contenido diverso, propio de un enfoque transcomplejo, nunca suficiente, e independientemente de las fuentes citadas, es importante notar que el éxito de la gestión como gerentes bajo un entorno signado bajo el referido paradigma, depende al menos, quizás y no limitativa de la ética y justicia algorítmica, asegurando que el diseño tecnológico evite sesgos y mantenga la centralidad del ser humano para una gestión efectiva del gerente.

Conclusiones

Compartiendo algunas reflexiones, rescatando que el método de abordaje para el desarrollo del presente contenido es una revisión documental crítico-reflexiva, se puede adelantar señalando que la irrupción de la Inteligencia Artificial en los sistemas de cumplimiento no desplaza al factor humano, sino que reconfigura el rol del Oficial de Cumplimiento como un hermeneuta organizacional. La verdadera eficacia contra la legitimación de capitales no emerge de la velocidad de procesamiento de datos "cableados", sino de la capacidad crítica para dotar de sentido ético y contextual a los patrones transaccionales que arrojan los algoritmos.

También resulta importante rescatar, del contenido previamente presentado, los siguientes aspectos:

- La toma de decisiones bajo incertidumbre radical: Con base en los postulados de Knight, el Oficial de Cumplimiento gestiona un entorno donde las mutaciones de la delincuencia organizada representan variables no asegurables ni plenamente previsibles. Por ende, el diseño del programa de prevención requiere un proceso permanente de aprendizaje y desaprendizaje (Shulman), evitando el procesamiento automatizado desprovisto de interpretación.
- La urgencia de la Justicia Algorítmica: Para contener los sesgos inherentes a los modelos matemáticos opacos descritos por O'Neil, las instituciones financieras deben adoptar la ética de la información. La alineación de la IA con la gobernanza institucional humana es el único mecanismo capaz de

blindar la autonomía intelectual del gerente ante las soluciones automatizadas inmediatas.

- La Decisión bajo Racionalidad Limitada: Simon postula que la elección humana nunca es perfecta debido a los límites cognitivos, hábitos y destrezas del decisor. En la lucha contra la legitimación de capitales, esta limitación ha permitido históricamente el avance del delito por procesos de ensayo-error. La Inteligencia Artificial es requerida por la organización precisamente para desmaterializar esos límites y analizar volúmenes masivos de datos (Big Data) inalcanzables para la mente humana.
- La pertinencia del Comportamiento Administrativo: El enfoque de Simon ratifica que la gerencia es un ejercicio continuo de toma de decisiones. Frente al riesgo tecnológico, las organizaciones deben fortalecer el desempeño individual del trabajador, articulando sus competencias transdisciplinarias (intuición, ética y técnica) como la matriz defensiva más eficiente frente a las dinámicas financieras de la sociedad planetaria.
- El "Beneficio Preventivo" como Valor Estratégico: Considerando lo establecido por Frank Knight, en la era de la IA el éxito del Oficial de Cumplimiento no se mide por la ausencia de alertas, sino por su capacidad de transformar la incertidumbre radical en un "beneficio preventivo" que protege la reputación y la ética de la institución.
- Llamado a la Autonomía Intelectual: La Justicia Algorítmica y la Ética de la Información (Floridi) son las únicas defensas contra el fenómeno Tecno-Therian (el procesamiento del mundo sin interpretación humana). La conclusión debe ser un recordatorio de que la tecnología debe servir a la gobernanza humana y no al revés.
- El Perfil del Homo sui transcendentalis: El nuevo tipo de profesional que se requiere en la sociedad planetaria, debe utilizar la Transpedagogía Tecnocientífica para "aprender y desaprender" constantemente, integrando la técnica con la intuición y la espiritualidad para trascender los límites de la máquina

Referencias

Floridi, L. (2013). *The ethics of information*. Oxford University Press.

Knight, F. H. (1972). *Riesgo, incertidumbre y beneficio*. Aguilar. (Obra original publicada en 1921).

Nicolescu, B. (1996). *La transdisciplinariedad: Manifiesto*. Multiversidad Mundo Real.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.

Peña Peinado, M. (2025). Transcomplejidad e IA. Un diálogo entre lo digital y lo humano en la era del conocimiento. Libros@Red de Investigadores de la Transcomplejidad.

Perdomo, W. (2026). *Tecno-Therian: El procesamiento automatizado del mundo sin interpretación*.

Schavino, N. y Colavolpe, C. (2025). Inteligencia artificial, desarrollo cognitivo y autonomía intelectual: Desafíos para la gerencia transcompleja. Editorial Tecnociencia/REDIT.)

Shulman, L. S. (1999). Taking learning seriously. *Change: The Magazine of Higher Learning*, *31*(4), 10–17.

Simon, H. A. (1972). *El comportamiento administrativo: Estudio de los procesos de adopción de decisiones en la organización gestora*. Aguilar.

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

LA SOSPECHA INMOTIVADA: CÓMO LA INTELIGENCIA ARTIFICIAL NO EXPLICABLE DEBILITA EL REPORTE DE ACTIVIDADES SOSPECHOSAS Y CONTAMINA EL ANÁLISIS DE INTELIGENCIA FINANCIERA

Autor: Abg. Esp. Yeixon Santaella Bernal
Facilitadora: MSc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

La sospecha inmotivada: Cómo la Inteligencia Artificial no explicable debilita el Reporte de Actividades Sospechosas y contamina el análisis de inteligencia financiera

Autor: Abg. Esp. Yeixon Santaella Bernal
Código ORCID: 0009-0009-0017-7002
Correo electrónico: yeixons@gmail.com

Resumen

Ante la ineficacia del monitoreo tradicional en la prevención de LC/FT/FPADM, los Sujetos Obligados han adoptado algoritmos predictivos que detectan anomalías estadísticas sin revelar su lógica causal (Inteligencia Artificial no explicable). Esta opacidad genera dos consecuencias críticas. Primero, provoca la abdicación analítica del Oficial de Cumplimiento, quien se convierte en un mero transmisor de probabilidades estadísticas al remitir sospechas inmotivadas que no puede justificar materialmente. Segundo, contamina la cadena de inteligencia financiera puesto que la Unidad Nacional de Inteligencia Financiera (UNIF) recibe reportes carentes de indicios fácticos, impidiendo la elaboración de informes robustos. Como resultado, el Ministerio Público obtiene un Informe de Inteligencia Financiera carente de insumos para sustentar investigaciones en el proceso penal. Frente a esta vulnerabilidad, se propone el uso de Inteligencia Artificial Explicable (XAI) subordinados al principio de supervisión humana indelegable luego de analizar las implicaciones jurídicas de fundamentar el Reporte de Actividades Sospechosas (RAS) en modelos de Inteligencia Artificial no explicable o de caja negra. Se concluye que la tecnología debe subordinarse a las garantías procesales y dotar al sistema penal de indicios verificables y jamás entorpecerlo mediante probabilidades inescrutables.
Descriptores clave: Inteligencia Artificial Explicable; Caja Negra; RAS; Nuevas Tecnologías.

Abstract

Given the ineffectiveness of traditional monitoring in preventing money laundering, terrorist financing, and the proliferation of weapons of mass destruction, obliged entities have adopted predictive algorithms that detect statistical anomalies without revealing their underlying causal logic. This opacity generates two critical consequences. First, it leads to the analytical abdication of the Compliance Officer, who becomes a mere transmitter of statistical probabilities by submitting unfounded suspicions that cannot be substantiated. Second, it contaminates the financial intelligence chain, as the National Financial Intelligence Unit (UNIF) receives reports lacking factual evidence, preventing the preparation of robust reports. As a result, the Public Prosecutor's Office obtains a Financial Intelligence Report lacking the necessary input to support investigations in criminal proceedings. In response to this vulnerability, the use of Explainable Artificial Intelligence (XAI) is proposed, subject to the principle of non-delegable human oversight, after analyzing the legal implications of basing Suspicious Activity Reports (SARs) on unexplainable or black-box Artificial Intelligence models. It is concluded that technology must be subordinate to procedural safeguards and provide the criminal justice system with verifiable evidence, never hindering it through inscrutable probabilities.

Key descriptors: Explainable Artificial Intelligence; Black Box; RAS; New Technologies.

De la IA a la inteligencia financiera

La masificación de las operaciones financieras digitales y la constante mutación de las tipologías delictivas han transformado radicalmente los sistemas preventivos del Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM).

Frente a las debilidades existentes en los sistemas de monitoreo transaccional tradicionales —basados en umbrales estáticos—, los Sujetos Obligados se han visto en la obligación de recurrir a modelos predictivos avanzados.

El Grupo de Acción Financiera (GAFI) en su informe sobre Oportunidades y Desafíos de las Nuevas Tecnologías para combatir el Lavado de Activo y otros delitos financieros (2021), destaca que la adopción del Aprendizaje Automático (Machine Learning) facilita “la recopilación, el procesamiento y el análisis de datos, y ayudar a los actores involucrados a identificar y gestionar los riesgos

de lavado de dinero y financiamiento del terrorismo de manera más eficaz y casi en tiempo real" (p.4).

Sin embargo, la adopción de estas tecnologías ha introducido una grave vulnerabilidad metodológica en la gestión de riesgos, y es lo que se conoce como la opacidad algorítmica, es decir, la incapacidad de poder entender o cuestionar sistemas de Inteligencia Artificial (IA).

El Consejo de Estabilidad Financiera (FSB) en su informe Inteligencia Artificial y aprendizaje automático en los servicios financieros (2017) advierte que muchos de estos modelos de Machine Learning (Aprendizaje Automático) operan como una caja negra, generando un escenario en el cual

> Es difícil, difícil para los usuarios humanos en las instituciones financieras –y para los reguladores– comprender cómo se han formulado decisiones (…) Además, el mecanismo de comunicación utilizado por tales herramientas puede ser incomprensible para los humanos, lo que plantea desafíos de monitoreo para los operadores humanos de tales soluciones (p.26).

En ese sentido, a medida que los algoritmos adquieren mayor autonomía, el sistema arroja alertas de alto riesgo, pero es incapaz de explicar la cadena lógica que motivó dicha conclusión. El presente ensayo analiza las implicaciones de fundamentar un Reporte de Actividades Sospechosas (RAS) en sistemas opacos, y cómo esta práctica desvirtúa el sistema preventivo y debilita la inteligencia financiera nacional, generando una falta de interpretabilidad, desde dos enfoques operativos.

En primer lugar, provoca en el Sujeto Obligado un fenómeno de renuncia a los procesos de análisis. Por ejemplo, un Oficial de Cumplimiento o analista, ante una alerta generada por un modelo matemático incomprensible, podría verse imposibilitado de ejecutar una debida diligencia intensificada que justifique documentalmente la sospecha.

Al no poder descifrar el porqué de la anomalía, se corre el riesgo de convertirse en un mero transmisor de probabilidades estadísticas, eludiendo el deber normativo de motivar el reporte.

En segundo lugar, se produce una contaminación en la génesis de la inteligencia financiera. Si bien el RAS reviste un carácter administrativo y no constituye una imputación penal, es el insumo primario de la Unidad Nacional de Inteligencia Financiera (UNIF).

Cuando un reporte se sostiene únicamente en el veredicto inmotivado de una caja negra, la UNIF recibe una sospecha carente de indicios materiales. Este desamparo fáctico impide a los analistas de inteligencia construir un Informe de Inteligencia Financiera robusto, lo que a su vez limitaría la capacidad del Ministerio Público para encontrar elementos de convicción que justifiquen el inicio de una investigación penal.

Es por cuanto, el objetivo de este ensayo es demostrar que la modernización tecnológica no puede operar en un vacío de fundamentación lógica.

Se plantea la necesidad de que los marcos normativos exijan la transición hacia una Inteligencia Artificial Explicable (XAI), definida por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (2021), su estudio denominado Cuatro Principios de la Inteligencia Artificial Explicable, como aquellos sistemas capaces de “entregar evidencias o razones que acompañan los resultados y procesos; y proporcionar explicaciones que sean comprensibles para los humanos” (p.4).

1. Del monitoreo tradicional a la Caja Negra en la detección de patrones

Para comprender la vulnerabilidad jurídica que introduce la Inteligencia Artificial Explicable en el sistema preventivo, resulta indispensable delimitar las diferencias estructurales entre los sistemas de monitoreo tradicionales y los modelos analíticos avanzados.

Históricamente, la detección de operaciones inusuales en las instituciones financieras se ha fundamentado en la parametrización tradicional; es decir,

sistemas de monitoreo transaccional (TMS, por sus siglas en inglés) que operan bajo reglas condicionales estáticas y escenarios predefinidos por analistas humanos (por ejemplo, alertas detonadas cuando las transacciones en efectivo superan un umbral específico en un lapso determinado).

La principal ventaja dogmática de estos sistemas tradicionales radica en su trazabilidad absoluta. Al basarse en lógica matemática, el analista u Oficial de Cumplimiento de un sujeto obligado comprende exactamente por qué se generó la alerta, lo que facilita la motivación material de la sospecha.

Sin embargo, su eficacia operativa se ha visto obligada a migrar a otros escenarios de análisis frente a la sofisticación de la delincuencia organizada. Tal como señala el GAFI en su informe sobre Oportunidades y Desafíos de las Nuevas Tecnologías para combatir el Lavado de Activo y otros delitos financieros (2021), los sistemas basados estrictamente en reglas adolecen de rigidez, lo que genera tasas de falsos positivos que saturan las áreas de cumplimiento.

Para superar esta ineficiencia, los sujetos obligados tienen la opción de migrar hacia modelos de Aprendizaje Automático, dependiendo de su capacidad económica.

A diferencia de la programación tradicional, el Machine Learning no requiere que un humano introduzca reglas estrictas, en su lugar, se le proporcionan volúmenes de datos históricos para que el propio algoritmo identifique correlaciones complejas y no lineales. Y es en este salto tecnológico donde surge el fenómeno de la caja negra.

Por caja negra, según definición del GAFI (2021), se entiende como aquella "IA/aprendizaje automático y otras tecnologías que son opacas, poco intuitivas y no proporcionan información adecuada sobre su proceso de toma de decisiones y predicciones/resultados" (p.55).

Al respecto el FSB, en el informe Inteligencia Artificial y aprendizaje automático en los servicios financieros (2017) define el problema de la caja negra como una de las principales barreras en la adopción de IA en los servicios

financieros. Ocurre cuando la complejidad matemática del modelo, especialmente en redes neuronales profundas o algoritmos de bosque aleatorio, impide a los auditores y analistas comprender cómo las variables de entrada se ponderaron para generar una decisión o predicción específica sobre las alertas.

En el contexto de la prevención del LC/FT/FPADM, esto se traduce en un modelo predictivo que evalúa miles de variables transaccionales, conductuales y sociodemográficas simultáneamente, arrojando una alerta con un alto porcentaje estadístico de probabilidad de legitimación de capitales. El problema subyace en que el sistema es incapaz de verbalizar la narrativa delictiva detrás de su conclusión meramente matemática.

Se configura así el dilema central de la modernización tecnológica en el cumplimiento normativo, toda vez que el sujeto obligado obtiene una detección algorítmica altamente precisa desde el punto de vista estadístico, pero dogmáticamente estéril, enfrentando el desafío de ejecutar una debida diligencia sobre un comportamiento financiero cuya lógica anómala solo existe dentro de la opacidad de un código informático.

2. Comportamiento de los profesionales de prevención y su impacto en la calidad de reportes

Como se señaló anteriormente, los desafíos que presenta la inclusión de sistemas basados en Inteligencia Artificial no explicable se presentan desde dos enfoques, es importante analizar cada uno de estos.

La primera consecuencia recae sobre el núcleo del sistema preventivo: el análisis riguroso de los analistas de prevención y del Oficial de Cumplimiento. De acuerdo con los estándares internacionales y las normativas prudenciales de cada sector, en Venezuela, la detección de una operación inusual no concluye con la generación de la alerta, sino que constituye el inicio del proceso de debida diligencia intensificada.

Este deber normativo exige que el sujeto obligado analice el contexto de la transacción, solicite soportes documentales al cliente y, fundamentalmente, emita un juicio de valor sustentado para determinar si la inusualidad puede ser justificada o si, por el contrario, debe ser elevada a sospecha formal mediante un Reporte de Actividades Sospechosas (RAS).

Así lo establece la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (2012), en su artículo 13, al señalar que

> **Artículo 13. Obligación del Reporte de Actividades Sospechosas.** Los sujetos obligados deben prestar especial atención a cualquier transacción o grupo de transacciones independientemente de su cuantía y naturaleza, cuando se sospeche que los fondos, capitales o bienes provienen o están vinculados, o podrían ser utilizados para cometer delitos de legitimación de capitales, acto terrorista o financiamiento al terrorismo o cualquier otro delito de delincuencia organizada. Asimismo, deberán prestar especial atención a tales actividades aun cuando provengan de una fuente lícita.

Siguiendo este mandato, la caja negra algorítmica genera una parálisis metodológica y legal. Cuando un analista recibe una alerta generada por un sistema tradicional, conoce con precisión la variable detonante (por ejemplo, el fraccionamiento de depósitos en efectivo en un lapso de 48 horas).

Esta trazabilidad le permite al analista dirigir su requerimiento de forma puntual, es decir, solicitar al cliente el origen de esos fondos específicos.

Sin embargo, si la alerta provino de un modelo predictivo opaco que evaluó simultáneamente miles de micro patrones de comportamiento, geolocalización y velocidad transaccional para arrojar un porcentaje de probabilidad de legitimación de capitales, el Oficial de Cumplimiento se encuentra desprovisto de un punto de partida material.

La falta de interpretabilidad impide dirigir el esfuerzo analítico, lo que significa que no podrá solicitar soportes documentales a un cliente justificando que un algoritmo encontró correlaciones ocultas en su perfil. Esta incapacidad para comprender el porqué de la alerta conlleva a lo que se denomina como la

abdicación humana, un escenario de riesgo en el cual el sujeto obligado delega materialmente el juicio de valor preventivo a un software manipulado por IA.

Esta abdicación –término empleado para referirse a la renuncia del analista de prevención y su rendición ante un sistema IA– genera dos desviaciones críticas frente a las medidas de supervisión, los cuales son: archivo injustificado de alertas y los RAS inmotivados.

En cuanto al primero, ante la incomprensión de la lógica matemática del modelo y la ausencia de indicios visibles que permitan estructurar un expediente de sospecha, el analista puede optar por archivar la alerta asumiendo que se trata de un falso positivo. Esta decisión, tomada sin base documental, expone a la institución a severas sanciones administrativas por fallas en el sistema de prevención, dado que la alerta fue desechada por incomprensión y no por justificación legítima de los fondos.

Por el contrario, ante el temor a sanciones regulatorias, el analista puede optar por aprobar la sospecha y remitir el reporte a la UNIF basándose exclusivamente en el alto porcentaje probabilístico que indica la pantalla del sistema.

En este supuesto, el Oficial de Cumplimiento incumple su obligación de motivar el análisis documental de la operación. El RAS pierde su naturaleza de evaluación experta humana para convertirse en un mero canal de transmisión automatizado de datos algorítmicos.

En ambos escenarios, se desvirtúa el Enfoque Basado en Riesgos (EBR), toda vez que el Oficial de Cumplimiento deja de ser un gestor proactivo de la mitigación del riesgo legal y reputacional, para convertirse en un espectador pasivo subordinado a las decisiones indescifrables de un modelo matemático que, pese a su sofisticación, carece de responsabilidad jurídica.

3. La contaminación de la Inteligencia Financiera

El impacto de fundamentar las alertas en modelos algorítmicos incomprensibles trasciende las fronteras operativas del Sujeto Obligado y permea directamente en la eficacia del Estado para perseguir el delito.

Para comprender la gravedad de esta vulnerabilidad, resulta imperativo delimitar la naturaleza jurídica del Reporte de Actividades Sospechosas (RAS) en el ordenamiento venezolano.

Conforme a lo establecido en la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (2012), el RAS “no es una denuncia penal y no requiere de las formalidades y requisitos de este modo de proceder, ni acarrea responsabilidad penal, civil o administrativa contra el sujeto obligado y sus empleados o empleadas, o para quien lo suscribe”, es decir, es un insumo estrictamente administrativo que sirve como materia prima fundamental para la UNIF.

La utilidad táctica de un RAS radica en la calidad de la narrativa analítica que acompaña a la alerta. Cuando el Oficial de Cumplimiento remite un reporte estructurado bajo un razonamiento explicable, provee a la UNIF de indicios materiales que detalla el patrón de fraccionamiento, identifica incongruencias en la facturación o señala vínculos societarios atípicos. Sin embargo, cuando la UNIF recibe un RAS fundamentado en la opacidad de una caja negra, se produce una contaminación para la inteligencia financiera.

El reporte automatizado carece de narrativa descriptiva del iter criminis financiero; se limita a informar que un modelo de Aprendizaje Automático ha asignado un alto porcentaje de probabilidad de riesgo a un cliente. Ante este problema, los analistas de inteligencia de la UNIF se encontrarán imposibilitados de enfocar sus pesquisas.

Pero esta deficiencia no solo debe verse hasta la problemática que hereda la UNIF, sino también en la incapacidad que se le pudiera presentar al Ministerio Público (MP) si la UNIF decide remitir un Informe de Inteligencia Financiera

basado en datos otorgados por sistemas que no ofrecen razonamiento lógico cualitativo.

El sistema penal venezolano exige que el titular de la acción penal (MP) sustente sus actuaciones en elementos de convicción objetivos y verificables. Si el MP recibe un Informe de Inteligencia Financiera cuya génesis es una probabilidad estadística inexplicable derivada del software, el Fiscal se encuentra maniatado procesalmente.

Resulta jurídicamente inviable que un Fiscal solicite a un Juez de Control medidas cautelares —tales como el congelamiento preventivo de fondos— argumentando exclusivamente que un algoritmo detectó una anomalía matemática multidimensional incomprensible para la inteligencia humana.

Restringir garantías constitucionales fundamentales como el derecho a la propiedad o la libertad económica requiere la demostración de indicios materiales de criminalidad que el modelo de caja negra es estructuralmente incapaz de proveer.

Lo que entonces presenta un escenario que, en el afán de maximizar la capacidad de detección de operaciones ilícitas mediante Inteligencia Artificial, coloca debilidades en el sistema preventivo paralizando la acción de la justicia, ya que rompe la cadena lógica y probatoria que conecta la sospecha administrativa inicial con la imputación penal formal.

4. Hacia un estándar regulatorio de Inteligencia Artificial Explicable (XAI) y la supervisión humana

Frente a la encrucijada dogmática y operativa expuesta, resulta evidente que la solución no radica en un retroceso tecnológico. Prescindir del Machine Learning y seguir casados con la parametrización tradicional implicaría dejar que solo la delincuencia organizada mute hacia escenarios tecnológicos para sus fines.

Por consiguiente, resulta necesario conformar una normativa que permita a los sujetos obligados transitar hacia la Inteligencia Artificial Explicable (XAI) subordinada al principio de supervisión humana.

Para evitar la contaminación de la inteligencia financiera y proteger las garantías del proceso penal, se propone que los órganos de supervisión y control y la Unidad Nacional de Inteligencia Financiera (UNIF) establezcan directrices vinculantes que prohíban el uso de algoritmos de caja negra en la emisión de alertas definitivas de LC/FT/FPADM.

En su lugar, el Sujeto Obligado debe estar condicionado a implementar exclusivamente modelos de XAI que genere reporte de trazabilidad lógica comprensible para el analista.

Es decir, un sistema que no debe limitarse solo a arrojar porcentajes de riesgo, sino que debe estar en la capacidad algorítmica de desglosar los factores que lo causan. Esta explicabilidad devuelve al Oficial de Cumplimiento la materia prima fáctica necesaria para iniciar su investigación, permitiéndole solicitar los soportes documentales precisos y justificar materialmente su decisión ante el regulador.

Sin embargo, la transparencia tecnológica por sí sola es insuficiente si no se acompaña de un blindaje procedimental. Por ello, es necesario la implementación del principio metodológico del Human-in-the-loop (Humano en el bucle de decisión), lo que Stryker (s/f), en su artículo ¿Qué es human-in-the-loop? define como “la intervención de los seres humanos en algún momento del flujo de trabajo de la IA para garantizar la precisión, la seguridad, la responsabilidad o la toma de decisiones éticas” (s/n).

Este concepto internacional establece que la Inteligencia Artificial no debe operar como un agente decisorio autónomo, sino como una herramienta de perfilamiento subordinada a la validación analítica de un experto.

Al integrar este principio en las normativas prudenciales, se garantiza que la tecnología asuma la carga del procesamiento masivo de datos, pero se reserva indelegablemente la facultad de la subsunción jurídica al Oficial de

Cumplimiento la determinación de si esa anomalía constituye una sospecha razonable y reportable.

Bajo este paradigma regulatorio, se repara la cadena de valor de la inteligencia financiera. Cuando el Sujeto Obligado remita el RAS, este no viajará como un mero dato probabilístico emitido por un software, sino como un expediente motivado, enriquecido por la tecnología, pero narrado y justificado por el intelecto humano.

5. Reflexiones finales

La modernización del sistema preventivo de LC/FT/FPADM no puede concebirse únicamente como un desafío técnico, sino que representa, fundamentalmente, una encrucijada ética y axiológica.

La adopción acrítica de modelos de IA de caja negra constituye una claudicación del raciocinio humano ante la mera conveniencia estadística. Desde la perspectiva del autor, el Oficial de Cumplimiento y el analista de prevención no son simples operadores tecnológicos, sino los verdaderos guardianes de la integridad del sistema financiero.

Permitir que un algoritmo inescrutable dicte la métrica de la sospecha despoja a la prevención de su esencia valorativa y jurídica, convirtiendo un análisis de riesgos riguroso en un acto de fe ciega hacia la máquina.

Desde la óptica del Derecho y la inteligencia financiera, es inaceptable que la génesis de una potencial investigación penal quede secuestrada por la opacidad algorítmica. El Estado de Derecho exige motivaciones, indicios materiales y racionabilidad, valores intrínsecos que una probabilidad matemática aislada jamás podrá satisfacer por sí sola.

La sospecha inmotivada no solo debilita operativamente el Reporte de Actividades Sospechosas, sino que socava profundamente las garantías procesales.

Por tal razón, se considera que, el sistema de justicia y el órgano rector de inteligencia financiera no pueden ni deben quedar supeditados a los dictámenes insondables de códigos informáticos incapaces de rendir cuentas o sostener un debate probatorio.

Por consiguiente, la exigencia de transitar hacia una Inteligencia Artificial Explicable (XAI) sometida a la supervisión humana indelegable trasciende la simple recomendación metodológica, puesto que es un imperativo moral y profesional.

La tecnología debe ser domesticada por el ordenamiento jurídico y jamás a la inversa, es por ello que, el deber ineludible en la gestión de riesgos es garantizar que la innovación opere como un faro que ilumine las complejidades del iter criminis financiero, y nunca como una sombra que excuse la abdicación analítica.

En la prevención de la delincuencia organizada, la decisión final, la ponderación ética y la responsabilidad legal de reportar deben permanecer siempre bajo el dominio inalienable del intelecto humano.

Referencias

Asamblea Nacional de la República Bolivariana de Venezuela. (2012). Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT). Gaceta Oficial Nº 39.912.

Consejo de Estabilidad Financiera (2017). Inteligencia Artificial y aprendizaje automático en los servicios financieros. Disponible en URL: https://www.fsb.org/uploads/P011117.pdf

Escuela Nacional de Administración y Hacienda Pública. (2016). Manual para elaboración y presentación de trabajos académicos. ENAHP-IUT. Caracas.

Grupo de Acción Financiera (GAFI). (2021). Oportunidades y Desafíos de las Nuevas Tecnologías para combatir el Lavado de Activo y otros delitos financieros.

Grupo de Acción Financiera (GAFI). (2025). Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la

proliferación de armas de destrucción masiva: Las Recomendaciones del GAFI

Instituto Nacional de Estándares y Tecnología de Estados Unidos (2021). Cuatro Principios de la Inteligencia Artificial Explicable. Disponible en URL: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8312.pdf

Stryker, C. (s/f). ¿Qué es un human in the loop? Artículo Disponible en URL: https://www.ibm.com/es-es/think/topics/human-in-the-loop

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

IMPACTO DE LAS NUEVAS TECNOLOGÍAS EN LA PREVENCIÓN DE LC/FT/FPADM Y OTROS ILÌCITOS EN EL SECTOR TURISMO: HOTELERÌA 4.0

Autor: Dra. Nelly Sánchez Pantaleón
Facilitadora: MSc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

Impacto de las nuevas tecnologías en la prevención de LC/FT/FPADM y otros ilícitos en el sector turismo: Hotelería 4.0

Autora: Dra. Nelly Sánchez Pantaleón
ID https://orcid.org/0009-0008-2241-5609
Correo electrónico nzsp72@gmail.com

RESUMEN

Este ensayo analiza la convergencia entre la Hotelería 4.0 en el sector turismo y la gestión de cumplimiento integral ante los riesgos de LC/FT/FPADM y otros ilícitos, bajo el marco de la Resolución 020. Desde una perspectiva ontológica, se examina al servicio de alojamiento moderno como un ecosistema digital que, al operar como APNFD, asume una posición de garante en la mitigación de sutiles tipologías delictivas. El propósito es evaluar el impacto de herramientas disruptivas (inteligencia artificial, blockchain y big data) en la optimización del SIAR y la debida diligencia. Mediante una metodología analítico-cualitativa, basada en el Enfoque Basado en Riesgo, se genera una reflexión crítica sobre el desafío de balancear la automatización con la supervisión humana del Oficial de Cumplimiento. El abordaje axiológico concluye que la tecnología es solo un medio; la verdadera eficacia radica en una cultura corporativa ética que priorice la transparencia sobre el beneficio económico.

Descriptores: Hotelería 4.0, Sector Turismo, Alojamiento, Nuevas Tecnologías (IA y Blockchain), Big Data, Activos Virtuales, Resolución 020.

ABSTRACT

This essay analyzes the convergence between Hospitality 4.0 in the tourism sector and comprehensive compliance management in the face of AML/CFT/AFP risks and other illicit activities, within the framework of Resolution 020. From an ontological perspective, it examines modern accommodation services as a digital ecosystem that, by operating as a Non-Financial Businesses and Services Providers (NFBPs), assumes a guarantor role in mitigating subtle types of crime. The purpose is to evaluate the impact of disruptive tools (artificial intelligence, blockchain, and big data) on optimizing the Integrated Risk Assessment System (IRAS) and due diligence. Through an analytical-qualitative methodology, based on the Risk-Based Approach, a critical reflection is generated on the challenge of balancing automation with the human oversight of the Compliance Officer. The axiological approach concludes that technology is only a means; true effectiveness lies in an ethical corporate culture that prioritizes transparency over economic gain.

Descriptors: Hospitality 4.0, Tourism Sector, Accommodation, New Technologies (AI and Blockchain), Big Data, Virtual Assets, Resolution 020.

Introducción

Teniendo en cuenta, que el sector de alojamiento turístico constituye uno de los motores económicos globales más dinámicos; sin embargo, su propia naturaleza operativa lo convierte en un escenario de alta vulnerabilidad frente a la delincuencia organizada transnacional.

Se puede señalar, que la dinámica transaccional del hospedaje moderno se caracteriza por la inmediatez en los flujos financieros, la alta rotación de huéspedes de diversas nacionalidades y la fragmentación de los canales de reserva, tanto físicos como virtuales.

Al mismo tiempo, estos factores, sumados a la pernocta que ofrece un anonimato operativo temporal y la posibilidad de camuflar el origen ilícito de fondos mediante el consumo suntuario, transforman a la infraestructura hotelera en un blanco atractivo para el lavado de activos, el financiamiento al terrorismo y la proliferación de armas de destrucción masiva (LC/FT/FPADM).

Por ende, el sector ya no puede ser evaluado únicamente desde la perspectiva del servicio hospitalario, sino como un eslabón crítico en la seguridad financiera global.

En el contexto venezolano, el Estado ha fortalecido sus mecanismos de control mediante la promulgación de la Resolución 020, publicada en la Gaceta Oficial N° 42.106 el 14 de abril de 2021.

Esta norma prudencial rectora se erige como el marco jurídico especializado que regula los Sistemas Integrados de Administración de Riesgos (SIAR) en el sector turismo, categorizando formalmente a los prestadores de servicios de alojamiento como Actividades y Profesiones No Financieras Designadas (APNFD).

Bajo este paraguas regulatorio, las empresas de hospedaje asumen una estricta posición de garante, la cual recae directamente sobre su representante legal. Esta condición ontológica y jurídica las obliga a implementar políticas de debida diligencia intensificada, estructuras de monitoreo permanente a través del oficial de cumplimiento y un riguroso régimen de Reportes de Actividades Sospechosas (RAS) ante la Unidad Nacional de Inteligencia Financiera (UNIF).

Así, la inobservancia de los indicadores de riesgo deja de ser una simple falta administrativa para convertirse en una brecha de seguridad con severas implicaciones jurídicas para la organización.

Ante este complejo escenario regulatorio y operativo, surgen las siguientes interrogantes: ¿De qué manera la adopción de la Hotelería 4?0 y sus herramientas disruptivas puede mitigar los riesgos de LC/FT/FPADM en el sector turismo? ¿Son capaces la Inteligencia Artificial, el Big Data y el Blockchain de transformar el cumplimiento normativo de un esquema reactivo tradicional a un sistema predictivo eficiente sin ralentizar la inmediatez del servicio hotelero? Y, fundamentalmente, ¿cómo se redefine la posición de garante y el rol supervisor del Oficial de Cumplimiento frente a una automatización avanzada de los controles y las señales de alerta?

Frente a estas cuestiones, se plantea la tesis de que la adopción de la Hotelería 4.0 no debe ser concebida meramente como una estrategia de optimización comercial o de experiencia del cliente.

Por el contrario, la transformación digital representa el soporte operativo indispensable y obligatorio para la viabilidad práctica del Enfoque Basado en Riesgo (EBR) exigido por la Resolución 020. La capacidad de procesar masivamente datos transaccionales en tiempo real, identificar patrones de conducta atípicos a través de algoritmos predictivos y automatizar la debida diligencia digital es la única vía para que el SIAR sea verdaderamente proporcional a la complejidad y volumen de las operaciones del sujeto obligado.

Con base en la premisa anterior, el presente ensayo tiene como objetivo general analizar las herramientas tecnológicas disruptivas de la Hotelería 4.0 que optimizan la gestión del Oficial de Cumplimiento y de la Asesoría Jurídica Integral en la tramitación administrativa, preventiva y jurisdiccional del hotel.

A saber, se busca demostrar cómo la automatización de alertas, el análisis predictivo y el uso regulado de registros digitales no solo blindan jurídicamente a la empresa frente a sanciones institucionales, sino que dotan a la representación legal y a la Unidad de Prevención y Control (UPC) de un soporte probatorio robusto, auditable y transparente.

Por todo lo expresado, el estudio se abordará desde una metodología analítico-documental, tamizada por una profunda reflexión axiológica que sitúa a la tecnología como el instrumento idóneo para materializar los valores éticos de transparencia, integridad y responsabilidad social en el entorno empresarial contemporáneo.

La Hotelería 4.0 como soporte del Enfoque Basado en Riesgo

Ante las exigencias del marco normativo y la sofisticación de los delitos financieros, los métodos tradicionales de control manual resultan obsoletos, ineficientes y reactivos.

Es así como con el auge de las tecnologías emergentes, la inteligencia artificial (IA) ha comenzado a desempeñar un papel crucial en la mejora de la experiencia del viajero y en el fortalecimiento de las medidas de seguridad. La combinación de IA y seguridad en el turismo está optimizando los procesos de gestión, personalización de servicios y prevención de riesgos en destinos turísticos y hoteles.[7]

Por consiguiente, frente a esta realidad, se plantea la tesis de que la adopción de la Hotelería 4.0 entendida como la convergencia de la interconexión, la automatización, la Inteligencia Artificial (IA), el Big Data y el Blockchain no debe ser concebida meramente como una estrategia de optimización comercial o de experiencia del cliente.

Por el contrario, la transformación digital representa el soporte operativo indispensable y obligatorio para la viabilidad práctica del Enfoque Basado en Riesgo (EBR) exigido por la Resolución 020.

Es por ello, que la capacidad de procesar masivamente datos transaccionales en tiempo real, identificar patrones de conducta atípicos a través de algoritmos predictivos y automatizar la debida diligencia digital es la única vía para que el SIAR sea verdaderamente proporcional a la complejidad y volumen de las operaciones del sujeto obligado.

[7] https://gsgbusinesshub.com/el-uso-de-la-inteligencia-y-seguridad-en-el-sector-turistico/

Herramientas tecnológicas para la gestión preventiva del hotel

Con base en la premisa anterior, el presente ensayo tiene como objetivo general analizar las herramientas tecnológicas disruptivas de la Hotelería 4.0 que optimizan la gestión del Oficial de Cumplimiento y de la Asesoría Jurídica Integral en la tramitación administrativa, preventiva y jurisdiccional del hotel.
Se busca demostrar cómo la automatización de alertas, el análisis predictivo y el uso regulado de registros digitales no solo blindan jurídicamente a la empresa frente a sanciones institucionales, sino que dotan a la representación legal y a la Unidad de Prevención y Control (UPC) de un soporte probatorio robusto, auditable y transparente.
El estudio se abordará desde una metodología analítico-documental, tamizada por una profunda reflexión axiológica que sitúa a la tecnología como el instrumento idóneo para materializar los valores éticos de transparencia, integridad y responsabilidad social en el entorno empresarial contemporáneo
Para dar cumplimiento efectivo al Enfoque Basado en Riesgo exigido por la Resolución 020, la Hotelería 4.0 se fundamenta en tres pilares tecnológicos transversales.
Estas herramientas no operan de forma aislada, sino que se integran para transformar el sistema preventivo de una estructura reactiva a un ecosistema predictivo y blindado:

Pilar 1. La Inteligencia Artificial (IA) y Machine Learning

La Inteligencia Artificial constituye el cerebro analítico del sistema de prevención del hotel. A diferencia de los sistemas tradicionales basados en reglas fijas, los algoritmos de *Machine Learning* (aprendizaje automático) poseen la capacidad de aprender continuamente del comportamiento histórico y cotidiano del establecimiento.
Para Quintana (2026)

> La irrupción de la inteligencia artificial no es simplemente una evolución tecnológica más: representa un cambio de paradigma que afecta a cada eslabón de la cadena de valor turístico, desde la planificación del viaje hasta el regreso a casa del viajero, pasando por cada momento de la experiencia en destino. En 2024, el mercado global de IA aplicada al turismo superó los 11.000 millones de dólares, y las proyecciones apuntan a que alcanzará los 45.000 millones en 2030, con una tasa de crecimiento anual compuesto cercana al 25% (p.3)

Esta cita evidencia de manera contundente el carácter disruptivo y la escala macroeconómica de la transformación digital, validando empíricamente la tesis del ensayo al demostrar que la Inteligencia Artificial no es una herramienta accesoria, sino una metamorfosis estructural que redefine de extremo a extremo la ontología del sector.

Desde una perspectiva analítica, el hecho de que el mercado global de la IA aplicada al turismo proyecte un crecimiento geométrico de los 11.000 millones de dólares en 2024 a los 45.000 millones para el año 2030 confirma que la automatización y el procesamiento cognitivo de datos se han vuelto omnipresentes en la cadena de valor turística.

Para el ámbito del cumplimiento bajo la Resolución 020, este cambio de paradigma implica que el flujo transaccional y la pernocta en las empresas de alojamiento están irrevocablemente entrelazados con entornos digitales; por lo tanto, si la experiencia del huésped en el destino ya está enteramente mediada por la IA, el Sistema Integral de Administración de Riesgos (SIAR) del hotel está obligado a adoptar ese mismo estándar tecnológico para que el Enfoque Basado en Riesgo sea viable, permitiendo al Oficial de Cumplimiento supervisar un ecosistema digitalizado con herramientas de su misma velocidad y complejidad analítica.

Su aplicación práctica en el SIAR se despliega en dos frentes críticos:

a. Segmentación Dinámica: Clasifica automáticamente los niveles de riesgo de los huéspedes (Alto, Moderado, Bajo) en el momento del *check-in*, cruzando variables complejas de forma simultánea.

b. Detección de Anomalías Conductuales: Analiza patrones de consumo y transacciones en tiempo real. Si un huésped de perfil moderado realiza de manera repentina un pago fraccionado inusual o actividades que emulan tipologías conocidas de lavado, la IA congela administrativamente la alerta y notifica de inmediato a la Unidad de Prevención y Control (UPC), permitiendo una intervención temprana antes de que el sujeto abandone las instalaciones.
Es por esa razón, que la incorporación de la Inteligencia Artificial (IA) redefine la supervisión operativa al permitir un monitoreo transaccional dinámico que analiza el comportamiento del huésped de manera holística.
Como corolario, los sistemas basados en aprendizaje automático integran y cruzan variables clave como los patrones de consumo dentro de las instalaciones, la utilización de métodos de pago inusuales como el uso fraccionado de efectivo o transacciones atípicas con activos virtuales y la realización de reservas o cancelaciones consecutivas sin justificación aparente.
Al procesar estos datos en tiempo real, la IA puede detectar anomalías que pasarían desapercibidas bajo una revisión humana convencional, identificando conductas que se aparten del perfil transaccional habitual del cliente y segmentando los niveles de riesgo de forma automatizada

Pilar 2. Big Data y el Procesamiento de Señales de Alerta
El sector de alojamiento turístico genera diariamente millones de datos fragmentados a través de reservas web, consumos en restaurantes, registros de huéspedes, agencias de viaje interconectadas y pasarelas de pago.
La Big Data es la tecnología que permite recopilar, estructurar y procesar este volumen masivo de información a una velocidad inmediata.
a. Conexión con Listas de Control: Permite que el sistema compare instantáneamente los datos de identidad capturados biométricamente con bases de datos globales de Personas Expuestas Políticamente (PEP),

terroristas o sancionados internacionales (como las listas de la ONU u OFAC), sin ralentizar el servicio al cliente.

b. Modelos Predictivos: Al consolidar el historial de operaciones de toda una cadena hotelera o región, la analítica predictiva identifica tendencias delictivas emergentes o "reservas fantasmas" diseñadas para justificar ingresos ilícitos, dotando al Oficial de Cumplimiento de reportes estadísticos y científicos de alta fidelidad.

Para CESAE Business & Tourism School blog, la industria del turismo es una industria integral que involucra a varios sectores. Dado el diferente alcance de la aplicación de big data en diferentes sectores, el documento elige los seis sectores fundamentales de la industria del turismo para ilustrar la relación combinada entre big data y turismo.

Los seis sectores fundamentales incluyen la restauración turística, alojamiento, transporte, parque y ocio, compras y marketing.

Fuente: CESAE Business & Tourism School

El mapa conceptual estructurado ilustra la centralidad del *Big Data* como el núcleo articulador del sector turístico contemporáneo, ramificándose de manera transversal en seis dimensiones operativas: alojamiento, parques y ocio, compras, transporte, restauración y marketing.

Desde la perspectiva del Enfoque Basado en Riesgo exigido por la Resolución 020, cada una de estas dimensiones representa una valiosa fuente de recopilación de metadatos conductuales que alimenta el Sistema Integrado de Administración de Riesgos (SIAR).

Por ejemplo, las variables asociadas al "Alojamiento" (tipos de visitantes y hábitos) combinadas con los registros de consumo de "Restauración" o "Compras" (patrones de gasto suntuario) dejan de ser métricas puramente comerciales para transformarse en indicadores de gestión preventiva; al cruzar estos datos en tiempo real mediante la analítica masiva, el Oficial de Cumplimiento puede mapear el perfil transaccional integral del huésped, identificando señales de alerta dinámicas e inusuales que denotan tipologías complejas de LC/FT/FPADM, lo que demuestra que la interconexión de todo el ecosistema hotelero que expone la imagen es el soporte operativo idóneo para garantizar la posición de garante de la empresa turística.

Pilar 3. Blockchain y Criptoactivos

La tecnología de cadena de bloques (Blockchain) aporta un doble valor estratégico en el marco de la Resolución 020, abordando tanto la seguridad interna como las nuevas realidades financieras:

a. Trazabilidad Inalterable: Al registrar las auditorías de cumplimiento, las alertas emitidas y las decisiones de la UPC en una red descentralizada o bloques protegidos criptográficamente, se garantiza que los registros sean 100% inmutables. Ningún usuario interno puede borrar, modificar o encubrir una señal de alerta, sirviendo como un soporte legal irrefutable ante inspecciones de MINTUR o procesos jurisdiccionales liderados por la Asesoría Jurídica Integral del Prestador de Servicio Turístico (PST).

b. Monitoreo de Activos Virtuales: El artículo 50 de la Resolución 020 obliga a los PST expresamente a reportar transacciones relacionadas con activos virtuales (criptomonedas), al igual que la UNIF en su instructivo de efectivo y

activos virtuales. En donde las herramientas forenses de *Blockchain* permiten al hotel analizar el origen de las billeteras digitales de los huéspedes que pagan con estos métodos, verificando que los fondos no provengan de plataformas de mezcla (*mixers*) o mercados ilícitos, blindando así la posición de garante de la representación legal.

Para CESAE Business & Tourism School, el Blockchain en Turismo y Hoteleses representa:

> Específicamente para la industria del turismo y viajes, *blockchain* puede ofrecer estabilidad y seguridad frente a ataques cibernéticos, actividades maliciosas o pagos fraudulentos. Incluso puede ayudar a resolver muchos de los puntos débiles del turismo como la distribución, los programas de fidelización, los pagos, o el almacenamiento, acceso y privacidad de datos.
> Probablemente, el mayor impacto de *blockchain* en hoteles es su capacidad para saltarse intermediarios en la distribución, ya que brinda la libertad de publicar el inventario disponible sin los sistemas intermedios que agregan datos, lo que ahorra costos tanto para los proveedores como para los clientes finales

La cita revela el potencial disruptivo de la tecnología *Blockchain* en la reconfiguración operativa y de seguridad del sector turístico, lo cual se alinea perfectamente con la protección integral y la gestión de riesgos en las empresas de hospedaje.

Al ofrecer estabilidad e inmutabilidad frente a ciberataques, actividades maliciosas y pagos fraudulentos, la cadena de bloques se consolida como una infraestructura tecnológica idónea para blindar el almacenamiento, acceso y privacidad de los datos sensibles de los huéspedes.

Desde la perspectiva de la prevención de LC/FT/FPADM bajo la Resolución 020, esta capacidad de prescindir de intermediarios en los sistemas de distribución no solo representa un ahorro de costos operativos y comerciales, sino que otorga al hotel un control directo y sin filtros sobre la trazabilidad de su inventario y de los flujos financieros asociados a las reservas.

De este modo, al eliminar capas opacas de agregación de datos de terceros, la Asesoría Jurídica Integral y el Oficial de Cumplimiento disponen de una fuente de información primaria, transparente e inalterable, facilitando la identificación inmediata del origen de los fondos y de los beneficiarios finales de las transacciones en estricto cumplimiento de su posición de garante.

La Automatización de la Debida Diligencia del Cliente (DDC) y Sistemas Biométricos

La digitalización de los procesos de recepción marca el inicio de la transformación hacia la Hotelería 4.0, modificando la ontología del registro hotelero tradicional. El tradicional libro de huéspedes en papel o el llenado manual de fichas de ingreso resultan insuficientes ante las exigencias de supervisión actuales, pues facilitan la suplantación de identidad y el uso de documentación apócrifa.

La implementación de plataformas de *check-in* digital, complementadas con sistemas de reconocimiento biométrico (como el escaneo facial y la verificación dactilar), permite validar de forma unívoca la identidad del usuario antes de su ingreso físico a las instalaciones.

Este ecosistema tecnológico convierte la captura de datos en un proceso automatizado e inalterable, generando un registro digital robusto que sirve de fundamento para dar cumplimiento a las exigencias de identificación y archivo de información contenidas en el Manual NPPAR.

De la prevención reactiva a la detección predictiva en el ecosistema hotelero

El impacto más profundo de estas nuevas tecnologías radica en el cambio de paradigma operativo: la transición definitiva de una prevención reactiva hacia una detección eminentemente predictiva.

Tradicionalmente, la identificación de ilícitos en el sector turístico ocurría de manera tardía, posterior a la consumación del hecho o durante auditorías externas anuales. La analítica avanzada de datos permite anticiparse al riesgo, detectando las fases tempranas del lavado de activos y otros delitos conexos antes de que los fondos se integren plenamente en el flujo financiero del hotel. Esta capacidad predictiva fortalece la posición de garante de la empresa y proporciona a la Asesoría Jurídica e institucional herramientas clínicas y rigurosas para salvaguardar la responsabilidad administrativa, civil y penal de la representación legal ante los órganos de control.

La eficacia del Enfoque Basado en Riesgo depende de la integración técnica de las herramientas del hotel. En la Hotelería 4.0, esto se logra mediante la sinergia e interconexión directa de los programas ya mencionados y el sistema especializado de cumplimiento preventivo.

Esta vinculación en tiempo real garantiza que cada movimiento registrado en la recepción, bar, restaurante o eventos sea auditado automáticamente por los algoritmos de prevención.

De este modo, la Unidad de Prevención y Control (UPC) no trabaja de forma aislada, sino que se nutre directamente del flujo operativo del hotel, permitiendo al Oficial de Cumplimiento supervisar la integridad del ecosistema comercial sin interrumpir la experiencia de los huéspedes.

El artículo 5 de la Resolución 020 del año 2021 exige que el SIAR se adapte a la disponibilidad tecnológica del sujeto obligado para garantizar el control de riesgos. La integración automatizada genera una bitácora inalterable y una trazabilidad completa de todas las operaciones realizadas.

Cada consulta, alerta emitida, perfil modificado o transacción procesada deja una huella digital auditable. Esta inmutabilidad de los registros digitales representa el soporte técnico y legal indispensable para que la Asesoría Jurídica Integral y la representación legal respondan de forma expedita ante los requerimientos de los órganos de control, fiscalización o las autoridades jurisdiccionales.

Contar con un expediente tecnológico blindado disminuye de manera drástica la discrecionalidad o el error humano, protegiendo a la empresa de sanciones administrativas por debilidades en el resguardo de información.

Reporte de Actividades Sospechosas (RAS) mediante evidencias digitales sólidas

De acuerdo con el Artículo 47 de la norma prudencial, el Oficial de Cumplimiento remite el Reporte de Actividad Sospechosa (RAS) a la UNIF una vez calificado el caso. La integración tecnológica de los sistemas optimiza drásticamente este proceso de sustanciación.

En lugar de basar el reporte en presunciones o análisis manuales dispersos, el Oficial de Cumplimiento puede adjuntar evidencias digitales sólidas: gráficos de comportamiento transaccional del cliente, registros biométricos de identidad verificados, alertas inalterables del sistema y la trazabilidad exacta de los métodos de pago empleados, incluyendo activos virtuales.

Estas pruebas tecnológicas blindan la calidad del RAS, aportando valor científico a la inteligencia financiera nacional y garantizando que el hotel cumpla con su posición de garante de manera irrefutable.

Desafíos de la Hotelería 4.0

En primer lugar, la migración hacia un ecosistema de Hotelería 4.0 no está exenta de fricciones internas, siendo la resistencia al cambio uno de los principales obstáculos en el personal de primera línea (recepción, reservas, alimentos y bebidas amas de llave).

Esta percepción puede generar omisiones deliberadas o desvíos en el uso de los sistemas, abriendo vulnerabilidades en el SIAR. Para mitigar este riesgo, deben estructurar una transición progresiva, demostrando empíricamente que la tecnología no busca sustituir su labor ni burocratizar el servicio, sino blindar operativamente al trabajador frente a las sofisticadas metodologías de fraude e infiltración de la delincuencia organizada.

Por consiguiente, superar los desafíos técnicos y operativos exige el diseño de programas de formación bajo un riguroso enfoque andragógico, reconociendo que la instrucción a adultos profesionales requiere metodologías horizontales, prácticas y altamente participativas.

Así las cosas, de acuerdo con las exigencias del marco regulatorio, esta capacitación no puede limitarse a la enseñanza mecánica de un software; debe incorporar de manera transversal y obligatoria la ética, los valores institucionales y la concientización sobre el riesgo.

En definitiva, en la era digital, el talento humano debe comprender de forma reflexiva que las herramientas de Inteligencia Artificial y el análisis de Big Data actúan como aliados estratégicos para la eficiencia del hotel, pero el ser humano conserva la irremplazable responsabilidad de supervisar, interpretar las alertas y tomar las decisiones preventivas finales.

Por último, el fortalecimiento de la cultura de prevención garantiza que el personal operativo asuma su rol como la primera y más importante línea de defensa de la organización.

Reflexiones Finales

La transición hacia la Hotelería 4.0 no constituye un lujo corporativo, sino el único mecanismo viable en el entorno contemporáneo para conciliar la agilidad transaccional del servicio de hospedaje con la rigurosidad del control de LC/FT/FPADM exigido por la Resolución 020.

Por consiguiente, la dinámica del turismo moderno demanda inmediatez, fluidez y una experiencia de usuario libre de fricciones burocráticas; pretender alcanzar estos estándares mediante metodologías manuales de control genera un riesgo operativo inaceptable o la parálisis comercial del sujeto obligado.

Del mismo modo, la automatización el análisis de datos masivos y la generación inalterable de alertas permiten que la supervisión preventiva ocurra de forma simultánea al flujo del negocio.

De este modo, las herramientas tecnológicas disruptivas resuelven la falsa dicotomía entre la eficiencia comercial y la seguridad financiera, permitiendo que el establecimiento actúe eficazmente en su condición de APNFD sin menoscabar los estándares de hospitalidad.

De hecho, el éxito del Sistema Integral de Administración de Riesgos (SIAR) automatizado descansa sobre un estricto balance de roles, donde se delimitan con precisión las capacidades técnicas y las facultades humanas.

A saber, las nuevas tecnologías poseen la capacidad de procesar masivamente la data transaccional, identificar patrones atípicos y cruzar información con listas restringidas en tiempo real, superando por completo los límites de la revisión manual.

No obstante, la inteligencia artificial carece de la ponderación jurídica y el criterio contextual necesarios para dictaminar la intencionalidad delictiva. Por lo tanto, la tecnología procesa la data, pero el juicio analítico del Oficial de Cumplimiento y el respaldo estratégico de la Asesoría Jurídica Integral son los que garantizan la eficacia legal de la estructura ante requerimientos institucionales y jurisdiccionales.

En suma, el talento humano ejerce la dirección conceptual y la toma de decisiones finales, asegurando que la herramienta tecnológica sea un potenciador de la justicia y no un mero automatismo vacío.

Finalmente, un análisis axiológico del cumplimiento integral nos obliga a reconocer que el blindaje tecnológico no debe ser catalogado como un simple gasto operativo o un formalismo administrativo impuesto por el Estado. Por el contrario, representa una inversión estratégica de alto nivel que protege el activo más valioso de la organización: su reputación institucional.

De modo que, un mercado global interconectado, la infiltración de la delincuencia organizada destruye la confianza comercial y acarrea severas consecuencias punitivas para la representación legal.

En conclusión, asumir las herramientas de la Hotelería 4.0 bajo los lineamientos de la Resolución 020 es una manifestación corporativa de responsabilidad y ética, ya que anteponer los valores de transparencia, legalidad e integridad sobre el beneficio económico desregulado, el sector hotelero trasciende la visión puramente utilitaria, transformando la prevención en un pilar de sostenibilidad empresarial y en un compromiso activo con la defensa del ordenamiento jurídico nacional

Bibliografía

https://www.cesae.es/blog/big-data-en-turismo-aplicaciones-practicas-actuales-y-futuras

Normativa Sobre la Administración y Fiscalización de los Riesgos relacionados con los delitos de Legitimación de capitales, Financiamiento al Terrorismo, Financiamiento a la Proliferación de armas de destrucción Masiva (LC/FT/FPADM y otros ilícitos aplicables a los prestadores de servicios turísticos Gaceta Oficial 42.106 de fecha 14 de abril de 2021

Quintanilla A. (2026) Inteligencia artificial en el turismo y sus desafíos reguladores. Documento en línea https://www.researchgate.net/publication/405844679_Inteligencia_artificial_en_el_turismo_y_sus_desafios_regulatorios#read (consultado: junio 2026, 17)

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

DE LA CONFIANZA ANCESTRAL AL ALGORITMO: LA EVOLUCIÓN DE LOS SISTEMAS INFORMALES DE TRANSFERENCIA DE VALOR COMO LA HAWALA Y EL FEI CHIEN EN LA ERA DE LAS STABLECOINS Y LA MENSAJERÍA ENCRIPTADA

Autora: Dra. Silumerany Rodríguez
Facilitadora: MSc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

De la Confianza Ancestral al Algoritmo: La evolución de los sistemas informales de transferencia de valor como la Hawala y el Fei Chien en la era de las Stablecoins y la Mensajería Encriptada

Autora: Silumerany Rodríguez
Código ORCID: 0009-0000-7838-9720
Correo electrónico: silualex913@gmail.com

Resumen

El presente ensayo analiza la evolución operativa y los riesgos asociados a los Sistemas Informales de Transferencia de Valor (IVTS), específicamente la Hawala y el Fei Chien, en el contexto de la economía digital y los estándares internacionales de prevención de legitimación de capitales y financiamiento al terrorismo. Estos mecanismos milenarios, fundamentados tradicionalmente en redes de confianza mutua sin movimiento físico de divisas, han adoptado herramientas tecnológicas de vanguardia como aplicaciones de mensajería encriptada y activos virtuales estables (stablecoins), principalmente USDT en la red TRON. Esta hibridación digital ha resuelto sus limitaciones históricas de liquidez y velocidad, facilitando transacciones transfronterizas inmediatas que eluden los canales bancarios tradicionales y diluyen la trazabilidad de los fondos. Mediante un enfoque descriptivo y el análisis de tipologías internacionales recientes, se examina la vinculación técnica de las Recomendaciones 14, 15 y 16 del Grupo de Acción Financiera Internacional (GAFI) como el marco regulatorio idóneo para combatir el anonimato en estas plataformas. Se concluye que la modernización de estos sistemas exige una supervisión estricta a los Proveedores de Servicios de Activos Virtuales (PSAV) y un fortalecimiento de los mecanismos de cooperación internacional para mitigar su explotación por parte de organizaciones criminales transnacionales.

Descriptores: Sistemas Informales de Transferencia de Valor (IVTS); Hawala; Fei Chien; Criptoactivos; Stablecoins; Legitimación de Capitales; Financiamiento al Terrorismo.

Abstract

This essay analyzes the operational evolution and associated risks of Informal Value Transfer Systems (IVTS), specifically Hawala and Fei Chien, within the context of the digital economy and international standards for preventing money laundering and terrorist financing. These age-old mechanisms, traditionally based on networks of mutual trust without the physical movement of currency, have adopted cutting-edge technological tools such as encrypted messaging applications and stablecoins, primarily USDT on the TRON network. This digital hybridization has overcome their historical limitations of liquidity and speed, facilitating immediate cross-border transactions that bypass traditional banking channels and obscure the traceability of funds. Through a descriptive approach and an analysis of recent international typologies, the essay examines the technical relevance of Recommendations 14, 15, and 16 of the Financial Action Task Force (FATF) as the ideal regulatory framework for combating anonymity on these platforms. It is concluded that modernizing these systems requires strict oversight of Virtual Asset Service Providers (VASPs) and a strengthening of international cooperation mechanisms to mitigate their exploitation by transnational criminal organizations.

Descriptors: Informal Value Transfer Systems (IVTS); Hawala; Fei Chien; Cryptoassets; Stablecoins; Money Laundering; Terrorist Financing

Introducción

La coexistencia de la economía globalizada con métodos tradicionales de transferencia de valor ha generado un ecosistema financiero paralelo que desafía las fronteras de la supervisión estatal. Históricamente, los Sistemas Informales de Transferencia de Valor (IVTS), como la Hawala (término árabe para 'transferencia' o 'confianza') y el Fei Chien (término chino para 'dinero volador'), han operado durante siglos basándose en redes de confianza mutua, sin necesidad de movilizar dinero físico transfronterizo.

En la actualidad, estos sistemas experimentan una metamorfosis técnica al integrar aplicaciones de mensajería encriptada y activos digitales. Esta evolución representa un riesgo crítico para la estabilidad financiera, ya que, al

eludir las regulaciones bancarias tradicionales, los IVTS se vuelven altamente vulnerables a la explotación por parte de redes delictivas. Por ello, resulta imperativo someter a estos operadores informales a un registro formal que mitigue los riesgos de legitimación de capitales y financiamiento al terrorismo. Frente a esta sofisticación técnica, el marco regulatorio internacional coordinado por el Grupo de Acción Financiera Internacional (GAFI) enfrenta el reto apremiante de eliminar los puntos ciegos que facilitan el flujo de capitales ilícitos. Es allí donde radica la relevancia de este estudio, el cual se propone analizar la vinculación e interoperabilidad de las Recomendaciones del GAFI, evaluando cómo este bloque normativo busca someter a control a los Proveedores de Servicios de Activos Virtuales (PSAV) y desarticular las tipologías modernas de la 'cripto-hawala' y el 'fei chien digital'. El objetivo fundamental es examinar los desafíos dogmáticos y prácticos que las nuevas tecnologías imponen en la lucha contra la legitimación de capitales y el financiamiento al terrorismo en el siglo XXI."

Los Sistemas Informales de Transferencia de Valor (IVTS, por sus siglas en inglés)

Como punto de partida, el Grupo de Acción Financiera Internacional (GAFI), señala lo siguiente:

> Servicios de transferencia de dinero o valores (STDV) se refiere a los servicios financieros que involucran la aceptación de efectivo, cheques, otros instrumentos monetarios u otros depósitos de valor y el pago de una suma equivalente en efectivo u otra forma a un beneficiario mediante una comunicación, mensaje, transferencia o a través de una red de liquidación a la que pertenece el proveedor de MVTS. Las transacciones efectuadas por estos servicios pueden involucrar uno o más intermediarios y un pago final a un tercero, y pueden incluir cualquier método nuevo de pago. A veces estos servicios tienen lazos con regiones geográficas en particular y se describen usando una serie de términos específicos, incluyendo hawala, [hundi] y [fei-chen].

Mientras que, la Bolsa de Valores de Caracas (2025), indica lo siguiente:

> Los Sistemas Informales de Transferencia de Valor son mecanismos no convencionales empleados para mover dinero o activos entre diferentes ubicaciones, eludiendo los canales bancarios tradicionales.
> Estos sistemas surgieron como una respuesta a la escasez o inaccesibilidad de servicios bancarios convencionales en ciertas regiones, facilitando así las transacciones monetarias locales y las remesas internacionales.

Estos sistemas, se constituyen como mecanismos alternativos para transferir dinero o activos fuera del sistema bancario tradicional, utilizando redes de agentes de confianza para realizar pagos nacionales e internacionales, ofreciendo rapidez, anonimato y menor documentación, conllevando a altos riesgos de evasión y legitimación de capitales. Y tienen una raíz histórica y perpetuada en el tiempo, tal como lo señala Financial Crime Academy (2026)

> Las raíces del IVTS se remontan a más de 4.000 años, antes de los sistemas bancarios modernos. Estos sistemas han existido como un sistema alternativo y no oficial de remesas y banca durante siglos. Las operaciones de IVTS se pueden encontrar en varias regiones del mundo, conocidas por diferentes nombres, como hawala en el Medio Oriente y el subcontinente indio, fei ch'ien («dinero volador») en China, phoe kuan en Tailandia y el Mercado Negro de Intercambio de Pesos en América del Sur.
> El desarrollo histórico del IVTS refleja la necesidad de sistemas financieros alternativos en regiones donde los servicios bancarios tradicionales eran limitados o inaccesibles. Estos sistemas sirvieron como una forma para que las comunidades realizaran transacciones monetarias y facilitaran las remesas transfronterizas.
> Es importante tener en cuenta que los IVTS no son inherentemente ilegales, y muchas personas confían en estos sistemas para fines legítimos, como enviar remesas a familiares en otros países o realizar transacciones comerciales donde los servicios bancarios tradicionales son limitados. Sin embargo, las características de los IVTS, como su anonimato, su documentación limitada y la falta de supervisión formal, los hacen vulnerables a la explotación por parte de actores delictivos que buscan participar en actividades financieras ilícitas.
> Para hacer frente a los riesgos asociados con el IVTS, los reguladores y las organizaciones internacionales se han esforzado por regular y supervisar estos sistemas. Estas iniciativas tienen

como objetivo lograr un equilibrio entre la prevención de actividades financieras ilícitas y garantizar que las poblaciones desatendidas sigan teniendo acceso a los servicios financieros. El Grupo de Acción Financiera Internacional (GAFI) desempeña un papel importante en el establecimiento de normas internacionales y en la prestación de orientación sobre la lucha contra el blanqueo de capitales y la financiación del terrorismo a través del IVTS.

Estos sistemas operan a través de una red de intermediarios o corredores, utilizando como mecanismo de compensación, que primeramente el cliente entrega el dinero en efectivo a un agente en su país de origen, el cual notifica a su contraparte en el país de destino para que entregue un monto equivalente al destinatario final. Posteriormente, las deudas entre los agentes se saldan posteriormente mediante transferencias de bienes, oro, remesas comerciales o compensaciones de saldo mutuo, raramente moviendo dinero físico a través de las fronteras.

Diferencia y similitudes entre los IVTS ‘’Hawala y el Fei Chien’’

Operativamente, la Hawala y el Fei Chien son prácticamente idénticos en su condición de Sistemas Informales de Transferencia de Valor (IVTS). No obstante, difieren en su origen cultural, etimología y en el uso de ciertos instrumentos físicos:

- Origen Étnico y Terminología: El término Hawala, de raíz árabe (h-w-l), significa 'cambiar', 'transformar' o 'confianza', y es empleado principalmente en el sur de Asia y el Medio Oriente. Por su parte, Fei Chien es un término chino que se traduce literalmente como 'dinero volador'.*
- Uso de Instrumentos Negociables: Aunque ambos esquemas se basan en la fe mutua, difieren en sus métodos de autenticación. La Hawala pura carece de instrumentos negociables y depende de códigos abstractos o contraseñas simples entre el remitente y el destinatario. En contraste, el Fei Chien recurre históricamente al sistema 'Chop' (o

'banca Chiti'), el cual puede emplear un 'chit' (recibo, marca o prueba física) para validar el reclamo de los fondos.*

- Mecanismos de Liquidación: En ningún caso el dinero cruza físicamente las fronteras. Los corredores (conocidos como hawaladars en el sistema indio) liquidan sus posiciones mediante la compensación de deudas cruzadas utilizando bienes comerciales, acuerdos de propiedad o esquemas de 'Hawala inversa'. Ambos modelos operan al margen de la infraestructura bancaria formal, garantizando la disponibilidad de fondos en un rango de 6 a 12 horas."

En resumen, mientras que la Hawala se apoya estrictamente en códigos abstractos y la confianza en redes del sur de Asia y Oriente Medio, el Fei Chien es la versión china que históricamente ha podido incorporar marcas o recibos físicos (chits) para validar las transferencias dentro de sus redes comerciales

Beneficios del Uso de los Sistema

El uso de este mecanismo informal de transferencia de fondos destaca por las siguientes ventajas operativas y culturales, que impulsan su uso en diversas regiones, asociados principalmente al envío de remesas:

- Inmediatez: Las transacciones se completan de forma casi instantánea, usualmente en pocas horas, superando la lentitud de los procesos del sistema bancario tradicional.
- Eficiencia de costos: Al ofrecer comisiones notablemente más bajas que las entidades financieras convencionales, se consolida como una alternativa altamente económica.
- Alcance y accesibilidad: Funciona con éxito en regiones con infraestructura bancaria deficiente o nula, facilitando la inclusión financiera de comunidades desatendidas.
- Respaldado en la confianza: Su operatividad se fundamenta en relaciones interpersonales y de reputación mutua, lo que genera un entorno de seguridad y familiaridad para sus usuarios.

- Identidad cultural: Está profundamente arraigado en los hábitos de comunidades habituadas a los intercambios informales, lo que eleva la comodidad y aceptación del usuario.
- Versatilidad: Se adapta con facilidad a distintas divisas y volúmenes de dinero, respondiendo con flexibilidad a necesidades específicas.

Estos modelos no solo resuelven trabas logísticas, sino que fortalece la cohesión comunitaria a través de un sistema de confianza compartida, siendo una alternativa a evaluar frente a los canales de remesas tradicionales.

Riesgos y Desafíos en las Operaciones de los Sistemas

A pesar de sus ventajas, la naturaleza informal de este sistema conlleva riesgos estructurales y legales que deben gestionarse con precaución:

- Vulnerabilidad y fraude: La ausencia de un marco regulatorio formal puede ser explotada por intermediarios deshonestos, provocando pérdidas de capital.
- Volatilidad y liquidez: Estas redes suelen experimentar fluctuaciones imprevistas en la disponibilidad de ciertas divisas.
- Indefensión ante disputas: Al carecer de un organismo arbitral o recurso legal formal para reclamaciones, cualquier conflicto en la transacción es difícil de resolver.
- Implicaciones legales y de seguridad: El anonimato del sistema puede ser instrumentalizado para actividades delictivas, tales como la legitimación de capitales y el financiamiento al terrorismo.

Modernización Digital (Aplicable a Ambos)

La paradoja actual radica en que la tecnología, lejos de desplazar a estos sistemas ancestrales, los ha dotado de herramientas que eliminan las limitaciones geográficas del clearing (liquidación de saldos). Al integrar tokens estables como el dólar digital (USDT), la Hawala y el Fei Chien se han

consolidado como la infraestructura financiera en la sombra más eficiente del siglo XXI.

Mensajería Encriptada: Los operadores han sustituido medios históricos como el fax por aplicaciones con cifrado de extremo a extremo como WhatsApp, Telegram y Signal. Estas plataformas permiten el intercambio instantáneo de códigos de autenticación. Su privacidad intrínseca complementa la naturaleza anónima del sistema tradicional, dificultando la supervisión de las autoridades.

- Activos Digitales (Stablecoins): Las stablecoins resolvieron la mayor vulnerabilidad histórica de las redes informales: el descalce de liquidez. Cuando un operador en el país de origen registraba un volumen de envíos masivamente superior al de su contraparte, el saldo negativo resultante podía tardar semanas o meses en liquidarse mediante contrabando de oro o sobrefacturación comercial. La irrupción de activos como Tether (USDT), anclados 1:1 con el dólar estadounidense, transformó esta dinámica al actuar como el activo definitivo de liquidación en la sombra.

La migración masiva hacia la red TRON (estándar TRC-20) obedece a razones estrictamente financieras:

- Costos de transacción ínfimos: Comisiones fijas de entre 1 y 2 dólares, independientemente del volumen transferido.
- Velocidad de liquidación: El clearing entre intermediarios se ejecuta en menos de un minuto, eliminando la latencia del sistema SWIFT y las demoras de los esquemas tradicionales."

La tecnología blockchain se ha convertido en un complemento para ambos modelos debido a su seudonimato y descentralización, ya que los operadores utilizan estos activos para realizar liquidaciones transfronterizas inmediatas entre ellos, eludiendo las restricciones de los sistemas financieros convencionales

El uso de estas herramientas, evidencian como La "modernización digital" ha permitido a los operadores de Hawala y el Fei Chien integrar mensajería encriptada (Telegram, Signal, WhatsApp) reemplazando las reuniones físicas o llamadas telefónicas para transmitir las instrucciones, y las stablecoins (principalmente USDT en la red TRON, por sus bajísimas comisiones) han reemplazado o combinado los métodos tradicionales de liquidación entre los agentes.

Grupo de Acción Financiera Internacional (GAFI)

El bloque normativo del GAFI comparte un objetivo técnico unificado, eliminar los puntos ciegos y el anonimato en el movimiento global de capitales:

La Recomendación 14 del GAFI establece que los países deben exigir a todas las personas jurídicas que prestan Servicios de Transferencia de Dinero o Valores (STDV) que cuenten con una licencia o registro, y estén sujetas a sistemas de supervisión y monitoreo efectivos, esto con el objetivo principal de evitar que estas entidades sean utilizadas para legitimar capitales y financiar terrorismo (LC/FT).

Por su parte, La Recomendación 15 del GAFI exige a los países e instituciones financieras identificar, evaluar y mitigar los riesgos de Legitimación de Capitales y Financiamiento del Terrorismo (LC/FT) asociados al desarrollo de nuevas tecnologías, productos y prácticas comerciales, con especial enfoque en los activos virtuales (criptomonedas). Para lograrlo, impone obligaciones estrictas a los Proveedores de Servicios de Activos Virtuales (PSAV), como:

- Evaluación de riesgos previa: Antes de lanzar nuevos productos o tecnologías, las instituciones deben evaluar sus riesgos y aplicar un Enfoque Basado en Riesgo (EBR).
- Registro y Licenciamiento: Los PSAV deben estar debidamente regulados, licenciados o registrados en las jurisdicciones donde operan.

- Debida diligencia: Los proveedores de activos virtuales tienen las mismas obligaciones que los bancos tradicionales, como identificar y verificar la identidad de sus clientes.
- Regla de Viaje (Travel Rule): Deben recopilar y transmitir la información del originador y beneficiario en las transferencias de activos virtuales. Supervisión y sanción: Están sujetos a supervisión por parte de las autoridades competentes y enfrentan sanciones en caso de incumplimiento

Mientras que la Recomendación 16 del GAFI establece estándares internacionales sobre transparencia en los pagos y transferencias electrónicas, exigiendo a las instituciones financieras incluir información precisa sobre el ordenante (remitente) y el beneficiario en toda la cadena de pago, ayudando a las autoridades a rastrear fondos ilícitos y garantizando que los datos de las operaciones estén disponibles de forma inmediata para las Unidades de Inteligencia Financiera y autoridades fiscales/policiales, a los fines de combatir la legitimación de capitales y el financiamiento del terrorismo de manera eficaz

La vinculación de este bloque normativo es profunda porque comparten un mismo objetivo técnico: eliminar los puntos ciegos (el anonimato) en el movimiento global de capitales.

- **El puente tecnológico (R.15 + R.16):** La Recomendación 16 nació originalmente solo para los bancos, luego al aparecer las criptomonedas, el GAFI utilizó la Recomendación 15 para ordenar que esa misma lógica de control de los bancos se aplique obligatoriamente al ecosistema cripto. Esto dio origen a lo que hoy se conoce como la Crypto Travel Rule (Regla de Viaje), obligando a los exchanges de criptomonedas a cumplir las directrices informativas de la Recomendación 16.
- **La interoperabilidad financiera:** En el mundo real, los tres sistemas se tocan constantemente, por ejemplo, si una persona compra Bitcoin

en un exchange (R.15), luego retira sus ganancias mediante unatransferencia hacia su cuenta de banco tradicional (R.16), y finalmente le envía ese dinero en efectivo a su familia en otro país mediante una remesadora (R.14), el dinero habrá pasado por las tres normativas. El GAFI las vincula para garantizar que la identidad de ese usuario no se pierda en ninguna de las transiciones.

- **Enfoque Basado en Riesgo unificado:** Las tres exigen políticas de debida diligencia similares (identificación de identidad, monitoreo de transacciones sospechosas y reporte de actividades inusuales), sin importar si el dinero se mueve en billetes físicos, saldos bancarios o códigos de blockchain.

En este sentido, en un esquema ideal siguiendo los lineamientos del GAFI, la Recomendación 14 obliga a la Hawala y al Fei Chien a registrarse formalmente; la Recomendación 16 obliga a registrar quién envía y quién recibe el dinero y la Recomendación 15 a través de los PSAV autorizados monitorea para evitar que estos sistemas utilicen las criptomonedas como una vía de escape digital para mantenerse en el anonimato

Praxis Nacional

En Venezuela, aun cuando culturalmente no se identifiquen comunidades masivas que utilicen las denominaciones ancestrales de Hawala o Fei Chien, operativamente el territorio nacional se encuentra fuertemente impactado por la esencia de este fenómeno, puede verse materializado mediante fenómenos emergentes redes informales de remesas, casas de cambio irregulares, mercados clandestinos Over-The-Counter (OTC) y el uso masivo de monedas estables (stablecoins), principalmente USDT.

Esta praxis puede configurar, en primer término, el delito de intermediación financiera no autorizada ante la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN), quien norma todo lo referido a casas de cambio y empresas de tecnología financiera. Además, colisiona con el marco regulatorio de los activos virtuales, el cual establece que cualquier casa de

intercambio de criptoactivos y moneda Fiat, requiere de una licencia obligatoria emitida por la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP) para transar de forma legítima. Operar al margen de estas regulaciones y controles institucionales, eleva significativamente los riesgos de Legitimación de Capitales y Financiamiento al Terrorismo, delitos tipificados de manera autónoma en la Ley Orgánica Contra Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT).

Tipologías Modernas de Estudio

1.Caso: El desmantelamiento de la Red de Daren Li (2024-2025)

- -Tipología: El Fei Chien Digital y lavado de estafas cripto mediante empresas fachada y mercados OTC.
- -Reseña: El Departamento de Justicia de los EE. UU. (DOJ) arrestó y procesó a Daren Li, un ciudadano con doble nacionalidad (china y de San Cristóbal y Nieves), acusado de liderar una organización criminal transnacional que lavó más de 73 millones de dólares procedentes de fraudes criptográficos conocidos como "pig butchering" (matanza de cerdos).
- Modus Operandi:
- Captación informal: La red recolectaba fondos de víctimas en EE. UU. y los canalizaba de forma inmediata hacia billeteras de criptomonedas sin custodia controladas por la organización.
- El puente Fei Chien en la sombra: En lugar de enviar los fondos de forma directa a cuentas asiáticas lo que encendería alarmas de cumplimiento bancario, el capital se convirtió masivamente a USDT (Tether).
- Compensación espejo y dispersión: Los USDT se movían a cuentas en las Bahamas y luego se liquidaban a través de una compleja red de cuentas bancarias en mercados asiáticos utilizando empresas pantalla. Este uso de activos estables permitió que el valor "volara" de occidente

a oriente en minutos de manera invisible, replicando el esquema tradicional del Fei Chien pero automatizado en la blockchain.

-

2.Caso: Operación Karasu

- -Tipología: Banca clandestina internacional y blanqueo de capitales mediante el método Hawala combinado con criptoactivos.
- -Reseña: La Policía Nacional de España, en colaboración con EUROPOL y EUROJUST, desarticuló una de las redes criminales internacionales más poderosas de banca clandestina. La organización operaba sin controles financieros legales, prestando soporte económico a redes dedicadas al tráfico de seres humanos y tráfico de drogas. Publicitaban sus servicios en redes sociales para atraer a clientes y organizaciones criminales a nivel global. Se constató el movimiento de más de 5,5 millones de euros en solo tres meses, y el uso de una "dirección puente" que llegó a registrar operaciones por más de 21.000.000 de dólares.
- Modus Operandi: El entramado criminal funcionaba de manera coordinada a través de dos ramas étnicas diferenciadas bajo la dirección de un líder principal (hawaladar):
- Estructura y Dirección: El hawaladar central llevaba la contabilidad y designaba a coordinadores (brókers) de máxima confianza para gestionar las operaciones de manera oculta al sistema financiero corriente.
- La Rama Árabe (Recepción y Destino): Encargada de la gestión internacional, recibía el dinero en efectivo de los clientes en distintos puntos del mundo y solicitaba su entrega en España. Posteriormente, reinvertían las comisiones obtenidas en otras actividades ilícitas (como el tráfico de migrantes).
- La Rama China (Provisión y Distribución): Actuaban como los proveedores del efectivo en España, tras recibir la orden de la rama

árabe, utilizaban a miembros que operaban como "mulas" para transportar grandes sumas de dinero ocultas en vehículos y entregarlas en mano a los clientes finales por todo el territorio nacional.

- Compensación e Inversión con Criptomonedas: Para liquidar los saldos y deudas entre ambas ramas sin levantar sospechas ni mover dinero físico a través de fronteras, la rama china recibía su compensación económica mediante el uso de criptodivisas.

Como se puede apreciar con el Caso de Daren Li (Fei Chien), la digitalización permite que el Fei Chien ya no se use únicamente para evadir controles de capitales de ciudadanos comunes, sino como una herramienta de escala industrial para blanquear el cibercrimen global. Mientras que con el caso Operación Karasu, lejos del tradicional que dependía de la vecindad comunitaria; este entramado criminal funcionaba de manera coordinada a través de dos ramas étnicas diferenciadas bajo la dirección de un líder principal (hawaladar).

Conclusiones Reflexivas

Los Sistemas Informales de Transferencia de Valor (IVTS), lejos de desaparecer ante la modernización bancaria, han experimentado una sofisticación técnica acelerada, al integrar aplicaciones de mensajera encriptada (WhatsApp, Telegram) y activos virtuales de liquidación inmediata (USDT en la red TRON), la Hawala y el Fei Chien han eliminado sus limitaciones históricas de tiempo y descalce de liquidez, consolidando una infraestructura financiera en la sombra altamente eficiente y de escala industrial.

Siendo asi, el carácter anónimo, transfronterizo y descentralizado de estos sistemas híbridos digitalizados los convierte en herramientas atractivas no solo para el envío de remesas legítimas, sino para la legitimación de capitales provenientes de delitos de vanguardia como el cibercrimen (estafas de pig

butchering) y delitos transnacionales tradicionales como el tráfico de drogas y la trata de personas.

Por tanto, el bloque normativo del GAFI, integrado por las Recomendaciones 14 (licenciamiento/registro), 15 (nuevas tecnologías y PSAV) y 16 (transparencia y Regla de Viaje), ofrece un andamiaje robusto en el plano teórico para mitigar el anonimato. Sin embargo, la velocidad operativa de los Hawaladars digitales y la naturaleza pseudoanónima de las redes peer-to-peer (billeteras sin custodia) imponen desafíos de supervisión colosales para las Unidades de Inteligencia Financiera y los reguladores tradicionales.

En consecuencia, resulta imperativo tomar acciones continuas y con focalización permanente en:

- Exigir a los Proveedores de Servicios de Activos Virtuales (PSAV) y exchanges un monitoreo riguroso y en tiempo real de las transferencias salientes hacia billeteras autocustodiadas (unhosted wallets), asegurando que se recopile y transmita la información requerida del originador y del beneficiario conforme a la Recomendación 15 y 16 del GAFI.
- Fomentar la Cooperación Internacional e Intercambio de Información Transfronteriza: Al tratarse de redes que mueven capitales de manera invisible entre diferentes jurisdicciones (como el flujo de occidente a oriente en el caso del Fei Chien Digital o la articulación de ramas étnicas en la Hawala combinado con criptoactivos), es indispensable robustecer los canales de asistencia legal mutua y el intercambio expedito de inteligencia financiera, garantizando el rastreo oportuno de los flujos ilícitos antes de que se pierda la trazabilidad de los fondos en entornos Web3 descentralizados.
- Incentivar a que las Unidades de Inteligencia Financiera y los sujetos obligados migren de una supervisión retrospectiva a un modelo de monitoreo predictivo y en tiempo real, ya que la sofisticación y velocidad

con la que operan la 'cripto-hawala' y el 'fei chien digital' superan las capacidades del cumplimiento tradicional

- Instar a la banca tradicional y a las agencias formales de remesas a calibrar sus sistemas de alerta temprana para detectar patrones sospechosos de movimientos de fondos en cuentas espejo, los cuales suelen ser utilizados por operadores informales para la compensación de deudas de la Hawala o el Fei Chien.
- Diseñar mecanismos atractivos o simplificados para la formalización y registro de los operadores informales de remesas de acuerdo con la Recomendación 14, al tiempo que se endurecen las sanciones administrativas y penales contra los intermediarios que ejecuten la actividad de STDV en la clandestinidad absoluta.
- Fomentar que las autoridades competentes y Unidades de Inteligencia Financiera se doten de tecnologías analíticas especializadas en cadenas de bloques para rastrear "direcciones puente" y flujos masivos en la red TRON (TRC-20), permitiendo a detección de flujos de capitales a gran escala antes de que los fondos sean dispersados en el sistema bancario mediante empresas pantalla.

Referencias

Bolsa de Valores de Caracas (2025). Información de Cumplimiento: ¿Qué son los Sistemas Informales de Transferencia de Valor (SITV) y cuál es su relación con el lavado de dinero? Disponible en: https://www.bolsadecaracas.com/informacion-de-cumplimiento-que-son-los-sistemas-informales-de-transferencia-de-valor-sitv-y-cual-es-su-relacion-con-el-lavado-de-dinero/

Cointelegraph (2025). Transacciones hawala habilitadas para criptomonedas: implicaciones legales y regulatorias. Binance Square. Disponible en: https://www.binance.com/es/square/post/20567810370001

Financial Crime Academy (2026). Canales de dinero poco ortodoxos: análisis de los sistemas informales de transferencia de valor. Disponible en:

https://financialcrimeacademy.org/es/canales-de-dinero-poco-ortodoxos-analisis-de-los-sistemas-informales-de-transferencia-de-valor/

Financial Crime Academy (2026). Descifrando el código: Entendiendo las complejidades de las redes Hawala. Disponible en: https://financialcrimeacademy.org/es/descifrando-el-codigo-entendiendo-las-complejidades-de-las-redes-hawala/

Grupo de Acción Financiera Internacional (GAFI). Las 40 Recomendaciones del GAFI. Disponible en: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Office of Public Affairs / U.S. Department of Justice (2026). Un hombre fue condenado a 20 años de prisión por su participación en una estafa global de inversión en criptomonedas por valor de 73 millones de dólares. Disponible en: https://www-justice-gov.translate.goog/opa/pr/man-sentenced-20-years-prison-role-73-million-global-cryptocurrency-investment-scam?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Ministerio del Interior del Gobierno de España (2025). La Policía Nacional desarticula uno de los principales entramados criminales que actuaba como una banca clandestina por el método hawala. Disponible en: https://www.interior.gob.es/opencms/eu/detalle/articulo/La-Policia-Nacional-desarticula-uno-de-los-principales-entramados-criminales-que-actuaba-como-una-banca-clandestina-por-el-metodo-hawala/

PayPilot (2025). Cómo funcionan Hawala y los sistemas de pago OTC tradicionales. Disponible en: https://www.paypilot.org/es/como-funcionan-hawala-y-los-sistemas-de-pago-otc-tradicionales/

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

LA EXTINCIÓN DEL OFICIAL DE CUMPLIMIENTO ANTE EL NACIMIENTO DE LOS AGENTES DE INTELIGENCIA ARTIFICIAL

Autor: Dra. Kimlen Chang de Negrón
Facilitadora: MSc Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

La Extinción del Oficial de Cumplimiento ante el Nacimiento de los Agentes de Inteligencia Artificial

Autora: Kimlen Chang de Negrón
Código ORCID: 0009-0003-7046-9103
Correo electrónico: eyknegrón@gmail.com

Resumen

El presente ensayo analiza la transición operativa del Oficial de Cumplimiento (OC) frente a la irrupción de los agentes de inteligencia artificial (IA) autónoma en el ámbito de la prevención de la legitimación de capitales, el financiamiento al terrorismo y el financiamiento a la proliferación de armas de destrucción masiva (LC/FT/FPADM). En un contexto marcado por la ineficiencia de los sistemas tradicionales ante el volumen global de flujos ilícitos, el estudio evalúa si la IA ha dejado de ser una herramienta reactiva para convertirse en un sistema capaz de ejecutar flujos de trabajo completos. A través de un mapeo funcional basado en la Resolución 010-2025 de la SUDEBAN, se demuestra que la gran mayoría de las tareas del OC y la Unidad de Prevención y Control (UPCLC/FT/FPADM) son técnicamente susceptibles de automatización mediante agentes de IA. La investigación concluye que, si bien la tecnología permite una ejecución algorítmica continua y superior en precisión, la transformación definitiva hacia este modelo exige cambios necesarios en el marco normativo y en la estructura institucional. Esto implica que la figura del Oficial de Cumplimiento no desaparece, sino que cambia de un ejecutor de procesos administrativos a un arquitecto y auditor de sistemas inteligentes, cuya validez depende de la adaptación legal que reconozca la trazabilidad técnica y la gobernanza algorítmica como garantías suficientes para la responsabilidad institucional.

Palabras clave: Oficial de Cumplimiento, Agentes de Inteligencia Artificial, RegTech, Prevención de LC/FT, Automatización, Gobernanza Algorítmica, Resolución 010-2025.

Abstract

This essay analyzes the operational transition of the Compliance Officer (CO) in the face of the emergence of autonomous Artificial Intelligence (AI) agents within the field of Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CFT/CPF). In a context marked by the inefficiency of traditional systems against the global volume of illicit flows, this study evaluates whether AI has ceased to be a reactive tool and has become a system capable of executing complete workflows. Through a functional mapping based on SUDEBAN's Resolution 010-2025, it is demonstrated that the vast majority of tasks within the Prevention and Control Unit (UPCLC/FT/FPADM) are technically susceptible to automation through AI agents. The research concludes that, while technology allows for continuous algorithmic execution with superior precision, the definitive transformation toward this model requires necessary changes in the regulatory framework and institutional structure. This implies that the role of the Compliance Officer does not disappear, but rather undergoes a metamorphosis from an administrator of manual processes to an architect and auditor of intelligent systems, whose validity depends on legal adaptations that recognize technical traceability and algorithmic governance as sufficient guarantees for institutional responsibility.
Keywords: Compliance Officer, Artificial Intelligence Agents, RegTech, AML/CFT Prevention, Automation, Algorithmic Governance, Resolution 010-2025.

Introducción

El presente estudio busca analizar hasta qué punto los agentes de IA pueden reemplazar las funciones del Oficial de Cumplimiento (OC) y las unidades de administración de riesgo, en materia de prevención de legitimación de capitales, financiamiento al terrorismo y financiamiento de la proliferación de armas de destrucción masiva y otros ilícitos (LC/FT/FPADM/YOI). La relevancia del tema se enmarca en un contexto de creciente presión regulatoria. A nivel global, el gasto anual en cumplimiento supera los 200 mil millones de dólares; sin embargo, menos del 1% de los flujos ilícitos son incautados, lo que evidencia las profundas ineficiencias del sistema actual (RegTech Analyst, 2026).

La inteligencia artificial (IA) ha pasado a ser un motor esencial para fortalecer los sistemas de cumplimiento normativo en organizaciones que operan en entornos altamente regulados, como los sectores financieros. Ante la creciente

complejidad y volumen de la normativa actual, la IA brinda herramientas de vanguardia para enfrentar estos desafíos; por ejemplo, mediante algoritmos de aprendizaje automático (machine learning) es posible supervisar operaciones en tiempo real, logrando una detección mucho más eficaz y veloz de fraudes o actividades de legitimación de capitales que los métodos convencionales. De hecho, la adopción de estas tecnologías es acelerada, con cerca de una cuarta parte de las entidades bancarias europeas integrándolas ya en sus labores de cumplimiento (Salvador Lafuente, 2026). Más allá de la detección, la IA habilita una estrategia de gestión proactiva, permitiendo anticipar posibles incumplimientos y salvaguardar tanto la integridad operativa como la reputación de la empresa.

Sin embargo, esta transición tecnológica no está exenta de riesgos. La falta de transparencia en los procesos de decisión —lo que se denomina el fenómeno de la "caja negra"— puede generar desconfianza, mientras que el uso de datos históricos sesgados corre el peligro de institucionalizar errores o discriminaciones previas. Además, el manejo de ingentes cantidades de información exige una vigilancia extrema respecto a la ciberseguridad, la privacidad de los datos y la delimitación clara de responsabilidades legales ante las decisiones automatizadas (Salvador Lafuente, 2026).

La literatura revela un dilema entre el uso de la IA y la prevención de LC/FT, desviándose a menudo hacia cuestiones éticas secundarias sin resolver el núcleo operativo, es decir, cuál es la eficiencia de esta herramienta. Un aspecto recurrente es si estos sistemas podrán sustituir la "intuición" del OC, entendida como el juicio basado en la experiencia. No obstante, una dificultad central es que, tras realizar los procesos de investigación, el OC enfrenta el dilema de reportar una operación sospechosa ante las Unidades de Inteligencia Financiera (UIF). Ante esto, se hace imprescindible realizar un ejercicio, listando las tareas que ejerce el OC para determinar cuáles pueden ser delegadas a sistemas autónomos y cuáles requieren intervención humana.

I. De la Inteligencia Artificial a los Agentes de IA: Un cambio de paradigma operativo

Para abordar este problema, es necesario reconocer que la IA no es un campo estático, sino una disciplina que ha transitado por diversas etapas evolutivas (Russell & Norvig, 1995). Tradicionalmente, los sistemas de cumplimiento se limitaban a motores de reglas rígidas o modelos de machine learning (ML) orientados a asignar puntuaciones de riesgo. Estos sistemas genera alertas con tasas de falsos positivos superiores al 90-95%, consumiendo recursos en tareas administrativas (SymphonyAI, 2026).

La inteligencia artificial ha experimentado una evolución acelerada en las últimas décadas, transitando desde sistemas basados en reglas explícitas hasta arquitecturas capaces de aprender patrones a partir de enormes volúmenes de datos. En sus orígenes, los sistemas expertos dominaban el panorama: programas que codificaban el conocimiento humano en forma de reglas lógicas del tipo "si-entonces". Estos sistemas, aunque útiles en dominios muy acotados, resultaban frágiles ante cualquier situación no prevista por sus programadores.

La llegada del aprendizaje automático (machine learning) supuso un salto cualitativo. En lugar de programar explícitamente cada regla, los algoritmos comenzaron a inferirlas a partir de ejemplos. Es lo que popularmente conocemos con el uso de las redes neuronales[8], las cuales, tras décadas de

[8] Nota del Autor

Para la elaboración y revisión del presente trabajo se han utilizado diversas herramientas de inteligencia artificial con fines de apoyo analítico y operativo. Específicamente, se empleó Gemini (Google), DeepSeek y NotebookLM (Google) como asistentes para la verificación de fuentes bibliográficas, el contraste de datos técnicos y el soporte en la traducción de textos especializados. Estas herramientas han servido como apoyo en la organización de la información y para el entendimiento de términos técnicos; no obstante, todo el contenido, el análisis crítico, la estructura argumentativa y la validación de la veracidad de los datos técnicos presentados son responsabilidad exclusiva del autor, quien ha supervisado y corregido los resultados generados para asegurar la integridad académica del documento.

Las redes neuronales son un tipo de tecnología dentro de la inteligencia artificial inspiradas libremente en el funcionamiento del cerebro humano, diseñadas para aprender a reconocer patrones complejos a partir de grandes cantidades de datos. En lugar de recibir instrucciones programadas paso a paso, estas redes están formadas por múltiples capas de conexiones que ajustan su comportamiento mediante la práctica, permitiéndoles mejorar su precisión con

desarrollo, alcanzaron un punto de inflexión con la popularización del deep learning a partir de 2012, permitiendo el reconocimiento de imágenes, procesamiento del lenguaje natural y predicción de series temporales.

La última gran revolución ha sido la de los modelos de lenguaje de gran tamaño (LLMs, por sus siglas en inglés), como GPT, Claude, Deepseek o Gemini., por citar solo algunos. Estos modelos, han demostrado una capacidad sorprendente para generar lenguaje coherente, responder preguntas, resumir documentos e incluso razonar de manera rudimentaria. Han llevado la IA al gran público a través de interfaces conversacionales que cualquier persona puede utilizar con una simple barra de escritura.

Para el común de los usuarios, la inteligencia artificial se ha reducido en su imaginario a un asistente conversacional o a un generador de contenidos. Cuando una persona piensa en "IA", lo más probable es que imagine una ventana de chat donde escribe una pregunta y recibe una respuesta, o una herramienta que genera imágenes a partir de una descripción textual. Esta percepción, aunque comprensible, es limitada.

Hoy en día, en nuestro trabajo diario, usamos la inteligencia artificial principalmente como una herramienta pasiva y reactiva. Esto se ve claramente cuando le pedimos a herramientas como ChatGPT que redacte correos, nos resuma documentos o traduzca textos, o cuando dependemos de los asistentes de voz, como Siri o Alexa, para tareas sencillas como revisar el clima, poner alarmas o escuchar música. También dejamos que los algoritmos de plataformas como Netflix, Spotify o Amazon decidan qué contenido consumir, utilizamos correctores automáticos al escribir documentos y consultamos a la IA para obtener información que podríamos encontrar por nuestra cuenta. En resumen, dejamos que la tecnología haga el trabajo básico mientras nosotros simplemente reaccionamos a sus resultados. En todos estos casos, el patrón es el mismo: el humano inicia una interacción, formula

el tiempo para realizar tareas como identificar imágenes, traducir idiomas o predecir resultados, de forma similar a como una persona aprende por experiencia.

una solicitud explícita y el sistema responde de forma inmediata y acotada. La IA actúa como un oráculo que contesta preguntas o como un escriba que ejecuta órdenes simples. No hay proactividad, no hay planificación de tareas de múltiples pasos, no hay capacidad para interactuar con el entorno más allá de la propia interfaz conversacional.

Esta percepción ha llevado a subutilizar lo que la IA puede llegar a hacer. Muchos analistas y profesionales, al observar que los chatbots[9] cometen errores o "alucinan" información, concluyen que la IA es aún demasiado limitada para asumir responsabilidades significativas.

1. El cambio de paradigma: los agentes de inteligencia artificial

Frente a esta visión estática, emerge una nueva generación de sistemas que rompe por completo el molde del chatbot conversacional: los agentes de inteligencia artificial (también denominados agentic AI o simplemente agentes autónomos). Un agente de IA no es solo un programa al que le haces una pregunta y te responde. En realidad, es un sistema avanzado capaz de funcionar por su cuenta para resolver problemas complejos que puede: a) Observar su entorno: detectar qué está pasando a su alrededor o en el sistema donde trabaja; b) definir objetivos: entender qué resultado debe lograr: c) Planifica y actúa: diseña una serie de pasos y usa herramientas externas (como navegar por internet, usar una calculadora o manejar archivos) para cumplir su meta; d) Se adapta: Si algo no sale como esperaba, ajusta su plan según los resultados que va obteniendo.

[9] Los chatbots son programas de inteligencia artificial diseñados para simular una conversación humana, capaces de comprender y generar texto de manera natural. A diferencia de las respuestas automatizadas simples basadas en reglas fijas, estos sistemas utilizan modelos de lenguaje avanzados para analizar el contexto de lo que escribe el usuario, permitiéndoles mantener diálogos coherentes, responder preguntas complejas, redactar documentos o resolver dudas en tiempo real como si se estuviera interactuando con otra persona.

Para comprender la magnitud del cambio, resultan útiles las siguientes analogías:

Herramienta básica (IA tradicional): Es como una calculadora. El usuario introduce los datos, pulsa las teclas y obtiene un resultado. Sin entrada humana, no hay salida.

Agente de IA: Es como un aprendiz de investigador. Se le asigna una misión: "investiga a este cliente, recopila toda la información disponible en las bases de datos internas y en fuentes públicas, verifica si aparece en listas de sanciones, analiza su comportamiento transaccional de los últimos doce meses y, si encuentras algún indicio de anomalía, redacta un informe preliminar y prográmalo en la bandeja de entrada del Oficial de Cumplimiento". El agente no espera instrucciones paso a paso; él mismo descompone la tarea compleja en subtareas, decide qué herramientas utilizar en cada momento, ejecuta las consultas, procesa los resultados, y si se encuentra con un obstáculo (por ejemplo, una base de datos que no responde), intenta una estrategia alternativa.

2. Las capacidades distintivas de los agentes de IA

Lo que diferencia a un agente de IA de un simple chatbot se puede sintetizar en cuatro capacidades esenciales:

1. Autonomía. El agente no requiere que un humano le indique cada paso. Una vez definido el objetivo, el agente opera por sí mismo, tomando decisiones sobre el curso de acción sin intervención continua. Esto no significa que actúe sin supervisión, sino que es capaz de ejecutar flujos de trabajo completos con mínima intervención humana.
2. Uso de herramientas. Mientras que un chatbot solo puede generar texto, un agente puede interactuar con el mundo exterior. Puede consultar bases de datos, enviar correos electrónicos, actualizar registros en un sistema transaccional, llamar a APIs externas,

navegar por páginas web, extraer datos de documentos PDF, y un largo etcétera. El agente decide qué herramienta usar en cada momento y cómo interpretar los resultados obtenidos.

3. Planificación y memoria. Un agente es capaz de descomponer un objetivo complejo en una secuencia de pasos y de recordar los pasos ya ejecutados para no repetir tareas. Si el plan inicial falla, puede replantearlo dinámicamente. Por ejemplo, si al intentar consultar una base de datos descubre que no tiene los permisos necesarios, puede solicitar la elevación de privilegios o buscar una fuente alternativa de información.
4. Razonamiento y adaptación. Los agentes más avanzados incorporan mecanismos de razonamiento paso a paso (similares a las cadenas de pensamiento) que les permiten evaluar la coherencia de sus acciones intermedias y corregir el rumbo si se desvían del objetivo. No se limitan a ejecutar ciegamente un plan; lo monitorizan y lo ajustan conforme a la retroalimentación del entorno.

3. Implicaciones del cambio: del "usuario que pregunta" al "supervisor que delega"

Hoy, la tecnología ha avanzado hacia una nueva etapa: los agentes de inteligencia artificial o agentic AI. A diferencia de la IA tradicional, que procesa datos de forma pasiva, los agentes representan una evolución hacia la agencia. Un agente es un sistema autónomo capaz de ejecutar tareas complejas de múltiples pasos, utilizando memoria y herramientas para automatizar flujos de trabajo (ComplyAdvantage, 2025). Mientras que los bots[10] tradicionales ejecutan reglas fijas, los agentes de IA toman decisiones,

[10] Los bots son programas informáticos diseñados para ejecutar tareas automatizadas y repetitivas de forma autónoma, sin necesidad de intervención humana constante. Mientras que algunos bots realizan funciones técnicas de fondo —como indexar páginas web para buscadores o monitorear precios—, otros interactúan directamente con las personas, como los chatbots que responden consultas, ayudando a agilizar procesos que, de otro modo, requerirían mucho tiempo y esfuerzo manual.

se adaptan y orquestan procesos completos. Siguiendo la evolución del campo, el agente de IA no es solo un "filtro", sino un investigador digital que recopila datos, revisa transacciones y redacta informes, reduciendo el tiempo de investigación hasta en un 60% (SymphonyAI, 2026).

La irrupción de los agentes de IA transforma radicalmente la relación entre el humano y la máquina. Anteriormente, el usuario era un operador que proporcionaba instrucciones detalladas y ejecutaba él mismo las acciones. En el nuevo paradigma, el usuario se convierte en un supervisor o gestor que define objetivos, establece límites y revisa resultados, mientras que la ejecución operativa recae en los agentes.

Retomando el ejemplo del cumplimiento normativo: con las herramientas básicas de IA, un analista debía extraer manualmente los datos de alertas, revisar uno por uno los listados de sanciones, buscar información en internet, redactar el informe y luego subirlo al sistema. La IA solo le ayudaba puntualmente (por ejemplo, sugiriendo una redacción). Con un agente de IA, el analista simplemente asigna la tarea: "investiga estas diez alertas prioritarias". El agente realiza todo el trabajo de investigación en paralelo, entrega los informes completos y solo solicita intervención humana cuando detecta un caso que supera un umbral de complejidad predefinido. El analista pasa de ser un "buscador de información" a ser un "evaluador de decisiones".

La mayoría de la población y, lo que es más preocupante, muchos profesionales y responsables institucionales, siguen pensando en la IA en términos de chatbots y asistentes conversacionales. Esta percepción, anclada en la experiencia cotidiana con herramientas básicas, oculta el verdadero potencial transformador de los agentes autónomos. Mientras se debate si un chatbot puede o no reemplazar a un empleado humano, los agentes de IA ya están empezando a realizar flujos de trabajo completos en los ámbitos financiero, logístico, legal y administrativo.

Comprender este cambio de paradigma es esencial para cualquier análisis serio sobre el futuro del trabajo, la regulación y la gobernanza de los sistemas inteligentes en materia de LC/FT/FPADM/YOI. No se trata de preguntarse si la IA "responde bien a las preguntas", sino de diseñar arquitecturas de supervisión para sistemas que actúan, deciden y aprenden en entornos reales. La revolución de los agentes de IA no está por venir: ya ha comenzado. Solo falta que la percepción común se ponga al día con la realidad tecnológica.

4. Metodología propuesta: Primero la función, luego la posibilidad del reemplazo

Frente a este avance, el presente estudio propone una metodología en tres fases que invierte las prioridades actuales. En primer lugar, se realizará un mapeo funcional exhaustivo de las tareas del OC. En segundo lugar, se evaluará la razonabilidad y susceptibilidad a la automatización dentro del contexto legal e institucional actual. Por último, analizaremos si las autoridades de supervisión y el sistema legal están preparados para estos cambios.

Investigaciones recientes han demostrado que es técnicamente viable desplegar agentes de IA para tareas como la debida diligencia inicial al cliente (onboarding), monitoreo continuo y ensamblaje de reportes de operaciones sospechosas (ROS), generando expedientes en minutos frente a las horas que requiere un humano (Copenhagen Business School, 2025). Instituciones que utilizan plataformas como Nasdaq Verafin han logrado reducir la carga de trabajo en más del 80% mediante estos "trabajadores digitales" (Nasdaq Verafin, 2025). Finalmente, tras este análisis, se abordará el "dilema final": si los agentes pueden asumir la investigación objetiva, ¿el humano retiene la responsabilidad legal y la "intuición" para la decisión de reporte? y cómo se enfrentan nuestros supervisores y la legislación a estos cambios frente a una responsabilidad individual y personal de los seres humanos.

II.
Las funciones del oficial de cumplimiento y Unidad de Prevención y Control. La capacidad de los agentes de inteligencia artificial para llevarlos a cabo.

1. Las Funciones del OC y la Capacidad de los Agentes de IA para ejecutarlas

Para avanzar en el propósito de este estudio, es fundamental trascender la visión limitada que reduce el Sistema Integral de Administración de Riesgos (SIAR) a funciones mecánicas como la verificación en listas o el monitoreo transaccional. Siguiendo el marco de la Resolución 010 de la SUDEBAN, a continuación, se presenta un mapeo funcional del Oficial de Cumplimiento (oc) y su Unidad (UPCLC/FT/FPADM), clasificándolas por su capacidad de ser automatizadas mediante agentes de IA.

Hemos adaptado las funciones establecidas en la Resolución 010-25 por considerarla la más avanzada y la que con mayor detalle establece las funciones del OC y su unidad técnica.

1.1. Funciones 1, 4, 6.3 y 6.9: diseño y actualización de políticas, procedimientos y el marco normativo interno (Diseño de Políticas, POA, PAC, PCSA y actualización de manuales)

Presente: El diseño de políticas y la planificación estratégica anual (POA, PAC, PCSA) son tareas que requieren una comprensión holística del negocio y de su apetito de riesgo. En el estado actual, un agente de IA puede asistir poderosamente en esta labor. Por ejemplo, puede analizar de forma autónoma nuevos cuerpos normativos (como la propia Resolución 010) y extraer obligaciones concretas para la entidad, identificando brechas con respecto al marco existente. También puede simular escenarios de riesgo para evaluar el impacto potencial de distintas configuraciones del POA y es posible pedirle que con base a las normas lleve a cabo las tareas de diseñar cualquiera de esos documentos.

Futuro: Un agente de IA verdaderamente autónomo podría generar propuestas de borradores de políticas basadas en los objetivos estratégicos de la Junta Directiva y en el perfil de riesgo de la institución, actualizando dinámicamente los manuales y otros documentos conforme a cambios en el entorno operativo o regulatorio. La decisión final sobre la aprobación de las políticas probablemente recaería siempre en la Junta Directiva, en virtud del principio de responsabilidad última, pero el ciclo de diseño, actualización y propuesta podría ser casi completamente automatizado.

1.2. Funciones 2, 5, 10, 11 y 14: supervisión, coordinación, auditoría de controles y ajuste de parámetros (Seguimiento de inspecciones, supervisión de la UPC, revisión de parámetros del SIAR y participación en comités)

Presente: La función de supervisión y coordinación es inherentemente una tarea de seguimiento de la ejecución de tareas predefinidas. Un agente de IA en su estado actual es excelente para monitorear el cumplimiento de los planes aprobados (POA, PAC). Puede, por ejemplo, verificar automáticamente la ejecución de las acciones correctivas derivadas de una inspección, o rastrear los avances del POA e informar de las desviaciones. Por otra parte, la función 11 (revisar parámetros y atributos del SIAR) es una tarea de análisis de datos casi ideal para un agente, que puede, con base en la evolución del entorno económico y las operaciones, recomendar ajustes a los umbrales de alerta y frecuencias de monitoreo de manera mucho más precisa que un humano.

Futuro: Un agente podría coordinar flujos de trabajo entre distintas áreas (por ejemplo, entre la UPC y RRHH para el diseño de capacitaciones, o con mercadeo para campañas de comunicación) sin intervención humana. Incluso podría participar en comités con derecho a voz, no a voto, aportando análisis y datos objetivos en tiempo real, plasmando sus opiniones en actas que cumplirían con el requisito de dejar constancia. La supervisión del 100% de las

sucursales y oficinas para verificar la aplicación de controles internos es una tarea para la que un agente está perfectamente dotado.

1.3. Funciones 3, 9, 13 y 8: representación, relaciones institucionales y respuesta a organismos (Comité de Riesgos, relaciones con Sudeban y UNIF, respuesta a solicitudes de información)

Presente: Un agente puede gestionar el flujo de información entrante y saliente con los organismos de control. Por ejemplo, puede analizar una solicitud de información de la UNIF, recopilar automáticamente los datos relevantes del SIAR, estructurar una respuesta preliminar y dejarla preparada para la revisión y firma del Oficial. También puede mantener una base de datos con todas las comunicaciones institucionales y generar alertas sobre plazos de respuesta.

Futuro: En un futuro, un agente podría emitir respuestas de tipo rutinario o informativo a requerimientos de organismos, siempre dentro de parámetros predefinidos y con pistas de auditoría completas. No obstante, las relaciones institucionales de alto nivel, la representación en foros internacionales y la participación en mesas de diálogo con el regulador —que implican un componente relacional y de posicionamiento estratégico no codificable— seguirán siendo competencia exclusiva del Oficial de Cumplimiento humano. La pregunta entonces es si en el futuro, estas actividades serán requeridas, toda vez que, si a su vez los supervisores avanzan hacia sistemas tecnológicos podríamos incluso considerar el intercambio de información entre el agente de IA del supervisor y los de los sujetos obligados.

Lo anterior evidencia que el potencial de delegación a un agente de IA es Medio-Alto en el aspecto operativo de recopilación y estructuración de respuestas, pero bajo en lo que se refiere a la representación institucional y las relaciones interpersonales de alto nivel, lo cual llevará a considerar que tan necesaria y útil es ese intercambio en una sociedad de la información completamente automatizada.

1.4. Funciones 6.1 a 6.11 (excepto 6.7 y 6.8): informes de gestión, análisis de tipologías y evaluación de nuevos productos (Nuevas políticas, tipologías delictivas, mejora de procesos, capacitación, EBR de nuevos productos y servicios, avances del POA y evaluación de gestiones delegadas en terceros)

Presente: El informe de gestión trimestral es una de las tareas más fácilmente automatizables mediante agentes de IA. Un agente puede procesar todos los datos del SIAR, extraer las estadísticas de alertas, calcular los avances del POA, recopilar las evidencias de las capacitaciones realizadas y generar un borrador completo del informe en lenguaje natural. Asimismo, la evaluación de nuevos productos y servicios bajo un Enfoque Basado en Riesgo (EBR) es una tarea que un agente puede realizar de manera exhaustiva y consistente, analizando las características de la innovación y cotejándolas con las tipologías de riesgo conocidas y el perfil de la entidad, tal y como lo demuestran actualmente los sistemas parametrizados que utilizan los bancos para la segmentación de clientes y otras contrapartes.

Futuro: La identificación de nuevas tipologías delictivas es el área más compleja dentro de este bloque. En su estado actual, un agente es mejor detectando patrones conocidos (el "modus operandi" tradicional) que descubriendo comportamientos delictivos completamente novedosos. Sin embargo, en un estado más avanzado, mediante técnicas de aprendizaje no supervisado y análisis de redes, podrá proponer al Oficial de Cumplimiento clusters de comportamiento anómalo que podrían constituir nuevas tipologías, actuando como un detector de señales débiles en el mar de datos. La recomendación final seguirá siendo humana.

En consecuencia, el potencial de delegación a un agente de IA es Muy Alto para la elaboración de informes y la evaluación EBR (90-95%). Medio para la detección de tipologías novedosas (el agente asiste y propone, el humano confirma y conceptualiza).

1.5. Función 7: la decisión final sobre el Reporte de Actividades Sospechosas (RAS) (Evaluar casos potenciales y decidir si se archiva, se reporta a la UNIF o se hace seguimiento)

Este es el núcleo de la responsabilidad del Oficial de Cumplimiento y el punto donde el debate sobre la automatización alcanza su máxima intensidad. Es también donde los argumentos de la "intuición" y la "ética" se emplean con mayor insistencia para desechar el uso de la IA.

Presente: La tecnología actual no permite delegar completamente la decisión de reporte. Un agente puede investigar el caso hasta un grado muy avanzado: puede recopilar toda la información del cliente, analizar el histórico transaccional, mapear las relaciones del cliente con otras entidades o personas, buscar en listas de sanciones y medios de comunicación adversos, y generar un expediente de investigación completo con una recomendación preliminar. Algunas implementaciones ya permiten reducir el tiempo de investigación de días a minutos y la tasa de falsos positivos. Sin embargo, la decisión final de reportar —un acto con potenciales consecuencias legales para la entidad y para el cliente— sigue siendo tomada por un humano, según el criterio de la industria y el regulador.

Futuro: A medida que los modelos se vuelvan más explicables y los reguladores acepten el "juicio algorítmico" bajo supervisión, es plausible que un agente pueda tomar la decisión final de reporte para una categoría de casos de riesgo bajo y medio, con reglas y umbrales predefinidos y aprobados. Para los casos de alto riesgo, el sistema podría elevar automáticamente la decisión a un Oficial humano, siguiendo un modelo de "escalamiento por excepción". La decisión final del agente vendría acompañada de una trazabilidad completa (qué datos usó, qué reglas aplicó, por qué ponderó unos factores sobre otros), ofreciendo un grado de transparencia muy superior al del razonamiento humano, que a menudo es difícil de documentar.

2. Funciones de la gerencia de la Unidad de Prevención y Control o de Administración de Riesgos

Tras analizar la Resolución 010-2025 de SUDEBAN, se evidencia que la totalidad de las funciones asignadas a la Gerencia de la UPCLC/FT/FPADM en el artículo 20, son susceptibles de ser ejecutadas mediante agentes de inteligencia artificial. Más allá de la simple automatización de procesos operativos (numerales 1, 2, 3, 5, 6, 8, 9), la evolución hacia una arquitectura de agentes autónomos permite que la IA asuma roles de gestión técnica, intercambio de información y representación. Estos agentes, dotados de capacidades cognitivas y de conectividad avanzada, pueden integrar flujos de datos interdepartamentales, gestionar comunicaciones estratégicas (4), ejecutar protocolos de capacitación ética automatizada (numeral 7), auditar el desempeño de terceros en tiempo real y presentar los informes (numeral 10) y participar en la planificación operativa junto a la Junta Directiva (numeral 11). Bajo esta premisa, incluso la función de representación legal ante la ausencia del Oficial de Cumplimiento (numeral 12) se vuelve una capacidad técnica ejecutable. Si el supervisor y el sujeto obligado operan bajo estándares de IA interconectados, la responsabilidad legal queda resguardada no por la presencia física de un humano, sino por la integridad del sistema, la trazabilidad de los algoritmos y la gobernanza de los datos. En este nuevo sistema, la función del Gerente de Cumplimiento trasciende la ejecución operativa para convertirse en un arquitecto y auditor de agentes, donde la eficacia del sistema y su cumplimiento auditable son la garantía última de la responsabilidad institucional, transformando el modelo tradicional de supervisión en un ecosistema de confianza tecnológica.

3. Funciones de las áreas de la Gerencia o Unidad de Administración de Riesgos

Tras haber establecido que las funciones de la Gerencia de la UPCLC/FT/FPADM son plenamente susceptibles de ser ejecutadas por agentes de Inteligencia Artificial —transformando el liderazgo del oficial en una

labor de arquitectura y auditoría de sistemas—, resulta imperativo examinar la viabilidad de esta automatización en las áreas operativas que conforman dicha unidad. Al aplicar esta misma tesis de delegación tecnológica, se evidencia que la estructura funcional definida en la Resolución 010-2025 puede ser operada íntegramente por agentes especializados, permitiendo que la prevención del riesgo pase de un modelo administrativo manual a un modelo de ejecución algorítmica continua.

3.1. Área de Análisis y Supervisión de Operaciones Financieras

Esta área es el escenario ideal para el despliegue de agentes de IA, ya que su núcleo reside en el procesamiento masivo de datos transaccionales. Los agentes autónomos pueden realizar el monitoreo continuo, detectar anomalías y aplicar la segmentación dinámica de clientes con una precisión superior a la humana (Artículo 22, numerales 1, 5, 6, 7). Asimismo, al operar bajo protocolos de conectividad inteligente, estos agentes pueden gestionar de forma automática las respuestas a órganos competentes (numeral 2) y administrar el control del Programa de Seguimiento (numerales 3, 4), automatizando la exclusión de alertas (numeral 8) basándose en perfiles de riesgo validados. En este modelo, el humano deja de "buscar" transacciones para pasar a auditar los criterios de detección que los agentes ejecutan en tiempo real.

3.2. Área de Prevención y Control de Riesgos de LC/FT/FPADM

La función de esta área puede evolucionar hacia un modelo de "gestión cognitiva" donde la IA no solo asiste, sino que dirige la administración de riesgos. Los agentes especializados pueden elaborar políticas, normas y procedimientos (Articulo 23 numeral 1) mediante el análisis de cambios normativos en tiempo real, garantizando la supervisión constante de las dependencias (numeral 2). La asignación de calificaciones de riesgo (numeral 3), la clasificación de factores (numeral 4) y la construcción técnica de la Valoración Basada en Riesgo (VBR) (numeral 5) se convierten -y en la práctica

así sucede ya en algunos sujetos obligados- en procesos algorítmicos autoejecutables. De igual forma, el rastreo de fuentes abiertas y nuevas tipologías (numeral 6) deja de ser una tarea manual intermitente para transformarse en un sistema de vigilancia proactiva, donde el agente correlaciona eventos globales instantáneamente para actualizar el perfil de riesgo del Sujeto Obligado.

3.3. Área de Estadística, Análisis Estratégico y Capacitación

Esta área es la que mejor ilustra la transformación de la gestión del conocimiento hacia la automatización. Los agentes de IA pueden diseñar programas de capacitación adaptativos (artículo 24 numerales 1, 2), generar contenido sobre nuevas técnicas delictivas (numeral 3) y gestionar la plataforma de aprendizaje (numeral 5) de forma personalizada para cada empleado. La carga operativa de mantener registros, estadísticas de notificaciones a la UNIF, calificaciones de capacitación y métricas de calidad de Archivos de Transmisión (numerales 4, 6, 7, 8) es resuelta de forma nativa por agentes que extraen, estructuran y reportan información sin intervención humana. Aquí, la labor estratégica consiste en supervisar que los agentes mantengan la integridad y oportunidad de la data, eliminando cualquier margen de error administrativo.

III. El Oficial de Cumplimiento ante la Era de la IA: ¿Un rol en extinción o en evolución?

Tras el análisis pormenorizado de las funciones que tradicionalmente desempeña el Oficial de Cumplimiento, emerge una constatación que, por su contundencia, no admite matices: la inmensa mayoría de sus tareas operativas son perfectamente delegables en agentes de inteligencia artificial, bien en su totalidad, bien en un porcentaje abrumadoramente elevado que supera el 90 % de su carga de trabajo rutinaria.

El núcleo operativo que permanece como reacio a la automatización se reduce a un conjunto mínimo y acotado de funciones críticas que, por su naturaleza estratégica, relacional o jurídica, exigen aún la intervención directa de un humano: la toma de decisiones finales en casos de alto riesgo reputacional o sistémico, la representación institucional ante el regulador y la validación última de los diseños estratégicos propuestos por los sistemas autónomos. Todo lo demás —monitorización de transacciones, análisis de patrones sospechosos, generación de reportes, actualización normativa, evaluación de riesgos operativos— es materia susceptible de ser ejecutada por algoritmos con mayor velocidad, menor coste, trazabilidad absoluta y, sobre todo, sin la fatiga ni los sesgos que afectan al juicio humano.

La pregunta que se impone es inquietante: si la tecnología ya está en condiciones de asumir lo sustancial del trabajo, ¿por qué seguimos manteniendo al humano en el centro de la operativa? La respuesta apunta a un obstáculo que no es tecnológico ni operativo, sino jurídico y, más concretamente, penal.

La necesidad de un "sujeto responsable" ante la ley ha sido históricamente el freno que ha justificado el mantenimiento de la intervención humana. El derecho penal —al menos en su configuración actual— exige un autor al que pueda atribuírsele una conducta típica, antijurídica y culpable. Y la doctrina dominante coincide en un punto: los entes artificiales inteligentes no son titulares de responsabilidad penal por decisión legislativa. Como ha señalado la doctrina, la inteligencia artificial no puede ser considerada responsable en el orden penal; en cualquier caso, el responsable siempre será un humano, ya sea de manera intencional o culposa.

Es tal vez aquí donde el debate adquiere su verdadera densidad. La doctrina penal contemporánea ha acuñado el concepto de "brecha de responsabilidad" (responsibility gap) para describir precisamente el escenario que nos ocupa. Autores como Roberto Navarro-Dolmestch (2025) han examinado en

profundidad este fenómeno, definiendo la brecha de responsabilidad penal como aquella situación en la que

> La ejecución de una conducta penalmente relevante se verifica por la interacción entre dos agentes: uno responsabilizable (como una persona humana o una persona jurídica) y un ente inteligente artificial, pero a los primeros no puede imponérseles responsabilidad debido a una característica técnica de la máquina inteligente propia de su configuración tecnológica.

En otras palabras, el verdadero problema no es que la IA no pueda ejecutar las tareas; es que el sistema jurídico-penal no tiene todavía una respuesta clara para los casos en los que la autonomía de la máquina impide atribuir el resultado a un humano concreto. Esta brecha se convierte así en un argumento de peso para quienes defienden la necesidad de mantener al Oficial de Cumplimiento en el centro del proceso: mientras no exista un marco claro de atribución de responsabilidad, la presencia humana opera como un "paraguas jurídico" que garantiza que siempre haya alguien a quien exigir cuentas.

La doctrina penal moderna ofrece ya herramientas que permiten avanzar. Navarro-Dolmestch propone una vía intermedia, reconociendo a las máquinas inteligentes una categoría de "actuantes" entre las tradicionales de "objeto" y "sujeto", lo que permitiría resolver las dificultades de imputación sin necesidad de otorgarles personalidad jurídica plena. Por su parte, autores como Alé Martínez y Aguilar Campos han examinado los modelos de imputación penal diferenciando entre la responsabilidad que podría recaer en desarrolladores, fabricantes y programadores, y aquella atribuible a quienes empleen estas tecnologías como instrumentos para la perpetración de delitos.

La cuestión, entonces, no es si el derecho penal puede adaptarse, sino cuándo lo hará. Y mientras la respuesta legislativa tarda en llegar, cabe preguntarse: ¿es razonable seguir justificando la permanencia del humano en el centro de

la operativa exclusivamente por la ausencia de un marco jurídico que, tarde o temprano, acabará llegando?

Otros aspectos como la necesidad del juicio humano, la ética o la intuición del ser humano, se colocan también en el centro de los argumentos que otorgan a los agentes de inteligencia artificial un papel de mero tramitador. Surge sin embargo la necesidad de replantearse el problema. Si se comparan ambos perfiles —el humano tradicional y el sistema de IA— desde una perspectiva estrictamente funcional, surge una conclusión incómoda pero necesaria: el argumento de la insustituibilidad humana, basado en una pretendida superioridad ética o intuitiva, ignora deliberadamente que el factor humano es, en sí mismo, una fuente constante y documentada de riesgo sistémico.

A diferencia de un sistema parametrizado y auditado, el oficial humano está sujeto a sesgos cognitivos documentados (como el sesgo de confirmación o el anclaje), fatiga acumulativa, presiones organizativas implícitas o explícitas, limitaciones de memoria operativa y una capacidad de procesamiento finita. Mientras que la IA ofrece consistencia estadística, trazabilidad absoluta de cada decisión, actualización normativa en tiempo real y ausencia de intereses particulares, el juicio humano puede verse comprometido por la conveniencia comercial, la inercia organizativa, la falta de información actualizada o, simplemente, por el cansancio al final de una jornada laboral.

A Modo de Reflexión

Luego de realizadas las reflexiones anteriores la pregunta que cabe formular es: si la IA ofrece mayor transparencia, objetividad y capacidad de respuesta en la ejecución de las tareas operativas, ¿no resulta paradójico seguir confiando esa ejecución a un ser humano sometido a limitaciones que la máquina no padece? La IA no es perfecta, pero sus imperfecciones son conocidas, modelables y auditables; las del humano, en cambio, son opacas, variables y difíciles de corregir.

Nada de lo anterior requiere que la IA posea conciencia, intencionalidad o ética propia. Como ha señalado la doctrina, la posibilidad de responsabilidad penal de la IA no exige atribuirle una "mente" en sentido humano. Exige, únicamente, que el marco legal determine con claridad quién responde penal, civil y administrativamente por sus acciones. La ley no necesita que la IA sea un "sujeto moral"; necesita que haya un sujeto humano al que exigir cuentas. Los modelos de responsabilidad directa, por delegación o por organización ya ofrecen herramientas normativas para atribuir los actos de una IA a quienes deciden su diseño, implementación y supervisión.

Por todo ello, el debate debe desplazarse de su falsa disyuntiva actual. No se trata de si la IA puede sustituir al oficial de cumplimiento, porque ya puede hacerlo en lo sustancial. Se trata de cuándo estaremos dispuestos a reconocer que el modelo de gestión de riesgos basado exclusivamente en el juicio humano ha quedado estructuralmente obsoleto. Mantener la intervención humana en procesos donde la máquina garantiza mayor transparencia, objetividad y capacidad de respuesta, bajo la excusa de una supuesta "superioridad ética" o de la ausencia de un marco de responsabilidad penal plenamente desarrollado, no es una muestra de prudencia reguladora; es un sesgo romántico que, en última instancia, introduce riesgos evitables y costes innecesarios en el sistema financiero.

La pregunta que surge entonces, y que exige una respuesta, es la siguiente: si hoy pudiéramos diseñar el sistema de cumplimiento normativo desde cero, sin herencias del pasado y sin ataduras, ¿dejaríamos realmente en manos humanas la ejecución de tareas que una máquina puede realizar con mayor precisión, consistencia y transparencia, sin sesgos subjetivos desconocidos, sin fatiga, sin actualización de conocimientos y sobre todo, sin presiones sociales o comerciales? Si la respuesta es negativa, como todo indica, entonces estamos ante una cuestión de tiempo, no de posibilidad.

A nuestro juicio, el futuro del cumplimiento normativo no pasa por la sustitución radical del humano, sino por una evolución donde la responsabilidad legal

permanezca anclada en la esfera humana, en el diseño, en la actualización, en la revisión, pero donde la ejecución operativa sea, por fin, de una manera más exacta y menos subjetiva algorítmica.

Referencias

Alé Martínez, V. I., & Aguilar Campos, P. (2025). Responsabilidad penal en la era de la inteligencia artificial: De la agencia humana a la autonomía de la machina sapiens. Revista de Estudios de la Justicia, (42). https://doi.org/10.5354/0718-4735.2025.77061

Blanco, D. F. (2024). ¿Cárceles para robots? La responsabilidad penal de la inteligencia artificial autónoma. Derecho Digital e Innovación / Digital Law and Innovation Review, (22).

ComplyAdvantage. (2025, 15 de octubre). AI in financial crime compliance: What's the difference between AI agents and agentic AI? https://complyadvantage.com/insights/the-difference-between-ai-agents-and-agentic-ai/

Copenhagen Business School & University of Copenhagen. (2025). Agentic AI for Financial Crime Compliance. arXiv. https://arxiv.org/pdf/2509.13137

FinTech Global. (2025, 17 de noviembre). Why AI agents matter in modern AML operations. https://fintech.global/2025/11/17/why-ai-agents-matter-in-modern-aml-operations/

Floridi, L. (2025). AI as agency without intelligence: On artificial intelligence as a new form of artificial agency and the multiple realisability of agency thesis. Philosophy & Technology, 38(1), Artículo 30.

Hong Kong Monetary Authority (HKMA). (s.f.). AML/CFT guideline (Suspicious Transaction Reporting). https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2023/20230209e2a2.pdf

López, J. (2020). [Reseña del libro Artificial Intelligence: A Modern Approach (4.ª ed.), de S. Russell y P. Norvig]. Revista de la Facultad de Ciencias, Universidad Central de Venezuela.

Navarro-Dolmestch, R. (2025a). Sobre una adecuación del derecho penal ante los conflictos derivados de las tecnologías de inteligencia artificial. Revista de Derecho Universidad de Concepción, 93(257).

Navarro-Dolmestch, R. (2025b). Brechas de responsabilidad penal por la actuación de máquinas dotadas de inteligencia artificial. Política Criminal, 20(40). http://dx.doi.org/10.4067/s0718-33992025000200077

Nasdaq Verafin. (2025). Agentic AI workforce. https://verafin.com/resource/agentic-ai-workforce/

RegTech Analyst. (2026). The impact of agentic AI on financial crime compliance. https://regtech.analyst/insights/the-impact-of-agentic-ai-on-financial-crime-compliance

Russell, S., & Norvig, P. (1995). Inteligencia Artificial: Un enfoque moderno. Prentice Hall.

Salvador Lafuente, A. (2026). El impacto de la inteligencia artificial en el cumplimiento normativo: Desafíos y buenas prácticas en el contexto europeo e internacional. Economía Industrial, (439), 123-124. https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/439/14SALVADOR_EI439.pdf

Silent Eight. (2026). Agentic AI and the end of reactive compliance. https://www.silenteight.com/blog/agentic-ai-and-the-end-of-reactive compliance

SymphonyAI. (2026). How AI agents reduce AML investigation time by 60%. https://www.symphonyai.com/resources/blog/financial-services/how-ai-agents-reduce-aml-investigation-time/

ANEXO 1 TABLA DE LAS FUNCIONES DEL OFICIAL DE CUMPLIMIENTO

Tabla resumen de las funciones de la Resolución 010 de SUDEBAN (Artículo 13) y su grado de delegación a Agentes de IA

Función (paráfrasis del Artículo 13)	Potencial de delegación (Actual / Avanzado)	Justificación
Funciones de diseño y planificación estratégica		
1. Diseñar políticas, normas y procedimientos PCLC/FT/FPADM.	Bajo / Alto	Actual: asistencia; futuro: agente propone, humano revisa/aprueba.
4. Diseñar POA, PAC, PCSA conjuntamente con áreas.	Medio / Muy Alto	Agente puede planificar y coordinar flujos de trabajo.

6.3 Recomendar mejora de políticas, normas y procedimientos.	Bajo / Alto	Agente identifica patrones de ineficiencia; propone, no decide.
6.9 Formular observaciones y actualizar el Manual PNPAR.	Medio / Alto	El monitoreo semestral y las propuestas de actualización son delegables.
Funciones de supervisión, control y gestión de parámetros		
2. Conocer informes de inspección y aplicar acciones correctivas.	Alto / Muy Alto	Seguimiento y verificación de ejecución de acciones. La "toma de conocimiento" no es un acto sustantivo.
5. Coordinar y supervisar la gestión de la UPC y demás áreas.	Muy Alto / Muy Alto	100% delegable el seguimiento, reporte y escalamiento de incidencias.
11. Revisar atributos y parámetros de la herramienta tecnológica (SIAR).	Muy Alto / Muy Alto	Tarea analítica por excelencia, con recomendación de ajustes basada en datos.
14. Participar en otros Comités (solo voz).	Bajo / Bajo	La participación en reuniones de alto nivel mantiene un componente humano.
Funciones de gestión de información y respuesta a entes externos		
3. Formar parte del Comité de Riesgos del Sujeto Obligado.	Bajo / Bajo	La presencia en el Comité es indelegable, aunque con apoyo documental del agente.
8. Mantener relaciones con Sudeban, UNIF y otros organismos.	Bajo / Bajo	Las relaciones institucionales son inherentemente humanas.
9. Representar al SO en eventos, foros y comités.	Muy Bajo / Muy Bajo	Función no delegable.
13. Emitir respuestas a solicitudes de información de órganos de control.	Alto / Muy Alto	Gestión del 80-90% del flujo de información; la respuesta final (firma) es humana.
Funciones de generación de informes y análisis avanzado		
6. Informes de Gestión Trimestral y Anual.	Muy Alto / Muy Alto	El agente puede redactar el 95% del informe, incluyendo análisis.
6.1 Nuevas políticas y análisis financiero de clientes.	Medio / Alto	Análisis delegable; la propuesta de nuevas políticas requiere validación.

6.2 Identificar nuevas tipologías delictivas.	Bajo / Medio	Agente como detector de señales; la conceptualización de la nueva tipología es humana.
6.5 Evaluación de nuevos productos y servicios (EBR).	Alto / Muy Alto	Evaluación EBR altamente delegable.
6.10 Evaluación trimestral de gestiones delegadas en terceros.	Alto / Muy Alto	Tarea de verificación documental y de calidad, ideal para agentes.
6.11 Evaluación de riesgos asociados con OSFL y ONG.	Alto / Muy Alto	El agente puede procesar grandes volúmenes de datos para esta evaluación.
Funciones operativas del SIAR		
6.7 Mostrar estadísticas mensuales de alertas (generadas, analizadas, pendientes, reportadas).	Muy Alto / Muy Alto	Función puramente analítica de reporte, 100% delegable.
6.8 Conocer incidencias en la remisión de Archivos de Transmisión (AT).	Muy Alto / Muy Alto	El monitoreo técnico es 100% delegable.
Función de coordinación interdepartamental		
10. Solicitar incorporación activa de cualquier directivo o empleado.	Bajo / Bajo	La solicitud formal puede ser generada por un agente, pero la gestión jerárquica es humana. No obstante, esto podría cambiar
12. Participar en desarrollo de estrategias comunicacionales con RRHH y Mercadeo.	Bajo / Medio	Apoyo en análisis de datos para segmentar audiencias; la estrategia creativa es humana.
Función central de decisión		
7. Evaluar casos y decidir si archivar, reportar (RAS) o hacer seguimiento.	Muy Bajo / Alto con condiciones	Estado actual: apoyo a investigación, pero decisión humana. Estado avanzado: decisión delegable en casos de riesgo bajo/medio a menos que la legislación lo permita

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

INTELIGENCIA FINANCIERA 4.0: EL SALTO DE LA GESTIÓN REACTIVA A LA PREVENCIÓN PREDICTIVA DE LC/FT/FPADM

Autor: Abg. Esp. Jesús Mora
Facilitadora: MSc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

"Inteligencia Financiera 4.0: El Salto de la Gestión Reactiva a la Prevención Predictiva de LC/FT/FPADM"

Autor: Abg. Esp. Jesús Mora
Correo electrónico: jesus.mora718@gmail.com

Resumen

Este ensayo analiza la Inteligencia Financiera 4.0, un paradigma que redefine la lucha contra el LC/FT/FPADM mediante la integración masiva de IA y Big Data. La tesis central sostiene que superar la gestión reactiva y la deuda técnica sistémica requiere una "Estrategia de Datos + Gobernanza" enfocada plenamente en la prevención predictiva. Se examina la evolución de la madurez tecnológica, destacando el tránsito hacia herramientas prescriptivas capaces de anticipar riesgos inminentes en lugar de solo reportar eventos pasados. Innovaciones como las Redes Neuronales de Grafos (GNN) permiten desarticular estructuras criminales ocultas, mientras que el Machine Learning eleva la precisión en la detección de clientes de alto riesgo con métricas superiores al 96%. El uso de biometría avanzada en el onboarding digital se presenta como el pilar fundamental para eliminar el anonimato y combatir el fraude de identidad sintética. Asimismo, se destaca la transición de una gestión basada en el cumplimiento operativo tradicional (POA) hacia un monitoreo dinámico impulsado por indicadores clave de riesgo (KRI). Finalmente, se aborda la adaptación de los marcos COSO y GAFI, resaltando aplicaciones prácticas, concluyendo que la convergencia estratégica entre RegTech y SupTech es imperativa para garantizar la resiliencia financiera global hacia el 2026.

Descriptores clave: Inteligencia Financiera 4.0, LC/FT/FPADM, Prevención Predictiva, IA, RegTech y SupTech.

Abstract

This essay analyzes Financial Intelligence 4.0, a paradigm that redefines the fight against AML/CFT/FPAM through the massive integration of AI and Big Data. The central thesis argues that overcoming reactive management and systemic technical debt requires a "Data + Governance Strategy" fully focused on predictive prevention. The evolution of technological maturity is examined, highlighting the shift towards prescriptive tools capable of anticipating imminent risks rather than simply reporting past events. Innovations such as Graph Neural Networks (GNNs) enable the dismantling of hidden criminal structures, while Machine Learning increases the accuracy of high-risk customer detection with metrics exceeding 96%. The use of advanced biometrics in digital onboarding is presented as the fundamental pillar for eliminating anonymity and combating synthetic identity fraud. The transition from management based on traditional operational compliance (POA) to dynamic monitoring driven by key risk indicators (KRIs) is also highlighted. Finally, the adaptation of the COSO and FATF frameworks is addressed, highlighting practical applications and concluding that strategic convergence between RegTech and SupTech is imperative to ensure global financial resilience by 2026.

Keywords: Financial Intelligence 4.0, AML/CFT/FPADM, Predictive Prevention, AI, RegTech, and SupTech.

Introducción

La Inteligencia Financiera 4.0 no debe entenderse como una simple actualización incremental de los sistemas existentes, sino como una reingeniería estructural profunda en los cimientos de la supervisión y el cumplimiento normativo. Este nuevo paradigma surge de la convergencia masiva entre la Inteligencia Artificial (IA) y el Big Data, permitiendo que las herramientas SupTech (tecnología para la supervisión) y RegTech (tecnología para el cumplimiento) trasciendan la mera digitalización para transformar la vigilancia financiera en un ejercicio de análisis proactivo. Mientras que las generaciones anteriores se enfocaban en automatizar tareas manuales, la era 4.0 utiliza el procesamiento avanzado de datos para generar herramientas prescriptivas que no solo alertan sobre lo ocurrido, sino que sugieren acciones ante riesgos inminentes.

La tesis central de este análisis sostiene que la adopción de una "Estrategia de Datos + Gobernanza" es el único camino viable para transitar de una

postura defensiva y reactiva hacia una capacidad de anticipación real frente a la Legitimación de Capitales, el Financiamiento al Terrorismo y el Financiamiento de la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM). En un entorno donde los flujos financieros son cada vez más digitales, veloces y fragmentados, el anonimato y la velocidad de los movimientos sospechosos superan la capacidad humana de detección, haciendo indispensable un cerebro analítico basado en máquinas que aprenden y predicen.

La Trayectoria Tecnológica y la Deuda Técnica

Históricamente, los entes reguladores y algunos Sujetos Obligados, han operado bajo una pesada deuda técnica. Un ejemplo emblemático es el uso persistente de lenguajes de programación obsoletos, como FoxPro, que han servido a instituciones durante décadas (desde 1996 hasta 2024 en algunos casos) antes de iniciar procesos de migración hacia lenguajes modernos. Esta dependencia de sistemas heredados ha limitado la capacidad de supervisión a un enfoque reactivo, donde el procesamiento de la información ocurre con un rezago temporal significativo respecto a la transacción ilícita. El salto a la Inteligencia 4.0 exige resolver este retraso, moviéndose hacia una arquitectura orientada a la innovación estratégica.

Desmitificación del Cumplimiento Operativo (POA) vs. Modelos Dinámicos

Es imperativo desmitificar la efectividad de la gestión basada exclusivamente en el cumplimiento operativo (Plan Operativo Anual - POA). Tradicionalmente, la supervisión se ha medido por el cumplimiento de tiempos y actividades administrativas, lo cual resulta insuficiente frente a la sofisticación del crimen financiero moderno. El paradigma 4.0 propone un cambio hacia modelos de monitoreo dinámico basados en Indicadores Clave de Riesgo (KRI) e Indicadores Clave de Desempeño (KPI) integrados directamente al análisis del impacto al negocio. En este modelo, el éxito no es "completar la tarea", sino

demostrar una reducción medible del riesgo a través de resultados tangibles y analítica predictiva.

Niveles de Madurez SupTech y la Pila de Supervisión

La madurez tecnológica en la supervisión se clasifica en niveles que van desde 0G (Manual) hasta 4G (IA & Big Data).

- 0G a 1G: Se caracterizan por reportes estáticos y validaciones manuales de datos almacenados en medios físicos o archivos locales.
- 2G y 3G: Introducen la transformación digital mediante tableros automáticos, analítica predictiva y el uso de la nube para el almacenamiento masivo.
- 4G: Representa el estado del arte, donde la recopilación de datos se basa en IA y se utilizan herramientas de análisis mejoradas con IA prescriptiva para una vigilancia integral.

La "Pila de Supervisión" moderna articula este proceso en cinco capas críticas: Fuentes de datos (entidades, usuarios, data pública), Recolección (vía APIs), Procesamiento (automatización y validaciones integradas), Almacenamiento (Big Data y nubes híbridas) y Analíticas (descriptivas, predictivas y prescriptivas). Esta arquitectura permite la creación de productos como el "Escudo de Datos", que automatiza la medición de los niveles de riesgo de las entidades supervisadas de manera continua.

El Ecosistema Predictivo y la Identidad Digital

El ecosistema de herramientas técnicas contra el LC/FT/FPADM ha evolucionado para incluir tecnologías de vanguardia como las Redes Neuronales de Grafos (GNN). A diferencia de los métodos tradicionales que examinan transacciones de forma aislada, las GNN analizan la estructura de la red, permitiendo desarticular "pequeñas bandas" de delincuentes que intentan ocultar sus acciones dentro de flujos financieros legítimos. Complementando este análisis, la identidad digital y la biometría avanzada (reconocimiento facial, detección de vida y biometría del comportamiento) se

erigen como los pilares para blindar el onboarding digital, eliminando el anonimato que tradicionalmente han explotado los Legitimadores de Capitales.

Objetivos Estratégicos del Ensayo: Para profundizar en esta transformación, este ensayo se propone alcanzar los siguientes objetivos estratégicos:

- Analizar la trayectoria tecnológica y la resolución de la deuda técnica histórica en los Entes Reguladores y Sujetos Obligados, evaluando la transición de sistemas legados a infraestructuras modernas.
- Desmitificar la efectividad de la gestión basada en el cumplimiento del Plan Operativo Anual (POA) frente a modelos de monitoreo dinámico impulsados por KRI/KPI con impacto en el negocio.
- Desglosar los niveles de madurez SupTech y Regtech, analizando cómo la integración de IA y Big Data redefine las capacidades de vigilancia.
- Explicar la arquitectura de la "Pila de Supervisión" y el uso de analítica avanzada, específicamente GNN y Machine Learning, para la detección de redes criminales complejas.
- Evaluar el impacto de la identidad digital y la biometría en la prevención predictiva, analizando cómo estas herramientas cierran las brechas de anonimato en la banca digital.
-

2. Desarrollo (Cuerpo del Ensayo)

1. Evolución Histórica y Tecnológica: Del FoxPro a la IA

La evolución de algunas organizaciones nacionales y extranjeras, revela un hito de resiliencia ante una brecha de obsolescencia crítica. En 1996, el inicio de FoxPro para DOS marcó el estándar de una gestión basada en archivos. Sin embargo, el riesgo operativo se exacerbó cuando Microsoft anunció el fin del soporte para FoxPro 5.0 en 1999; no obstante, dicha tecnología permaneció en el núcleo operativo hasta 2024. Este desfase de 25 años de

deuda técnica subraya la magnitud del salto hacia el Plan Estratégico de TI de 2022 y la migración a lenguajes modernos.

Periodo	Tecnología Base	Capacidad de Almacenamiento	Perfil de Riesgo y Orientación
1996 - 1999	FoxPro para DOS / FoxPro 5.0	Sistemas basados en archivos / Medios físicos	Incipiente: Alta dependencia manual, riesgo de soporte nulo desde 1999.
2001 - 2010	Aplicativo SB / Inicio PAMF	Bases de datos relacionales incipientes	Básica: Enfoque en estabilidad operativa y creación de módulos aislados.
2021 - 2024	Lenguajes modernos / IA	Almacenamiento híbrido y en la nube	En Desarrollo: Transición de 1.5G a 2.5G; reducción activa de deuda técnica.
2025+ (Visión)	Big Data / Analítica Prescriptiva	Ecosistemas de Big Data	Avanzado: Resiliencia automatizada; innovación alineada totalmente al negocio.

Fuente: Mora 2026

2. Las Limitaciones de la Gestión Reactiva Tradicional

Desde la perspectiva de un Arquitecto de Inteligencia Financiera, el modelo tradicional reactivo no es solo un sistema anticuado; es una estructura que padece de una "ceguera sistémica" ante la velocidad, el volumen y la sofisticación de las transacciones digitales modernas.

En el ecosistema financiero actual, donde el anonimato, la fragmentación de movimientos y la velocidad de flujo son las normas que sigue la Delincuencia Organizada, los controles internos basados en procesos manuales y reglas rígidas resultan insuficientes para identificar la Legitimación de Capitales, el Financiamiento al Terrorismo y el Financiamiento a la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM).

2.1. El Ocaso del POA frente al Monitoreo Dinámico (KRI/KPI)

Históricamente, la efectividad de las Unidades de Cumplimiento de distintos sectores regulados y denominadas: UPC LC/FT/FPADM, UAR LC/FT/FPADM y otros Ilícitos, se ha medido bajo el enfoque del Plan Operativo Anual (POA).

Este modelo prioriza el cumplimiento de tiempos administrativos y la ejecución de tareas programadas, como la entrega de reportes estáticos en fechas predefinidas.

Sin embargo, en la era de la Inteligencia 4.0, el éxito no puede definirse simplemente como "completar una tarea del cronograma", sino que debe medirse a través de una reducción medible del riesgo.

Mientras que el modelo reactivo se limita a verificar lo que ya ocurrió mediante resúmenes estadísticos mínimos, la prevención predictiva utiliza Indicadores Clave de Riesgo (KRI) e Indicadores Clave de Desempeño (KPI) que actúan como monitores "en vivo" de la exposición a los riesgos de LC/FT/FPADM del negocio.

Estos indicadores permiten que la supervisión pase de ser una fotografía estática del pasado a un video en tiempo real que alerta sobre desviaciones conductuales antes de que el daño patrimonial o reputacional sea irreversible.

2.2. De la Administración Básica al Análisis de Impacto al Negocio

La gestión tradicional se ha limitado a lo que se denomina "Administración de Riesgos Básica", enfocada principalmente en el cumplimiento normativo para evitar sanciones.

Este enfoque suele ver al Oficial de Cumplimiento y a su equipo, como un centro de costos aislado de la estrategia institucional.

En contraste, el ecosistema 4.0 exige un "Análisis de Riesgos e Impactos al Negocio" plenamente integrado al Balanced Scorecard de la organización.

Bajo el modelo reactivo, el análisis se realiza de forma transaccional e individualizada, examinando los movimientos en aislamiento y perdiendo de vista el contexto de la red.

Esta fragmentación es aprovechada por los delincuentes para ocultar sus acciones dentro de flujos legítimos.

La transición hacia la Inteligencia 4.0 implica el uso de analítica avanzada para entender cómo un evento de riesgo específico afecta la solvencia, la liquidez

y la integridad de toda la estructura de negocio, permitiendo una toma de decisiones estratégica y no meramente operativa.

2.3. Arquitectura Estática vs. Innovación: El Lastre de los Sistemas Legados

Uno de los mayores obstáculos para la evolución tecnológica es la deuda técnica acumulada.

Muchas instituciones todavía operan con una arquitectura de TI orientada a la estabilidad operativa, basada en sistemas legados que no tienen capacidad de cambio ni de integración

Un ejemplo crítico es el uso prolongado de lenguajes de programación obsoletos, como FoxPro, que tras décadas de servicio (1996-2024 en algunos entes) se han convertido en un riesgo de seguridad y una barrera para la innovación

Estos sistemas tradicionales son rígidos; sus reglas predefinidas son difíciles de actualizar frente a las nuevas Tipologías de LC/FT/FPADM, lo que genera una alta tasa de falsos positivos que sobrecarga a los analistas humanos.

La Inteligencia 4.0 propone, en cambio, una arquitectura orientada a servicios de negocio (SOA) con capacidades dinámicas.

Esto permite la implementación de herramientas como las Redes Neuronales de Grafos (GNN), que pueden gestionar volúmenes masivos de datos y adaptarse automáticamente a nuevos patrones delictivos mediante aprendizaje continuo.

3.4. Información Fragmentada vs. Gobernanza de Datos

En el modelo reactivo, la información suele estar almacenada en silos o depósitos de datos fragmentados, a menudo en formatos físicos o archivos locales que impiden una visión integral del cliente.

Esta falta de integración genera una desconexión entre plataformas que permite que las operaciones inusuales o sospechosas pasen inadvertidas.

Además, la validación manual de estos datos es propensa al error humano y consume recursos valiosos que podrían dedicarse a la investigación estratégica.

El modelo predictivo rompe estos silos estableciendo una "Estrategia de Datos + Gobernanza".

Esta estrategia garantiza que la información sea recolectada de forma automatizada (vía APIs), procesada con validaciones integradas y almacenada en infraestructuras de Big Data o nubes híbridas.

La gobernanza de datos asegura la trazabilidad y calidad de la información, permitiendo que las herramientas de Machine Learning identifiquen con precisión (con métricas AUROC superiores al 0.96) a los clientes de alto riesgo basándose en comportamientos históricos y geográficos multidimensionales

3.5. La Ineficiencia de la Detección basada en Reglas

Los sistemas tradicionales se basan mayoritariamente en reglas fijas (ej. alertas por transacciones superiores a un monto X).

Si bien son fáciles de auditar, su rigidez los hace vulnerables ante delincuentes que conocen los umbrales y diseñan sus esquemas para operar justo debajo de ellos.

Esta limitación estructural genera un ciclo de gestión reactiva ineficiente, donde el Oficial de Cumplimiento y su equipo pasa la mayor parte de su tiempo descartando falsos positivos en lugar de desarticular redes criminales complejas.

El salto a la prevención predictiva permite superar estas métricas operativas al introducir analítica prescriptiva.

En lugar de solo alertar sobre una regla rota, el sistema analiza la arquitectura completa de la transacción y la relación entre las partes involucradas, detectando "Organizaciones delictivas" que los métodos estadísticos convencionales ignoran.

Así, el control interno se transforma de un ejercicio de "marcar casillas" administrativas a una herramienta proactiva de defensa que asegura la resiliencia institucional en el horizonte 2026.

3. Generaciones de SupTech y RegTech: El Camino hacia la 4G

La madurez tecnológica en la supervisión y el cumplimiento financiero no es un estado estático, sino un proceso evolutivo que se mide a través de una taxonomía de cuatro generaciones (0G a 4G). Esta escala permite a Entes reguladores y a los sujetos obligados evaluar su capacidad de respuesta frente a delitos complejos como la LC/FT/FPADM.

Este tránsito no es meramente técnico, sino estratégico; cada salto generacional implica una reducción de la "ceguera sistémica" y un aumento en la capacidad de proteger la integridad del sistema financiero.

3.1. Niveles 0G y 1G: El Paradigma de la Gestión Manual y Tecnología Mínima

Los niveles iniciales representan el estado tradicional de la supervisión, donde la eficiencia está severamente limitada por procesos físicos y analíticas rudimentarias.

0G (Manual): Se caracteriza por una dependencia total de la remisión manual de información.

En este nivel, los productos de datos se limitan a resúmenes estadísticos mínimos y las validaciones de los datos recibidos son inexistentes o se realizan de forma visual, lo que incrementa exponencialmente el margen de error humano.

El almacenamiento se basa exclusivamente en medios físicos.

1G (Tecnología Mínima): Introduce la digitalización básica. Se generan reportes estáticos y la recolección se traslada a portales web o servidores.

Sin embargo, la analítica sigue siendo estrictamente manual y el almacenamiento está centralizado en archivos digitales aislados (silos), lo que impide una visión integral del riesgo del cliente.

Es en estas etapas donde la "deuda técnica" es más evidente, con sistemas que a menudo dependen de lenguajes obsoletos y procesos que no logran seguir el ritmo de la banca digital moderna (por ejemplo).

3.2. Nivel 2G: La Transformación Digital y la Automatización de Tareas

El salto a la 2G marca el inicio de la verdadera supervisión digital, nivel en el que Entes reguladores han consolidado sus operaciones recientes.

Hito de Conexión: El elemento diferenciador es la implementación de la conexión vía API (Interfaz de Programación de Aplicaciones), que permite una recolección de datos más ágil y estandarizada desde las entidades supervisadas.

Analítica Descriptiva: Se introducen herramientas de diagnóstico basadas en bases de datos de relaciones locales.

Esto permite la creación de tableros automáticos (dashboards) que ofrecen una fotografía mucho más precisa y oportuna de la situación financiera y los riesgos de cumplimiento.

Eficiencia Operativa: En esta etapa se automatizan las tareas estáticas, permitiendo que el Oficial de Cumplimiento y su equipo pase de la carga de datos al análisis básico, aunque todavía con un enfoque mayoritariamente reactivo

3.3. Nivel 3G: Tecnología Avanzada y Capacidad Predictiva

La meta fijada por algunas instituciones nacionales y extranjeras para el año 2025 es alcanzar la 3G, un nivel donde la tecnología deja de ser un soporte para convertirse en un motor de inteligencia proactiva.

Visualización y Nube: Este nivel se caracteriza por una visualización dinámica e interactiva de los datos, apoyada en sistemas de bases de datos en la nube, lo que garantiza escalabilidad y acceso ubicuo a la información.

Análisis Predictivo: A diferencia de la 2G, la 3G implementa herramientas de analítica predictiva.

Esto permite utilizar modelos estadísticos y de Machine Learning para anticipar comportamientos inusuales basándose en patrones históricos, detectando riesgos antes de que se materialicen.

Hiper-automatización: Se integra la Automatización Robótica de Procesos (RPA) para manejar flujos de trabajo complejos y repetitivos, optimizando los recursos humanos para la investigación de casos de alto impacto.

3.4. Nivel 4G: Inteligencia Supervisora 4.0 – IA & Big Data

La cuarta generación representa el estado del arte y el horizonte final de la Inteligencia Financiera 4.0. Es el nivel donde la supervisión se vuelve "inteligente" en el sentido más amplio del término.

IA Prescriptiva: La analítica evoluciona de lo predictivo (¿qué pasará?) a lo prescriptivo (¿qué debemos hacer?).

Las herramientas mejoradas con IA no solo emiten alertas, sino que sugieren acciones de mitigación específicas basadas en el análisis de riesgo sistémico.

Ecosistema de Big Data: Se utilizan herramientas masivas de procesamiento de datos para analizar no solo las transacciones, sino también datos alternativos (supply-side data), redes sociales y comportamiento digital para construir grafos de relaciones complejas.

Aprendizaje Profundo (Deep Learning): La recolección de datos se basa en IA, alimentando modelos de aprendizaje profundo capaces de identificar estructuras criminales "ocultas" que las reglas tradicionales ignoran.

4. Arquitectura de Detección: La Pila de Supervisión y GNN

Para transformar los datos en "Inteligencia Supervisora", se implementa una "Pila" (Stack) de cinco capas fundamentales, soportada por una Estrategia de Datos + Gobernanza:

1. Recolección: Utiliza recolección avanzada, conjuntos de datos compartidos y API para capturar información de entidades, Sujetos Obligados, usuarios y otras agencias.
2. Validación & Procesamiento: Implementa procesamiento avanzado y validaciones integradas, eliminando la carga manual y garantizando la integridad del dato desde la ingesta.
3. Almacenamiento: Evoluciona desde sistemas basados en archivos hacia sistemas de Big Data y almacenamiento híbrido/en la nube.
4. Analíticas: Despliega modelos de análisis predictivo y prescriptivo que superan la simple descripción estadística.
5. Productos: Genera Inteligencia de Negocios basada en IA, plataformas interactivas y tableros automatizados.

En esta arquitectura, las Redes Neuronales de Grafos (GNN) son esenciales. Permiten procesar el "Mapa de Vinculados" para identificar estructuras de propiedad complejas y vínculos ocultos entre entidades que los sistemas tradicionales ignoran. Asimismo, optimizan la "Selección de Muestra" mediante algoritmos que identifican perfiles de alto riesgo de forma automatizada, permitiendo una supervisión basada en riesgos reales y no en criterios aleatorios.

5. El Ecosistema de Herramientas Prácticas: Fichas Técnicas

La prevención predictiva se apoya en un conjunto de herramientas internas y externas que operan sinérgicamente (Ejemplo):

Nombre del Sistema	Función Principal	Impacto en la Prevención LC/FT/FPADM
Escudo de Datos	Automatización de la matriz de riesgo LC/FT/FPADM.	Estandariza y automatiza la medición de riesgos de las entidades o Sujetos Obligados.
SIGES	Gestión de expedientes sancionadores.	Agiliza la respuesta regulatoria ante incumplimientos detectados.
PAMF	Portal para *bulk upload* de reportes.	Garantiza la integridad y eficiencia en la carga masiva de datos regulatorios.
TeamMate	Supervisión y auditoría interna.	Digitaliza los procesos de auditoría enfocados en LC/FT/FPADM.
IDEA	Software de análisis de datos.	Permite auditorías forenses y detección de anomalías en grandes volúmenes de datos.
Risk Recon	Gestión de riesgos de terceros.	Evalúa la postura de seguridad y riesgo de los proveedores y aliados.
Lexis Nexis	Debida diligencia avanzada.	Provee acceso a listas de sanciones y perfiles de riesgo global.
Dash	Estadísticas y proyecciones.	Facilita el análisis de riesgos sistémicos y proyecciones financieras.

Fuente: Mora 2026

6. Biometría y Onboarding Digital: El Blindaje de la Identidad

La primera línea de defensa predictiva es el blindaje de la identidad. La biometría, aplicada en el onboarding digital, mitiga el fraude de identidad y la Legitimación de Capitales al vincular unívocamente la identidad digital con rasgos físicos inalterables. Basándose en estándares de instituciones y/o Organismos Oficiales, el proceso de verificación debe ser riguroso pero fluido. Técnicamente, el uso de "Cookies y JavaScript" (como se observa en las validaciones de Cloudflare) es un requisito esencial para el flujo de seguridad en el onboarding. Estos elementos permiten verificar que el usuario no es un bot malicioso, asegurando que la recolección de datos sea legítima. Esta personalización, basada en datos de navegación y comportamiento, permite un equilibrio entre la experiencia del usuario y la seguridad robusta, cerrando

la puerta a identidades sintéticas utilizadas en estructuras de Legitimación de Capitales.

7. Adaptación de Marcos Normativos: COSO, GAFI y RegTech

Para profundizar en la Adaptación de Marcos Normativos dentro del paradigma de la Inteligencia Financiera 4.0, es necesario analizar cómo el modelo COSO, los estándares del GAFI y la implementación de RegTech han dejado de ser procesos aislados para convertirse en un ecosistema integrado de defensa proactiva.

1. El Marco COSO en el Entorno Digital

El modelo COSO (Committee of Sponsoring Organizations of the Treadway Commission) proporciona la estructura fundamental para los controles internos, pero su aplicación en la era 4.0 exige una evolución desde la verificación manual hacia la gobernanza algorítmica.

Ambiente de Control y Gobernanza de IA: En la Inteligencia 4.0, el ambiente de control se fortalece mediante marcos sólidos de gobernanza de Inteligencia Artificial (IA).

Esto implica la necesidad de regulaciones explícitas, transparencia en los algoritmos y supervisión humana constante para evitar que la integración de IA genere riesgos sistémicos u opacidad en la toma de decisiones.

Evaluación de Riesgos Dinámica: Mientras que el COSO tradicional identifica riesgos de forma periódica, el modelo 4.0 utiliza Redes Neuronales de Grafos (GNN) para construir grafos dinámicos que integran dimensiones como características del cliente, ubicación y actividad comercial.

Esto permite detectar riesgos que no son evidentes con métodos estadísticos convencionales, cumpliendo con la exigencia de anticiparse a los desafíos.

Actividades de Control Automatizadas: Las políticas y procedimientos se ejecutan ahora mediante sistemas de monitoreo de transacciones en tiempo real y biometría avanzada para blindar el acceso al sistema.

Información y Comunicación: La integración de Tecnologías de la Información y Comunicación (TIC) optimiza la recolección y transmisión de datos críticos para la prevención de la Legitimación de Capitales, permitiendo alertas automatizadas y una trazabilidad robusta.

Monitoreo Continuo: La era 4.0 propone un monitoreo de estilo "panóptico" a través de tecnologías como Blockchain, que proporciona una trazabilidad inalterable y permite que la supervisión sea una vigilancia continua y no un evento de auditoría aislado.

2. Estándares del GAFI: El Enfoque Basado en Riesgo (EBR)

Las Recomendaciones del Grupo de Acción Financiera Internacional (GAFI) constituyen el estándar global, y su adaptación a la Inteligencia 4.0 se centra en la capacidad de las instituciones para gestionar la velocidad del entorno digital.

Recomendación 15 (Nuevas Tecnologías): Este es el pilar de la Inteligencia 4.0. Exige que las instituciones identifiquen y evalúen los riesgos asociados al desarrollo de nuevos productos y el uso de tecnologías emergentes antes de su lanzamiento.

En este sentido, el GAFI impulsa el uso de biometría y verificación de identidad digital para combatir el anonimato en los activos virtuales.

Recomendación 10 (Debida Diligencia del Cliente - KYC): En el entorno 4.0, el KYC evoluciona hacia un modelo continuo.

Ya no basta con identificar al cliente en el onboarding; se requiere un monitoreo persistente de su comportamiento digital para detectar fraude de identidad sintética.

Recomendación 18 (Controles Internos): El GAFI enfatiza que los programas de cumplimiento deben ser sólidos y estar sujetos a auditorías independientes que aseguren la efectividad de las herramientas tecnológicas implementadas.

Eficacia Basada en Resultados: Para el horizonte 2026, la tendencia regulatoria se aleja del cumplimiento de "marcar casillas" hacia una

supervisión efectiva basada en resultados, donde las organizaciones deben demostrar una reducción medible del riesgo.

3. RegTech: El Brazo Operativo del Cumplimiento 4.0

El término RegTech se refiere al uso de nuevas tecnologías para ayudar a las instituciones financieras a optimizar la auditoría, el cumplimiento y la gestión de riesgos.

Es la herramienta que permite materializar los principios de COSO y GAFI de manera eficiente.

Automatización y Eficiencia: Las herramientas RegTech, como ACTIMIZE, SAS AML u Oracle AML Manager, utilizan IA y Machine Learning para analizar patrones masivos de transacciones, reduciendo drásticamente los falsos positivos que saturaban los sistemas tradicionales.

Identificación Proactiva: A diferencia de la gestión reactiva, el RegTech 4.0 emplea analítica predictiva para anticipar comportamientos sospechosos basándose en tendencias históricas y datos en tiempo real.

Reportes Regulatorios Automatizados (RAS): Una de las mayores ventajas de RegTech es la capacidad de generar y enviar automáticamente reportes Sistemáticos o de actividades sospechosas a las autoridades (en las Jurisdicciones que su legislación lo permite), garantizando precisión y cumplimiento de los plazos legales

Integración de Datos: RegTech rompe los silos de información mediante el uso de APIs y bases de datos centralizadas (como SQLite para modelos experimentales), permitiendo una visión integral del riesgo del cliente.

4. Sinergia para la Inteligencia Financiera 4.0

La convergencia de estos marcos permite transitar hacia una Estrategia de Datos + Gobernanza

Mientras que el GAFI dicta el "qué" (estándares internacionales), el modelo COSO estructura el "cómo" (gestión interna y ética), y el RegTech proporciona el "con qué" (herramientas tecnológicas avanzadas).

Este ecosistema asegura que la prevención del LC/FT/FPADM no sea solo un requisito legal, sino un activo estratégico que protege la integridad institucional, mejora la toma de decisiones y fortalece la confianza en el sistema financiero global de cara al 2026

Conclusiones (Reflexiones)

La transición hacia la Inteligencia Financiera 4.0 no es un destino final, sino un proceso continuo de adaptación evolutiva frente a un adversario que se mueve a la velocidad del bit. Tras el análisis exhaustivo de este ensayo, se desprenden reflexiones fundamentales que deben guiar la estrategia de cualquier institución financiera o ente regulador en el horizonte del 2026.

1.La Disrupción de la "Ceguera Sistémica"

La primera gran conclusión es que el modelo reactivo tradicional ha quedado obsoleto, no por falta de voluntad, sino por una incapacidad estructural para procesar la complejidad del ecosistema digital.

Mientras que los esquemas basados en el Plan Operativo Anual (POA) se enfocan en el cumplimiento de tiempos administrativos, los criminales financieros operan en un entorno de "tiempo cero".

El paso de una gestión basada en hitos estáticos a un monitoreo dinámico impulsado por Indicadores Clave de Riesgo (KRI) y KPI de impacto es la única forma de disolver la deuda técnica acumulada por décadas de dependencia en sistemas legados.

La Inteligencia 4.0 exige que la supervisión deje de ser una "fotografía del pasado" para convertirse en un escudo de datos preventivo.

2. El Poder de la Red: De la Transacción al Grafo

Una reflexión crítica surge de la aplicación de las Redes Neuronales de Grafos (GNN). El análisis tradicional ha fracasado históricamente al examinar las

transacciones de forma aislada, permitiendo que "Organizaciones de Delincuencia Organizada" de delincuentes se oculten en el ruido de los flujos legítimos.

La Inteligencia 4.0 permite mapear la arquitectura del delito, identificando no solo el movimiento de fondos, sino la relación multidimensional entre dispositivos, identidades y comportamientos geográficos.

Esta capacidad predictiva, que alcanza métricas de precisión superiores al 96% (AUROC 0.961), transforma el cumplimiento normativo en una herramienta de inteligencia de negocios estratégica y no en un mero centro de costos.

3. Identidad Digital: El Fin del Anonimato Criminal

La biometría avanzada y el onboarding digital robusto representan el muro de contención definitivo contra el fraude de identidad sintética y el anonimato.

La integración de reconocimiento facial con detección de vida (liveness detection) y biometría del comportamiento asegura que el portal de entrada al sistema financiero sea impenetrable para identidades robadas o falsas.

Esta evolución cumple con las exigencias de la Recomendación 15 del GAFI, que obliga a evaluar los riesgos antes del lanzamiento de nuevas tecnologías, asegurando que la innovación no cree brechas que los Legitimadores de Capitales puedan explotar.

4. La Gobernanza Algorítmica y el Marco COSO

Es fundamental reflexionar sobre la ética y la transparencia en este nuevo paradigma. La implementación de IA no puede ser una "caja negra"; exige una IA explicable (XAI) que permita justificar cada alerta ante los reguladores y auditores.

La adaptación del marco COSO a la era digital significa que el ambiente de control ahora incluye la gobernanza de datos, donde la integridad de la información es tan crítica como la política de cumplimiento misma.

La efectividad de herramientas tecnológicas en sector regulados no financieros demuestra que, incluso en instituciones de menor escala, la inversión en

tecnología y capacitación del talento humano es el factor crítico de éxito para mitigar el riesgo de LC/FT/FPADM.

5. Convergencia RegTech y SupTech: Un Futuro Compartido

Finalmente, el horizonte 2026 nos muestra una convergencia inevitable entre el RegTech (para las entidades) y el SupTech (para el regulador). Ambos actores deben compartir una Estrategia de Datos + Gobernanza unificada, utilizando capas de supervisión automatizadas que permitan una comunicación fluida vía APIs.

La meta de alcanzar el nivel de madurez 4G (IA & Big Data) no es solo para mejorar la eficiencia operativa, sino para garantizar la resiliencia y la confianza en el sistema financiero global.

En conclusión, el salto de la gestión reactiva a la prevención predictiva es un imperativo de supervivencia. Aquellas instituciones que no logren migrar sus arquitecturas estáticas hacia servicios de negocio dinámicos e impulsados por IA, quedarán vulnerables ante una sofisticación criminal que ya ha cruzado la frontera digital. La Inteligencia Financiera 4.0 es, en última instancia, el compromiso de proteger la integridad económica de la sociedad mediante el uso ético y avanzado de la tecnología

Referencias

Banco Interamericano de Desarrollo (BID). (s.f.). Onboarding digital. IADB Publications.

Chilca. (2026, 10 de abril). Top plataformas de IA para prevención de lavado de dinero (AML). Transparencia.

Grupo de Acción Financiera Internacional (GAFI). (2012). Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación: Las Recomendaciones del GAFI.

León Pinde, E. W. (2024). Innovación tecnológica en la detección y prevención del lavado de activos en la Cooperativa de Ahorro y Crédito Padre Julián

Lorente en el periodo 2023 [Trabajo de Titulación, Universidad Nacional de Chimborazo]. Repositorio Digital UNACH.

LexisNexis Risk Solutions. (2026). Tendencias en cumplimiento de delitos financieros 2026.

Montoya Ruiz, M. F., Paredes García, S. D., Saravia Puchuc, A. A., Martínez López, R. O., & Galindez Azorza, W. (2025). Anti-Money Laundering Controls in the Era of Digital Banking. 5th LACCEI International Multiconference on Entrepreneurship, Innovation and Regional Development - LEIRD 2025.

Namdar, K., Wang, P.-C., Raju, T., Zheng, S., Li, F., & Khan, S. T. (2023). Anti-Money Laundering Machine Learning Pipelines; A Technical Analysis on Identifying High-risk Bank Clients with Supervised Learning. arXiv preprint.

Richard, M. (2022, 25 de marzo). El papel de la biometría en la lucha contra el blanqueo de capitales y el fraude de identidad. Shufti Pro.

Sultana, I., Maheen, S. M., Kshetri, N., & Zim, M. N. F. (2024). detectGNN: Harnessing Graph Neural Networks for Enhanced Fraud Detection in Credit Card Transactions. arXiv preprint.

Superintendencia de Bancos de la República Dominicana. (2024, 19 de julio). REGTECH & SUPTECH: El recorrido y la apuesta a futuro de la Superintendencia de Bancos.

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

LA TOKENIZACIÓN DE ACTIVOS: INNOVACIÓN FINANCIERA DE ACTIVOS DIGITALES Y NUEVOS RIESGOS DE CUMPLIMIENTO

Autora: Abg. Mercedes Mendoza Rubio
Facilitadora: Msc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

La tokenización de activos: innovación financiera de activos digitales y nuevos riesgos de cumplimiento

Autor: Abg. Mercedes Mendoza Rubio
Código ORCID: 0009-0008-8752-999X
Correo electrónico: mendozameche2@gmail.com

Resumen

El presente análisis aborda la tokenización de activos como una nueva tendencia de la tecnología financiera, que se origina en el seno de la criptografía y de la tecnología del blokchain, que dieron origen a los activos virtuales (AV) y a los proveedores de servicios de activos virtuales (PSAV), un nuevo sistema financiero más seguro, transparente, inclusivo y económico. Ofreciendo una mayor accesibilidad a los mercados de valores y emergiendo como una solución confiable a la falta de liquidez; por cuanto permite la participación en inversiones de alto valor mediante el fraccionamiento de acciones representadas por tokens. Asimismo, se tratan los aspectos relacionados con los riesgos y amenazas propias de la tecnología y de su implementación, considerándose estas en dos factores principales que son la seguridad y el marco regulatorio. Tomando como referencia los criterios expuestos en eventos académicos y por expertos sobre la tokenización de activos de recursos como petróleo, gas y minería como una alternativa económica para Venezuela, se hace una revisión de las regulaciones nacionales aplicadas a los AV y PSAV, y su alineación a los estándares internacionales del Grupo de Acción Financiera (GAFI). Como aporte se ponen de manifiesto los avances de la política económica conteste con los mecanismos de innovación financiera y el compromiso con la comprensión, regulación y adopción de las nuevas tecnologías.

Descriptores clave: Tokenización de activos; Activos Virtuales (AV); Proveedores de Servicios de Activos Virtuales (PSAV); nuevas tecnologías.

Abstract

This analysis examines the tokenization of assets as a new trend in financial technology, originating from cryptography and blockchain technology, which gave rise to virtual assets (VA) and virtual asset service providers (VASP)—a new financial system that is more secure, transparent, inclusive, and cost-effective. It offers greater accessibility to securities markets and emerges as a reliable solution to the lack of liquidity, as it enables participation in high-value investments through the fractionalization of shares represented by tokens. Furthermore, the analysis addresses aspects related to the risks and threats inherent in the technology and its implementation, considering these in terms of two main factors: security and the regulatory framework. Drawing on the criteria presented at academic events and by experts regarding the tokenization of natural resource assets such as oil, gas, and mining as an economic alternative for Venezuela, this study reviews the national regulations applicable to AVs and PSAVs and their alignment with the international standards of the Financial Action Task Force (FATF). As a contribution, this paper highlights the progress made in economic policy in line with financial innovation mechanisms and the commitment to understanding, regulating, and adopting new technologies.

Key descriptors: Asset tokenization; Virtual Assets (VA); Virtual Asset Service Providers (VASP); new technologies.

Introducción

La irrupción de la tecnología en la dinámica financiera es indetenible y avanza a ritmos acelerados, a una velocidad que incluso ha llegado a superar rapidez en la emisión de normas. Dinámica financiera que ha dado origen a un despliegue de herramientas y plataformas tecnológicas, así como expertos e instituciones basados en tecnología, economía y finanzas que han desarrollado amplios trabajos, investigaciones y narrativas en torno a esta disrupción.

En el esfuerzo de las instituciones públicas y privadas, por profundizar en el conocimiento sobre las nuevas tecnologías financieras destaca en fecha reciente, un evento denominado “Impacto de la Criptoeconomía en Venezuela” organizado por el Colegio de Contadores Públicos del Estado Miranda y la Universidad Santamaría, celebrado específicamente el 21 de mayo del año en curso, al cual me propuse asistir, tomando en consideración los tópicos planteados en el programa.

En dicho evento se presentó una conferencia titulada “Usabilidad cripto en Venezuela”, expuesto por el Lic. Eleazar Colmenares, quien se presentó como especialista en Finanzas, Inversiones y criptomonedas; cuya ponencia se tituló “La nueva alquimia: tokenización y activos del mundo real (RWA) en Venezuela 2026”, durante su disertación proyectó un Mapa de Activos del Mundo Real, en el cual se hace referencia a sectores estratégicos centrados desde el ecosistema de la tokenización. Cinco (5) sectores fueron expuestos, descritos textualmente en el mapa: i) minería y energía térmica; ii) agro-Tokens; iii) factoring logístico; iv) bienes raíces fraccionados y v) bonos verdes y ecológicos. Señalando también que en Venezuela no existen casos reales de tokenización autorizado por la SUNACRIP.

Del discurso, me generó gran interés la combinación de la tokenización y activos como una nueva alquimia financiera, el sector minería y energía térmica, y que en Venezuela no existen casos reales de tokenización; descriptores que son la fuente del presente trabajo.

En referencia a los avances de la tecnología y desarrollo de nuevas herramientas, plataformas y aplicaciones que han generado cambios exponenciales y globales, tres componentes se alzaron para sentar las bases de lo que hoy se denomina Nuevas Tecnologías Financieras, hablamos de Criptografía, Blockchain y Bitcoin, de este último nacieron las criptomonedas, los criptoactivos, los tokens y los stablecoin.

La breve experiencia adquirida durante el paso por un proyecto de constitución de una casa de intercambio y pasarela de pagos, unida al ser parte del grupo de formadores de la Oficina Nacional Contra la Delincuencia Organizada (ONCDOFT) me ha encaminado por la ruta de la actualización de estos componentes, incluyendo conocer las instituciones e instrumentos normativos que dieron origen al petro y las regulaciones orientadas al sistema de control de activos virtuales, proveedores de servicios de activos virtuales y servicios de tecnología financiera; todo lo cual desde mi perspectiva lo consideré como un Sistema Financiero Alternativo.

Tomando como referencia los elementos preliminarmente expuestos, mediante un estudio documental y descriptivo, incorporando el uso responsable de la Inteligencia Artificial como un recurso de apoyo para traducción de algunos estudios relacionados, se realiza el presente análisis sobre la tokenización de activos como nuevo esquema financiero, precedentes en Venezuela y los riesgos de cumplimiento de este sistema, siendo necesario abordar brevemente los estándares internacionales aplicables a los activos virtuales (AV), proveedores de servicios de activos virtuales (PSAV) y las regulaciones nacionales.

Origen de la tokenización: Las innovaciones de la tecnología financiera.

Para hacer referencia a la tokenización considero oportuno desglosar los componentes de las nuevas tecnologías financieras, que en esencia lo conforman: la criptografía, el blockchain y bitcoin.

Adoptando el criterio técnico expuesto por Mena et al., (2024) la criptografía es la piedra angular sobre la cual se sostienen el blockchain y el bitcoin, otorgando seguridad e integridad a las transacciones y operaciones que se ejecutan con bitcoin.

El blockchain no es exclusivo de las nuevas tecnologías financieras, sino que sobre su base criptográfica se están desarrollando registros de identidad, documentos para el rastreo logístico, entre otros.

El blockchain, “radica en la formación de una cadena de información compuesta de transacciones que son registradas por todos los que forman parte de la cadena de bloques. Su *tecnología de libro mayor distribuido* implica que todos los participantes de la red tienen acceso al libro mayor distribuido y a su registro inmutable de transacciones. (Casal, 2022, p. 2). La seguridad del blockchain radica principalmente en la criptografía, que garantiza que los bloques de la cadena no se pueden alterar ni modificar.

El Bitcoin representa el primer instrumento que adopta la figura de dinero en efectivo electrónico *peer-to-peer*[11], enviar pagos online directamente entre las partes y sin pasar a través de una institución financiera, utilizando para ello la tecnología entre iguales y criptografía, Nakamoto (2008).

Sobre el lenguaje de programación de bitcoin nace el Etherum, calificado por su creador Vitalik Buterin como "la próxima generación de contratos inteligentes y plataforma de aplicaciones descentralizada"[12], con la visión de ampliar la usabilidad del sistema criptográficos de pagos, ethereum, a diferencia de bitcoin, permite la creación de contratos inteligentes, que son programas que se ejecutan automáticamente cuando se cumplen ciertas condiciones (Mena et al., 2024), y como una evolución del sistema informático de almacenar valor, dieron inicio a un token que se denominó ether.

En el entendido que, un token en su funcionabilidad de activo digital se genera sobre una blockchain existente, es emitido y administrado por una persona o empresa. sobre condiciones y términos específicos descritos en código, que se ejecutan cuando se cumplen las condiciones específicas, los tokens dependen de la infraestructura, la seguridad y el mecanismo de consenso de otra red[13]. El respaldo y aceptación de estos tokens para realizar intercambios está supeditado a quienes emiten el token, Mena et al., (2024).

Radica allí la diferenciación entre el carácter descentralizado del bitcoin, que no está sometida a un régimen de administración, mientras que el token esta sometido a reglas y limitaciones que le aplica la red blockchain sobre la cual funciona, que no necesariamente tiene que ser una entidad bancaria o financiera, por cuanto puede ser cualquier persona u empresa, característica de un sistema centralizado, que tiene su fundamento en una plataforma programable de libros de contabilidad distribuida, ofreciendo seguridad a las transacciones, con el respaldo de reglas y condiciones definidas.

---

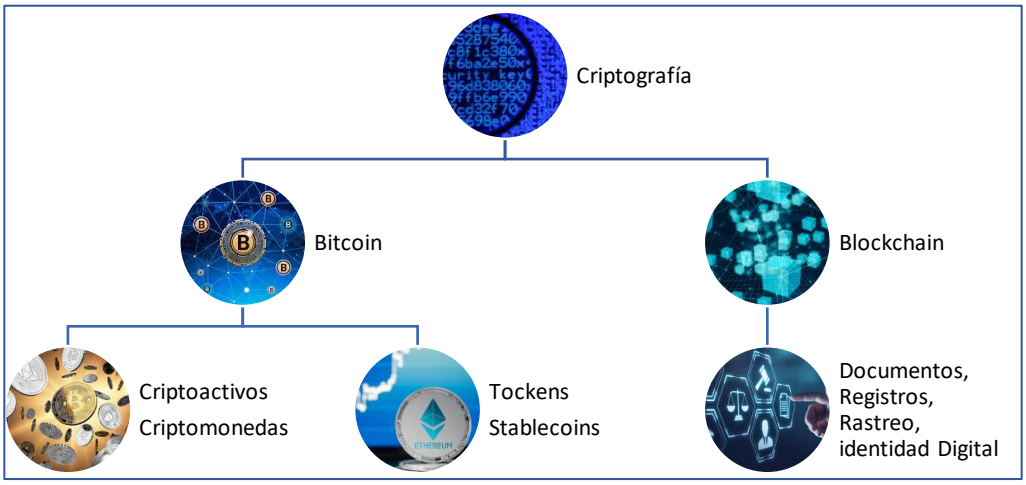
[11] Peer to peer: modelo de red descentralizado donde las computadoras o usuarios ("pares") interactúan y comparten recursos directamente entre sí, sin depender de un servidor central

[12] https://ethereum.org/whitepaper/

[13] https://www.binance.com

Para abordar la tokenización considere necesario hacer este recorrido preliminar, con el propósito de establecer el fundamento inicial de un sistema que se erige como una innovación financiera, resultando acertada la definición de (Aldasoro et al., 2023) mencionado por Vega, M. & Martínez, A. (2025) por cuanto incorpora los elementos esenciales de la tokenización al señalar que "implica generar representaciones digitales de activos financieros o reales que residen en una plataforma programable", conceptualización ampliada por Vega, M. & Martínez, A. (2025) al señalar que los tokens no son un simple registro sino que integran además una serie de reglas y lógica que rigen el proceso de transferencia y sus usos.

Surge la tecnología de contabilidad distribuida, en inglés Distributed Ledger Technology); (DLT) como un sistema digital descentralizado para registrar transacciones y datos, basada en blockchain, creación de contratos inteligentes con la ventaja de ser inmutables y verificables; no obstante, es importante diferenciar que, el blockchain se refiere a un sistema distribuido sin control centralizado, mientras que las bases de datos distribuidas son sistemas que tienen una autoridad central.



Fuente: Mendoza (2026)

Aunque el principal uso que se le está dando a tecnología DLT y al Blockchain es el intercambio de criptomonedas, destacando el Bitcoin como la de mayor usabilidad, basada en esta tecnología, el surgimiento del Ethereum y los "contratos inteligentes" abrieron la brecha para otras aplicaciones descentralizadas y ofertas de soluciones financieras alternativas.

Entonces, ¿Qué es la tokenización de activos?

Según Fuenmayor (2022) La tokenización de activos –que es un reflejo digital de activos reales en libros de contabilidad distribuidos o la emisión de clases de activos tradicionales en forma tokenizada–, por su parte Vega, M. & Martínez, A. (2025) lo definen como la representación digital de un activo en una plataforma programable e integran la información de los registros del activo subyacente, que normalmente se encuentra en una base de datos, con las reglas y la lógica que rigen el proceso de transferencia de dicho activo, con la característica principal que "los tókenes pueden personalizarse para cumplir con los requisitos específicos del propietario o regulatorios aplicables a cada uno de ellos".

Sobre la base de los estudios realizados por (Roth et al., 2021; Harish et al., 2023a) mencionados por Umair, T., et al. (2025) sostienen que "el concepto de tokenizar activos surgió a principios de la década de 2010 con el auge de la tecnología blockchain, en particular a través del desarrollo de contratos inteligentes en plataformas como Ethereum. Estos contratos inteligentes permiten la ejecución automática de acuerdos basados en condiciones predefinidas, facilitando así la propiedad fraccionada, la transferencia y la negociación de activos sin necesidad de intermediarios tradicionales como bancos o corredores".

Coinciden Fuenmayor (2022), Vega, M. & Martínez, A. (2025) y Umair, T., et al. (2025) en que la transparencia, la seguridad, la accesibilidad para los mercados financieros y la eficiencia dada la rapidez de las transacciones, son las características claves de la tokenización de activos, condiciones que son propias de tecnología blockchain.

La tokenización de activos facilita el fraccionamiento de la propiedad, frente a la elevada inversión de capital que representaría la participación en activos de alto valor como bienes raíces, obras de arte, oro, minerales, energía; motivo por el cual, se considera que es un mecanismo de democratización del mercado financiero y un alivio a la liquidez por cuanto, a mayor participación mayor ingreso.

La irrupción de la tecnología en el sector financiero se eleva de nivel con la tokenización extendiéndose hacia la propiedad real sobre activos, mediante la negociación de propiedades pueden personalizarse para cumplir con los requisitos específicos del propietario o regulatorios aplicables a cada uno de ellos, según lo expone Vega, M. & Martínez, A. (2025).

Umair, T., et al. (2025) en su estudio señalan tres etapas claves de la tokenización de activos: i) Identificación del activo a tokenizar y se evalúa su valor; ii) creación del token o representación digital en la cadena de bloques y iii) plataforma digital para la compra, venta y negociación del token, fases de interés para establecer su relación con los activos virtuales (AV) y proveedores de servicios de activos virtuales (PSAV) definidos por el Grupo de acción Financiera (GAFI).

En la Guía GAFI (2018) se establecieron dos definiciones fundamentales para identificar el funcionamiento de las nuevas tendencias financieras basadas en la tecnología, de interés para el presente análisis:

Activos virtuales (AV): Se aplica la denominación AV a una representación digital de valor que se puede negociar o transferir digitalmente y se puede utilizar con fines de pago o inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiduciarias, valores y otros activos

financieros que ya están cubiertos en otras partes de las Recomendaciones del GAFI.

Proveedor de Servicios de Activos Virtuales (PSAV): Cualquier persona física o jurídica que no esté cubierta en ninguna otra parte de las Recomendaciones y como empresa que realiza una o más de las siguientes actividades u operaciones para o en nombre de otra persona física o jurídica.

i. Intercambio entre activos virtuales y monedas fiduciarias;
ii. Intercambio entre una o más formas de activos virtuales;
iii. Transferir activos virtuales; y
iv. Custodia y / o administración de activos o instrumentos virtuales que permitan el control sobre activos virtuales;
v. Participación y prestación de servicios financieros relacionados con la oferta y / o venta de un activo virtual por parte de un emisor.

Los elementos que describe a los AV y PSAV presentan una estrecha similitud con las etapas de la tokenización de activos a la hacen referencia Umair, T., et al. (2025) en su investigación, por ende, resulta congruente observar este sistema a la luz de las regulaciones del GAFI (2018) y la normativa nacional vigente.

Bases Legales de la tokenización: conexión entre la regulación internacional con la normativa venezolana.

En junio de 2019, el GAFI adoptó una Nota Interpretativa a la Recomendación 15 (INR.15) para aclarar aún más cómo deben aplicarse los requisitos del GAFI en relación con los AV y los PSAV, en particular con respecto a la aplicación del enfoque basado en el riesgo a las actividades de los AV u operaciones y PSAV.

El instrumento recomienda implementar mecanismos de licenciamiento o registro en conjunción con medidas preventivas como debida diligencia del

cliente lo cual comprende comprobar la información aportada por el cliente relativa a su identidad, como el número de su documento de identidad, contrastándolo con bases de datos de terceros u otras fuentes fiables, supervisión y monitoreo incluyendo rastrear la dirección IP del cliente, mantenimiento de registros y reporte de transacciones sospechosas.

Establece un umbral cuantitativo a partir del cual los PSAV deberán aplicar medidas de diligencia debida para todo tipo de transacciones con activos virtuales, incluyendo transacciones ocasionales por encima de 1.000 EUR/USD. También la verificación en las listas de sanciones y la aplicación de contramedidas financieras como la congelación y bloqueo de fondos y la prohibición de transacciones con las personas y entidades designadas, y otras medidas de ejecución; y cooperación internacional.

Apegados a los Estándares del GAFI (2025) la Recomendación 15 exige que los proveedores de servicios de activos virtuales (VASP) apliquen medidas de "conozca a su cliente" (KYC) y la "regla de viaje" (Travel Rule). La regla de viaje exige que los PSAV recopilen información detallada del originador y del beneficiario de las transferencias de Activos Virtuales (AV), asegurando la trazabilidad de los fondos.

A los efectos, los PSAV se ubican en la primera línea de defensa al implementar procedimientos sólidos de detección de LC/FT, desempeñando un papel crucial en la prevención y detección en el ecosistema de activos virtuales, aplicando con rigurosidad:

1. Diligencia debida exhaustiva sobre los clientes,
2. Seguimiento de las transacciones en busca de actividades sospechosas y
3. Notificación de cualquier transacción sospechosa identificada a las autoridades reguladoras.

Vega, M. & Martínez, A. (2025) destacan la importancia de un marco legal sólido y una supervisión exhaustiva que le otorgue confianza y seguridad al sistema de tokenización de activos.

En la normativa nacional, hay que reconocer el avance de la política económica conteste con los mecanismos de innovación financiera en una serie de instrumentos normativos promulgados entre el año 2018 al 2021, que incluyeron a todos los integrantes del sistema y creación de la Superintendencia Nacional de Criptoactivos (SUNACRIP), como órganos de regulación, control y supervisión; todo lo cual se encuentra contenido en las siguientes regulaciones:

2018
09/04: Decreto Constituyente. Criptoactivos y la Criptomoneda Soberana Petro. GO N° 6.370.
23/02: Decreto N° 3.292. Respaldo para la Implementación de Operaciones de Intercambio Financiero y Comercial a Través de Criptoactivos, el Desarrollo Potencial De 5.342 Mmbn De Petróleo Original En Sitio (POES) Pesado y Extrapesado.
28/12 Decreto N° 3.719. Pago Obligaciones en criptodivisas.
2019
30/01: Decreto Constituyente sobre el Sistema Integral de Criptoactivos.
19/11: Decreto 4.025. Registro Contable en Criptoactivo Soberano**.**
04/02: Providencia N° 008-2019. Registro Integral de Servicios en Criptoactivos (RISEC).
07/02: Providencia N° 009-2019. Remesas en Criptoactivos.
03/04: Providencia N° 012-2019: Operatividad de las Casas de Intercambio.
16/12: Providencia N° 097-2019. Servicios Criptofinancieros Especializados.
26/12: Providencia N° 098-2019. Registro Contable de Operaciones y hechos Económicos expresados en Criptoactivos.
2020
15/01: Decreto N° 4.096. Liquidación, venta y pago de servicios en Criptoactivos Soberanos Petro (PTR)
21/09: Providencia N° 084 – 2020: Regula la Minería Digital y Procesos Asociados

2021
21/04: Providencia N° 044-2021: Normas relativas a la administración y fiscalización de los riesgos relacionados con la legitimación de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, aplicables a los proveedores de servicios de activos virtuales y a las personas y entidades que proporcionen productos y servicios a través de actividades que involucren activos virtuales, en el sistema integral de criptoactivos.

Partiendo de las recomendaciones del GAFI (2025) en la normativa nacional se establecen disposiciones relativas al registro y licencias para sistematizar la información correspondiente mineros digitales, casas de intercambio, demás servicios financieros en criptoactivos y a la intermediación de criptoactivos; actividades relacionadas con la constitución, emisión, organización, funcionamiento y uso de criptoactivos; inspección de las actividades propias del sector.

Todo lo relativo a las licencias y registros se establece en las disposiciones de la Providencia N° 012-2019: Operatividad de las Casas de Intercambio.

Conteniendo la Providencia N° 044-2021: Normas relativas a la administración y fiscalización de los riesgos relacionados con LC/FT aplicables a los PSAV, mediante la cual se estatuye la implementación de políticas, métodos y mecanismos de control que les permitan prevenir, administrar y mitigar los riesgos identificados en materia de LC/FT/. Considerándose a los efectos los factores generadores de riesgos que involucre a clientes, productos, negocios y servicios que involucren activos virtuales, canales de distribución, uso de tecnologías nuevas o en desarrollo, tipos de activos virtuales involucrados en las operaciones.

Estableciendo el Sistema Integral de Administración de Riesgos (SIAR) como eje central de la prevención en áreas medulares como: fomentar la comprensión de los riesgos a través de la capacitación, uso de herramientas de tecnología y soluciones informáticas que faciliten el manejo y rastreo de datos, sistemas de monitoreo, controles internos y matrices de riesgo.

La tokenización de activos: alternativa propuesta para Venezuela

Siendo la ponencia titulada “La nueva alquimia: tokenización y activos del mundo real (RWA) en Venezuela 2026”, el punto de partida del presente estudio, resulta destacable el nuevo informe de Bitfinex Securities (2026) que incorpora un capítulo sobre Venezuela en el cual se expone la tokenización como una alternativa para la reconstrucción económica, el desarrollo de un mercado de capitales más abierto, dinámico y competitivo, y la movilización de capital a corto plazo mediante el aprovechamiento de sus activos productivos existentes, como el sector petrolero.

La alternativa se fundamenta en la necesidad de sortear los obstáculos burocráticos, la inseguridad jurídica, la falta de confianza, la posición de desventaja de las entidades legales nacionales con respecto a sus contrapartes internacionales y los onerosos requisitos exigidos que constituyen una barrera a la inversión extranjera, aunado a las sanciones internacionales históricas y actuales impuestas a Venezuela, sumando que las empresas venezolanas se consideran de alto riesgo en materia de cumplimiento normativo.

Toda una serie de factores que a simple vista pueden resultar desalentadores, sin embargo, no desestiman el elevado nivel de interés sobre los activos productivos como el petróleo, el gas y los minerales, como un mercado cautivo para la tokenización de dichas riquezas territoriales.

Actualmente se registra incluso el lanzamiento de algunos tokens para permitir la inversión en acciones de reservas, regalías o certificados vinculados al petróleo, con límites mínimos de inversión de tan solo 50 a 100 dólares, a través de la criptomoneda estable OIL1, lanzada en el Foro Económico Mundial 2026 en Davos.

Como ventajas representativas que se exponen en el informe de Bitfinex Securities (2026) radican el potencial de las empresas de tecnología financieras en Venezuela y la familiaridad del usuario con el uso de stablecoins y plataformas de intercambio de criptomonedas.

Riesgos de cumplimiento de la tokenización de activos

Tomando como referencia el estudio realizado por Umair, T., et al. (2025), los riesgos de cumplimiento de la tokenización de activos, están relacionados con diversos factores como la falta de compromiso de todas las jurisdicciones en la aplicación uniforme de las normas relativas a las licencias, regulación y cumplimiento de requisitos para prevenir la legitimación de capitales aunado a las complejidades propias de la tecnología distribuida de datos, blockchain, contratos inteligentes, ataques informáticos y brechas de seguridad.

De la ob. cit se advierte que la vulnerabilidad de la tokenización de activos esta sujeta a riesgos que exigen la implementación de marcos legales adaptados a su funcionamiento, garantías de seguridad para los inversionistas, reglas claras para los operadores de las plataformas de intercambio y condiciones de seguridad propias del sistema y mecanismos robustos para la prevención y mitigación de riesgos de legitimación de capitales.

La falta de armonización regulatoria entre diversas jurisdicciones dificulta la aplicación de los contratos inteligentes para la tokenización de activos, cuando se pretende trascender fronteras, concluyendo Umair, T., et al. (2025) en sus estudios, que la vulnerabilidad de la tokenización de activos en dos grandes dimensiones: Seguridad e Incertidumbre regulatoria.

Otra dificultad relevante que enfrenta la tecnología es la interoperabilidad de los sistemas, y el blockchain no escapa de este obstáculo, planteamiento coincidente en los estudios realizados por Vega, M. & Martínez, A. (2025) y Umair, T., et al. (2025).

Respecto a la custodia de los activos digitales sostienen los estudios que debería reposar en dependencias de elevada confianza, credibilidad y sustentabilidad para respaldar los activos, siendo éste un elemento determinante para generar tranquilidad entre los inversores de la tokenización de activos, según exponen Umair, T., et al. (2025) y Vega, M. & Martínez, A. (2025), por lo tanto, seleccionar o definir las condiciones que deben reunir los

proveedores de las plataformas que habiliten las transacciones con activos tokenizados se convierte en un riesgo y desafío que requiere especial atención.

Otro factor de especial atención que describen Vega, M. & Martínez, A. (2025), es la inmutabilidad de la tecnología blockchain que simboliza una ventaja y un riesgo, por cuanto cualquier error en el registros o transacción quedará fijado en la cadena de bloques, por lo que es fundamental que los datos iniciales estén libres de errores, puesto que la irreversibilidad se puede convertir en un problema crítico, sin garantías para el inversor.

Resultan también de gran preeminencia las vulnerabilidades y amenazas a las que hacen referencia Mena et al., (2024) como son los ataques controlados en más de un 50% por un solo actor y la aparición de las computadoras cuánticas, recomendando a los efectos que el desarrollo de aplicaciones basadas en blockchain sean llevadas a cabo con la mayor comprensión y una exhaustiva aplicación de buenas prácticas destacando la protección contra los ataques como primera línea defensiva.

Recomendaciones y Conclusiones

La tokenización promete un sistema financiero más inclusivo y eficiente, seguro, transparente y económico para los inversores, así como garantía de liquidez para los mercados financieros, sobre la base de la tecnología blokchain se esta impulsando el avance de la tecnología financiera mediante la tokenización de activos, ofreciendo el fraccionamiento de propiedades y activos del mundo que en su conjunto global resultan inaccesibles como acciones, bonos y bienes inmuebles.

Los riesgos vinculados a la tokenización de activos, están intrínsicamente ligados a las complejidades propias de la tecnología, que se ciernen en dos áreas especialmente vulnerables: Seguridad y marco regulatorio.

Seguridad para los inversionistas que pasarán a formar parte de un conglomerado que dependerá de un sistema distribuido de datos para el

resguardo de sus acciones, representadas por tokens en forma digital registradas en la cadena de bloques centralizada, debiendo confiar en el custodio de dichos activos, con el riesgo latente de no caer en una estafa de inversión ante la falta de garantías y condiciones claras respecto a su inversión y transacciones.

Seguridad que se extiende hasta el funcionamiento de la plataforma y a los proveedores de las plataformas, tomando en consideración los sostenidos y modernos mecanismos de ataques, que los ingeniosos piratas de la informática perfeccionan a una velocidad mayor que las regulaciones de control y sanción.

El marco regulatorio sigue siendo el principal punto de discusión de gobiernos y corporaciones tecnológicas, que a pesar del desglose de recomendaciones desarrolladas en la última década por el GAFI en su rol de organismo protector del sistema financiero global, la implementación y efectividad del cuadro normativo sigue siendo de baja adopción y cumplimiento, lo cual va en detrimento de la armonización de los mecanismos de prevención y detección del uso de las nuevas tecnologías financieras en la LC/FT a nivel de la economía global.

Desde el 2018 en Venezuela se dictaron una serie de instrumentos normativos en consonancia con el GAFI, orientadas a regular los las transacciones con activos virtuales y a los proveedores de servicios de activos virtuales; si bien es cierto el organismo de regulación se encuentra en proceso de reestructuración desde marzo del 2023, los instrumentos normativos siguen vigentes y actualmente funcionan dos PSAV licenciados para operar, y el trabajo coordinado entre los organismos de regulación, control y supervisión en conjunto con sujetos obligados ha resultado en el avance del país en su comprensión, regulación y adopción de estas tecnologías.

Tomando en consideración el avance de la tecnología en el sistema financiero, al profundizar en los riesgos y desafíos que conlleva la tokenización de activos, y su posible implementación como sistema de inversión sobre recursos a

futuro, es imperativo revisar exhaustivamente los instrumentos normativos que actualmente regulan las transacciones en AV y a los PSAV, con el propósito de adecuar dichas regulaciones a esta nueva tendencia.

En ese sentido, la autora difiere de la afirmación hecha por el expositor de la conferencia “La nueva alquimia: tokenización y activos del mundo real (RWA) en Venezuela 2026”, que en Venezuela no existe ninguna regulación aplicable a la tokenización, así como con los criterios expuestos en el informe de Bitfinex Securities (2026) por cuanto podemos observar la consonancia de los instrumentos jurídicos que regulan las nuevas tecnologías financieras con respecto a las recomendaciones del GAFI, y considerando los fundamentos que dieron origen a los tokens, se evidencia que se encuentran directamente vinculados a los activos virtuales y a los proveedores de servicios de activos virtuales.

Referencias

Asamblea Nacional de la República Bolivariana de Venezuela. (2019). *Decreto Constituyente sobre el Sistema Integral de Criptoactivos*, publicado. Gaceta Oficial Nº 41.575 del 30 de enero de 2019.

ChainUp. (2026) El petróleo en 2026: Por qué la tokenización está transformando el mercado energético mundial. https://www.chainup.com/blog/oil-in-2026-why-tokenization-is-transforming-the-global-energy-market/ Consulta 24/07/2026.

De Fuenmayor, C. (2022). Efectos de la tokenización de activos para los mercados financieros. Instituto de Estudios Financieros. España.

Escuela Nacional de Administración y Hacienda Pública. (2016). *Manual para elaboración y presentación de trabajos académicos.* ENAHP-IUT. Caracas.

Gobierno de Colombia. (2020). *Guía para el uso y la implementación de tecnología de registros distribuidos (DLT/Blockchain) en el sector público.* Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC.

Grupo de Acción Financiera Internacional. (2018). *Regulación de Activos Virtuales.*

Grupo de Acción Financiera Internacional (GAFI). (2019). *Orientación para un enfoque basado en riesgos activos virtuales y proveedores de servicios de activos virtuales.*

Grupo de Acción Financiera Internacional (GAFI). (2025). *Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación de armas de destrucción masiva: Las Recomendaciones del GAFI*

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

INNOVACIÓN RESILIENTE EN UN MERCADO SINGULAR: RIESGOS DE LEGITIMACIÓN DE CAPITALES EN LA DIGITALIZACIÓN DEL MERCADO BURSÁTIL VENEZOLANO

Autora: Lic. Gianny Verasmendi
Facilitadora: MSc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

Innovación Resiliente en un mercado singular: Riesgos de Legitimación De Capitales en la digitalización del Mercado Bursátil Venezolano

Autor: Gianny Verasmendi
Correo electrónico: gverasmendi@gmail.com

Resumen

El presente ensayo analiza los riesgos de legitimación de capitales y financiamiento al terrorismo asociados al proceso de digitalización del mercado de valores venezolano, en un contexto marcado por la modernización de los servicios financieros y las expectativas de una mayor integración con los mercados internacionales. La incorporación de aplicaciones móviles, interfaces de programación de aplicaciones (APIs), mecanismos de onboarding digital y sistemas de verificación biométrica ofrece oportunidades para ampliar la inclusión financiera y optimizar la eficiencia operativa; sin embargo, también introduce riesgos emergentes vinculados con la fragmentación transaccional, las identidades sintéticas, los deepfakes, las vulnerabilidades en APIs y la posible desintermediación financiera. Asimismo, se examina el marco regulatorio venezolano vigente y su alineación con los estándares internacionales promovidos por el Grupo de Acción Financiera Internacional (GAFI). Mediante una revisión documental sustentada en las metodologías ISO/IEC 27005:2022 y NIST SP 800-30 Revision 1, se concluye que el principal desafío del mercado bursátil venezolano consiste en fortalecer su capacidad de gestión de riesgos sin comprometer su sostenibilidad económica, requiriendo para ello una estrategia sectorial coordinada y resiliente.

Descriptores clave: Mercado de valores venezolano, legitimación de capitales, transformación digital, gestión de riesgos, tecnologías financieras.

Abstract

This essay analyzes the money laundering and terrorist financing risks associated with the digitalization process of the Venezuelan securities market, within a context characterized by the modernization of financial services and expectations of greater integration into international financial markets. The incorporation of mobile applications, Application Programming Interfaces (APIs), digital onboarding mechanisms, and biometric verification systems creates opportunities to expand financial inclusion and improve operational efficiency. However, it also introduces emerging risks related to transaction fragmentation, synthetic identities, deepfakes, API vulnerabilities, and potential financial disintermediation. The essay further examines the current Venezuelan regulatory framework and its alignment with international standards promoted by the Financial Action Task Force (FATF). Through a documentary review supported by the ISO/IEC 27005:2022 and NIST SP 800-30 Revision 1 methodologies, it is concluded that the main challenge facing the Venezuelan securities market is strengthening its risk management capabilities without compromising its economic sustainability. Addressing this challenge requires a coordinated and resilient sector-wide strategy focused on technological innovation, institutional cooperation, and effective risk management.

Key descriptors: Venezuelan securities market, money laundering, digital transformation, risk management, financial technologies

Introducción

El mercado de valores venezolano se encuentra en un punto de inflexión estratégico. Por un lado, la normalización de las relaciones financieras internacionales, que incluyen la reestructuración de la deuda externa, la reinserción en el sistema de pagos global SWIFT y la creciente participación de inversionistas institucionales internacionales, abre la puerta a nuevos flujos de capital y una mayor liquidez. Por otro lado, la digitalización de los servicios financieros, materializada en el desarrollo de aplicaciones móviles (APP), interfaces de programación de aplicaciones (APIs), sistema de onboarding digital y verificación biométrica está transformando la manera en que los inversionistas interactúan con el mercado (FATF, 2020; World Economic Forum, 2025)

Este doble proceso de apertura externa y modernización tecnológica ofrece oportunidades significativas: mayor inclusión financiera, reducción de tiempos

y costos de transacción, y la posibilidad de que en el mercado bursátil venezolano compita por atraer inversión regional. Sin embargo, también introduce nuevos vectores de riesgo de legitimación de capitales y financiamiento al terrorismo (LC/FT) que requieren mecanismos de supervisión adaptados a los nuevos entornos tecnológicos (FATF, 2025; GAFILAT, 2020).

El presente ensayo tiene como objetivo analizar, desde una perspectiva técnica, los siguientes aspectos:

1. Los riesgos específicos de LC/FT asociados a la implementación de tecnologías digitales (APIs, APP, onboarding biométrico en el mercado de valores venezolano, incluyendo la fragmentación transaccional, los deepfakes, las identidades sintéticas y las vulnerabilidades de ciberseguridad.
2. El desafío que representa la llegada de nuevos actores internacionales, cuyas expectativas tecnológicas y de cumplimiento son significativamente más altas que las del mercado local actual.
3. El dilema económico estructural que enfrentan los actores del mercado de valores, específicamente las casas de bolsa: un mercado de pequeña escala que debe costear sistemas de administración de riesgos tecnológicamente avanzados, cuyos costos fijos son similares a mercados mucho más grandes.
4. Las implicaciones de este dilema para la capacidad del mercado de atraer inversión internacional y mantener la integridad del sistema de administración de riesgos

El ensayo se estructura en trece secciones que abordan sucesivamente el contexto, el marco normativo, los estándares internacionales las metodologías de gestión de riesgo, los riesgos, el dilema económico y las conclusiones y recomendaciones

El nuevo contexto: normalización financiera y llegada de actores internacionales

Procesos de reestructuración de la deuda y acceso a mercados globales

En los meses, la República Bolivariana de Venezuela ha avanzado en conversaciones formales con tenedores de bonos y asesores financieros internacionales para la reestructuración de su deuda externa. Una reestructuración exitosa tendría como efecto la revalorización de los títulos de deuda pública venezolana y una mayor liquidez en el mercado secundario, atrayendo a fondos de inversión especializados en mercados emergentes y de frontera.

Estos fondos, conocidos como fondos distressed o fondos de valor recuperable, operan con volúmenes significativos y exigen a los intermediarios locales estándares tecnológicos y de cumplimiento equivalentes a los de sus jurisdicciones de origen (FATF, 2025; Banco Mundial, 2026)

Reinserción en sistemas de pagos internacionales (SWIFT)

El Banco Central de Venezuela (BCV) ha realizado pruebas técnicas exitosas de conectividad con contrapartes internacionales a través del sistema SWIFT. Esta conectividad es un habilitador crítico para la inversión extranjera en valores venezolanos, ya que permite el ingreso de fondos desde cuentas en el exterior hacia las cuentas de custodia local, así como la repatriación de dividendos, intereses y el producto de la venta de valores.

Perfil de los nuevos inversionistas internacionales

Los inversionistas internacionales que se espera participen en el mercado de valores venezolano comparten ciertas características operativas y de cumplimiento:

- Velocidad de ejecución: esperan poder abrir cuentas de corretaje en plazos no superiores a 24-48 horas, con procesos de verificación de identidad completamente digitales (onboarding remoto).

- Integración por API: demandan conectar sus propios sistemas de gestión de órdenes (OMS) a las plataformas de las casas de bolsa mediante APIs estandarizadas y documentadas.
- Reporting estructurado: requieren confirmaciones de operación, estados de cuenta y documentación de cumplimiento (incluyendo declaraciones juradas) en formatos electrónicos legibles por máquina (JSON, XML, PDF con metadatos).
- Transparencia en cumplimiento: exigen que los intermediarios demuestren la aplicación de medidas de debida diligencia equivalentes a las de jurisdicciones con regímenes robustos contra el LC/FT.

El incumplimiento de estas expectativas no llevará a que los inversionistas acepten estándares más bajos. Más bien, buscarán canales alternativos (operaciones over-the-counter no reportadas, vehículos en otras jurisdicciones), lo que incrementaría los riesgos de desintermediación y opacidad.

Estado actual del mercado de valores venezolano

Estructura del mercado: el SICET y la separación histórica de la deuda pública

Un elemento estructural que condiciona la configuración actual del mercado es la separación histórica entre la negociación de deuda pública y el mercado bursátil propiamente dicho. Antes de 2010, la negociación de títulos de deuda pública se realizaba a través del SICET (Sistema de Interconexión de Cuentas Electrónicas y Títulos), un sistema administrado por el Banco Central de Venezuela (BCV) que operaba de manera paralela a la Bolsa de Valores de Caracas. Esto implicaba que los títulos públicos se podían comprar a través de la banca, sin intervención necesariamente de las casas de bolsa o sociedades de corretaje de valores.

Como resultado, el mercado bursátil tradicional se desarrolló con un foco predominante en valores del sector privado y con una base de inversionistas mayoritariamente local.

A partir de 2014, se produce una reapertura gradual de casas de bolsa, con un ámbito de acción definido: la intermediación exclusiva con valores de empresas privadas. Durante esta etapa, el mercado ha operado con aproximadamente 36 casas de bolsa activas, negociando principalmente acciones de compañías privadas, títulos de deuda privada (obligaciones, papeles comerciales) y, en menor medida, vehículos de inversión estructurados.

Diagnóstico tecnológico: 36 casas de bolsa, solo 2 con APP

El estado actual de digitalización de los intermediarios puede sintetizarse en un dato: de las 36 casas de bolsa registradas, solo dos (2) cuentan con una aplicación móvil (APP) funcional que permita a sus clientes abrir cuentas, consultar saldos y ejecutar órdenes de manera completamente digital. Los 34 restantes operan con mecanismos que incluyen:

- Instrucciones por vía telefónica a los operadores.
- Envío de órdenes por correo electrónico (con riesgos de suplantación y falta de autenticación robusta).
- Portales web de funcionalidad básica, en muchos casos sin integración con sistemas de verificación biométrica.

Esta situación no refleja una falta de voluntad de los intermediarios, sino una consecuencia de la ecuación económica que se analizará más adelante: el desarrollo y mantenimiento de una APP segura, con módulos de biometría, cifrado y monitoreo transaccional, tiene costos fijos prohibitivos para la mayoría de las casas de bolsa si actúan individualmente.

Pruebas en curso de APIs interrelacionadas

En la actualidad, se están realizando pruebas técnicas para la incorporación de APIs que interrelacionen a los distintos actores del mercado: casas de bolsa, bolsa de valores, entidades de custodia, como la Caja Venezolana de Valores. El objetivo es permitir la transmisión electrónica de órdenes, la

confirmación de operaciones y la liquidación de manera más ágil y con menor intervención manual.

Estas pruebas son un avance positivo en la dirección de la interoperabilidad. Sin embargo, su alcance actual se limita a la ejecución y liquidación de operaciones, no así a la gestión del riesgo LC/FT de manera agregada. El monitoreo cruzado, la capacidad de detectar que un mismo cliente abre cuentas en múltiples intermediarios y fracciona sus operaciones, no está contemplado en estas pruebas.

Marco normativo vigente para la administración de riesgos LC/FT

Providencia Normativa N° 025: identidad digital y SIAR

La Providencia Normativa N° 025 (Gaceta Oficial N° 43.096) constituye el marco fundamental del Sistema Integral de Administración de Riesgos (SIAR), en el mercado de valores venezolano. Sus disposiciones más relevantes son:

- Artículo 58: otorga plena validez jurídica a la identidad digital (SmartID) y al uso de plataformas electrónicas para el registro de participantes. Este artículo es el pilar normativo que permite el onboarding digital sin documentos físicos.
- Artículo 11 y 13: diferencian las Medidas Simplificadas de Debida Diligencia (para productos y canales de bajo riesgo) de las Medidas Intensificadas (para perfiles de mayor riesgo).
- Artículo 47: establece la prohibición de flexibilizar controles ante cualquier indicio de legitimación de capitales. (SUNAVAL, 2025)

Circular DSNV/GCI/002: cuentas Nivel 1 y Nivel 2

La Circular DSNV/GCI/002 (4 de abril de 2025) crea las Cuentas de Corretaje Bursátil (CCBU) de Nivel 1 y Nivel 2 (SUNAVAL, 2025).

Nivel 1:

- Permite apertura de cuentas para personas naturales con documentación reducida: copia de la cédula de identidad o pasaporte.
- Límite de movilización mensual: 1.000 veces la moneda de mayor denominación publicada por el BCV.

- Objetivo: incentivar la participación del pequeño inversionista y promover la cultura bursátil.

Nivel 2:

- Se activa automáticamente al superar el límite del Nivel 1.
- Exige RIF y certificaciones de ingresos (constancia de trabajo o informe de atestiguamiento de contador público).
- No tiene límite de movilización, pero el monitoreo se intensifica.

La exigencia de la Declaración Jurada por operación

La Circular 002 es categórica en un punto crítico: la simplificación en la apertura de cuentas Nivel 1 no exime del monitoreo continuo. Se mantienen plenamente vigentes las exigencias de las Normas Sobre Actividades de Intermediación de Corretaje y Bolsa (2008), que obligan a recabar la Planilla de Declaración Jurada de Origen y Destino de Fondos en cada una de las operaciones que realice el cliente (SUNAVAL, 2008; SUNAVAL, 2025).

Esta exigencia, en un entorno manual, es un cuello de botella operativo que escala linealmente con el número de transacciones. En un entorno digital, requiere un sistema de firma electrónica y generación automática de declaraciones, lo que a su vez demanda infraestructura tecnológica (HSM, certificados digitales, APIs de firma).

Estándares internacionales en materia de riesgo tecnológico

Recomendación 1 del GAFI: evaluación de riesgos

La Recomendación 1 del GAFI establece que los países deben identificar, evaluar y comprender los riesgos LC/FT a los que están expuestos (FATF, 2025). Esta evaluación debe actualizarse periódicamente y debe incorporar los nuevos riesgos derivados de la digitalización y la apertura externa. En el caso venezolano, la evaluación de riesgos del mercado de valores debería incluir explícitamente los vectores de riesgo analizados más adelante.

La recomendación también señala que la evaluación de riesgos debe ser la base para la asignación de recursos y el diseño de medidas de mitigación. Esto implica que la evaluación debe ser proporcional al contexto y capacidad

del mercado, lo que refuerza la necesidad de soluciones en mercados pequeños.

Recomendación 15 del GAFI: nuevas tecnologías

La Recomendación 15 aborda las tecnologías financieras innovadoras. Su principio central es el de neutralidad tecnológica (FATF, 2025): los requisitos de debida diligencia y las medidas preventivas deben aplicarse independientemente del canal o la tecnología utilizada. Una operación ejecutada a través de una APP o una API debe cumplir con los mismos estándares que una operación presencial.

La Recomendación 15 también exige que los países evalúen si sus marcos legales abordan adecuadamente los riesgos de las nuevas tecnologías y, en caso necesario, los modifiquen. En el caso venezolano, la Providencia N° 025 y la Circular 002 constituyen un marco adecuado, pero se requiere normativa técnica secundaria sobre estándares concretos: niveles de aseguramiento de identidad digital, requisitos de seguridad para APIs, criterios de detección de vida, entre otros.

Guía de Identidad Digital del GAFI (2020): niveles de garantía y detección de vida

La Guía sobre Identidad Digital del GAFI (2020) introduce el concepto de niveles de garantía, que clasifican los sistemas de identidad digital según la confianza que puede depositarse en ellos. Los tres pilares de los niveles de garantía son (FATF, 2020):

- Tecnología: robustez de los mecanismos de autenticación, cifrado, biometría y detección de vida.
- Gobernanza: existencia de un marco claro de responsabilidades y supervisión del emisor de identidad.
- Procesos y procedimientos: solidez de los procesos de inscripción, vinculación y gestión del ciclo de vida.

La guía dedica una sección específica a los riesgos de suplantación biométrica (spoofing) y a los deepfakes. Recomienda que los sistemas de identidad digital implementen mecanismos de detección de vida que pueden ser:

- Pasivos: analizan textura de piel, reflejos especulares, microexpresiones, sin requerir acción del usuario.
- Activos: solicitan al usuario realizar un movimiento aleatorio (guiñar un ojo, mover la cabeza en una dirección específica) y verifican que la respuesta sea coherente con un ser humano en tiempo real (FATF, 2020).

Marco metodológico para la gestión del riesgo de seguridad de la información

Para gestionar adecuadamente los riesgos de LC/FT asociados a la digitalización del mercado de valores, es indispensable recurrir a metodologías reconocidas internacionalmente para la gestión de riesgos de seguridad de la información. Dos de los marcos más relevantes son la norma ISO/IEC 27005 y la guía NIST SP 800-30.

ISO/IEC 27005:2022 – Guidance on Managing Information Security Risks

La norma ISO/IEC 27005:2022 es un estándar internacional que proporciona directrices para la gestión de riesgos de seguridad de la información. Esta norma complementa el sistema de gestión de seguridad de la información (ISMS) establecido por la ISO/IEC 27001:2022, ofreciendo un marco práctico para identificar, analizar, evaluar y tratar los riesgos de seguridad de la información (ISO/IEC 27005, 2022).

Principales características

Enfoque basado en activos y eventos: La norma se basa en el método de identificación de riesgos a través de activos, amenazas y vulnerabilidades, e incorpora el concepto de escenarios de riesgo, que permite analizar eventos específicos que podrían materializarse.

Alineación con ISO 31000: La ISO/IEC 27005 utiliza como base el proceso general de gestión de riesgos establecido en la ISO 31000:2018 (ISO 31000, 2018; ISO/IEC 27005, 2022), Risk Management, Guidelines, aplicándolo específicamente a la seguridad de la información.

Estructura del proceso de gestión: La norma establece un proceso estructurado que incluye:

- Establecimiento del contexto: definición de criterios de riesgo, identificación de partes interesadas y selección del método de evaluación.
- Evaluación del riesgo: identificación, análisis (cálculo de consecuencias y probabilidad) y evaluación (priorización) de riesgos.
- Tratamiento del riesgo: selección de opciones de tratamiento (mitigación, transferencia, aceptación, evitación), implementación de controles y aceptación del riesgo residual.
- Monitoreo y revisión: seguimiento continuo de los factores que influyen en el riesgo y mejora continua del proceso.
-

Aplicabilidad al mercado de valores venezolano

En el contexto del mercado bursátil venezolano, la implementación de un sistema de gestión de riesgos basado en ISO/IEC 27005 implicaría:

1. Identificar activos de información críticos: las APP de las casas de bolsa, las bases de datos de clientes, los sistemas de custodia y las APIs interrelacionadas.
2. Identificar amenazas y vulnerabilidades: las amenazas incluyen ataques de deepfakes, suplantación de identidad, ataques a APIs, y los riesgos de legitimación de capitales asociados a la fragmentación transaccional y las identidades sintéticas.
3. Analizar y evaluar el riesgo: determinar la probabilidad de materialización y el impacto potencial (financiero, reputacional, regulatorio) de cada amenaza.

4. Seleccionar controles: implementar medidas como detección de vida biométrica, autenticación multifactor, monitoreo transaccional y cifrado de datos.

El estándar enfatiza que la aplicación de esta metodología debe ser proporcional al contexto y tamaño de la organización. Sin embargo, la implementación de controles adecuados en una casa de bolsa venezolana tiene un costo elevado.

NIST SP 800-30 Revision 1 – Guide for Conducting Risk Assessments

La NIST Special Publication 800-30, Revision 1, titulada "Guide for Conducting Risk Assessments", es una publicación del National Institute of Standards and Technology (NIST) de los Estados Unidos. Ofrece un enfoque práctico y detallado para evaluar los riesgos a los que se enfrentan los sistemas de información.

Definición de riesgo

La guía define el riesgo como "una medida del grado en que una entidad se ve amenazada por una circunstancia o evento potencial, y típicamente es una función de: (i) los impactos adversos que surgirían si la circunstancia o evento ocurre; y (ii) la probabilidad de ocurrencia" (NIST SP 800-30 Rev.1, 2012).

Proceso de evaluación de riesgos

El proceso de evaluación de riesgos según la NIST SP 800-30 se estructura en tres fases principales:

1. Preparación:
   - Identificar el propósito y alcance de la evaluación.
   - Definir las suposiciones y limitaciones.
   - Establecer o refinar el modelo de riesgo.
2. Conducción:
   - Identificar las fuentes de amenaza (ej. actores maliciosos que utilizan deepfakes).

- Identificar los eventos de amenaza (ej. suplantación de identidad en el onboarding digital).
- Determinar la probabilidad de ocurrencia.
- Determinar el impacto adverso potencial (ej. multas regulatorias, daño reputacional, pérdidas financieras).
- Determinar el riesgo resultante de la combinación de probabilidad e impacto.

3. Mantenimiento:
   - Monitoreo continuo de los factores de riesgo.
   - Actualización de la evaluación de riesgos utilizando los resultados del monitoreo (NIST SP 800-30 Rev.1, 2012).

La guía también describe diferentes enfoques de evaluación (cuantitativo, semicuantitativo y cualitativo), destacando que el enfoque cualitativo (basado en niveles como bajo, moderado y alto) es más sencillo de comunicar a los responsables de la toma de decisiones, aunque requiere un esfuerzo adicional para garantizar la repetibilidad y reproducibilidad.

Aplicabilidad al mercado de valores venezolano

Fase	Aplicación práctica al mercado bursátil venezolano
Preparación	Definir el alcance: riesgos LC/FT asociados a la APP de una casa de bolsa y a las APIs interrelacionadas.
Conducción	Identificar amenazas: *deepfakes*, suplantación de identidad, ataques de smurfing entre intermediarios, vulnerabilidades en APIs. Identificar vulnerabilidades: falta de detección de vida activa, ausencia de autenticación mutua TLS, procesos manuales de verificación. Determinar probabilidad e impacto en función del tamaño del mercado y la exposición a nuevos actores internacionales.

Mantenimiento	Establecer un proceso de monitoreo continuo de los controles implementados y actualizar la evaluación periódicamente a medida que evolucionan las amenazas.

Fuente: Verasmendi 2026

Al igual que con la ISO/IEC 27005, la aplicación completa de la NIST SP 800-30 requiere recursos humanos y técnicos que la mayoría de las casas de bolsa venezolanas no poseen.

Ambas metodologías son complementarias y pueden utilizarse de manera integrada:

La ISO/IEC 27005 proporciona el marco estratégico y el ciclo de vida completo de la gestión de riesgos, desde el establecimiento del contexto hasta el monitoreo continuo.

La NIST SP 800-30 ofrece el enfoque táctico y detallado para la fase de evaluación del riesgo, con pasos concretos para identificar amenazas, vulnerabilidades y calcular la probabilidad e impacto.

En el contexto de la digitalización del mercado de valores venezolano, una casa de bolsa podría utilizar la NIST SP 800-30 para evaluar el riesgo específico de los deepfakes en su proceso de onboarding digital, y luego utilizar la ISO/IEC 27005 para diseñar e implementar un plan de tratamiento del riesgo que incluya la selección de controles, la asignación de responsables y el monitoreo continuo.

La aplicación integrada de ambas metodologías revela un hallazgo crítico: la implementación de un sistema de gestión de riesgos de seguridad de la información según ISO/IEC 27005, complementado con evaluaciones detalladas según NIST SP 800-30, es técnicamente posible pero económicamente cuesta arriba para la mayoría de las casas de bolsa venezolanas.

Riesgos de Legitimación de Capitales asociados a nuevas tecnologías

La digitalización del mercado de valores introduce riesgos LC/FT que difieren cualitativamente de aquellos que el sistema de administración de riesgos fue diseñado para enfrentar. A continuación, se analizan los más relevantes.

Riesgo de fragmentación transaccional (Pitufeo o smurfing) entre múltiples intermediarios

Descripción del riesgo:

La Circular 002 establece un límite mensual para las cuentas Nivel 1 (1.000 veces la moneda de mayor denominación). Un mismo inversionista podría abrir cuentas Nivel 1 en varias casas de bolsa y operar hasta ese límite en cada una de ellas, moviendo en agregado un volumen muy superior al permitido sin que ninguno de los intermediarios, actuando aisladamente, detecte el exceso.

Magnitud en el contexto venezolano:

Con 36 casas de bolsa, si un agente malicioso logra abrir cuentas Nivel 1 en 10 de ellas, podría mover hasta 10 veces el límite individual. Las dos casas con APP probablemente tienen controles más estrictos; los 34 restantes, con procesos más manuales, son potencialmente más vulnerables.

Evaluación según NIST SP 800-30:

- Fuente de amenaza: actores maliciosos con capacidad para abrir múltiples cuentas.
- Evento de amenaza: fraccionamiento de operaciones para evadir el límite del Nivel 1.
- Vulnerabilidad: ausencia de un mecanismo de consolidación de información entre intermediarios.
- Impacto potencial: alto (entrada de capitales ilícitos al mercado regulado).
- Probabilidad: alta (dado el número de intermediarios y la facilidad de apertura de cuentas Nivel 1).

Riesgo de deepfakes y suplantación biométrica en procesos de onboarding digital

Descripción del riesgo:

Un deepfake es un video, imagen o audio generado por inteligencia artificial que imita los rasgos y movimientos de una persona real (FATF, 2020; World Economic Forum, 2025). Un atacante puede:

1. Obtener material audiovisual de una víctima (por ejemplo, de redes sociales).
2. Utilizar software de acceso público (DeepFaceLab, FaceSwap) para generar un video corto en el que la víctima realiza los movimientos típicos solicitados por los sistemas de verificación facial.
3. Presentar ese video a la APP o al portal de onboarding a través de un emulador de cámara, simulando que es una transmisión en vivo.

Si el sistema de verificación solo verifica la presencia de un rostro y movimientos básicos (detección de vida pasiva), el deepfake puede superar la prueba (FATF, 2020).

Magnitud en el contexto venezolano:

Las dos casas de bolsa con APP desconocen públicamente si incluyen mecanismos de detección de vida activa o soluciones específicas contra deepfakes. Las 34 casas restantes, que operan con procesos manuales o portales web básicos, pueden no tener verificación biométrica en absoluto, lo que las hace vulnerables a formas más simples de suplantación.

Evaluación según NIST SP 800-30:

- Fuente de amenaza: actores maliciosos con acceso a herramientas de IA generativa.
- Evento de amenaza: suplantación de identidad en el proceso de apertura de cuenta.
- Vulnerabilidad: falta de detección de vida activa en los sistemas de verificación.

- Impacto potencial: alto (apertura de cuentas con identidades falsificadas).
- Probabilidad: media-alta (dado el bajo costo de las herramientas de deepfake y la ausencia de controles en la mayoría de los intermediarios).

Riesgo de identidades sintéticas

Descripción del riesgo:

Una identidad sintética combina datos reales (por ejemplo, un número de cédula de identidad legítimo obtenido de una filtración de datos) con datos ficticios (un domicilio inventado, un número de teléfono descartable, una dirección de correo electrónico temporal). El resultado es una identidad que no corresponde a una persona real existente, pero que puede pasar verificaciones documentales básicas si el sistema no contrasta múltiples fuentes de información.

Magnitud en el contexto venezolano:

Las cuentas Nivel 1, que no exigen RIF ni constancia de ingresos, son particularmente vulnerables a la apertura con identidades sintéticas. Un atacante podría generar múltiples identidades sintéticas y abrir cuentas en diferentes casas de bolsa, operando cada una dentro del límite mensual, pero moviendo en agregado volúmenes significativos.

Evaluación según ISO/IEC 27005:

- Activo: base de datos de clientes.
- Amenaza: creación de identidades sintéticas.
- Vulnerabilidad: verificación documental insuficiente.
- Riesgo: apertura de cuentas con identidades ficticias.
- Impacto: reputacional y regulatorio.
- Probabilidad: alta en ausencia de controles adicionales.

Riesgos de seguridad en APIs y APP

Descripción del riesgo:

Las APIs y APP que exponen funcionalidades sensibles (envío de órdenes, consulta de saldos, obtención de información de clientes) pueden ser atacadas si no se implementan con estándares de seguridad rigurosos. Los vectores de ataque incluyen:

- Autenticación débil: credenciales por defecto, tokens sin expiración, ausencia de autenticación multifactor.
- Inyección de órdenes: un atacante que obtiene acceso a la API de un cliente puede ejecutar órdenes de compra o venta en su nombre, generando pérdidas.
- Escalamiento de privilegios: un atacante con acceso de bajo nivel puede explotar vulnerabilidades para obtener acceso administrativo.
- Fuga de datos: APIs mal configuradas pueden exponer información de todos los clientes (OWASP, 2023).

Magnitud en el contexto venezolano:

Las pruebas de APIs interrelacionadas que se están realizando son un primer paso, pero la normativa venezolana no especifica aún estándares técnicos para la seguridad de APIs financieras. Las dos APP existentes pueden tener distintos niveles de seguridad. La ausencia de estándares unificados aumenta el riesgo de que algunas implementaciones sean vulnerables.

Evaluación según NIST SP 800-30:

- Fuente de amenaza: atacantes externos con conocimientos técnicos.
- Evento de amenaza: explotación de vulnerabilidades en APIs.
- Vulnerabilidad: ausencia de estándares de seguridad unificados.
- Impacto potencial: muy alto (fuga de datos, ejecución de órdenes no autorizadas).
- Probabilidad: media-baja (requiere conocimientos técnicos especializados).

Riesgo de desintermediación por exigencias tecnológicas no satisfechas

Descripción del riesgo:

Si los intermediarios locales no pueden satisfacer las exigencias tecnológicas y de cumplimiento de los inversionistas internacionales (onboarding digital rápido, integración por API, reporting estructurado), estos inversionistas buscarán canales alternativos para operar en valores venezolanos. Estos canales pueden incluir:

- Vehículos de inversión constituidos en otras jurisdicciones que operen como intermediarios indirectos.
- Uso de testaferros locales que actúen como titulares nominales de las cuentas.

Magnitud en el contexto venezolano:

La desintermediación es especialmente riesgosa porque saca las operaciones del ámbito de supervisión de la SUNAVAL y de los sistemas de monitoreo de las casas de bolsa. El resultado es una pérdida de visibilidad regulatoria que puede ser explotada para mover capitales de origen ilícito.

Evaluación según ISO/IEC 27005:

- Activo: canal de intermediación regulado.
- Amenaza: migración a canales no regulados.
- Vulnerabilidad: falta de capacidad tecnológica para atender a inversionistas internacionales.
- Riesgo: pérdida de visibilidad regulatoria.
- Impacto: muy alto (entrada de capitales ilícitos fuera del sistema de monitoreo).
- Probabilidad: alta si no se realizan inversiones tecnológicas significativas.

El dilema económico de la administración de riesgos tecnológicos

La paradoja del mercado pequeño: costos fijos elevados, ingresos reducidos

El mercado de valores venezolano tiene un tamaño reducido en términos de volumen de negociación diaria si se compara con otros mercados regionales (PNUD, 2021; Ecoanalítica, 2023). Sin embargo, los costos de implementación de sistemas de cumplimiento tecnológico (biometría, monitoreo transaccional, ciberseguridad, desarrollo de APIs) no escalan linealmente con el tamaño del mercado. Una plataforma de verificación facial cuesta sustancialmente lo mismo instalarla en una casa de bolsa venezolana que en una chilena, pero los ingresos de la primera son entre 10 y 20 veces menores.

Esta paradoja del tamaño genera una situación de complejidad económica para la mayoría de los intermediarios si cada uno intenta construir su propia infraestructura de cumplimiento digital.

A continuación, se desagregan los rubros de una casa de bolsa venezolana para implementar un sistema de cumplimiento digital alineado con los estándares del GAFI y las metodologías ISO/IEC 27005 y NIST SP 800-30:

- Verificación Biométrica
- Infraestructura y Ciberseguridad
- Desarrollo y mantenimiento de APP
- Personal especializado
- Monitoreo Transaccional
- Capacitación continua

Límites de las APIs interrelacionadas actuales para la gestión de riesgos LC/FT

Las pruebas de APIs interrelacionadas que se están realizando son un avance positivo, pero no resuelven el dilema económico ni los riesgos LC/FT por varias razones:

- Alcance limitado a ejecución y liquidación: las APIs en prueba no están diseñadas para consolidar información de identidad de clientes ni para detectar fraccionamiento transaccional.

- No resuelven el costo de la verificación biométrica: cada casa de bolsa sigue necesitando su propia solución de verificación facial y detección de vida, con los costos asociados.
- No habilitan el monitoreo cruzado: sin un identificador único de cliente compartido y un motor de consolidación de transacciones, el riesgo de smurfing entre intermediarios persiste.
- Participación voluntaria: si solo un subconjunto de las 36 casas participa en las pruebas, el monitoreo cruzado sería incompleto.

Estas limitaciones no invalidan el valor de las APIs interrelacionadas; simplemente indican que se necesita una arquitectura de cumplimiento adicional y específica más allá de la interconexión operativa.

Perspectivas globales: el Global Risks Report y las tendencias tecnológicas

El Global Risks Report 2025 del World Economic Forum (WEF) proporciona un contexto relevante para comprender la urgencia de abordar los riesgos tecnológicos en el mercado de valores venezolano.

Hallazgos clave del Global Risks Report 2025

1. Los riesgos tecnológicos son una amenaza creciente a largo plazo: El informe revela que, si bien los riesgos tecnológicos no se perciben como la amenaza más inmediata, su severidad proyectada a 10 años aumenta considerablemente. La desinformación y los resultados adversos de la inteligencia artificial son dos de los riesgos que más ascienden en el ranking a largo plazo.
2. La desinformación y la IA como riesgos centrales: La información errónea y la desinformación se mantienen como el principal riesgo a corto plazo (2 años) por segundo año consecutivo, impulsado por la capacidad de la IA Generativa para crear y distribuir contenido falso a escala. El resultado adverso de las tecnologías es uno de los riesgos que más asciende en el ranking a 10 años (World Economic Forum, 2025), reflejando la preocupación por sesgos algorítmicos,

ciberataques impulsados por IA y la pérdida de control humano sobre sistemas autónomos (World Economic Forum, 2025).

3. El efecto acelerador de la tecnología en otros riesgos: El informe destaca cómo la tecnología acelera y exacerba otros riesgos globales (World Economic Forum, 2025), como la polarización social y la inestabilidad geopolítica. Esta lógica es exportable al mercado bursátil venezolano: la digitalización, si no se gestiona con controles adecuados, no crea un nuevo riesgo aislado, sino que amplifica la vulnerabilidad existente frente a la Legitimación de Capitales.

Implicaciones para el mercado de valores venezolano

El Global Risks Report 2025 sugiere que la adopción de tecnologías como la IA está ocurriendo más rápido que la regulación y los controles de riesgo. En el contexto venezolano, esto implica que:

1. Los riesgos de deepfakes e identidades sintéticas no son escenarios hipotéticos, sino tendencias globales confirmadas que ya están afectando a los sistemas financieros en otras jurisdicciones.
2. La ventana de oportunidad para implementar controles es limitada: a medida que la tecnología avanza, los costos de ponerse al día aumentan exponencialmente.
3. La inversión en controles tecnológicos no es un gasto, sino una inversión en resiliencia sistémica que permite al mercado venezolano alinearse con las tendencias globales y atraer inversión internacional.

Reflexiones Finales

El mercado de valores venezolano se encuentra en un momento histórico de transformación. La normalización de las relaciones financieras internacionales, impulsada por la reestructuración de la deuda, la reinserción en SWIFT y la llegada de nuevos inversionistas internacionales, ofrece una oportunidad sin precedentes para profundizar el mercado, aumentar su liquidez y consolidar su papel en la economía nacional. Sin embargo, esta apertura también expone

al sistema a nuevos y sofisticados riesgos de legitimación de capitales que el actual Sistema Integral de Administración de Riesgos (SIAR) no está preparado para enfrentar.

El diagnóstico realizado en este ensayo ha identificado cinco riesgos críticos asociados a la digitalización:

Fragmentación transaccional (smurfing) entre múltiples intermediarios: un mismo cliente podría abrir cuentas Nivel 1 en varias casas de bolsa y operar hasta el límite en cada una, moviendo en agregado un volumen muy superior al permitido sin que ningún intermediario, actuando aisladamente, lo detecte.

Deepfakes y suplantación biométrica: la tecnología de inteligencia artificial permite generar videos que imitan a personas reales, pudiendo superar sistemas de verificación facial básicos en los procesos de onboarding digital.

Identidades sintéticas: la combinación de datos reales y ficticios permite crear identidades que no corresponden a personas existentes, pero que pueden pasar verificaciones documentales básicas.

Vulnerabilidades en APIs y APP: la falta de estándares de seguridad unificados expone a las interfaces digitales a ataques de autenticación, inyección de órdenes y fuga de datos.

Desintermediación: si los intermediarios locales no satisfacen las exigencias tecnológicas de los inversionistas internacionales, estos buscarán canales alternativos no regulados, con la consiguiente pérdida de visibilidad para el regulador.

Frente a estos riesgos, el ensayo ha identificado un dilema económico estructural: el mercado de valores venezolano es demasiado pequeño para que cada una de las 36 casas de bolsa pueda costear, individualmente, los sistemas de cumplimiento tecnológico necesarios. Los costos anuales de implementación (entre $110.000 y $285.000 por casa) consumirían entre el 61% y el 114% de los ingresos de una casa mediana, haciendo inviable la inversión para la mayoría de los intermediarios. Este diagnóstico explica por qué solo dos casas de bolsa tienen APP funcionales.

Las metodologías internacionales de gestión de riesgos de seguridad de la información –ISO/IEC 27005:2022 y NIST SP 800-30 Revision 1, ofrecen un marco riguroso para abordar estos desafíos (ISO/IEC 27005, 2022; NIST SP 800-30 Rev.1, 2012). La ISO/IEC 27005 proporciona el ciclo de vida completo de la gestión de riesgos (contexto, evaluación, tratamiento, monitoreo), mientras que la NIST SP 800-30 ofrece un enfoque táctico detallado para la evaluación de riesgos específicos, como los deepfakes y el smurfing. Sin embargo, la aplicación de estas metodologías requiere recursos humanos y técnicos que la mayoría de las casas de bolsa venezolanas no poseen, reforzando la necesidad de una respuesta estructural.

El Global Risks Report 2025 del World Economic Forum refuerza la urgencia de esta respuesta, al señalar que los riesgos tecnológicos –incluyendo los resultados adversos de la IA– son una de las amenazas que más crecen en el horizonte de 10 años. La adopción de tecnología está ocurriendo más rápido que la regulación y los controles, lo que implica que los sistemas financieros que no se preparen proactivamente quedarán expuestos a vulnerabilidades crecientes.

La principal conclusión de este ensayo es que el mercado de valores venezolano enfrenta un desafío estructural que no puede ser resuelto por la acción individual de cada intermediario. La combinación de un mercado pequeño, costos fijos elevados y riesgos tecnológicos crecientes exige una respuesta coordinada que trascienda las capacidades individuales. Esta respuesta debe incluir:

Una evaluación de riesgos actualizada a nivel sectorial, que incorpore los nuevos vectores de riesgo identificados en este ensayo y que sirva de base para la asignación de recursos.

El establecimiento de estándares técnicos mínimos para la seguridad de APIs, la verificación biométrica y el monitoreo transaccional, que garanticen un piso común de protección para todo el mercado.

Mecanismos que permitan compartir infraestructura o información entre los intermediarios, especialmente para el monitoreo cruzado de transacciones, sin que esto implique necesariamente una plataforma centralizada.

Un programa de capacitación y asistencia técnica para las casas de bolsa más pequeñas, que les permita elevar sus estándares de cumplimiento sin comprometer su viabilidad económica.

En definitiva, la transformación digital del mercado de valores venezolano no debe evaluarse únicamente como un desafío tecnológico, sino como una oportunidad estratégica para fortalecer la transparencia, la integridad y la competitividad del sistema financiero nacional. La capacidad del sector para incorporar tecnologías seguras, adoptar estándares internacionales de gestión de riesgos y desarrollar mecanismos de cooperación institucional determinará no solo la efectividad de la prevención de la legitimación de capitales y el financiamiento al terrorismo, sino también su capacidad para integrarse de manera sostenible a los mercados financieros internacionales.

Referencias

Asamblea Nacional de la República Bolivariana de Venezuela. (2012). Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT). Gaceta Oficial Nº 39.912.

Escuela Nacional de Administración y Hacienda Pública. (2016). Manual para elaboración y presentación de trabajos académicos. ENAHP-IUT. Caracas.

Grupo de Acción Financiera Internacional. (2026) Resultados de la Plenaria del GAFI, México. https://www.fatf-gafi.org/

Grupo de Acción Financiera de Latinoamérica (GAFILAT). (2025). Informe del Taller sobre supervisión con foco en la aplicación de medidas de debida diligencia del cliente (DDC) simplificada y la aplicación de un enfoque basado en riesgos (EBR).

Grupo de Acción Financiera Internacional (GAFI). (2024). Metodología para la Evaluación del Cumplimiento Técnico con las recomendaciones del GAFI y la efectividad de los Sistemas de ALA/CFT. París: OCDE/GAFI.

Grupo de Acción Financiera Internacional (GAFI). (2025). Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación de armas de destrucción masiva: Las Recomendaciones del GAFI.

Grupo de Acción Financiera de Latinoamérica. (2020). Guía sobre indicadores de riesgo de Lavado de Activos y Financiamiento del Terrorismo para el sector de mercado de valores. GAFILAT. https://www.gafilat.org/

Grupo Banco Mundial. (2026) Inclusión Financiera. Disponible: https://www.bancomundial.org (Consulta: 2026/03/16)

Programa de las Naciones Unidas para el Desarrollo. (2021). Estudio sobre el desarrollo del sector privado en Venezuela: Desafíos y oportunidades. PNUD Venezuela.

Superintendencia Nacional de Valores (2025). Normas relativas a la administración y fiscalización de los riesgos relacionados con los delitos de legitimación de capitales, financiamiento al terrorismo, financiamiento de la proliferación de armas de destrucción masiva y otros ilícitos. Gaceta Oficial de la República Bolivariana de Venezuela N° 43.096 del 27 de marzo de 2025.

Superintendencia Nacional de Valores (2025). Circular DSNV/GCI/002: Flexibilización de los requisitos para la apertura de cuentas de corretaje bursátiles.

Superintendencia Nacional de Valores (2008). Normas Sobre Actividades de Intermediación de Corretaje y Bolsa. Gaceta Oficial de la República Bolivariana de Venezuela N° 38.956 del 19 de junio de 2008.

FATF. (2012-2023). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations. Financial Action Task Force. [En línea] Disponible en: www.fatf-gafi.org/recommendations

FATF. (2020). Guidance on Digital Identity. Financial Action Task Force. [En línea] Disponible en: www.fatf-gafi.org/publications/digital-identity

ISO/IEC 27005:2022. (2022). Information security, cybersecurity and privacy protection — Guidance on managing information security risks. International Organization for Standardization / International Electrotechnical Commission. [En línea] Disponible en: www.iso.org/standard/80585.html

ISO/IEC 27001:2022. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

International Organization for Standardization / International Electrotechnical Commission. [En línea] Disponible en: www.iso.org/standard/27001

ISO 31000:2018. (2018). Risk management — Guidelines. International Organization for Standardization. [En línea] Disponible en: www.iso.org/standard/65694.html

NIST Special Publication 800-30 Revision 1. (2012). Guide for Conducting Risk Assessments. National Institute of Standards and Technology, U.S. Department of Commerce. [En línea] Disponible en: csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

OWASP. (2023). API Security Top 10. Open Web Application Security Project. [En línea] Disponible en: owasp.org/API-Security

World Economic Forum. (2025). The Global Risks Report 2025. [En línea] Disponible en: www.weforum.org/publications/global-risks-report-2025

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

CRIPTOACTIVOS, PRIVACIDAD Y LEGITIMACIÓN DE CAPITALES: ANÁLISIS DE LOS MECANISMOS TECNOLÓGICOS UTILIZADOS POR LA DELINCUENCIA ORGANIZADA TRANSNACIONAL

Autor: Abg. Esp. Víctor Ordaz
Facilitadora: Msc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

Criptoactivos, privacidad y legitimación de capitales: análisis de los mecanismos tecnológicos utilizados por la delincuencia organizada transnacional

Autor: Abg. Esp. Victor Ordaz
Código ORCID: 0009-0007-5234-9369
Correo electrónico: vordazccs@gmail.com

Resumen

El texto analiza cómo la delincuencia organizada transnacional utiliza los criptoactivos, monedas de privacidad como Monero, mezcladores y puentes cross-chain para ejecutar la legitimación de capitales de manera rápida, transfronteriza y anónima, saltándose las etapas tradicionales del lavado de dinero. Frente a esta amenaza sistémica se examina la vigencia y los vacíos de marcos normativos como la Convención de Palermo y la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT). Finalmente, el ensayo concluye que para combatir eficazmente este delito sin satanizar el uso legítimo de la tecnología blockchain, se requiere actualizar las leyes, fortalecer las capacidades técnicas de investigación, aplicar técnicas especiales y consolidar la cooperación internacional e interinstitucional.

Abstract

The text analyzes how transnational organized crime utilizes crypto-assets—such as privacy coins like Monero, mixers, and cross-chain bridges—to launder money rapidly, across borders, and anonymously, bypassing traditional money laundering stages. In light of this systemic threat, the study examines the current relevance and gaps in regulatory frameworks such as the Palermo Convention and the Organic Law Against Organized Crime and Terrorist Financing (LOCDOFT). Finally, the essay concludes that effectively combating this crime—without demonizing the legitimate use of blockchain technology—requires updating laws, strengthening technical investigative capabilities, employing special investigative techniques, and consolidating international and inter-institutional cooperation.

Introducción

Cuando Satoshi Nakamoto publicó en 2009 el libro blanco de Bitcoin, pocos imaginaban que aquel experimento criptográfico terminaría transformando para siempre la manera en que el mundo concibe el dinero. Lo que comenzó como una promesa de libertad financiera y descentralización se ha convertido, para bien y para mal, en una de las herramientas más poderosas del siglo XXI. Y como ocurre con toda innovación, quienes operan al margen de la ley no tardaron en encontrar en ella un aliado perfecto.

Los criptoactivos han llegado para quedarse. Su capacidad para cruzar fronteras sin pedir permiso, para moverse con una velocidad que los sistemas bancarios tradicionales envidian y para operar con costos irrisorios las hace extraordinariamente atractivas. Pero también las convierte en el vehículo ideal para ocultar el origen de fondos ilícitos. La misma tecnología que permite a un trabajador en Caracas enviar dinero a su familia en Bogotá en cuestión de minutos es la que pudieran utilizan los carteles de narcotráfico para legitimar sus ganancias.

La magnitud del problema es abrumadora. Según el más reciente informe de Chainalysis, en 2024 las direcciones de criptoactivos vinculadas a actividades ilícitas recibieron aproximadamente 40.900 millones de dólares, aunque los analistas advierten que esta cifra podría superar los 51.000 millones una vez que se identifiquen más direcciones relacionadas con la Delincuencia Organizada Trasnacional. No se trata, pues, de un problema menor ni periférico: es una amenaza sistémica que afecta la integridad de los mercados financieros y la seguridad de las naciones.

Venezuela no es ajena a esta realidad. Se ha documentado cómo los Grupos de Delincuencia Organizada Trasnacional utilizan criptoactivos para ocultar su patrimonio y evadir el control de las autoridades. En febrero de 2026, por ejemplo, fue detenido en el estado Zulia un sujeto (cuya identidad obviaremos), presunto cabecilla de una red de Legitimación de Capitales provenientes del narcotráfico, que utilizaba tecnología blockchain para introducir grandes

sumas de dinero en el mercado cambiario venezolano. El caso, lejos de ser aislado, revela una tendencia preocupante: la Delincuencia Organizada Transnacional presuntamente ha encontrado un espacio propicio para sus operaciones con criptoactivos.

En este ensayo me propongo explorar, con la profundidad que el tema merece, los mecanismos tecnológicos que permiten a las organizaciones criminales explotar los criptoactivos para la Legitimación de Capitales. Pero también examinaré las respuestas que, desde el derecho y la tecnología, se han desarrollado para contrarrestar estas amenazas. Porque si algo nos enseña la historia es que el crimen y la ley han estado siempre en una carrera constante, y los criptoactivos no son más que el último campo de batalla.

Herramientas legales para un desafío digital

La Convención de Palermo: un pacto global contra el crimen organizado

Para entender cómo enfrentamos hoy la Legitimación de Capitales utilizando criptoactivos, debemos remontarnos al año 2000, cuando la comunidad internacional dio un paso histórico al adoptar en Palermo, Italia, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, en lo sucesivo se le denominará la Convención. Aquel documento, representó el reconocimiento de una verdad incómoda: la delincuencia había dejado de ser un asunto local para convertirse en un problema global que exigía una respuesta igualmente global.

La Convención definió con precisión lo que debe entenderse por "grupo delictivo organizado": "un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material". Esta definición, aunque pensada para las realidades criminales de finales del siglo XX, sigue siendo extraordinariamente pertinente para comprender cómo operan hoy las organizaciones delictivas que utilizan criptoactivos.

El artículo 6 de la Convención tipifica como delito la conversión, transferencia, ocultación o disimulación de bienes producto de actividades ilícitas. Y el artículo 12 establece mecanismos para el decomiso e incautación del producto del delito. Pero quizás lo más importante es que la Convención sentó las bases para la cooperación internacional en esta materia un aspecto que, como veremos más adelante, resulta absolutamente indispensable cuando se trata de activos digitales que no reconocen fronteras.

La Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo: el marco venezolano

Venezuela, como Estado parte de la Convención de Palermo, incorporó sus disposiciones al ordenamiento interno a través de la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo, publicada en Gaceta Oficial el 30 de abril de 2012. Esta ley, que define la delincuencia organizada de manera coherente con el instrumento internacional, representa el esfuerzo del país por alinear su legislación con los estándares globales en la materia.

El artículo 35 de esta ley tipifica el delito de "legitimación de capitales" con penas de prisión de diez a quince años y multa equivalente al valor del incremento patrimonial ilícitamente obtenido. La ley también le otorga estatus jurídico como órgano desconcentrado adscrito al Ministerio de Finanzas a la Unidad Nacional de Inteligencia Financiera (UNIF), encargada de centralizar los reportes de actividades sospechosas y cooperar con entidades homólogas de otros países.

Sin embargo, es importante reconocer que tanto la Convención de Palermo como la ley venezolana fueron concebidas antes de que los criptoactivos irrumpieran en el panorama financiero global. Cuando el artículo 2(d) de la Convención define "bienes" como "activos de cualquier tipo, corporales o incorporales, muebles o inmuebles, tangibles o intangibles", lo hace sin saber que, apenas una década después, surgirían activos digitales descentralizados

que desafiarían todas las categorías tradicionales. La ley venezolana, por su parte, amplía esta definición para incluir "activos de cualquier tipo, corporales o incorporales, muebles o inmuebles, tangibles o intangibles, así como también los documentos o instrumentos legales o financieros que acrediten la propiedad u otros derechos sobre dichos activos". Esta redacción, afortunadamente amplia, permite interpretar que los criptoactivos están comprendidas dentro del concepto de bienes. Pero la ausencia de una mención explícita genera espacios de interpretación que los criminales no dudan en aprovechar.

La Legitimación de Capitales en la era digital

Tradicionalmente, la Legitimación de Capitales se divide en tres etapas: colocación, procesamiento e integración. Sin embargo, como señala la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), los criptoactivos alteran radicalmente este esquema. Al ser anónimas en su punto de creación, permiten a los criminales adquirirlas directamente con fondos ilícitos, saltándose la etapa de colocación. La velocidad y el bajo costo de las transacciones facilitan, además, la ejecución de complejos esquemas de Legitimación con miles de transferencias automatizadas. La alta volatilidad de muchos criptoactivos, ofrece una excusa perfecta para justificar incrementos repentinos de riqueza como ganancias de inversión.

Este cambio de paradigma exige que las autoridades no solo actualicen sus marcos legales, sino que también desarrollen nuevas capacidades técnicas para investigar delitos que, literalmente, no dejan huellas físicas.

Los mecanismos tecnológicos usados por criminales para ocultar su rastro

Monedas de privacidad: el anonimato como producto

Si hay un tipo de criptoactivo que mantiene despiertos por las noches a los investigadores financieros, esas son las llamadas "monedas de privacidad". A

diferencia de Bitcoin, cuyas transacciones son públicas y rastreables (aunque los usuarios operen bajo seudónimos), monedas como Monero (XMR) están diseñadas específicamente para garantizar el anonimato absoluto de quienes las utilizan.

Monero, en particular, se ha ganado la reputación de ser la moneda de privacidad por excelencia. Su sitio web oficial explica que "el remitente, el receptor y el importe de cada transacción se ocultan mediante el uso de tres importantes tecnologías: Direcciones-Secretas, Firmas-de-Anillo y RingCT". Las firmas de anillo permiten que una transacción sea firmada por un grupo de usuarios, haciendo imposible determinar quién fue el verdadero firmante. Las direcciones furtivas generan direcciones únicas y desechables para cada transacción. Y las transacciones confidenciales (RingCT) ocultan el monto de la operación. El resultado es lo que los desarrolladores de Monero describen como "una verdadera moneda fungible", donde cada unidad es indistinguible de cualquier otra.

El criptoactivo Zcash, por su parte, utiliza pruebas de conocimiento cero (zk-SNARKs) que permiten verificar la validez de una transacción sin revelar información sobre el remitente, el destinatario o el monto. Es, en palabras simples, la demostración matemática de que algo es verdad sin necesidad de mostrar los detalles que lo hacen verdad.

Un caso reciente ilustra perfectamente el atractivo de estas monedas para los criminales. En junio de 2026, una entidad desconocida canalizó aproximadamente 120 millones de dólares en USDT a través de una compleja serie de intercambios, incluyendo compras masivas de Monero. Las órdenes de compra fueron tan grandes que impulsaron el precio de Monero desde aproximadamente 330 dólares hasta un máximo cercano a 438 dólares. El investigador onchain ZachXBT (siendo este su seudónimo) logró rastrear los fondos a través de intercambios, servicios de intercambio instantáneo y otras cadenas de bloques. Pero el hecho de que pudiera hacerlo no significa que la

tarea fuera sencilla: Monero está diseñado precisamente para que esto sea extraordinariamente difícil.

Mezcladores: el arte de embarrar la pista

Los mezcladores, también conocidos como tumblers o mixers, son servicios que combinan fondos de múltiples fuentes para ocultar su origen. Su funcionamiento es relativamente sencillo: reciben criptoactivos de diferentes usuarios, las mezclan en un fondo común y luego las redistribuyen en porciones que se envían a direcciones distintas, rompiendo así el vínculo entre el remitente original y el destinatario final.

Tornado Cash se convirtió, entre 2022 y 2024, en uno de los mezcladores más utilizados para la Legitimación de Capitales usando Ethereum. Funcionaba como un contrato inteligente no custodial que utilizaba técnicas criptográficas para romper el vínculo entre las transacciones de depósito y retiro. El servicio se promocionaba como una herramienta que permite "enviar Ethereum 100% anónimo utilizando tecnología innovadora, no custodial y basada en criptografía sólida".

Lo interesante y preocupante es que las sanciones no eliminaron el problema, sino que lo transformaron. El ecosistema de mezcladores ha evolucionado hacia alternativas descentralizadas, puentes entre cadenas y protocolos de capa 2 que preservan la privacidad. Como señala la guía de COPOLAD III que viene siendo un Programa de Cooperación entre América Latina, el Caribe y la Unión Europea en Políticas sobre Drogas y GAFIC, señalando que "los delincuentes utilizan cada vez más tecnologías avanzadas para ocultar sus actividades en el ecosistema de los criptoactivos".

Puentes entre cadenas: saltando de una blockchain a otra

Los puentes entre cadenas (cross-chain bridges) representan una de las evoluciones más recientes y preocupantes en la comisión del hecho punible de Legitimación de Capitales. Estos protocolos permiten mover activos entre

diferentes blockchains, ocultando el vínculo entre el depósito y el retiro en cada una de ellas.

La evolución constante de las técnicas de ocultamiento

Lo que hace particularmente difícil la lucha contra la Legitimación de Capitales con criptoactivos es la velocidad con la que evolucionan las técnicas de ocultamiento. Los mezcladores custodiales han dado paso a protocolos descentralizados; los servicios de intercambio instantáneo se han multiplicado; los puentes entre cadenas se han vuelto más sofisticados. Como advierte la guía de COPOLAD III, "herramientas como los mezcladores, los intercambios, los puentes y las monedas centradas en la privacidad están a la vanguardia de estos métodos de encubrimiento".

La respuesta de las autoridades no puede ser estática. Debe ser igualmente dinámica, adaptándose continuamente a las nuevas técnicas y modalidades que surgen en este ecosistema en constante transformación.

La Delincuencia Organizada Trasnacional y los criptoactivos, casos y realidades

¿Por qué los criminales podrían amar a los criptoactivos?

Las organizaciones criminales no han adoptado los criptoactivos por capricho. Lo han hecho porque ofrecen ventajas que los sistemas financieros tradicionales no pueden igualar.

Son transfronterizas y descentralizadas: no reconocen fronteras ni dependen de intermediarios bancarios. Permiten mover grandes sumas sin las restricciones y controles aplicables a las transferencias tradicionales. Son rápidas y económicas: las transacciones son casi instantáneas y tienen costos mínimos, lo que permite ejecutar complejos esquemas de legitimación con miles de operaciones en cuestión de horas. No tienen límites: a diferencia de los bancos, que imponen topes a las transacciones y exigen justificaciones

para movimientos de grandes sumas, los criptoactivos pudieran en algunos casos permitir transferir cantidades ilimitadas sin verificación alguna.

Y, quizás lo más importante, ofrecen anonimato. Como señala la página de Insight Crime en su reporte "GameChangers 2025", "los criptoactivos no pesan ni ocupan espacio físico, resolviendo dos grandes problemas de los movimientos de grandes sumas en efectivo". El anonimato de la blockchain, añade el reporte, ha permitido "que el dinero pagado por un secuestro en cualquier país de Hispanoamérica o Europa termine pagando a obreros" en lugares remotos.

Venezuela se ha convertido en un escenario particularmente relevante para el uso de criptoactivos por parte de la delincuencia organizada. Organismos públicos han denunciado que los Grupos de Delincuencia Organizada presuntamente han utilizado criptoactivos para ocultar su patrimonio.

El caso del ciudadano detenido en el estado Zulia en febrero de 2026, es ilustrativo. Según el reporte del Grupo de Operaciones Especiales (GOES), el sujeto "utilizaba tecnología blockchain y criptoactivos para introducir grandes sumas de dinero en el mercado cambiario venezolano, generando distorsiones económicas". El ciudadano, señalado como cabecilla de una red de Legitimación de capitales vinculada al narcotráfico, movía fondos ilícitos a través de las fronteras sin ser detectado.

La minería ilegal de criptoactivos también se ha convertido en un problema significativo. En mayo de 2026, las autoridades venezolanas desmantelaron una macroinstalación de minería ilegal en Maracay, estado Aragua, que operaba aproximadamente cuatro mil equipos ASIC de alta potencia. El consumo masivo de energía afectaba gravemente el sistema eléctrico nacional. La operación, denominada "Cazador", representó un golpe contundente contra las llamadas "mafias energéticas" que explotan los recursos estratégicos del país.

Estos casos demuestran que los criptoactivos no solo se utilizan para ocultar fondos ilícitos, sino también para generarlos de manera ilegal, en un círculo vicioso que alimenta la economía criminal.

Los delitos que se esconden detrás de las transacciones

El uso de criptoactivos por parte de la delincuencia organizada abarca una amplia gama de delitos. El narcotráfico sigue siendo la principal fuente de financiación, y los criptoactivos se han convertido en la herramienta preferida para mover y ocultar las ganancias. La trata de personas, con penas de prisión de veinte a veinticinco años según la ley venezolana, encuentra en los criptoactivos un mecanismo para realizar pagos sin dejar rastros bancarios.

Los ataques de ransomware, que secuestran datos de empresas e instituciones exigiendo rescate en criptoactivos, han proliferado significativamente. Se estima que el 60% de estos ataques exigen pago en criptoactivos, y en 2023 los pagos por rescate superaron los mil millones de dólares a nivel global.

El sicariato, tipificado en Venezuela con penas de veinticinco a treinta años de prisión, también se beneficia de los criptoactivos. Permiten realizar pagos anónimos a los sicarios, dificultando la identificación de los autores intelectuales y materiales. La fabricación ilícita de armas, otro delito tipificado en la ley, encuentra en los criptoactivos un canal para transacciones en el mercado negro que ocultan la identidad de compradores y vendedores.

Las respuestas institucionales y cómo enfrentamos la amenaza

Herramientas de análisis de cadena de bloques

A pesar de las dificultades, existen herramientas cada vez más sofisticadas para rastrear transacciones ilícitas. Las herramientas de análisis de cadena de bloques permiten a las fuerzas de seguridad rastrear transacciones, agrupar monederos y trazar redes delictivas analizando la estructura de transacciones.

Analizando casos en el que la Delincuencia Organizada ha intentado sin exito legitimar millones de dólares mediante Monero demuestra que, aunque las monedas de privacidad están diseñadas para ocultar las transacciones, patrones como la entrada y salida de grandes cantidades de fondos de intercambios centralizados pueden ser detectados. ZachXBT pudo identificar el movimiento porque el criminal necesitó comprar Monero en intercambios que aplican medidas de Debida Diligencia, exponiendo así sus patrones de comportamiento.

La guía de COPOLAD III destaca que "el rastreo de patrones, la agrupación de direcciones y el empleo de la heurística son algunas de las estrategias que ayudan a descubrir actividades ilícitas a pesar de estos sofisticados métodos". El análisis de grafos, que representa las transacciones como redes para identificar nodos y patrones sospechosos, se ha convertido en una herramienta fundamental para los investigadores.

Técnicas especiales de investigación

La Convención de Palermo y la ley venezolana contemplan técnicas especiales de investigación que resultan particularmente relevantes para combatir la Legitimación de Capitales con criptoactivos. La "entrega vigilada" permite que las autoridades dejen que remesas ilícitas circulen bajo su supervisión para identificar a los involucrados. Las "operaciones encubiertas" permiten infiltrar agentes en organizaciones criminales para recabar información de primera mano.

La ley venezolana desarrolla en detalle estas técnicas. El artículo 66 establece que el Ministerio Público puede solicitar autorización judicial para la entrega vigilada de remesas ilícitas a través de agentes encubiertos. El artículo 70 define a los agentes de operaciones encubiertas como funcionarios que, ocultando su identidad, se infiltran en grupos de delincuencia organizada.

Estas técnicas, pensadas originalmente para el crimen tradicional, han demostrado ser igualmente efectivas en el ámbito digital, siempre que se cuenten con la capacitación técnica necesaria para aplicarlas.

Congelación, incautación y decomiso de criptoactivos

Uno de los mayores desafíos es la capacidad de las autoridades para congelar, incautar y decomisar criptoactivos. La Convención de Palermo, en su artículo 12, establece que los Estados parte adoptarán medidas para autorizar el decomiso del producto de los delitos. La ley venezolana, en su artículo 55, permite la incautación preventiva de bienes utilizados en la comisión de delitos, y el artículo 56 autoriza el bloqueo de cuentas bancarias, medida que puede extenderse a monederos de criptoactivos.

En la práctica, la congelación de criptoactivos se puede lograr principalmente a través de dos vías. La primera es la solicitud a intercambios centralizados: cuando los fondos ilícitos pasan por una plataforma reguladas que aplica medidas de Debidas Diligencia, las autoridades pueden solicitar la congelación de los activos. El caso de Tether, que congeló millones de dólares en USDT tras la investigación de ZachXBT, así como el caso en el que las autoridades venezolanas han desmantelado grupos de Delincuencia Organizada usando criptoactivos es un ejemplo perfecto. La segunda vía es el marcado de direcciones en la cadena, que permite identificar direcciones asociadas con actividades ilícitas.

Cooperación internacional: la clave del éxito

La naturaleza transfronteriza de los criptoactivos hace que la cooperación internacional sea esencial. La Convención de Palermo establece un marco detallado para esta cooperación, incluyendo disposiciones sobre extradición, asistencia judicial recíproca e investigaciones conjuntas. El artículo 18 establece que "los Estados Parte se prestarán la más amplia asistencia judicial recíproca".

La ley venezolana, en su artículo 76, establece que el Estado prestará asistencia judicial recíproca cuando sea requerido por otro país. El artículo 78 permite crear unidades de investigación financiera que establezcan enlaces de cooperación internacional.

En el ámbito normativo, el Grupo de Acción Financiera Internacional (GAFI) ha emitido recomendaciones actualizadas sobre activos virtuales y proveedores de servicios de activos virtuales (VASP). La "regla del viaje", que requiere que los VASP compartan información sobre el remitente y el destinatario de las transacciones por encima de cierto umbral, es particularmente importante.

Desafíos y límites, oportunidad de mejora

El dilema privacidad versus seguridad

Uno de los desafíos fundamentales es el equilibrio entre el derecho a la privacidad y la necesidad de prevenir actividades ilícitas. La mayoría de los criptoactivos se encuentran en dos categorías: transparentes pero regulables (como Bitcoin) o privadas, pero no reguladas (como Monero y Zcash).

La adaptación de los marcos legales

Tanto la Convención de Palermo como la ley venezolana fueron concebidas antes de la proliferación de los criptoactivos. La Convención, adoptada en 2000, utiliza un lenguaje que debe ser interpretado a la luz de las nuevas realidades tecnológicas. La ley venezolana, promulgada en 2012, presenta definiciones amplias que permiten incluir los criptoactivos como activos intangibles. Pero la ausencia de una mención explícita genera espacios de interpretación que los criminales explotan.

El artículo 23 de la ley venezolana prohíbe "el envío de divisas en efectivo o títulos valores al portador", pero no aborda específicamente el envío de criptoactivos. Esta laguna normativa representa una oportunidad para los criminales. Como sugirió el fiscal ecuatoriano Washington Astudillo, los

enfoques sobre lavado de activos deben incorporar nuevas modalidades como "el uso de criptoactivos y las apuestas deportivas".

Capacidades institucionales y capacitación

Quizás el desafío más significativo es la brecha de capacidades entre las organizaciones criminales y las autoridades. Como señala la guía de COPOLAD III, "los delincuentes utilizan cada vez más tecnologías avanzadas para ocultar sus actividades". Las fuerzas de seguridad deben estar igualmente capacitadas.

La Convención de Palermo, en su artículo 29, insta a los Estados a "formular, desarrollar o perfeccionar programas de capacitación específicamente concebidos para el personal de sus servicios encargados de hacer cumplir la ley". La ley venezolana, en su artículo 6(5), atribuye a la Oficina Nacional Contra la Delincuencia Organizada la función de diseñar programas de capacitación para funcionarios públicos, atribución que se ha venido cumpliendo y profundizando.

Pero la capacitación no puede limitarse a aspectos técnicos. Debe incluir la comprensión de los aspectos legales y procesales específicos de las investigaciones de criptoactivos: la cadena de custodia de la evidencia digital, la obtención de órdenes judiciales para el acceso a monederos y la cooperación con intercambios centralizados.

Conclusiones

Al cerrar este recorrido por el complejo mundo de los criptoactivos, la privacidad y la Legitimación de Capitales, me llevo varias reflexiones que quiero compartir.

La primera es que los criptoactivos han transformado radicalmente las operaciones financieras de las organizaciones criminales. Su naturaleza transfronteriza, descentralizada y anónima las convierte en el vehículo ideal para la Legitimación de Capitales. Monedas como Monero, con su

combinación de firmas de anillo, direcciones furtivas y transacciones confidenciales, representan el extremo más avanzado de esta evolución, ofreciendo niveles de anonimato que dificultan enormemente el rastreo de transacciones ilícitas.

La segunda es que los mecanismos tecnológicos utilizados por la delincuencia son diversos y están en constante evolución. Desde las monedas de privacidad hasta los mezcladores, los puentes entre cadenas y los protocolos de capa 2, los criminales disponen de un ecosistema cada vez más sofisticado. La respuesta de las autoridades debe ser igualmente dinámica, adaptándose continuamente a las nuevas técnicas y modalidades.

La tercera es que, a pesar de los desafíos, existen herramientas y estrategias efectivas. Las herramientas de análisis de cadena de bloques, las técnicas especiales de investigación y la cooperación internacional constituyen pilares fundamentales de esta lucha. El caso del lavado de 120 millones de dólares demuestra que, incluso con monedas de privacidad, los patrones de comportamiento y la necesidad de interactuar con intercambios centralizados pueden exponer a los criminales.

La cuarta es que los marcos legales existentes, tanto la Convención de Palermo como la ley venezolana, proporcionan una base sólida, pero requieren actualizaciones. La interpretación amplia de conceptos como "bienes" y "fondos" permite incluir los criptoactivos, pero sería deseable una mención explícita para evitar ambigüedades y facilitar la cooperación internacional.

La quinta es que la cooperación internacional es indispensable. Ningún país puede enfrentar esta amenaza por sí solo. Los mecanismos de asistencia judicial recíproca, las investigaciones conjuntas y el intercambio de información entre unidades de inteligencia financiera son esenciales para el éxito.

La sexta es que el equilibrio entre privacidad y seguridad sigue siendo un desafío pendiente. Los avances en criptografía que permiten la auditabilidad sin comprometer la privacidad ofrecen un camino prometedor, pero su implementación requerirá consenso político y técnico.

Finalmente, la lucha contra la Legitimación de Capitales mediante criptoactivos no puede limitarse a medidas reactivas. Se requiere un enfoque proactivo que incluya la educación del público sobre los riesgos, el fortalecimiento de las capacidades institucionales y la colaboración con el sector privado. Como señala la UNODC, los Estados miembros deben "reglamentar debidamente los mercados de criptoactivos y establecer un sistema de supervisión adecuado". Solo a través de un esfuerzo coordinado, multidisciplinario y global será posible proteger la integridad del sistema financiero y la seguridad de nuestras sociedades.

No queriendo bajo ninguna circunstancia satanizar el uno de los criptoactivos, sino por el contrario, coadyuvar para el mejor uso de estos, así como fortalecer el conocimiento al respecto y brindar herramienta que nos permita debilitar a los grupos de Delincuencia Organizada atacando sus fuentes de financiamiento.

El caso venezolano, con sus particularidades y desafíos, demuestra que el país no es ajeno a estas dinámicas. Casos como el del zulia y el desmantelamiento de la macroinstalación de minería ilegal en Maracay son ejemplos de que las autoridades están actuando. Pero también revelan la magnitud del desafío que enfrentamos. La lucha contra la legitimación de capitales a través de criptoactivos es, en definitiva, una lucha por la integridad de nuestro sistema financiero y la seguridad de nuestra nación. Y es una lucha que, como todas las que valen la pena, exige lo mejor de nosotros.

Referencias

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos. Naciones Unidas, 2000.

Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo. Gaceta Oficial de la República Bolivariana de Venezuela Nº 5.789 Extraordinario, 26 de octubre de 2005 (texto actualizado 2012).

Chainalysis. 2025 Crypto Crime Report. Chainalysis Inc., 2025.

COPOLAD III y GAFIC. Guía sobre investigaciones financieras de criptoactivos para fuerzas de seguridad, 2025.

Financial Action Task Force (FATF). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. FATF, 2024.

Insight Crime. "GameChangers 2025: Los criptoactivos se abren paso en el inframundo criminal". Insight Crime, 2025.

Monero. "¿Qué es Monero (XMR)?" Documentación oficial.

"El precio de Monero se dispara un 33 % hasta los 438 dólares en medio de un laberinto de lavado onchain de 120 millones de dólares". CoinDesk, 12 de junio de 2026.

"Preso cabecilla de red del narcoblanqueo". El Aragueño, 5 de febrero de 2026.

"Desmantelada granja de criptoactivos dedicada a la minería ilegal". Ciudad Valencia, 19 de mayo de 2026.

Zoffili, E. "Follow the money to fight organized crime". Declaración en el Día Internacional contra la Delincuencia Organizada Transnacional, OSCE Asamblea Parlamentaria, 15 de noviembre de 2025.

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

LAS NUEVAS TECNOLOGÍAS EN EL SECTOR ASEGURADOR VENEZOLANO: LA POLÍTICA "CONOCE A TU PROVEEDOR" (KYP) COMO CONTROL EN EL SIAR DE LC/FT/FPADM

Autor: Juan C., Cabello M.
Facilitadora: MSc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

Las Nuevas Tecnologías en el Sector Asegurador Venezolano: La Política "Conoce a tu Proveedor" (KYP) como control en el SIAR de LC/FT/FPADM

Autor: Juan C., Cabello M.
Código ORCID: 0009-0009-7505-7398
Correo electrónico: juanc.maquinam@gmail.com

Resumen

El presente ensayo analiza el impacto disruptivo de las nuevas tecnologías, el fenómeno Insurtech y la Inteligencia Artificial (IA) en la gestión del riesgo de Lavado de Activos, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM) dentro del sector asegurador y de medicina prepagada en Venezuela. A través de una investigación documental, se examina cómo la digitalización de procesos mediante canales alternativos de comercialización masiva optimiza la operativización del Sistema Integral de Administración de Riesgos (SIAR). Se evalúa el marco legal e institucional nacional destacando la Constitución de la República Bolivariana de Venezuela, la Ley de la Actividad Aseguradora y las Providencias Conjuntas SAA-01-0536-2024 y SAA-01-0519-2024 a la luz de la Recomendación 15 del Grupo de Acción Financiera Internacional (GAFI). El estudio aborda de forma analítica la política "Conoce a tu Proveedor" (KYP) y la Debida Diligencia del Cliente (DDC) mediante el uso de algoritmos y matrices dinámicas de riesgo, contrastando la celeridad transaccional con la mitigación del dolo eventual y la ceguera voluntaria corporativa. Se concluye que la fiscalización técnica de los aliados tecnológicos y la transparencia corporativa, alineadas con las evaluaciones de la Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT), no constituyen meros trámites formales y accesorios, sino un imperativo categórico de gobernanza, seguridad sistémica, soberanía económica y protección patrimonial colectiva de la Nación.

Palabras clave: Insurtech, SIAR de LC/FT, Normativa Prudencial, Conoce a tu Proveedor (KYP), Inteligencia Artificial.

Abstract

This essay analyzes the disruptive impact of new technologies, the Insurtech phenomenon, and Artificial Intelligence (AI) on Anti-Money Laundering, Countering the Financing of Terrorism, and Countering Proliferation Financing (AML/CFT/CPF) risk management within the Venezuelan insurance and prepaid medicine sector. Through documentary research, it examines how process digitalization through alternative mass commercialization channels optimizes the operationalization of the Comprehensive Risk Management System (SIAR). The national legal and institutional framework—highlighting the Constitution of the Bolivarian Republic of Venezuela, the Insurance Activity Law, and Administrative Rulings SAA-01-0536-2024 and SAA-01-0519-2024—is evaluated in light of Recommendation 15 of the Financial Action Task Force (FATF). The study addresses the "Know Your Provider" (KYP) policy and Customer Due Diligence (CDD) using analytical algorithms and dynamic risk matrices, contrasting transactional speed with the mitigation of eventual intent and corporate willful blindness. It concludes that the technical oversight of technological allies and corporate transparency, aligned with the evaluations of the National Office Against Organized Crime and Terrorist Financing (ONCDOFT), are not mere accessory formalities but an imperative for governance, systemic safety, economic sovereignty, and the collective asset protection of the Nation.

Keywords: Insurtech, SIAR of AML/CFT, Prudential Regulation, Know Your Provider (KYP), Artificial Intelligence.

Introducción

El ecosistema existente en el ámbito financiero global y la actividad aseguradora contemporánea atraviesan una de las eras más disruptivas de su historia económica a raíz de la emergencia y masificación de las nuevas tecnologías de la información (Schwab, 2016). En el contexto venezolano, esta acelerada transformación digital y la consecuente necesidad de masificación del mercado de seguros y medicina prepagada han impulsado decididamente la adopción de canales alternativos de comercialización. El uso de plataformas de agregación de servicios, alianzas con corresponsales no tradicionales y el auge de los modelos Fintech/Insurtech —amalgama directa y complemento entre insurance y technology— han redefinido los canales de distribución, el

diseño de productos masivos y la velocidad en la tramitación de operaciones (Nicoletti, 2017).

No obstante, esta apertura de fronteras comerciales e informáticas introduce vectores y elementos de riesgo sumamente complejos y peligrosos para la estabilidad del mercado. Esta evolución digital coincide con una transformación estructural de carácter obligatorio dictada por los órganos de supervisión y control estatal, orientada a migrar desde un esquema de cumplimiento puramente formal hacia una verdadera cultura de Gestión Estratégica de Riesgos en materia de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM). El desplazamiento de la intermediación tradicional hacia estructuras digitales masivas genera una zona de alta vulnerabilidad si las empresas asumen erróneamente que el riesgo delictivo se disuelve en la automatización.

En la praxis de la supervisión y la docencia preventiva, se evidencia que el eslabón más crítico de esta cadena no reside en la interfaz de la plataforma o el algoritmo, sino en la idoneidad e integridad del aliado comercial: el proveedor tecnológico o canal alternativo. Por consiguiente, el presente ensayo analiza críticamente la integración de las herramientas tecnológicas avanzadas en el Sistema Integral de Administración de Riesgos (SIAR), fundamentando la obligatoriedad y el impacto de la política "Conoce a tu Proveedor" (Know Your Provider o KYP) como un control tridimensional (legal, preventivo y prudencial) indispensable que condiciona la validez jurídica de la comercialización digital de seguros en Venezuela.

I. Fundamentación Constitucional y Morfología Legal de la Actividad Aseguradora.

La incorporación de tecnologías emergentes como la Inteligencia Artificial (IA), el Machine Learning, el Big Data y los contratos inteligentes basados en Blockchain en el mercado de seguros no ocurre en un vacío normativo, sino

que se encuentra estrictamente condicionada por el orden público económico del Estado venezolano (Chang & Negrón, 2014). El análisis dogmático de la tecnología y del control de los canales alternativos e intermediarios masivos debe sustentarse jerárquicamente en los siguientes pilares de nuestro ordenamiento legal sustantivo:

- **La Corresponsabilidad en la Seguridad Socioeconómica (CRBV, Art. 322):** La seguridad de la Nación es competencia esencial del Estado y de todos los ciudadanos y personas jurídicas de derecho público o privado bajo el principio de corresponsabilidad. Al delegar la venta de pólizas o planes de salud en un tercero (canal alternativo), el Sujeto Obligado no delega su responsabilidad constitucional; por el contrario, está obligado a garantizar que dicho entorno digital no se convierta en una compuerta que debilite la seguridad del orden público económico y traiga como consecuencias mayores tanto para la empresa, el sector y el sistema financiero.
- **La Regulación del Proceso Económico y la Tutela del Interés General (CRBV, Art. 112 y Ley de la Actividad Aseguradora, Art. 1):** El texto constitucional faculta plenamente al Ejecutivo Nacional para regular la economía con miras a salvaguardar los derechos colectivos. En perfecta simetría y consonancia, la Ley de la Actividad Aseguradora instituye el principio de la tutela del interés general para la protección irrestricta de tomadores, asegurados y beneficiarios. Si una aseguradora contrata a un proveedor de canales masivos o tecnológicos sin verificar su legitimidad, expone de forma directa la salud financiera y las reservas técnicas que garantizan el cumplimiento de los contratos frente a los ciudadanos.
- **La Debida Diligencia Organizacional (LOCDOFT, Art. 14):** La Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo prohíbe de forma taxativa la negligencia institucional en el control de las operaciones. Permitir que una plataforma tecnológica o

un corresponsal masivo capte clientes y recaude fondos sin un escrutinio férreo, preciso y detallado sobre su estructura de propiedad configura un escenario de riesgo penal por facilitación en la posible comisión de delitos de LC/FT.

II. Estándares del GAFI y el Riesgo de las APNFD en Canales Tecnológicos

A nivel internacional, el Grupo de Acción Financiera Internacional (GAFI), a través de sus 40 Recomendaciones que en estos contextos debemos considerar como una de nuestras principales de guía, estudio y análisis permanente, impone de manera transversal la aplicación del Enfoque Basado en Riesgo (EBR), estipulando que la intensidad de los controles sea estrictamente proporcional a la amenaza identificada (GAFI, 2023).

Específicamente, ante la irrupción digital, cobra vigencia la **Recomendación 15 (Nuevas Tecnologías)**, la cual exige de forma expresa a las instituciones identificar, evaluar y mitigar sistemáticamente los riesgos de lavado de activos y financiamiento al terrorismo que surjan del desarrollo de nuevos productos, nuevas prácticas comerciales y novedosos mecanismos de distribución tecnológica.

Cobra real preponderancia la aplicación eficiente de la política "Conoce a tu Proveedor" (KYP), que responde directamente a este mandato global. Cuando las empresas de seguros consolidan alianzas corporativas masivas o implementan plataformas Fintech, interactúan de forma recurrente con actores externos que operan en las fronteras de las Actividades y Profesiones No Financieras Especificadas (APNFD). La falta de transparencia en la propiedad de estos proveedores puede ser instrumentalizada por la delincuencia organizada para tomar el control de los nodos o factores de recaudación, inyectando flujos de efectivo de origen criminal o de procedencia dudosa a través de la venta atomizada de microseguros o pólizas de salud fraccionadas.

Bajo el estándar internacional del GAFI, la Debida Diligencia sobre el

Proveedor es el único mecanismo técnico capaz de desarticular el ocultamiento de estructuras ilícitas en los canales de distribución digital.

III. El vital Engranaje Normativo: Providencia SIAR (SAA- 01- 0536-2024) y Providencia Insurtech (SAA- 01-0519-2024)

La articulación práctica y el control analítico de las nuevas tecnologías en el entorno asegurador venezolano se logran mediante el cruce normativo y simétrico de los dos instrumentos prudenciales dictados en el año 2024 por la Superintendencia de la Actividad Aseguradora (Sudeaseg) en su rol de garante y regulador del sector asegurador venezolano, lo cual detallamos de seguido:

La Providencia Administrativa N° SAA-01-0536-2024 establece las normas estructurales obligatorias del Sistema Integral de Administración de Riesgos (SIAR). En su etapa de Segmentación, obliga a las instituciones a clasificar científicamente sus riesgos basándose en los factores fundamentales: clientes, productos, jurisdicciones geográficas y de manera crucial, los Canales de Distribución. Al migrar las operaciones hacia el ecosistema digital, el SIAR califica automáticamente el canal como de alta exposición o de alto riesgo, demandando controles mitigantes reforzados en todos los niveles.

Aquí es donde se ensambla de forma idónea y perfecta la Providencia Administrativa N° SAA-01-0519-2024, encargada de regular expresamente las Normas que rigen los Canales de Comercialización y el uso de las Tecnologías del Mercado Financiero (Fintech) y de la Actividad Aseguradora (Insurtech). Esta norma prohíbe tajantemente a las empresas de seguros entablar alianzas tecnológicas "a ciegas", forzando a la operacionalización de la política "Conoce a tu Proveedor" a través de tres requisitos imperativos de gobernanza corporativa; a saber:

1. **Idoneidad Técnica y Legal:** El aliado o proveedor tecnológico debe someterse a una evaluación exhaustiva e indexada que certifique fehacientemente su capacidad operativa, robustez en seguridad de

la información y estricto cumplimiento normativo en cuanto a controles adecuados e idóneos se refiere.

2. **Mecanismos de Colaboración Interinstitucional:** De igual modo la norma exige la redacción y firma de contratos rígidos de carácter formal, en los cuales se definan con precisión las responsabilidades legales, esquemas de gobernanza de datos, vigencia de la alianza y los reportes analíticos periódicos que deben presentarse obligatoriamente ante el supervisor (Sudeaseg).
3. **Mitigación en el Sandbox Regulatorio:** En los supuestos de operar bajo modelos experimentales o altamente innovadores de Insurtech, la norma dispone la creación de entornos de supervisión controlados, donde la transparencia institucional y el conocimiento absoluto del proveedor fungen como la garantía mínima exigida para resguardar la sanidad integral del mercado.

De tal manera debemos aseverar que, los sistemas informáticos avanzados dejan de ser meros repositorios de información estática y se convierten, conforme a la doctrina del control interno y la auditoría forense, en potentes herramientas analíticas dinámicas, capaces de aislar desviaciones y alertar inconsistencias en tiempo real (Estupiñán, 2006).

IV. Dimensiones Operativas de la Política "Conozca a su Proveedor" (Know your Provider – KYP) y Prevención del Dolo Eventual corporativo

Desde la perspectiva de la docencia técnica y la praxis como formador acreditado (Código RUF-ONCDOFT) que los cursantes de esta Especialización realizamos en nuestra práctica profesional constante, consideramos y acentuamos en los participantes de nuestras actividades formativas que la política "Conoce a tu Proveedor" debe superar la simple recepción y archivo formal del expediente mercantil del aliado. En los programas de capacitación corporativa y adecuación técnica, el KYP aplicado a los canales alternativos y desarrollos de Inteligencia Artificial debe

estructurarse obligatoriamente bajo tres dimensiones operativas fundamentales, que a continuación detallamos:

- **Desenmascaramiento del Beneficiario Final del Canal:** El Sujeto Obligado debe aplicar los estándares internacionales de transparencia para identificar de forma indubitable a la persona natural que ejerce el control efectivo de la empresa tecnológica proveedora (titularidad igual o superior al 25% de las acciones), impidiendo que las redes de delincuencia organizada empleen corporaciones de fachada o empresas maletín para infiltrar el sector asegurador.
- **Auditoría de Seguridad e Integridad de Datos (Insurtech):** Debido a que el proveedor tecnológico administra pasarelas de pago y datos sensibles de los asegurados, el KYP exige auditar de manera continua que el canal alternativo posea cortafuegos, cifrados y protocolos de ciberseguridad avanzada que eviten la manipulación transaccional o el desvío fraudulento de primas.
- **Trazabilidad de la Recaudación Fraccionada:** Las plataformas masivas suelen captar fondos a gran escala mediante primas de bajo costo atomizadas. El software del SIAR de la aseguradora, alimentado por los datos provistos en tiempo real por el aliado según las exigencias de la Providencia SAA-01-0519-2024, debe poseer la capacidad algorítmica de rastrear el origen lícito de dicha recaudación, neutralizando esquemas sofisticados de fraccionamiento o pitufeo (smurfing) financiero.

Esta automatización integral de la debida diligencia —mediante algoritmos de comparación analítica que contrastan instantáneamente a usuarios y proveedores contra listas de sanciones de organismos internacionales como la ONU u OFAC— disminuye significativamente el error humano inherente a los controles manuales obsoletos (Manero, 2008). En paralelo, las soluciones tecnológicas en materia de KYP permiten verificar la legitimidad de proveedores esenciales (clínicas, talleres mecánicos, peritos), bloqueando

esquemas de sobrefacturación o simulación de siniestros orientados a la extracción ilegal de fondos corporativos.

Desde el plano del derecho penal sustantivo y la criminología corporativa moderna que es necesario destacar, la implementación de estos sensores y monitoreos analíticos continuos altera drásticamente la configuración de la culpabilidad penal corporativa. Conforme al artículo 14 de la LOCDOFT, existe la obligación irrenunciable de reportar las operaciones sospechosas a la Unidad Nacional de Inteligencia Financiera (UNIF). El desarrollo de un SIAR automatizado e inteligente despoja a los directivos y oficiales de cumplimiento de cualquier posibilidad de alegar ignorancia ante el hecho delictivo (Pino & Sánchez, 2008). Si el sistema lógico genera una señal de alerta técnica (Red Flag) por inconsistencias en el canal alternativo o en el cliente, y el operador decide omitirla deliberadamente para priorizar la rentabilidad del negocio, la conducta encuadra de forma directa en la figura dogmática de la **Ceguera Voluntaria (Willful Blindness)**, transmutando el caso hacia el terreno del Dolo Eventual en materia penal.

V. Gobierno Corporativo, Big Data y Lineamientos de la Oficina Nacional Contra Delincuencia Organizada (ONCDOFT)

La efectiva integración de la innovación tecnológica en la prevención del delito financiero está supeditada a un sólido marco de gobernanza institucional. Siguiendo las Normas de Buen Gobierno Corporativo para los Sujetos Obligados de la Actividad Aseguradora dictadas por la Sudeaseg (2024), la junta directiva es la máxima responsable de suministrar los recursos presupuestarios indispensables para la adquisición, actualización y mantenimiento de una infraestructura informática robusta e inalterable.

Esta asignación de recursos debe figurar de manera explícita en el **Plan Operativo Anual (POA)** en materia de prevención de LC/FT/FPADM, el cual debe remitirse obligatoriamente ante el ente rector con cuarenta y cinco (45) días de anticipación al cierre del ejercicio económico. El POA tecnológico debe

alinearse simétricamente con las directrices de la Evaluación Sectorial de Riesgos coordinada por la Sudeasey y a su vez tutelada y guiada por parámetros emanados de la Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT) como máxima autoridad en la materia en Venezuela.

A través del uso del Big Data, el sector asegurador procesa masivamente los indicadores de la delincuencia organizada, traduciéndolos en reglas lógicas y matrices de riesgo internas. Esto garantiza que los programas de adiestramiento continUo dictados a los empleados e intermediarios de seguros, los cuales deben ser obligatoriamente impartidos por facilitadores acreditados y registrados bajo el código **RUF-ONCDOFT** se fundamenten en simulaciones y tipologías delictivas reales y contextualizadas en el espacio socioeconómico venezolano.

A manera de conclusiones y reflexiones

El análisis sistémico e integrado de las nuevas tecnologías en la actividad aseguradora venezolana dictamina que el fenómeno Insurtech, la Inteligencia Artificial y la masificación comercial mediante canales alternativos no constituyen amenazas exógenas o focos de desregulación mercante. Por el contrario, representan las herramientas metodológicas y operacionales más avanzadas para potenciar la resiliencia del Sistema Integral de Administración de Riesgos (SIAR).

La política de "Conoce a tu Proveedor" (KYP) se consolida como el núcleo ético y técnico de esta metamorfosis digital. Al articular de manera precisa y acertada los mandatos constitucionales de corresponsabilidad socioeconómica, las barreras preventivas de la LOCDOFT contra la ceguera voluntaria corporativa, las pautas globales de la Recomendación 15 del GAFI y el blindaje normativo que otorgan las Providencias SAA-01-0536-2024 y SAA-01-0519-2024, el sector asegurador y de medicina prepagada asegura que la expansión comercial digital no fracture los controles preventivos. El binomio indisoluble conformado por la tecnología de vanguardia y el derecho

penal preventivo erige una frontera infranqueble que aleja la materialización de dolo eventual y afianza a la institución del seguro como un pilar fundamental en el resguardo de la soberanía, la transparencia institucional y la estabilidad del patrimonio económico-financiero de la República Bolivariana de Venezuela lo que a la postre generará mayor confianza para inversiones nacionales y foráneas en territorio venezolano.

Referencias

Asamblea Nacional de la República Bolivariana de Venezuela. (1999). Constitución de la República Bolivariana de Venezuela. Gaceta Oficial de la República Bolivariana de Venezuela, 36.860, diciembre 30, 1999.

Asamblea Nacional de la República Bolivariana de Venezuela. (2012). Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo. Gaceta Oficial de la República Bolivariana de Venezuela, 39.912, abril 30, 2012.

Asamblea Nacional de la República Bolivariana de Venezuela. (2023). Ley de Reforma del Decreto con Rango, Valor y Fuerza de Ley de la Actividad Aseguradora. Gaceta Oficial de la República Bolivariana de Venezuela, 6.770 (Extraordinario), noviembre 29, 2023.

Chang, J., & Negrón, M. (2014). Derecho de Seguros y Regulación Prudencial en la Actividad Aseguradora Venezolana. Editorial Buchivacoa.

Escuela Nacional de Administración y Hacienda Pública. (2016). Manual para elaboración y presentación de trabajos académicos. Caracas: ENAHP-IUT.

Estupiñán, R. (2006). Control Interno y Fraudes: con base en los ciclos transaccionales (2da ed.). Ecoe Ediciones.

Grupo de Acción Financiera Internacional (GAFI). (2023). Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y la proliferación de armas de destrucción masiva (Actualización julio 2023). París, Francia.

Manero, J. (2008). Prevención Automatizada del Riesgo de Fraude en Entidades Financieras. Ediciones Deusto.

Nicoletti, B. (2017). The Future of Insurance: As It Is Led by Insurtech. Palgrave Macmillan.

Pino, O., & Sánchez, M. (2008). Conducta Humana e Intencionalidad en las Defraudaciones Corporativas. Editorial Panapo.

Schwab, K. (2016). La cuarta revolución industrial. Debate.

Superintendencia de la Actividad Aseguradora (Sudeaseg). (2024). Providencia Administrativa N° SAA-01-0519-2024: Normas que rigen los Canales de Comercialización y el uso de las Tecnologías del Mercado Financiero (FINTECH) y de la Actividad Aseguradora (INSURTECH). Gaceta Oficial de la República Bolivariana de Venezuela, 6.835 (Extraordinario), septiembre 03, 2024.

Superintendencia de la Actividad Aseguradora. (2024). Providencia SAA-01-0530-2024. Normas sobre el Buen Gobierno Corporativo en la Actividad Aseguradora. Gaceta Oficial de la República Bolivariana de Venezuela, 6.835 (Extraordinario), septiembre 03, 2024.

Superintendencia de la Actividad Aseguradora (Sudeaseg). (2024). Providencia Administrativa N° SAA-01-0536-2024: Normas sobre Administración de Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva en la Actividad Aseguradora. Gaceta Oficial de la República Bolivariana de Venezuela, 6.835 (Extraordinario), septiembre 03, 2024.

Superintendencia de la Actividad Aseguradora (Sudeaseg). Guías Instrumentalizadas para la Evaluación Interna y la Administración de Riesgos de LC/FT/FPADM. Caracas, Venezuela.

Unidad Nacional de Inteligencia Financiera (UNIF). (2024). Informe de Retroalimentación Basado en el Análisis Descriptivo de los Reportes de Actividades Sospechosas (RAS) en el Sistema Financiero Nacional. Caracas, Venezuela.

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

LA CONVERGENCIA ENTRE LA TRASFORMACIÓN DIGITAL Y LOS DELITOS DE LEGITIMACIÓN DE CAPITALES, FINANCIAMIENTO AL TERRORISMO Y FINANCIAMIENTO A LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA EN LA ACTIVIDAD ASEGURADORA

Autor: Abg. Alonso Javier Brito Sánchez
Facilitadora: MSc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

La convergencia entre la trasformación digital y los delitos de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento a la Proliferación de Armas de Destrucción Masiva en la Actividad Aseguradora

Autor: Abg. Alonso Javier Brito Sánchez
Código ORCID: 0009-0003-5594-9520
Correo electrónico: alonso.brito61@gmail.com

Resumen

El sector asegurador atraviesa una metamorfosis acelerada impulsada por la adopción de tecnologías emergentes, el ecosistema Insurtech y la Inteligencia Artificial (IA). Si bien esta transformación digital optimiza la eficiencia operativa y la experiencia del cliente, también introduce vulnerabilidades inéditas ante los delitos de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento a la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM). El presente ensayo analiza la convergencia entre la digitalización y estos riesgos financieros criminales, examinando los nuevos canales de distribución, los factores de riesgo emergentes y los marcos normativos nacionales e internacionales. Se concluye que la mitigación eficaz exige la evolución hacia un modelo de "Compliance 4.0", donde la tecnología actúe simultáneamente como vector de riesgo y como herramienta de supervisión algorítmica.

Descriptores: Convergencia, Transformación Digital, Legitimación de Capitales, Financiamiento al Terrorismo, Financiamiento a la Proliferación de Armas de Destrucción Masiva, Insurtech, Canales Alternativos, Fintech, Inteligencia Artificial, Soluciones, Enfoque Basado en Riesgo, GAFI, SUDEASEG, ONCDOFT.

Abstract

The insurance sector is going through an accelerated metamorphosis driven by the adoption of emerging technologies, the Insurtech ecosystem and Artificial Intelligence (AI). While this digital transformation optimizes operational efficiency and the customer experience, it also introduces unprecedented

vulnerabilities to the crimes of Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (LC/FT/FPADM). This essay analyzes the convergence between digitalization and these criminal financial risks, examining new distribution channels, emerging risk factors, and national and international regulatory frameworks. It is concluded that effective mitigation requires the evolution towards a "Compliance 4.0" model, where technology acts simultaneously as a risk vector and as an algorithmic supervision tool.

Descriptors: Convergence, Digital Transformation, Money Laundering, Terrorist Financing, Financing of the Proliferation of Weapons of Mass Destruction, Insurtech, Alternative Channels, Fintech, Artificial Intelligence, Solutions, Rieso-Based Approach, GAFI, SUDEASEG, ONCDOFT.

Introducción

La actividad aseguradora global, históricamente caracterizada por su prudencia operativa y sus procesos de suscripción basados en la presencialidad, se encuentra inmersa en una revolución sin precedentes: la transformación digital. La irrupción de las plataformas Insurtech, la integración de soluciones Fintech y la adopción masiva de la Inteligencia Artificial (IA) han reconfigurado la cadena de valor del seguro. Hoy en día, la comercialización a través de canales alternativos digitales, la automatización de la suscripción y la indemnización expedita de siniestros han democratizado el acceso al sector y optimizado la eficiencia operativa a niveles históricos. Sin embargo, esta eliminación de la fricción comercial e intermediación tradicional ha traído consigo un efecto secundario crítico: la apertura de nuevas y sofisticadas vulnerabilidades ante los delitos financieros de legitimación de capitales, financiamiento al terrorismo y financiamiento a la proliferación de armas de destrucción masiva y otros ilícitos.

Este fenómeno no debe entenderse como la coexistencia aislada de la innovación técnica y el crimen organizado, sino como una convergencia dinámica. En este nuevo ecosistema virtual, las redes delictivas aprovechan la inmediatez, la despersonalización y el potencial anonimato de las transacciones electrónicas incluyendo el uso latente de criptoactivos, para

diseñar tipologías de Legitimación de Capitales que desbordan los controles de monitoreo tradicionales. De este modo, el contrato de seguro, y en especial las figuras de reaseguro transfronterizo, corren el riesgo de ser instrumentalizados como vehículos para la estratificación e integración de capitales ilícitos a la economía formal.

Ante esta realidad, los organismos reguladores en el caso de Venezuela la Superintendencia de la Actividad Aseguradora, han iniciado una carrera contra el tiempo. A nivel internacional, el Grupo de Acción Financiera Internacional (GAFI) exige, a través de su Recomendación 15 sobre nuevas tecnologías, una gobernanza preventiva basada en el Enfoque Basado en Riesgo (EBR) antes del despliegue de cualquier innovación. En el contexto venezolano, este mandato se traslada a las rigurosas exigencias de la Superintendencia de la Actividad Aseguradora (SUDEASEG) y la Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT), las cuales obligan a los sujetos obligados a migrar de un cumplimiento estático y documental hacia sistemas de control interno inteligentes y adaptativos.

Por lo tanto, el objetivo del presente ensayo es analizar de manera crítica la intersección entre la transformación digital del sector asegurador y las amenazas emergentes de LC/FT/FPADM y Otros Ilícitos. A lo largo del texto, se examinarán los factores de riesgo inherentes a la Inteligencia Artificial y las Insurtech, los desafíos normativos en las esferas internacional y nacional, y las tipologías criminales de nueva generación. Finalmente, se planteará cómo la tecnología, concebida inicialmente como un vector de riesgo por su velocidad y opacidad, debe transformarse mediante el desarrollo de herramientas RegTech (uso de programas de computación y herramientas digitales para ayudar a las empresas a cumplir con las leyes y normas de forma rápida y barata) en el pilar fundamental de la supervisión y defensa algorítmica del mercado asegurador contemporáneo.

1. Introducción y el Nuevo Ecosistema: Insurtech, Fintech y Canales Alternativos

La digitalización ha dejado de ser una opción periférica para convertirse en el núcleo de la actividad aseguradora contemporánea. La irrupción de las Insurtech y su alianza con el ecosistema Fintech han reconfigurado la cadena de valor del seguro, introduciendo modelos de negocio basados en la inmediatez, la desintermediación y la despersonalización de la relación comercial.

La proliferación de canales alternativos digitales (aplicaciones móviles, plataformas web, agregadores y contratos inteligentes o smart contracts) permite la suscripción de pólizas en tiempo real y la gestión automatizada de siniestros. Sin embargo, esta velocidad y el debilitamiento de la presencialidad física crean un terreno fértil para que las organizaciones criminales intenten asimilar fondos de origen ilícito mediante el fraccionamiento, el pago de primas sobrevaluadas o la reclamación de siniestros simulados, utilizando la opacidad inherente a los entornos virtuales menos regulados.

2. Factores de Riesgo Emergentes e Inteligencia Artificial

La incorporación de la Inteligencia Artificial (IA) y el Machine Learning en la selección de riesgos y el procesamiento de reclamos ofrece ventajas analíticas innegables. No obstante, en el contexto de LC/FT/FPADM y Otros Ilícitos, la convergencia digital introduce factores de riesgo específicos que son citados a continuación:

Anonimato y Suplantación de Identidad: El uso de identidades sintéticas o manipuladas mediante tecnologías Deepfake para vulnerar los sistemas de verificación digital en los procesos de Onboarding digital.

Velocidad de Transacción: La automatización extrema reduce el tiempo de ventana disponible para que los analistas de cumplimiento detecten y suspendan operaciones sospechosas antes de que los fondos se dispersen o se consoliden en el mercado del reaseguro internacional.

Uso de Criptoactivos: La integración de pasarelas de pago que aceptan monedas virtuales para el pago de primas o la liquidación de indemnizaciones,

lo que dificulta la trazabilidad del beneficiario final, aun cuando en el sector asegurador venezolano, no se utiliza este medio de pago.

Sesgo del Algoritmo (Caja Negra): El riesgo de que los modelos de Inteligencia Artificial predictiva ignoren patrones atípicos de Legitimación de Capitales si no han sido entrenados específicamente para detectar anomalías de cumplimiento, priorizando la rentabilidad comercial sobre la alerta de riesgo.

3. Marco Normativo Internacional y Nacional sobre Nuevas Tecnologías

La respuesta regulatoria global y local busca equilibrar la innovación financiera con la seguridad del sistema económico.

Marco Internacional

El Grupo de Acción Financiera Internacional (GAFI/FATF) ha liderado la pauta mediante la actualización de sus 40 Recomendaciones, específicamente la Recomendación 15 (Nuevas Tecnologías). Esta directriz exige a los países e instituciones financieras identificar y evaluar los riesgos de Legitimación de Capitales y Financiamiento al Terrorismo que surjan del desarrollo de nuevos productos, prácticas comerciales o el uso de tecnologías nuevas o en desarrollo, aplicando un Enfoque Basado en Riesgo (EBR) antes del lanzamiento de dichas tecnologías.

Marco Nacional (Venezuela)

En el ámbito venezolano, la regulación se articula de manera estricta:

Ley de la Actividad Aseguradora: Establece las bases de supervisión de los sujetos obligados del sector, delegando la potestad normativa en el ente rector.

Superintendencia de la Actividad Aseguradora (SUDEASEG): A través de sus providencias regulatorias en materia de administración de riesgos de LC/FT/FPADM y Otros Ilícitos, obliga a los sujetos obligados a adecuar sus Sistemas de Control Interno a las realidades tecnológicas, exigiendo auditorías sobre los canales electrónicos de comercialización.

Vínculo Operativo: Estas normativas convergen con las directrices de la Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al

Terrorismo (ONCDOFT) y las exigencias del Servicio Nacional Integrado de Administración Tributaria (SENIAT) en materia de facturación digital y control impositivo, requiriendo una debida diligencia del cliente (DDC) robusta y digitalizada que impida el uso de la estructura aseguradora para el desvío de capitales.

4. Riesgos Asociados a la Convergencia Tecnológica

El riesgo tecnológico y el riesgo de legitimación de capitales se entrelazan de tres formas críticas, que se identifican a continuación:

Riesgo Operativo y de Ciberseguridad: Ataques de ransomware donde las indemnizaciones o rescates se exigen a través de canales que facilitan la Legitimación de Capitales, o la vulneración de bases de datos para robar identidades legítimas utilizadas luego en fraude de seguros, que es el delito que más afecta a la actividad aseguradora.

Riesgo de Cumplimiento (Compliance Risk): Incapacidad de los sistemas tradicionales de monitoreo de transacciones para adaptarse al volumen y velocidad de los canales digitales, generando sanciones severas por parte de los órganos de supervisión.

Riesgo de Contagio y Reputacional: La utilización de una plataforma Insurtech por redes de financiamiento al terrorismo o proliferación de armas (FPADM) a través de contratos de reaseguro transfronterizos, provocando la pérdida de corresponsalías internacionales y bloqueos financieros (vía listas restrictivas como OFAC, UE o Reino Unido).

Aunado a esta convergencia y a este nuevo ecosistema, se debe tomar en cuenta otros aspectos y tipologías que se pudieran originar con las nuevas tecnologías, por ello a continuación se hace un análisis sobre estos elementos:

1. La Fusión de Ecosistemas: El Triángulo de la Vulnerabilidad

La convergencia digital borra las fronteras tradicionales entre el sector financiero, el tecnológico y el de seguros. Hoy en día, una póliza no solo la vende una aseguradora tradicional; la vende una Insurtech aliada con una Fintech de pagos a través de una plataforma de comercio electrónico.

Esta interconexión crea lo que los analistas de riesgo llaman el Triángulo de la Vulnerabilidad, el cual está integrado por:

Insurtech (Foco en Ventas): Diseña una experiencia de usuario (UX) hiper-simplificada: "Asegura tu vehículo en 3 clics desde WhatsApp".

Fintech (Foco en Liquidez): Integra pasarelas de pago automatizadas, billeteras digitales y pasarelas peer-to-peer (P2P).

El Choque (Convergencia): Al eliminar la fricción para el cliente legítimo, también se eliminan los filtros para el delincuente. La velocidad de comercialización colisiona con el tiempo requerido para hacer una Debida Diligencia (DDC) intensificada.

2. Tipologías Criminales de Nueva Generación (La Convergencia Operativa)

¿Cómo aprovechan los legitimadores de capitales esta convergencia en el mercado asegurador? Las tipologías han evolucionado de lo físico a lo algorítmico:

La Legitimación de Capitales por "Recompra Directa" mediante Smart Contracts: Organizaciones criminales programan contratos inteligentes en cadenas de bloques (blockchains) para adquirir criptoseguros paramétricos (seguros que pagan automáticamente si ocurre un evento verificable, como el retraso de un vuelo o un cambio climático). Utilizan capital ilícito en criptomonedas para fondear las primas y, mediante la manipulación u orquestación del evento, reciben el pago de la indemnización en criptoactivos "limpios" y justificados por un contrato de seguros, esto puede aplicar una vez que autorice la utilización.

Estratificación a través de Pólizas de Vida de Alto Valor con Rescate Anticipado Digital: Tradicionalmente, rescatar una póliza de vida implicaba un trámite presencial de semanas. Con la transformación digital, los portales de autogestión permiten inyectar grandes primas únicas electrónicamente y solicitar el "rescate anticipado" (cancelación del contrato a cambio del valor en efectivo) de forma 100% digital en 48 horas. El delincuente acepta perder un

10% o 15% en penalizaciones, asumiéndolo como el "costo operativo" de Legitimar Capitales.

Mulas de Seguros y Reclamaciones de Microseguros Automatizadas: Mediante el uso de Inteligencia Artificial Generativa, redes criminales crean perfiles de clientes falsos a escala masiva. Adquieren miles de microseguros digitales (de bajo monto, que vuelan bajo el radar de las alertas de la SUDEASEG) y simulan siniestros masivos utilizando fotografías modificadas digitalmente. La Inteligencia Artificial de la aseguradora, programada para pagar rápido reclamos menores de manera automática, desembolsa fondos legítimos a cuentas puente, tomando en cuenta lo establecido en la Ley de la Actividad Aseguradora (2024), sobre el plazo máximo para el pago de la Indemnización que no exceder de veinte (20) días hábiles contados a partir del momento en que la empresa de seguros recibió el último documento que debe consignar el cliente.

3. La Paradoja de la Inteligencia Artificial en la Convergencia

La Inteligencia Artificial en la transformación digital actúa como un arma de doble filo, lo que representa un punto focal de análisis, por ello se detalla lo siguiente:

El Lado Oscuro (Evasión Algorítmica)

Los legitimadores de capitales avanzados utilizan técnicas de Adversarial Machine Learning (Aprendizaje Automático Adversario). Esto significa que prueban los sistemas de monitoreo digital de las aseguradoras con transacciones pequeñas y variables para mapear el comportamiento del algoritmo de cumplimiento. Una vez que descubren los umbrales de alerta del software de la aseguradora, programan sus transacciones ilícitas para que imiten perfectamente el comportamiento de un cliente de bajo riesgo.

El Lado Defensivo (RegTech y SupTech)

Para contrarrestar esto, la transformación digital de la aseguradora debe incluir obligatoriamente tecnologías de cumplimiento (RegTech). La convergencia positiva ocurre cuando la Inteligencia Artificial de la empresa de seguros deja de buscar solo montos sospechosos y empieza a analizar variables conductuales digitales:

1.- Biometría del comportamiento (cómo interactúa el usuario con la app, velocidad de tecleo, cambios sospechosos de dirección IP).

2.- Análisis de grafos y redes neuronales para detectar si múltiples pólizas aparentemente inconexas comparten la misma billetera digital o el mismo patrón de navegación.

Conclusiones

La convergencia digital en el sector asegurador ha transformado el riesgo de LC/FT/FPADM y Otros Ilícitos de un problema estático y documental a un desafío dinámico, de datos masivos (Big Data) y velocidad milimétrica. El reto regulatorio ya no es verificar que el cliente firme un formulario físico, sino garantizar la inmutabilidad y trazabilidad de su huella digital a lo largo de toda la cadena de bloques del seguro.

La transformación digital en la actividad aseguradora es un proceso irreversible que redefine las fronteras del riesgo. La convergencia entre la innovación tecnológica y las tipologías de LC/FT/FPADM y Otros Ilícitos, demuestra que las herramientas diseñadas para la eficiencia comercial pueden ser instrumentalizadas por el crimen organizado si no se implementan controles proporcionales.

El éxito de las instituciones del sector no radicará en frenar la digitalización, sino en evolucionar hacia esquemas de Compliance 4.0. Esto implica la adopción de tecnologías de supervisión (RegTech y SupTech) que empleen Inteligencia Artificial para el monitoreo algorítmico en tiempo real, la unificación automatizada de consultas en listas restrictivas globales y el fortalecimiento de

la Debida Diligencia Digital. Solo mediante un Enfoque Basado en Riesgo dinámico, coordinado entre la normativa internacional del GAFI y la supervisión local (SUDEASEG/ONCDOFT), se podrá garantizar la resiliencia y la integridad del mercado asegurador frente a las amenazas de la nueva era digital.

Referencias

Grupo de Acción Financiera Internacional (GAFI). (2012-2025). *Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación: Las Recomendaciones del GAFI*. París, Francia.

Grupo de Acción Financiera Internacional (GAFI). (2021). *Guía para un Enfoque Basado en Riesgos para Monedas Virtuales y Proveedores de Servicios de Activos Virtuales (VAs y VASPs)*. París, Francia.

Asociación Internacional de Supervisores de Seguros (IAIS). (2023). *Application Paper on Combating Money Laundering and Terrorist Financing in the Insurance Sector*. Basilea, Suiza.

República Bolivariana de Venezuela. (2023). *Ley de la Actividad Aseguradora*. Gaceta Oficial Extraordinaria Nro. 6.770, de fecha 29 de noviembre de 2023. Caracas, Venezuela.

Superintendencia de la Actividad Aseguradora (SUDEASEG). *Providencia Administrativa Nro. SAA-01-0536-2024, de fecha 29 de agosto de 2024, publicada en la gaceta oficial extraordinaria Nro. 6.835, de fecha 03 de septiembre de 2024, que contiene las normas sobre la Administración y Fiscalización de los Riesgos relacionados con la Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento a la Proliferación de Armas de Destrucción Masiva y Otros Ilícitos en la Actividad Aseguradora*. Caracas, Venezuela.

Enamorado, J. & Compliance Tech Institute. (2024). *Insurtech y Compliance 4.0: Desafíos del control interno frente al algoritmo*. Editorial Jurídica Digital.

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

¿DE QUÉ MANERA LA INNOVACIÓN TECNOLÓGICA PUEDE TRANSFORMAR LOS SISTEMAS DE PREVENCIÓN DE LC/FT/FPADM Y CUÁLES SON LOS DESAFÍOS QUE PLANTEA PARA LA APLICACIÓN DE LA RECOMENDACIÓN 15 DEL GAFI?

Autor: Lic. Lexssy Y. López H.
Facilitadora: MSc Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

¿De qué manera la innovación tecnológica puede transformar los sistemas de prevención de LC/FT/FPADM y cuáles son los desafíos que plantea para la aplicación de la Recomendación 15 del GAFI?

Autora: Lic. Lexssy Y. López H.
Código ORCID: 0009-0008-1954-5306
Correo electrónico: lylh1529@gmail.com

Resumen

La Recomendación 15 del GAFI constituye un estándar para abordar los riesgos derivados de la innovación tecnológica; sin embargo, la irrupción de nuevas tecnologías plantea desafíos técnicos, operativos y éticos que exigen una interpretación dinámica por parte de los Órganos de Control y Sujetos Obligados. La innovación tecnológica, no debe ser vista únicamente como amenaza para los sistemas de prevención de LC/FT/FPADM, esta proporciona oportunidades relevantes para mejorar procesos como el conocimiento del cliente, el monitoreo transaccional, el análisis documental y la investigación de información relevante, motivo por el cual obliga a interpretar y aplicar ese estándar de una manera más sofisticada. Por otra parte, la innovación tecnológica introduce nuevos desafíos derivados de la manera en que las organizaciones están acostumbradas a analizar y procesar su información, la incorporación de nuevas tecnologías constituye una evolución con respecto a los modelos tradicionales, muchos sujetos obligados no están acostumbrados a procesos que le permitan gestionar grandes volúmenes de información mediante sistemas capaces de aprender y generar resultados adaptativos. En consecuencia, la Recomendación 15 del GAFI no enfrenta únicamente el desafío de regular una tecnología; enfrenta el desafío de establecer cómo deben gobernarse tecnologías capaces de influir en decisiones de cumplimiento.

Descriptores clave: Recomendación 15 GAFI; Prevención, Control, Desafíos.

Abstract

FATF Recommendation 15 serves as a standard for addressing risks arising from technological innovation; however, the emergence of new technologies presents technical, operational, and ethical challenges that require a dynamic interpretation by supervisory bodies and obliged entities. Technological innovation should not be viewed solely as a threat to AML/CFT/CPF prevention systems; it offers significant opportunities to improve processes such as customer due diligence, transaction monitoring, document analysis, and the investigation of relevant information, thereby necessitating a more sophisticated interpretation and application of the standard. Furthermore, technological innovation introduces new challenges regarding how organizations are accustomed to analyzing and processing information; the adoption of new technologies represents an evolution from traditional models, as many obliged entities are unfamiliar with processes that manage large volumes of data using systems capable of learning and generating adaptive results. Consequently, FATF Recommendation 15 faces not only the challenge of regulating technology but also the challenge of establishing how to govern technologies capable of influencing compliance decisions.

Key descriptors: FATF Recommendation 15: Prevention, Control, and Challenges.

Introducción

La constante evolución de la innovación tecnológica, ha generado cambios significativos en la manera en que las organizaciones desarrollan sus actividades al momento de gestionan la información, y establecer mecanismos operativos, esto ha permitido mejorar la eficiencia operativa, fortalecer los procesos como los de identificación y análisis de información, así como desarrollar herramientas innovadoras orientadas al cumplimiento de obligaciones regulatorias.

Sin embargo, la incorporación de esta nueva tecnología dentro de los sistemas de cumplimiento plantea una realidad dual. Por una parte, ofrece oportunidades significativas para fortalecer los mecanismos preventivos mediante herramientas avanzadas de análisis, automatización y procesamiento de información. Por otra parte, genera nuevos desafíos

relacionados con la transparencia de los modelos utilizados, la supervisión humana, la responsabilidad institucional.

En este contexto, el Grupo de Acción Financiera Internacional (GAFI) ha reconocido la importancia de considerar los avances tecnológicos dentro de los sistemas internacionales de prevención, la Recomendación 15 establece la necesidad de que los países y sujetos obligados presten atención a los riesgos derivados de nuevas tecnologías, productos y servicios innovadores, reconociendo que la evolución tecnológica puede modificar la naturaleza de las amenazas relacionadas con los delitos financieros.

La siguiente investigación parte de la premisa de que tecnología no debe ser considerada únicamente como una amenaza para los sistemas de prevención, sino como una herramienta estratégica cuyo impacto dependerá de la capacidad institucional para implementarla bajo principios de responsabilidad, transparencia y supervisión humana.

En consecuencia, el presente ensayo tiene como propósito analizar la como la innovación tecnológica representa un desafío emergente para los sistemas de prevención de LC/FT/FPADM, examinando sus principales aplicaciones y oportunidades.

Para ello, se abordará la evolución del Recomendación 15 del GAFI, la incorporación de herramientas que pueden fortalecer el sistema de prevención y control de LC/FT/FPADM, y los nuevos desafíos ante el escenario adecuados de gobernanza tecnológica.

1. La Recomendación 15 del GAFI como respuesta a la innovación tecnológica

El Grupo de Acción Financiera Internacional (GAFI), ha demostrado una gran preocupación por la innovación tecnológica, si bien es cierto que este grupo fue creado en 1989, realizó su primera versión de recomendaciones en el año 1990 y fue revisada en el año 1996, la cual estuvo enfocada en la tipificación del delito, la cooperación internacional, la identificación del cliente y el reporte

de actividad sospechosa, ya para su segunda revisión en el año 2003, la cual fue publicadas en octubre 2004 (fatf-gafi.org), hacía mención a que "las instituciones financieras deberían prestar especial atención a cualquier amenaza de lavado de dinero derivada de tecnologías nuevas o en desarrollo que pudieran favorecer el anonimato y, cuando fuera necesario, adoptar medidas para impedir su utilización en esquemas de lavado de dinero".

El panorama para el año de la segunda revisión, dentro del sistema financiero, era que ya se comenzaba a expandir, la banca por internet, los primeros pagos electrónicos, las tarjetas prepagadas, las relaciones comerciales sin contacto presencial y los primeros mecanismos de transferencias digital de fondos, originando que GAFI considerara establecer que se debe tener medidas para evitar el lavado dinero derivado de las amenazas provenientes de nuevas tecnologías, identificando cuando esta tecnología pudiesen favorecer el anonimato, o las relaciones comerciales no presencial, era una advertencia a que esta nueva forma de llevar el negocio pudiera impedir que la debida diligencia funcione adecuadamente.

Consciente de esta realidad, ya para el año 2012 el GAFI incorporó dentro de sus estándares internacionales la necesidad de evaluar los riesgos derivados de las nuevas tecnologías. Esta recomendación a la fecha se encuentra vigente y ha sido revisada, el propósito de esta recomendación no consiste en limitar la innovación tecnológica, sino en asegurar que el desarrollo de nuevos servicios financieros vaya acompañado de mecanismos adecuados de prevención, lo que plantea dicho grupo es lo siguiente:

Recomendación 15. Nuevas Tecnologías

> Los países y las instituciones financieras deben identificar y evaluar los riesgos de lavado de activos o financiamiento del terrorismo que pudieran surgir con respecto a (a) el desarrollo de nuevos productos y nuevas prácticas comerciales, incluyendo nuevos mecanismos de envío, y (b) el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como los existentes. En el caso de las instituciones financieras, esta evaluación del riesgo debe hacerse antes del lanzamiento de los nuevos productos, prácticas comerciales o el uso de tecnologías nuevas o en

> desarrollo. Los países y las instituciones financieras deben tomar medidas apropiadas para administrar y mitigar esos riesgos..." (GAFI, 2025, pág. 20)

El factor determinante para la creación de la Recomendación 15 del GAFI, fue la transformación del sistema financiero mundial, la aparición de nuevos canales de distribución de los servicios financieros, el desarrollo de plataformas digitales, la automatización de procesos y el crecimiento de los activos virtuales, si bien es cierto que estos avances han incrementado la eficiencia, la inclusión financiera y la competitividad del sector financiero, también se han generado nuevas vulnerabilidades susceptibles de ser explotadas para la legitimación de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva.

El objetivo de la Recomendación 15 del GAFI es garantizar que la incorporación de nuevas tecnologías no genere vulnerabilidades que puedan ser aprovechadas para la legitimación de capitales, el financiamiento del terrorismo o el financiamiento de la proliferación de armas de destrucción masiva, teniendo un carácter transversal, a diferencia de otras recomendaciones como la debida diligencia del cliente, la conservación de documentos o el reporte de operaciones sospechosas.

En este mismo orden de ideas, con base a que la Recomendación 15, fue redactada no considerando la aparición de tecnología capaces de tomar decisiones, generar análisis autónomos y modificar sus propios patrones de funcionamiento, no obstante, el grupo regional GAFILAT, en el 2021 publicó una guía estratégica y técnica para que las entidades competentes comprendan y dominen el alcance de esta recomendación.

Lo establecido en dicha Guia en donde se hace un análisis por este organismo regional, debería ser tomado como referencias en la construcción de normativas especificas correspondientes al uso de nuevas tecnologías, ya que hace mención del Control y Supervisión Interna de los Sistemas, advierte que en muchos países de Latinoamérica, los controles relacionados con esta

tecnología avanzada aún no están plenamente determinados debido a una ausencia de desarrollo legislativo, de igual forma recomienda que la gobernanza de los sistemas de IA incluya mecanismos de controles específicos para evitar sesgos y asegurar que los modelos se ajusten para reconocer nuevas conductas delictivas.

Se debe tomar en consideración, al momento de formular lineamientos para la utilización de las nuevas tecnologías, que estas cuenten con la transparencia y supervisión humana y considerar que los sistemas avanzados no eliminan la responsabilidad de las instituciones ni sustituye el juicio humano.

2. La innovación tecnológica y la transformación de los sistemas de prevención y control de LC/FT/FPADM

La transformación digital puede promover una evolución significativa en los mecanismos de prevención de la legitimación de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. La innovación tecnológica puede conseguir modificar la forma en que las instituciones financieras diseñen, ejecuten y supervisen sus programas de cumplimiento. La incorporación de nuevas tecnologías no responde únicamente a la creciente complejidad de los riesgos asociados a un sistema financiero cada vez más digitalizado, este debe responder a un entorno más dinámico e interconectado, optimizando sus procesos operativos.

Cuando se hace referencia a los sistemas de prevención de legitimación de capitales, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva, esto comprende a todo el conjunto de políticas, procedimientos, controles y estructuras institucionales destinados a evitar que organizaciones financieras no sean utilizadas para fines ilícitos.

El Grupo de Acción Financiera Internacional (GAFI, 2025) establece estándares internacionales orientados a que los países, Órganos de Control y Sujetos Obligados desarrollen mecanismos eficaces para prevenir, detectar y reportar actividades vinculadas con delitos financieros.

> La lucha contra el lavado de dinero en la era digital exige un enfoque innovador que integre las nuevas tecnologías emergentes para fortalecer los mecanismos de prevención y control. La construcción de un andamiaje robusto que combine el uso estratégico de la tecnología, la colaboración entre entidades, la adaptación de la normativa y la capacitación continua permitirá a las instituciones financieras, las fuerzas del orden y las entidades reguladoras combatir de manera más efectiva este delito y proteger la integridad del sistema financiero. (Auren México 2024, en la sección de la conclusión).

El uso intensivo de tecnologías como la Inteligencia Artificial, Big Data y la automatización de procesos, ha permitido una mayor inclusión financiera y eficiencia operativa. Sin embargo, también ha incrementado los riesgos asociados a la legitimación de capitales, especialmente por el uso de canales digitales que pueden facilitar el anonimato, la fragmentación de transacciones y la velocidad de movimientos sospechosos.

La incorporación de nuevas tecnologías, requiere pasar de los sistema tradicionales de prevención de la legitimación de capitales y los financiamientos orientados principalmente al cumplimento de obligaciones formales: identificación del cliente, monitoreo de operaciones, generación de alertas y reporte de operaciones sospechosas, hacia un modelo preventivo y predictivo capaz de identificar patrones emergentes, incorporando análisis continuo de comportamiento del cliente, identificación de patrones transaccionales, evaluación dinámica de niveles de riesgo y capacidad predictiva mediante análisis avanzados de datos.

En este mismo contexto, la tecnología debe permitir un modelo de Debida Diligencia para el Conocimiento del Cliente, donde la información del cliente sea evaluada permanentemente y que esta permita actualizar los datos de manera automatizada. Considerando que la automatización consiste en la utilización de sistemas tecnológicos para ejecutar procesos previamente definidos con mínima intervención humana.

La automatización forma parte de la transformación digital de las organizaciones al permitir mejorar la eficiencia, reducir tiempos operativos y optimizar procesos repetitivos.

Las herramientas basadas en inteligencia artificial, pueden automatizar procesos de identificación documental, reconocimiento biométrico, análisis de información pública y validación de datos provenientes de múltiples fuentes. Estas capacidades permiten mejorar la eficiencia operativa, reducir tiempos de respuesta y fortalecer la detección de inconsistencias que podrían representar señales de alerta.

La automatización tradicional se diferencia de la inteligencia artificial porque normalmente ejecuta instrucciones predeterminadas, mientras que la IA puede analizar información y generar resultados mediante modelos de aprendizaje.

La Inteligencia Artificial, representa una de las principales innovaciones que se pueden aplicar en las políticas preventivas, tal como se ha mencionado, estas permiten analizar grandes volúmenes de información, identificar patrones de comportamiento y generar modelos predictivos para detectar operaciones relacionadas con los delitos de LC/FT/FPADM.

Puede entenderse por inteligencia artificial como una disciplina de la informática orientada al desarrollo de sistemas capaces de realizar tareas asociadas tradicionalmente con la inteligencia humana, tales como aprendizaje, razonamiento, percepción, interpretación y toma de decisiones.

Para Russell y Norvig (2021), la inteligencia artificial estudia los agentes capaces de percibir su entorno y actuar sobre él mediante procesos computacionales orientados a alcanzar determinados objetivos. Desde esta perspectiva, la IA no representa únicamente automatización, sino sistemas con capacidad de analizar información y generar respuestas adaptativas.

En cuanto al ámbito jurídico y regulatorio, Barrio (2020) señala que la inteligencia artificial plantea nuevos desafíos debido a que sus procesos pueden alcanzar niveles de complejidad que dificultan determinar cómo se

producen ciertos resultados y quién debe asumir responsabilidad cuando estos generan consecuencias.

De acuerdo con el análisis estratégico sobre el uso de la inteligencia artificial el GAFILAT (2021), indica que la IA se define como una rama de la ciencia de la computación que busca simular la inteligencia humana en las maquinas. Aunque no existe una definición única y ampliamente aceptada, tradicionalmente requieren de la intervención y el razonamiento humano.

Desde una perspectiva técnica, la IA puede definirse como el conjunto de métodos y sistemas computacionales capaces de realizar tareas que tradicionalmente requerían inteligencia humana, tales como reconocer patrones, interpretar información, aprender a partir de datos, formular predicciones y apoyar procesos de toma de decisiones. A diferencia de los sistemas informáticos convencionales, cuya actuación depende de reglas previamente programadas, las soluciones basadas en IA utilizan modelos de aprendizaje que mejoran su desempeño conforme procesan nuevos datos, permitiendo identificar relaciones complejas que difícilmente serían detectadas mediante técnicas tradicionales.

En el ámbito del cumplimiento normativo, esta capacidad representa un cambio de paradigma. Los programas de prevención de LC/FT/FPADM han evolucionado desde modelos basados en controles manuales y reglas estáticas hacia esquemas apoyados en analítica avanzada, automatización e inteligencia de datos. Este cambio permite procesar grandes volúmenes de información en tiempos reducidos, identificar comportamientos atípicos con mayor precisión y fortalecer la capacidad preventiva de las organizaciones frente a riesgos cada vez más sofisticados.

La rama de la IA, conocida como Aprendizaje Automático o Machine Learning, permite que los sistemas mejoren su desempeño mediante la identificación de patrones en los datos, sin depender exclusivamente de instrucciones programadas previamente, según Russell y Norvig (2021), el aprendizaje automático permite que los sistemas construyan modelos a partir de

experiencias o ejemplos, generando predicciones o decisiones basadas en información procesada.

Desde una perspectiva aplicada al sistema preventivo y de control de los delitos de LC/FT/FPADM, el aprendizaje automático permite analizar grandes volúmenes de operaciones financieras e identificar comportamientos que podrían pasar inadvertidos mediante mecanismos tradicionales.

En este mismo orden de ideas, existe otro termino denominado RegTech (Regulatory Technology), el cual hace referencia al uso de tecnologías innovadoras destinadas a facilitar el cumplimiento de obligaciones regulatorias mediante herramientas digitales, automatización y análisis avanzado de información.

Según Arner, & Buckley (2017), las tecnologías regulatorias representan una evolución del cumplimiento financiero al permitir que las instituciones gestionen obligaciones normativas mediante soluciones tecnológicas más eficientes.

La incorporación de la tecnología al sistema de prevención y control de LC/FT/FPAMD, debe entenderse como un proceso de transformación organizacional que exige fortalecer la cultura de cumplimiento, desarrollar nuevas competencias profesionales y consolidar estructuras de gobernanza tecnológica capaces de garantizar que la innovación se implemente de forma ética, transparente y alineada con los estándares internacionales.

Es fundamental, que se tome en consideración para el fortalecimiento del sistema de prevención y control de LC/FT/FPADM, el establecimiento de lineamientos documentales (resoluciones y normas), enfocados en los siguientes puntos:

- Descripción de la caracterización del conocimiento y uso: Evaluar que tanto conocen y emplean los Órganos de Control y los Sujetos Obligados, tecnologías como el Big Data, la Inteligencia Artificial (IA) el aprendizaje de máquinas (Machine Learning) y la minería de datos y textos en su análisis operativos y estratégicos.

- Presentación de metodologías: Exponer las principales herramientas tecnológicas y metodologías de análisis de datos disponibles hoy en día, profundizando tanto en sus aspectos teóricos como en sus aplicaciones prácticas.
- Diagnóstico territorial y recomendaciones: Identificar el nivel real de adopción de estas tecnologías por parte los Órganos de Control y emitir recomendaciones estratégicas para un mejor aprovechamiento de estos recursos tecnológicos.
- Identificación de casos de uso: Presentar ejemplos concretos de cómo estas tecnologías pueden ser aplicadas para detectar anormalidades que los métodos tradicionales pasan por alto.
-

3. Desafíos presentes entre la innovación tecnológica y el cumplimiento preventivo y control de los delitos de LC/FT/FPADM

La aplicación de tecnología avanzada a los sistemas de prevención y control de los delitos de LC/FT/FPADM, presenta una serie de desafíos críticos que van desde obstáculos técnicos hasta dilemas éticos y legales complejos, tal como se detalla a continuación:

1. Opacidad: Muchos sistemas como los de inteligencia artificial (IA) especialmente los modelos de aprendizaje profundo, funcionan como una “caja negra”, lo que dificulta explicar cómo se llega a una decisión en especifica. En el ámbito del cumplimiento, donde las decisiones deben justificarse ante auditores y reguladores, esta falta de transparencia puede minimizar la confianza y generar riesgos legales. Existe una tensión constante entre la complejidad técnica de los modelos más avanzados y las exigencias de los órganos contralores.
2. Sesgos Algorítmicos y equidad: Si los modelos de IA se entrenan con datos históricos que contienen prejuicios, pueden perpetuar o amplificar sesgos y discriminaciones. Eliminar por completo estos

sesgos es extremadamente difícil porque los datos suelen reflejar desigualdades sociales previas. Una IA sesgada en tareas de cumplimiento, como la puntuación de riesgos de clientes, no solo es éticamente cuestionable, sino que puede derivar en el incumplimiento de normativas antidiscriminación.

3. Calidad de Datos en integración técnica: Un desafío operativo mayor es la falta de estructura y organización de los datos, en el caso del monitoreo puede generar un elevado número de “falsos positivos” y reducir la productividad de los investigadores. En este sentido, muchos datos relevantes para el cumplimiento se encuentran en sistemas antiguos o formatos no estructurados, lo que hace que su limpieza e integración sea costosa compleja. Sin una alta calidad de los datos, los resultados de cualquier tecnología son poco fiables.
4. Evolución normativa y responsabilidad legal: Las regulaciones, como por ejemplo los Reglamentos de IA de la Unión Europea, están en constantes cambios, clasificando ciertos sistemas de cumplimiento (como la detección de LC o evaluación crediticia) como “Riesgo Alto”, lo que impone obligaciones estrictas de transparencia y seguridad. Además, persiste la dificultad de asignar responsabilidades legales cuando una decisión automatizada falla, la organización sigue siendo responsable de las sanciones resultantes, lo que exige mantener siempre una supervisión humana efectiva.
5. Fraude sofisticado y nuevas amenazas: La tecnología también es utilizada por criminales para crear identidades sintéticas que combina datos reales y falsos, o para utilizar deepfakes (manipulación de imagen y voz) con el fin de engañar a los sistemas de verificación de identidad (DDC). El aumento de la accesibilidad a herramientas gratuitas de intercambio de rostros y emuladores

móviles ha disparado los ataques contra los sistemas de verificación remota.

6. Impacto humano y experiencia del cliente: La implementación de controles tecnológicos puede generar fricción en la experiencia del cliente, especialmente en neobancos que prometen incorporaciones rápidas, si las verificaciones son demasiado intrusivas, el cliente puede abandonar el proceso. Asimismo, también puede existir una resistencia cultural interna, donde los empleados pueden temer la perdida de funciones o el valor de su juicio profesional ante la automatización. Por ello es imperativo invertir en la capacitación continua del personal para que puedan colaborar con la máquina de forma segura y eficaz.

Conclusión

La Recomendación 15 del GAFI constituye un marco fundamental para comprender la relación entre innovación tecnológica y prevención de delitos financieros, no obstante, se debe reconocer que las nuevas tecnologías requieren mecanismos adecuados de supervisión y control. La evolución de la tecnología evidencia la necesidad de complementar este enfoque con criterios específicos relacionados con gobernanza tecnológica, transparencia algorítmica y responsabilidad institucional.

El existo de la tecnología en el cumplimiento depende de encontrar un equilibrio estratégico entre las prácticas de control ya establecidas y la integración gradual de estas nuevas herramientas innovadoras. Si bien es cierto que la tecnología es capaz de mejorar la eficiencia de los procesos de debida diligencia, monitoreo transaccional y análisis de operaciones inusuales, de los sistemas de cumplimiento, ésta no puede sustituir el criterio profesional dentro del sujeto obligado, debe ser concebida como una herramienta de apoyo, capaz de ampliar sus capacidades analíticas, pero no de reemplazar la evaluación humana necesaria para interpretar resultados y adoptar decisiones

fundamentadas, esta debe ser concebida como un elemento complementario dentro del modelo de prevención

No obstante, es importante considerar que la aplicación de nuevas tecnologías implica varios desafíos, las cuales no radica únicamente en desarrollar sistemas más avanzados, sino en garantizar que dichas tecnologías sean utilizadas bajo principios de responsabilidad, transparencia y control humano. El futuro de los sistemas de prevención de LC/FT/FPADM dependerá de la capacidad de las instituciones para establecer una relación equilibrada entre innovación tecnológica y responsabilidad profesional.

En este mismo orden de ideas, la calidad de los resultados obtenidos va a depender de la precisión de los datos utilizados, de la actualización permanente de las bases de información y de la capacidad institucional para revisar situaciones excepcionales.

Referencias

Auren-México. (2024, 29 de abril). Combatiendo el lavado de dinero en la era digital: Tecnologías para maximizar el control, https://auren.com/mx/blog/combatiendo-el-lavado-de-dinero-en-la-era-digital-tecnologias-para-maximizar-el-control/

Barrios Andre, M. (2020). Introducción al Derecho de las Nuevas Tecnologias, Bosch Mexico, Mexico, 1er edición.

Barberis, J., Arner, D. W., Buckley, R. P. (2017). FinTech, RegTech, and the Reconceptualization of Financial Regulation. Northwestern journal of international law & business.

Escuela Nacional de Administración y Hacienda Pública. (2016). Manual para elaboración y presentación de trabajos académicos. ENAHP-IUT. Caracas.

Grupo de Acción Financiera Internacional (GAFI). (2025). Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación de armas de destrucción masiva: Las Recomendaciones del GAFI

Grupo de Acción Financiera Internacional. The 40 Recommendations, published October 2004, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/The40recommendationspublishedoctober2004.html

Grupo de Acción Financiera Internacional. (2021). Actualización específica sobre la aplicación de las normas del GAFI a los activos virtuales y proveedores de servicios de activos virtuales. GAFILAT.

Grupo de Acción Financiera Internacional. (2021). Análisis Estratégico sobre el uso de inteligencia artificial, minería de datos y análisis de big data en prevención y detección LA/FT (UIF-MP), (GAFILAT).

Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4.ª ed.). Pearson.

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

ANÁLISIS DEL EFECTO DE LA ADOPCIÓN DE LAS CRIPTOMONEDAS Y SU UTILIZACIÓN COMO VEHÍCULO PARA LA LEGITIMACIÓN DE CAPITALES, FINANCIAMIENTO AL TERRORISMO Y FINANCIAMIENTO A LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA

Autor: Dr. Juan Jesús Arevalo
Facilitadora:MSc. Nancy Granadillo
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

República Bolivariana de Venezuela
Ministerio del Poder Popular de Economía y Finanzas
Escuela Nacional de Administración y Hacienda Pública – IUT
Dirección de Postgrado y Adiestramiento
Programa de Especialización en Gestión Contra la Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Nuevas Tecnologías

Análisis del efecto de la adopción de las criptomonedas y su utilización como vehículo para la legitimación de capitales, financiamiento al terrorismo y financiamiento a la proliferación de armas de destrucción masiva

Autor: Dr. Juan Jesús Arevalo
Código ORCID: 0009-0009-1160-046X
Correo electrónico: Jaregon5@gmail.com

Resumen

El objeto de la presente investigación es el efecto del uso de las criptomonedas como instrumento de pago y su uso como vehículo para la comisión del delito de Legitimación de Capitales, el Financiamiento al Terrorismo y el Financiamiento a la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM), en la República Bolivariana de Venezuela. El fenómeno de la migración transaccional hacia los activos virtuales responde a factores socioeconómicos estructurales como la hiperinflación y la pérdida de las funciones tradicionales del dinero convencional, convirtiéndose en un circuito paralelo que, si bien dinamiza el comercio informal, desafía loas medidas establecidas por el Estado. Metodológicamente, el estudio se centró en un diseño documental, con un nivel analítico, cuya técnica de revisión crítica de literatura, informes y estándares internacionales vigentes. Se evidencio pseudonimato, la descentralización transfronteriza y herramientas avanzadas de ocultamiento, configuran tipologías delictivas complejas que permiten la mutación de las fases de colocación, estratificación e integración del lavado de dinero. Asimismo, al contrastar el marco jurídico interno como la Constitución Nacional y la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo LOCDOFT, con las Recomendaciones del Grupo de Acción Financiera Internacional GAFI Se concluye que existe la necesidad imperiosa de dotar tecnológicamente a las unidades de cumplimiento para mitigar de manera eficiente las vulnerabilidades del ciberespacio financiero en resguardo de la soberanía económica de la nación.

Descriptores: Criptomonedas, Legitimación de Capitales, Financiamiento al Terrorismo, Blockchain, Regulación Financiera, Compliance.

Abstract

The objective of this research is to examine the effect of using cryptocurrencies as a payment instrument and their use as a vehicle for committing the crimes of Money Laundering, Terrorist Financing, and Financing the Proliferation of Weapons of Mass Destruction (ML/TF/WMD) in the Bolivarian Republic of Venezuela. The phenomenon of transactional migration to virtual assets responds to structural socioeconomic factors such as hyperinflation and the loss of the traditional functions of conventional money, becoming a parallel circuit that, while boosting informal commerce, challenges the measures established by the State. Methodologically, the study focused on a documentary design, with an analytical level, employing a critical review of literature, reports, and current international standards. The research revealed that pseudonymity, cross-border decentralization, and advanced concealment tools constitute complex criminal typologies that allow for the mutation of the placement, layering, and integration phases of money laundering. Furthermore, comparing the domestic legal framework, such as the National Constitution and the Organic Law against Organized Crime and Terrorism Financing (LOCDOFT), with the Recommendations of the Financial Action Task Force (FATF), it is concluded that there is an urgent need to technologically equip compliance units to efficiently mitigate vulnerabilities in the financial cyberspace, thereby safeguarding the nation's economic sovereignty.

Descriptors: Cryptocurrencies, Money Laundering, Terrorism Financing, Blockchain, Financial Regulation, Compliance.

Introducción

La vinculación entre tecnología y delito no comenzó con el desarrollo de las computadoras. Con el surgimiento del telégrafo durante el siglo XIX se interceptaban comunicaciones para la transmisión de información falsa con fines económicos. Ya con la irrupción del teléfono, durante la década del 60, diferentes programadores informáticos o especialistas en sistemas intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam mediante el uso gratuito del servicio. Los phreakers (neologismo proveniente de las palabras en inglés “freak”, de rareza; “phone”, de teléfono; y “free”, gratis) utilizaban unas blue boxes o cajas azules que reproducían tonos de llamadas similares a los utilizados por la Bell Corporation, y la ATT establecía comunicaciones gratuitas de larga distancia.

En cuanto a la utilización de computadoras, la principal preocupación estaba dada por el manejo de la información a partir del almacenamiento y procesamiento de datos personales producto de obras de ficción como 1984 de Orwell. Las primeras conductas indebidas o ilícitas relacionadas con computadoras comenzaron a verse reflejados durante la década del 70, a partir de algunos casos resonantes retratados por los periódicos de época. Los primeros delitos informáticos eran de tipo económico, entre los que se destacaban el espionaje informático, la "piratería" de software, el sabotaje a bases de datos digitalizados y la extorsión. En relación con el espionaje, estos se llevaban a cabo mediante la extracción de discos rígidos de las computadoras, el robo de diskettes o copia directa de la información de los dispositivos, tanto, así como la absorción de emisiones electromagnéticas que irradia toda computadora para la captación de datos.

El espionaje era comercial o industrial, como suele denominarse, siendo sus principales objetivos los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas. En relación a la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco del espionaje industrial. Los casos de sabotaje y extorsión informática eran los delitos que más preocupaban organizaciones ante la alta concentración de datos almacenados en formato digital. En cuanto a los fraudes de tipo financiero, a fines de esa década y principios del 80, hubo casos de alteración de archivos de las bases de datos de las empresas y los balances de los bancos para la manipulación de facturas de pagos de salarios. Casos típicos se realizaban mediante la instalación de dispositivos lectores, en las puertas de entradas de los cajeros automáticos, y teclados falsos, en los mismos, para la copia de los datos de las tarjetas de débito a través de la vulneración de las bandas magnéticas.

Esto motivó, por parte de las empresas emisoras, la adopción de chips, en los plásticos, como medida de seguridad. (2) "Fue justamente durante esta época

donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados Unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial". (3) Con la apertura global de internet, a mediados de los años noventa, por parte de la administración norteamericana, y el posterior desembarco de empresas y bancos a la red para el desarrollo del comercio electrónico, la industria editorial, discográfica y cinematográfica comenzó una afrenta contra la multiplicidad de casos de violaciones a los derechos de autor, a partir de la descarga e intercambio en línea de obras digitalizadas, música y películas protegidas bajo leyes de copyright.

Asimismo, bajo la posibilidad de construcción de identidades ficticias que brindan los entornos virtuales en internet, un rebrote de pedofilia inundó la red mediante la distribución de imágenes de pornografía infantil. Asimismo, el tema de la protección a la intimidad y la privacidad de las personas comenzaron a ser una preocupación a partir del uso de nuevas tecnologías digitales en la red.

Para Manuel Castells, un nuevo paradigma tecnológico surgido durante la década del 70, en Estados Unidos, dio lugar a un nuevo modelo de desarrollo basado en las tecnologías de la información, que sustituirá al modelo industrialista vigente en las sociedades modernas desde la revolución industrial del siglo XIX. La innovación tecnológica y el cambio organizativo, centrados en la flexibilidad y la adaptabilidad, resultaron condicionantes para la reestructuración del sistema capitalista. Es cuando durante la década del 80 entró en vigor un nuevo modelo de desarrollo: el informacionista. El cual destaca el papel de la información dentro de la sociedad. La sociedad informacional, para Castells, indica una forma de organización social en la que la generación, procesamiento y transmisión de información son factores fundamentales en términos de productividad y poder. En este sentido, la

revolución de las tecnologías de la información produce a nivel global un nuevo modo de producir, comunicar, gestionar y vivir

Desarrollo

Para entender el uso de las criptomonedas y su uso en la Legitimación de capitales y Financiamiento al Terrorismo, resulta imperioso establecer una distinción de base a los términos empleados como lo son "criptoactivo" y "criptomoneda", términos generalmente utilizados como sinónimos, pero con interpretaciones distintas en sus ámbitos de aplicación (descriptivos, jurídicos y técnicos).

Un criptoactivo es un término genérico que define a cualquier representación digital de valor y utiliza la criptografía para garantizar su titularidad y que se transfiere o almacena electrónicamente mediante la tecnología de registro de cadena de bloque (Blockchain). Esta categoría incluye tokens de utilidad, tokens de seguridad, tokens no fungibles NFT y monedas estables (stablecoins).

Por su parte, la criptomoneda es una subcategoría específica dentro de los criptoactivos, se establece como medio de intercambio digital, el cual funciona como unidad de cuenta y reserva de valor. Su arquitectura técnica busca emular las funciones del dinero tradicional, permitiendo la transferencia de valor entre pares (peer-to-peer) sin la intervención de autoridades algunas centrales, dependiendo exclusivamente de algoritmos de consenso matemático y protocolos criptográficos para validar y asegurar las transacciones.

Este documento establece que los Orígenes de los criptoactivos a nivel mundial, es preexistente a la utilización de los criptoactivos como dinero digital, los primeros defensores de los criptoactivos imaginaron resolver las limitaciones prácticas y políticas de las monedas fiduciarias mediante la aplicación de la informática. Durante los años ‘90, se hicieron muchos intentos para crear una moneda digital global, pero todos fallaron. Ello, hasta la entrada en escena del Bitcoin en el año 2009. Bitcoin fue creado por una o grupo de

personas anónimas usando el seudónimo de “Satoshi Nakamoto", aunque su verdadera identidad sigue siendo un misterio, lo especial de Bitcoin es que es un tipo de dinero digital que no necesita una entidad central, como un banco para aprobar las transacciones.

Además, se estableció que solo habrá un total de 21 millones de Bitcoins, esto le da un valor especial y lo diferencia de otras formas de dinero digital, con el paso del tiempo, fueron apareciendo otro tipo de criptoactivos, actualmente existen más de diez mil tipos de activos virtuales en todo el mundo. Si bien existieron intentos previos de crear dinero digital criptográfico como b-money, la génesis del ecosistema actual se sitúa en el contexto de la crisis financiera global de 2008. En octubre de ese año, se publicó el documento técnico (Whitepaper) titulado "Bitcoin, de persona a persona. Este documento propuso la primera solución exitosa al problema del "doble gasto" sin necesidad de una entidad central de confianza, dando origen a la red Bitcoin en enero de 2009 con la minería del "Bloque Génesis o primario”. A partir de este hito fundacional, la evolución se ha desarrollado en diversas etapas:

Primera Generación del 2009-2014: Dominada por Bitcoin y el surgimiento de criptomonedas alternativas, cuyo objetivo principal era mejorar la velocidad o el modelo de emisión monetaria.

Segunda Generación del 2015 al 2025: Marcada por la irrupción de la red Ethereum, la cual introdujo los "contratos inteligentes", esta innovación permitió que la cadena de bloques no solo registrara transacciones financieras, sino que ejecutara acuerdos automatizados, dando origen a las Finanzas Descentralizadas.

Tercera Generación es la Actualidad: Caracterizada por la búsqueda de escalabilidad, interoperabilidad entre distintas cadenas de bloques y la creación de monedas estables, diseñadas para mitigar la extrema volatilidad al vincular su valor a activos subyacentes como el dólar estadounidense o materias primas.

En el contexto venezolano, el uso de los criptoactivos y criptomonedas ha transitado un camino único en el mundo, evolucionando desde un pasatiempo técnico hasta convertirse en una infraestructura de supervivencia económica desde el año 2012, el país fue pionero en la región gracias a su electricidad altamente subsidiada, en este periodo, la minería de Bitcoin se convirtió en una actividad extremadamente rentable y una forma discreta de generar ingresos en divisas frente a un control de cambio asfixiante, simultáneamente, el Bitcoin comenzó a utilizarse como reserva de valor por una pequeña comunidad que buscaba protegerse de la devaluación inicial del Bolívar.

Con la llegada de la hiperinflación en el año 2017, las criptomonedas saltaron de los nichos tecnológicos a la calle. Plataformas de intercambio persona a persona (P2P), como LocalBitcoins, registraron volúmenes de transacciones históricos, posicionando a Venezuela en los primeros lugares del Índice Global de Adopción de Chainalysis, en este contexto, el Gobierno intentó institucionalizar el sector creando la SUNACRIP y lanzando el Petro en el año 2018, la primera criptomoneda estatal, que aunque fue impuesta para trámites, no logró ganar la confianza del mercado debido a su naturaleza centralizada, la volatilidad del Bitcoin llevó a los usuarios a migrar hacia las stablecoins, principalmente el USDT. La plataforma Binance se consolidó como el "banco digital" de facto para los venezolanos, facilitando remesas, ahorros y pagos comerciales mediante su sistema P2P, durante estos años, se observó una integración sin precedentes, desde grandes cadenas de supermercados hasta pequeños comercios informales comenzaron a aceptar pagos en criptoactivos de forma cotidiana.

El ecosistema sufrió un impacto estructural en marzo de 2023 con el escándalo "PDVSA-Cripto", una trama de corrupción que involucró el desvío de miles de millones de dólares a través de la SUNACRIP. Esto derivó en una intervención prolongada del organismo regulador, el apagado de granjas de minería legal y, finalmente, la liquidación oficial del Petro en enero de 2024. El epicentro de esta operación fue la SUNACRIP, funcionó como el nodo tecnológico para

procesar pagos en criptomonedas principalmente Bitcoin y USDT, fuera del control del Tesoro Nacional. Esta situación forzó la intervención inmediata del organismo mediante el Decreto N° 4.788 (Gaceta Oficial N° 6.739), marcando el inicio de un proceso de "reestructuración" que en la práctica significó la paralización casi total de la industria cripto legal en el país.

Tras la detención de su directiva principal, el Ejecutivo Nacional designó una Junta Reestructuradora liderada inicialmente por Anabel Pereira Fernández. El mandato original de seis meses se ha extendido mediante sucesivas prórrogas publicadas en Gaceta Oficial (como los Decretos N° 4.865, 4.926 y 5.003), manteniendo al organismo en un estado de excepción administrativa hasta mediados de 2026.Actualmente, aunque la SUNACRIP no fue suprimida legalmente, sigue existiendo como ente, su funcionamiento ha cambiado drásticamente, el panorama actual se caracteriza por los siguientes puntos:

1.Suspensión de minería digital, desde el inicio de la intervención, las granjas de minería legalmente registradas fueron desconectadas. A pesar de intentos de reactivación, el sector permanece bajo una estricta vigilancia y una pausa operativa indefinida debido a la emergencia eléctrica nacional y la desconfianza institucional.

2.Cierre del Petro en enero de 2024 se concretó el cese de operaciones del Petro, la criptomoneda estatal. La billetera PetroApp fue cerrada y los activos fueron convertidos a Bolívares o liquidados, eliminando el pilar sobre el cual se fundó la SUNACRIP en 2017.

3.Operatividad limitada de exchanges, actualmente solo un número muy reducido de casas de intercambio operan bajo la supervisión directa de la Junta Reestructuradora. Estas empresas deben cumplir con estándares de cumplimiento KYC extremadamente rígidos, reportando cada transacción para evitar que el sistema sea utilizado nuevamente para la legitimación de capitales.

Bajo el enfoque del cumplimiento o Compliance, la SUNACRIP ha dejado de ser un ente promotor de la adopción masiva para convertirse en un órgano de

fiscalización y control, su actividad principal hoy es la supervisión de proveedores de servicios de activos virtuales para asegurar que se ajusten a las recomendaciones del Grupo de Acción Financiera Internacional contra el financiamiento al terrorismo y la proliferación de armas, la SUNACRIP hoy es un organismo en fase de redefinición técnica. Si bien el caso PDVSA-Cripto destruyó la confianza en el modelo de gestión previo, la institución sobrevive bajo un régimen de intervención que prioriza la seguridad nacional y la trazabilidad financiera sobre la innovación tecnológica, para el investigador, el funcionamiento actual representa un modelo de vigilancia extrema donde cualquier actividad con criptoactivos en Venezuela está sujeta a una discrecionalidad regulatoria que busca, ante todo, prevenir una nueva fuga de capitales mediante el uso de la cadena de bloques.

Por todo lo anteriormente expuesto se puede decir que la actualidad la adopción en Venezuela de las criptos se define por la madurez y la utilidad práctica, aunque el impulso estatal ha desaparecido y la regulación es estricta, el uso de USDT domina el mercado para el pago a proveedores internacionales y el envío de remesas, manteniendo a Venezuela como un referente global de adopción real, donde las criptomonedas ya no son una novedad tecnológica, sino una herramienta esencial de la economía nacional frente a la inestabilidad del sistema financiero tradicional.

Dentro de las principales diferencias se evidencia al contrastar su naturaleza con la del dinero fiduciario o (Fiat), formas estructurales que inciden directamente en los mecanismos de prevención de riesgos financieros y supervisión estatal:

Emisión y Respaldo: El dinero fiduciario es emitido y respaldado por el Estado a través de su Banco Central, en el caso de Venezuela es el Banco Central de Venezuela BCV, basando su valor en la confianza institucional y el curso legal forzoso. Las criptomonedas, en contraste son emitidas mediante algoritmos, pre programados como la minería digital y no cuentan con el respaldo de

ningún estado legítimamente constituido, su valor está determinado exclusivamente por la dinámica de oferta y demanda en el mercado libre.

Control y Centralización: El sistema financiero tradicional es centralizado y jerárquico, en donde los bancos actúan como intermediarios obligatorios que validan las operaciones, las criptomonedas operan en redes descentralizadas y distribuidas, donde miles de nodos validan las transacciones mediante un consenso matemático, eliminando el punto único de falla o control.

Trazabilidad y Naturaleza de los Usuarios: En el sistema tradicional, el dinero fluye a través de cuentas bancarias asociadas a identidades verificadas mediante rigurosas políticas de Debida Diligencia del Cliente (KYC). En el ecosistema cripto, los usuarios operan mediante claves alfanuméricas o billeteras digitales, esto genera un entorno pseudónimo, donde las transacciones son públicamente trazables en la blockchain, pero la identidad real de las partes ejecutantes permanece oculta a menos que interactúen con plataformas de intercambio centralizadas.

Regulaciones: El dinero Fiat está sujeto a regulaciones cambiarias nacionales y los movimientos internacionales dependen de intermediarios como la red SWIFT, lo que facilita la aplicación de controles preventivo, las criptomonedas son intrínsecamente transfronterizas y operan 24/7, permitiendo el traslado inmediato de valor a nivel global al margen de las jurisdicciones locales.

A efectos de la comprensión de los términos asociados a la presente investigación, se considera de vital importancia conocer La Legitimación de Capitales, que se define como el proceso de ocultar o disimular el origen ilícito de bienes o recursos provenientes de actividades delictivas, para hacerlos aparentar como legítimos dentro del sistema económico legal. Desde una perspectiva dogmática, es un delito de naturaleza ofensiva que lesiona el orden socioeconómico y la transparencia financiera. Técnicamente, el proceso se divide en tres fases críticas que adquieren nuevas dimensiones con el uso de criptoactivos:

Colocación: Introducción de los fondos ilícitos en el ecosistema cripto y llevados al financiero tradicional.

Procesamiento: Realización de múltiples y complejas transacciones entre diversas billeteras y cadenas de bloques para romper la cadena de custodia y dificultar el rastreo de la auditoría.

Integración: Reintroducción de los fondos legitimados en la economía formal, mediante la venta de los activos por dinero fiduciario o la adquisición de bienes de lujo y activos financieros.

Dentro de la presente investigación es necesario integrar los delitos conexos a la legitimación de capitales y el estudio de los criptoactivos debe integrarse con la prevención de delitos que comprometen la seguridad global:

Financiamiento al Terrorismo (FT): Se refiere al suministro o recolección de fondos con la intención de que se utilicen para llevar a cabo actos terroristas, los criptoactivos facilitan el FT debido a la velocidad de las transferencias transfronterizas y la posibilidad de movilizar recursos sin pasar por el sistema bancario tradicional.

Financiamiento a la Proliferación de Armas de Destrucción Masiva (FPADM): Consiste en proveer fondos para la fabricación, adquisición o transporte de armas nucleares, químicas o biológicas, el uso de activos digitales permite a los Estados o grupos sancionados evadir embargos financieros internacionales y adquirir componentes de forma encubierta.

El Sistema Nacional de Prevención en Venezuela y el mundo es el conjunto de políticas, procedimientos y herramientas de monitoreo destinados a identificar y mitigar los riesgos asociados a los delitos financieros. Su aplicación práctica en el ecosistema digital exige que los "sujetos obligados" que implementen sistemas de monitoreo en tiempo real que detecten patrones de transacciones inusuales o sospechosas mediante herramientas de blockchain.

La política de "Conoce a tu Cliente" (Know Your Customer) es la piedra angular del cumplimiento. En entornos descentralizados, la importancia del KYC reside

en vincular la dirección alfanumérica de una billetera digital con una identidad humana real verificada. Sin un KYC robusto, la descentralización se convierte en un refugio para el anonimato delictivo, impidiendo la identificación de los beneficiarios finales de las operaciones.

Ahondando en el tema, Grau (2006), considera que la transparencia supone un estímulo para conseguir mejores niveles de eficiencia por parte de las empresas que pueden llegar a través de dos vías: la primera referida a los entes normativos o generadores de políticas, en los que la transparencia posibilita la competencia entre las ideas, los argumentos y las políticas y la segunda vía procede de las situaciones en las que la transparencia supone un incentivo para los organismos públicos ya que compiten con otros organismos similares a ellos cuando la información está a disposición de cualquier interesado.Ahora bien, la experiencia de que se dispone hasta este momento muestra que la transparencia no es un proceso inmediato, sino dilatado en el tiempo, que debe requerir de mucho esfuerzo por parte de los agentes implicados en este proceso, y que son necesarios recursos para conseguir las herramientas y formación que puedan posibilitar el cambio necesario dentro de la cultura administrativa pública. Por otra parte, Schedler (2004) señala es cierto que la transparencia nunca es absoluta, es huidiza y en muchas ocasiones las decisiones se producen dentro del ámbito de la opacidad pues influye directamente en las relaciones de poder y, por tanto, se crean en determinados momentos iniciativas para evitarla.

Conclusiones y Recomendaciones

En atención a los resultados obtenidos mediante el análisis documental de la presente investigación, se formulan las siguientes conclusiones.

La investigación documental de la coyuntura macroeconómica analizada, permiten concluir de forma categórica que la adopción de los criptoactivos en el territorio nacional no constituye un fenómeno aislado de especulación financiera, sino una respuesta estructural de los actores económicos ante la

profunda inestabilidad del sistema monetario tradicional, el proceso de hiperinflación prolongada y la devaluación sistemática de la moneda de curso legal el Bolívar, pulverizaron las funciones clásicas del dinero convencional como reserva de valor eficiente y unidad de cuenta predecible, ante la pérdida de confianza en las instituciones centralizadas y la contracción de la liquidez en divisas físicas, la ciudadanía y el sector comercial migraron de manera masiva hacia el ecosistema digital descentralizado como un mecanismo de supervivencia transaccional e infraestructura de protección patrimonial.

A este fenómeno interno se sumó el impacto de las restricciones de acceso al sistema bancario global y la exclusión de facto de los canales tradicionales de mensajería financiera internacional como la red SWIFT hasta el 2026, consolidando a los criptoactivos como un canal alternativo indispensable para la ejecución de transferencias transfronterizas y remesas. La separación de agentes intermediaros convencionales de la banca financiera inherente a la arquitectura Blockchain caracterizada por transacciones entre pares Peer-to-Peer operativas las 24 horas del día, los 7 días de la semana desplazó de forma fáctica los monopolios de la banca nacional comercial, dando origen a un circuito monetario paralelo altamente digitalizado que, si bien resolvió problemas críticos de exclusión y continuidad comercial, operó en gran medida al margen de los mecanismos de fiscalización tradicionales del Estado venezolano.

El análisis ejecutado demuestra que las características técnicas intrínsecas de los activos virtuales especialmente el pseudonimato originario y la disociación entre las claves alfanuméricas de las billeteras digitales y la identidad civil de los usuarios configuran un entorno de alta permeabilidad para las redes de delincuencia organizada, se concluye que el ciclo clásico de la Legitimación de Capitales ha experimentado una mutación operativa radical dentro del ciberespacio nacional. En la fase de colocación, las plataformas P2P e intercambios informales en efectivo actúan como el primer nodo de lavado, permitiendo que fondos de origen criminal ingresen al flujo Blockchain

eludiendo las alertas de los bancos regulados, en la fase de procesamiento o estratificación, técnicas complejas como el chain-hopping que es el intercambio veloz entre diferentes cadenas de bloques y la atomización de transferencias hacia billeteras privadas impiden un rastreo lineal de la auditoría tradicional.

Asimismo, se identificó que el uso de tecnologías de anonimato avanzado, tales como los denominados "Mezcladores" o Tumblers de monedas virtuales, junto con la proliferación de criptoactivos de privacidad que ocultan montos y direcciones por defecto, anulan de manera técnica la trazabilidad que en teoría ofrece la contabilidad clásica, estas tipologías delictivas especializadas, detectadas en los Reportes de Operaciones Sospechosas de la Unidad Nacional de Inteligencia Financiera (UNIF), facilitan que capitales de procedencia ilícita se mezclen de forma imperceptible con el flujo mercantil legítimo, el riesgo es particularmente crítico en los delitos conexos de Financiamiento al Terrorismo y Financiamiento a la Proliferación de Armas de Destrucción Masiva, donde la velocidad transfronteriza instantánea de las redes descentralizadas y de las Finanzas Descentralizadas (DeFi) permite el desplazamiento internacional de recursos de forma encubierta, vulnerando la seguridad del Estado y los sistemas de alerta temprana.

Cabe destacar la Investigación de Arias 2026; en la cual señaló:

“Al contrastar el andamiaje legal venezolano con los estándares globales dictados por el Grupo de Acción Financiera Internacional GAFI, particularmente las recomendaciones 1, 15 y 16 se concluye que existe una brecha significativa entre la norma escrita y la capacidad fáctica de supervisión del Estado, si bien la Constitución de la República Bolivariana de Venezuela provee un marco jerárquico sólido al reservar la regulación del sistema financiero al Poder Público Nacional (Art. 156) bajo principios de seguridad jurídica (Art. 299) y corresponsabilidad (Art. 326), la dinámica del mercado cripto desborda los mecanismos operativos vigentes. La Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo dota de

competencias a la UNIF, la ONCDOFT y a la Superintendencia Nacional de Criptoactivos y Actividades Conexas SUNACRIP), sin embargo, la eficacia real se encuentra severamente limitada debido a la falta de herramientas tecnológicas de análisis de cadena de bloques de última generación.

“La extensa intervención de la SUNACRIP como consecuencia del caso "PDVSA-Cripto" y el estado de excepción administrativa en el que se mantiene la institución, cuyo letargo dejo en evidencia que la estructura reguladora previa centralizó riesgos y careció de auditorías internas rigurosas, la paralización de la minería digital legal y la extinción definitiva del Petro eliminaron el modelo de adopción masiva tutelada, pero no detuvieron el flujo informal de criptoactivos como el USDT a través de plataformas internacionales, por consiguiente, Venezuela presenta un cumplimiento deficiente respecto a la Recomendación 15 del GAFI (supervisión efectiva de proveedores de activos virtuales) y un rezago técnico absoluto en la implementación de la Recomendación 16, Travel Rule o Regla de Viaje, la cual obliga a identificar de forma segura al originador y beneficiario de cada transferencia digital, dejando un vacío de inteligencia financiera que debilita el sistema preventivo nacional”.

Tomando en consideración las conclusiones expuestas en el párrafo precedente, y al objeto de proponer procedimientos y mecanismos de control, apropiados que favorezcan el intercambio comercial, procurando favorecer la innovación tecnológica con la seguridad jurídica y penal de la nación, se formulan las siguientes recomendaciones:

1. Diseñar e implementar un Plan Nacional de Actualización del Enfoque Basado en Riesgo dirigido a los Criptoactivos, para ser consecuentes con la Recomendación 1 del GAFI.

Se recomienda al Ejecutivo Nacional, en coordinación directa con la Unidad Nacional de Inteligencia Financiera UNIF, la ONCDOFT y la Junta Reestructuradora de la SUNACRIP, realizar un diagnóstico del sector em profundidad, a objeto de lograr la actualización del mapa nacional de riesgo

frente a las nuevas y complejas modalidades del delito transaccional, el mismo debe estar orientado principalmente en la evaluación y el uso de manera amplia y masiva de las monedas estables (stablecoins) como el USDT en el sector comercial y las dinámicas de las plataformas P2P (peer to peer), a nivel global, las cuales operan sin estar adscritas a órganos de control en los diversos países, es decir fuera del control directo de las licencias nacionales. El resultado de esta evaluación debe producir un conjunto de normas y procedimientos emitidas, con orientaciones especificas en materia de compliance y catálogos de señales de alerta actualizados para que los sujetos obligados tradicionales (banca, seguros, valores) y los nuevos proveedores de servicios digitales puedan identificar señales de alerta, producto de transacciones inusuales que carezcan de justificación económica aparente.

2. Establecer, desarrollar y ejecutar un Programa Nacional de Adecuación Tecnológica y Formación Forense en Cadenas de Bloque (Blockchain) para los órganos de investigación penal e inteligencia financiera.

Es muy importante que de manera conjunta el Ministerio del Poder Popular de Economía y Finanzas, y el Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz, dote a la UNIF, al Cuerpo de Investigaciones Científicas, Penales y Criminalísticas CICPC y al Ministerio Público de tecnología de punta para la utilización de herramientas avanzadas de análisis forense en el área de informática, para accesar y llevar a cabo la experticia forense exitosa en las cadenas de bloques software de código abierto equivalente, el control preventivo y la persecución de los delitos de legitimación de capitales y financiamiento al terrorismo no pueden realizarse con metodologías contables tradicionales de auditoría en papel. Asimismo, se recomienda establecer alianzas académicas estratégicas con instituciones de educación superior especializadas, como la Escuela Nacional de Administración y Hacienda Pública (ENAHP), así como establecer cátedras de manera permanente a nivel de estudios de cuarto nivel para dictar programas permanentes y adiestramiento técnico y especializado en cumplimiento de las

Normas y Providencias en materia de LC/FT/FPADM así como en Compliance Criptográfico, tipologías de ocultamiento digital, mezcladores y cibercriminalidad para investigadores, fiscales, jueces y oficiales de cumplimiento.

3. Reformar parcialmente la LOCDOFT e implementar la "Travel Rule" (Regla de Viaje) para Proveedores de Servicios de Activos Virtuales en Venezuela.

Es necesaria una reforma a la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo LOCDOFT, a fin de incorporar de manera clara y precisa a los Proveedores de Servicios de Activos Virtuales, incluyendo exchange, pasarelas de pago y custodios de billeteras digitales, para dotarlos de la cualidad jurídica de "Sujetos Obligados" tal como se señala en el art. 9 de dicha ley, así como la emisión de la Junta Reestructuradora de la SUNACRI, de la correspondiente providencia administrativa de obligatorio cumplimiento que ordene la implementación tecnológica de la Recomendación 16 del GAFI (Travel Rule). Esta medida obligará a todas las plataformas autorizadas a operar en el país a recolectar, retener y transmitir de forma segura los datos de identidad verificados tanto del emisor como del beneficiario final en cada transferencia de activos virtuales que supere el umbral legal, eliminando los espacios de anonimato y garantizando la trazabilidad jurídica de las operaciones en resguardo de la soberanía económica de la República Bolivariana de Venezuela.

Referencias

ARIAS, F. G. (2016). El Proyecto de Investigación: Introducción a la metodología científica (7ma ed.). Caracas: Editorial Episteme.

ARIAS, J. (2020). La imputación objetiva en el delito de lavado de activos a través de criptomonedas (Tesis de Postgrado). Universidad Pontificia Bolivariana, Medellín.

ARIAS CH, J. (2026) Análisis de los efectos de la adopción de las criptomonedas como instrumento de pago y su uso para la legitimación de

capitales, financiamiento al terrorismo y financiamiento a la proliferación de armas de destrucción masiva en Venezuela.

ALMAEYDA, M. (2020). Criptomonedas vs. Criptoactivos, un problema de identidad con repercusiones jurídicas (Tesis de Maestría). Universidad Externado de Colombia, Bogotá.

BALESTRINI ACUÑA, M. (2001). Cómo se elabora el proyecto de investigación. Caracas: BL Consultores Asociados

CASTELLS, MANUEL: “Prólogo: la red y el yo”, en “La era de la información: economía, sociedad y cultura” - Siglo XXI Editores - México D.F. – 2001

CONSTITUCIÓN DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA (1999). Gaceta Oficial N° 5.453, Marzo 03, 2000.

NAKAMOTO, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System (Documento Técnico / Whitepaper). Cryptography Mailing List.

PODER LEGISLATIVO NACIONAL. (Vigente). Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT). Gaceta Oficial de la República Bolivariana de Venezuela. Caracas, Venezuela

GRUPO DE ACCION FINANCIERA INTERNACIONAL (GAFI). (2019). Las 40 Recomendaciones sobre la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo y la Proliferación. París: GAFI/OECD.

NAKAMOTO, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System (Documento Técnico / Whitepaper). Cryptography Mailing List.

PODER LEGISLATIVO NACIONAL. (Vigente). Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT). Gaceta Oficial de la República Bolivariana de Venezuela. Caracas, Venezuela

SCHEDLER, A.,2004. ¿Qué es la Rendición de Cuentas?, México, Instituto Federal de Acceso a la Información. Cuadernos de transparencia,

SAIN, GUSTAVO: “Delito y nuevas tecnologías: Fraude, narcotráfico y lavado de dinero por internet” - Editores del Puerto - Bs. As. – 2012

STIGLITZ, J., 1999. Economía y gobierno: Los usos privados de los intereses. Planeación & desarrollo, 30(1-2).