

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 Señales De Alerta

**Compendio Académico de Señales de Alerta: Enfoque Práctico para la
Prevención de Riesgos LC/FT/FPADM**

Facilitadora: Lic. Elizabeth Pelaez
Asesor metodológico: Dr. Mario Morales

Caracas, julio 2026

PRÓLOGO

Es un verdadero placer y honor presentar el prólogo relacionado con la Unidad Curricular de Señales de Alerta, fundamentado en las investigaciones académicas contenidos en los ensayos desarrollados por los aspirantes a especialistas en Gestión contra la Legitimación de Capitales y Financiamiento al Terrorismo, dentro del convenio de formación suscrito entre la Oficina Nacional contra la Delincuencia Organizada y Financiamiento del Terrorismo (ONCDOFT) y la Escuela Nacional de Administración y Hacienda Pública (ENAHp).

Estas instituciones están altamente comprometidas con la constante formación especializada de profesionales capacitados para enfrentar y entender cómo opera la cambiante "Delincuencia Organizada" a nivel nacional e internacional. Este portafolio es el resultado que demuestra el alto nivel de actualización, compromiso de los estudiantes para investigar cómo las señales de alerta se identifican, y evolucionan a operaciones inusuales o sospechosas y, mediante el debido proceso de documentación, se transforman en denuncias administrativas.

Asimismo, destaca la relevancia estratégica de la Unidad Nacional de Inteligencia Financiera (UNIF), la cual transforma los Reportes de Actividades Sospechosas (RAS) en insumos clave para activar procedimientos de investigación penal destinados a sancionar los delitos de LC/FT/FPADM.

En tal sentido, se debe considerar que la efectividad de los Sistemas Integrados de Administración de Riesgos (SIAR) contra estos delitos no descansa en formalismos documentales, sino en la capacidad técnica para detectar, interpretar y adaptarse rápidamente a la inusualidad en tiempo real.

En el dinámico contexto normativo venezolano, marcado por las exigencias del Grupo de Acción Financiera Internacional (GAFI), las evaluaciones sectoriales de la ONCDOFT, las providencias administrativas de los diferentes sectores (Banca, Seguros, Valores, Criptoactivos) y las regulaciones dirigidas a las Actividades y Profesiones No Financieras Designadas (APNFD), las señales de alerta se consolidan como la piedra angular de la inteligencia financiera defensiva.

Este conocimiento busca anticipar, interpretar e implementar controles que disminuyan el impacto negativo de la criminalidad organizada en la estabilidad financiera de los sujetos obligados y en la economía del país.

Este compendio reúne las contribuciones dogmáticas, técnico-operativas y criminológicas analizadas por los estudiantes para generar una detección temprana. Frente a la «ceguera voluntaria» o ignorancia deliberada, la doctrina

expuesta ratifica que omitir las banderas rojas quiebra la posición de garante y deriva en responsabilidades administrativas y penales sustantivas bajo la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT). Datos empíricos consolidados por la UNIF confirman la urgencia de esta obra: la abrumadora mayoría de los RAS a nivel nacional se concentran en inconsistencias del perfil financiero y transacciones sin justificación económica clara.

En resumen, desde la actuación del intermediario de seguros en la preventa hasta la supervisión de los responsables de cumplimiento en áreas sensibles y las tipologías asociadas a activos virtuales, los ensayos reunidos trazan una hoja de ruta rigurosa para trascender el compliance superficial.

Finalmente, esta obra se posiciona como una herramienta indispensable para estudiantes, docentes, oficiales de cumplimiento y juristas orientados a fortalecer el orden público económico y la soberanía financiera del Estado venezolano.

Lic. Elizabeth Peláez

INDICE

Prólogo	1
Línea de Investigación	
Marco Constitucional, Gobierno Corporativo Y Fundamentos Dogmáticos Para Algunos Sujetos Obligados, Sectores Y Actividades Económicas	
Responsabilidad Penal y Administrativa de las APNFD ante la Omisión de Señales de Alerta en la LOCDOFT Autora: Dra. Nelly Sánchez Pantaleón	6
Rol del Intermediario de Seguros en la detección de señales de alerta de LC/FT vinculadas al cliente. Autor: Abg. Juan C. Cabello M.	19
Rol Estratégico de los Profesionales Jurídicos y Financieros en libre ejercicio profesional: Señales de alerta, controles internos y directrices para la prevención de LC/FT/FPADM Autor: Dra. Silumerany Rodríguez.	38
Línea de Investigación	
Gestión Operativa del Riesgo, SIAR y Líneas de Defensa	
La Administración de Riesgos de Legitimación de Capitales, Financiamiento Al Terrorismo y Financiamiento a La Proliferación de Armas de Destrucción Masiva En Venezuela y La Importancia de La Identificación de Señales de Alerta, para La Consolidación de La Inteligencia Financiera Nacional. Autor: Abg. Esp. Jesús Mora.	63
Áreas sensibles y gestión de riesgos: rol de los responsables de cumplimiento en la detección de señales de alerta en el sector asegurador y valores. Autora: Abg. Yabandra N. Lorca Cabeza.	79
De la detección temprana a la mitigación del Riesgo 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.	93
Línea de Investigación	
Tipologías Criminológicas, Activos Virtuales y Análisis de Reportes de Actividad Sospechosa (RAS).	
Arquitectura sistémica de las señales de alerta para la prevención de LC/FT: un enfoque basado en riesgo e inteligencia financiera para las instituciones bancarias. Autor: Dr. Oscar Perdomo.	108
De la intuición al algoritmo: El papel del aprendizaje automático en la detección de señales de alerta para la gestión de riesgos de delincuencia organizada. Autora: Dra. Kimlen Chang de Negrón.	138

Luces, cámara y acción: El marketing de impacto como señal de alerta primaria en la legitimación de capitales dentro del ecosistema Fintech.	157
Autora: Abg. Mercedes Mendoza Rubio	
El radar bursátil: Señales de alerta, actores ocultos e inteligencia financiera como escudo del mercado de valores venezolano.	172
Autora: Lic. Gianni Verasmendi.	
Tipologías de legitimación de capitales más recurrentes en el contexto venezolano.	188
Autor: Abg. Esp. Víctor Ordaz.	
¿Son las Señales de Alerta de Legitimación de Capitales Financiamiento al Terrorismo y Financiamiento a la Proliferación de Armas de Destrucción Masiva, un elemento estratégico para el Enfoque Basado en Riesgo?	205
Autora: Lic. Lexssy Y. López H.	
La evolución del azar: señales de alerta para mitigar riesgos de LC/FT en las rifas digitales en Venezuela.	224
Autor: Abg. Esp. Yeixon Santaella Bernal.	
Abordaje de La Señal de Alerta Como Instrumento Que Señala Comportamientos Atípicos Cuya Interpretación Muestra El Grado De Desviación Con Relación Al Cumplimiento De La Norma En Materia De Legitimación De Capitales, Financiamiento Al Terrorismo, El Financiamiento De La Proliferación De Armas De Destrucción Masiva Y Otros Ilícitos.	241
Autor: Dr. Juan Arévalo.	

REPÚBLICA BOLIVARIANA DE VENEZUELA MINISTERIO DEL
PODER POPULAR DE ECONOMÍA Y FINANZAS
ESCUELA NACIONAL DE ADMINISTRACIÓN Y HACIENDA PÚBLICA DIRECCIÓN
DE POSTGRADO Y ADIESTRAMIENTO
ESPECIALIZACIÓN EN GESTIÓN CONTRA LEGITIMACIÓN DE CAPITAL Y
FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR: SEÑALES DE ALERTA LC/FT

**RESPONSABILIDAD PENAL Y ADMINISTRATIVA DE LAS APNFD ANTE LA
OMISIÓN DE SEÑALES DE ALERTA EN LA LOCDFT**

Autora: Dra. Nelly Sánchez Pantaleón
Facilitadora: Lic. Elizabeth Pelaez
Asesor metodológico: Dr. Mario Morales

REPÚBLICA BOLIVARIANA DE VENEZUELA MINISTERIO DEL
PODER POPULAR DE ECONOMÍA Y FINANZAS
ESCUELA NACIONAL DE ADMINISTRACIÓN Y HACIENDA PÚBLICA DIRECCIÓN
DE POSTGRADO Y ADIESTRAMIENTO
ESPECIALIZACIÓN EN GESTIÓN CONTRA LEGITIMACIÓN DE CAPITALS Y
FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR: NUEVAS TECNOLOGÍAS

**RESPONSABILIDAD PENAL Y ADMINISTRATIVA DE LAS APNFD ANTE LA
OMISIÓN DE SEÑALES DE ALERTA EN LA LOCDOFT**

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

RESUMEN

El presente ensayo aborda la responsabilidad penal y administrativa de las Actividades y Profesiones No Financieras Designadas (APNFD) ante la inobservancia de los indicadores de riesgo de LC/FT/FPADM. Tiene como objetivo analizar las consecuencias jurídicas de la omisión de reportar operaciones sospechosas bajo la LOCDOFT y la Circular UNIF-DG-DSU-04409-2023. La investigación se fundamenta ontológicamente en la posición de garante del profesional en libre ejercicio, el Enfoque Basado en Riesgo (EBR) y el deber objetivo de cuidado. Metodológicamente, se desglosan las señales de alerta (generales, operacionales y tecnológicas), el rol sistémico de las líneas de defensa y la ingeniería técnica del Formulario PE-UNIF-005 como blindaje de debida diligencia. El núcleo del debate axiológico se sitúa en la colisión ética entre el valor de la confidencialidad tradicional representado por el secreto profesional y el imperativo deontológico de la transparencia, exigido por el bienestar colectivo y la justicia material. Las reflexiones finales evidencian que la "ceguera voluntaria" ante el riesgo trasciende la mera negligencia técnica para configurarse como una transgresión moral y una abdicación del ethos profesional; una conducta omisiva que desvanece la frontera entre la legítima asesoría técnica y la complicidad penal por asunción del dolo. Se concluye que el contexto normativo venezolano impone una redefinición axiológica del secreto profesional, subordinándolo al principio de corresponsabilidad social y a la preservación del orden público constitucional.

Descriptor: APNFD; Señales de alerta; LOCDOFT; UNIF; Responsabilidad penal.

ABSTRACT

This essay addresses the criminal and administrative liability of Designated Non-Financial Businesses and Professions (DNFBPs) for failing to comply with

AML/CFT/AFP risk indicators. Its objective is to analyze the legal consequences of failing to report suspicious transactions under the Organic Law Against the Financing of Terrorism (LOCDOFT) and Circular UNIF-DG-DSU-04409-2023. The research is ontologically grounded in the guarantor position of the self-employed professional, the Risk-Based Approach (RBA), and the objective duty of care. Methodologically, it breaks down the warning signs (general, operational, and technological), the systemic role of the lines of defense, and the technical engineering of Form PE-UNIF-005 as a due diligence safeguard. The core of the axiological debate lies in the ethical clash between the value of traditional confidentiality, represented by professional secrecy, and the deontological imperative of transparency, demanded by collective well-being and substantive justice. The final reflections demonstrate that "willful blindness" to risk transcends mere technical negligence, constituting a moral transgression and an abdication of professional ethics; an omission that blurs the line between legitimate technical advice and criminal complicity through the assumption of intent. It is concluded that the Venezuelan legal framework necessitates an axiological redefinition of professional secrecy, subordinating it to the principle of social co-responsibility and the preservation of constitutional public order.

Descriptors: NFPs; Warning signs; LOCDOFT; UNIF; Form PE-UNIF-005; Criminal liability.

Introducción

El sistema global de prevención contra la Legitimación de Capitales, el Financiamiento al Terrorismo y el Financiamiento a la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM) ha experimentado una evolución doctrinal que redefine el alcance del libre ejercicio profesional.

Tradicionalmente, los abogados, contadores, administradores y economistas operaban bajo un paradigma de asesoría técnica blindada por un esquema de confidencialidad absoluta de cara a sus clientes.

No obstante, las complejas dinámicas de la delincuencia organizada para instrumentalizar estructuras societarias, fideicomisos y transacciones comerciales forzaron un cambio sustancial en la política criminal del Estado venezolano, materializado en la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT).

A la luz de este marco normativo, específicamente en lo consagrado en el numeral 9 del artículo 9 de la LOCDOFT, estos profesionales han dejado de ser simples asesores para erigirse formalmente como "Sujetos Obligados" cuando

llevan a cabo operaciones clave como la compraventa de inmuebles, la administración de activos o la creación y gestión de personas jurídicas.

Esta transposición legal alineada con las Recomendaciones 22 y 23 del Grupo de Acción Financiera Internacional (GAFI) y la Circular UNIF-DG-DSU-04409-2023 los cataloga como Actividades y Profesiones No Financieras Designadas (APNFD), convirtiéndolos en corresponsales jurídicos y aliados estratégicos en la detección temprana de capitales ilícitos.

Este nuevo estatus legal traslada la carga del riesgo y establece el núcleo del problema que ocupa a la presente investigación: la imperatividad del deber objetivo de cuidado. Conforme al artículo 12 y 13 de la LOCDFT, los sujetos obligados deben implementar mecanismos para detectar cualquier transacción inusual o sospechosa, independientemente de su cuantía o naturaleza.

Bajo este enfoque, la desatención de una señal de alerta ya no puede ser tipificada como una falta administrativa menor. Por el contrario, la inobservancia deliberada sitúa al profesional en una zona de alta peligrosidad punitiva; el incumplimiento de la obligación expedita de reportar no solo acarrea severas multas pecuniarias de hasta unas mil unidades tributarias (1.000 U.T.), sino que la omisión puede ser interpretada penalmente por los órganos jurisdiccionales como una facilitación, cooperación necesaria o complicidad en el delito de legitimación de capitales.

Asimismo, la arquitectura preventiva de la ley impone una dualidad de obligaciones rigurosas: por un lado, el deber de informar de manera inmediata a la Unidad Nacional de Inteligencia Financiera (UNIF) órgano desconcentrado cuyas atribuciones de centralización y análisis analítico se delimitan en los artículos 24 y 25 de la ley y, por el otro, la estricta obligación de confidencialidad dispuesta en el artículo 14, la cual prohíbe taxativamente revelar al cliente o a terceros que se está examinando o reportando una operación, bajo pena de sanciones que duplican su gravedad en caso de reincidencia.

Frente a este escenario de alta responsabilidad corporativa, el presente ensayo se propone analizar críticamente el bloque de sanciones administrativas y penales aplicables a las APNFD, evaluando cómo el conocimiento dogmático de las señales de alerta y el uso riguroso del Formulario PE-UNIF-005 no constituyen cargas burocráticas opcionales, sino el único blindaje técnico y legal válido para salvaguardar la libertad y la integridad en el ejercicio profesional.

Las Señales de Alerta como Presunción de Licitud o Illicitud

El abordaje del Enfoque Basado en Riesgo (EBR) exige que los sujetos obligados segmenten e identifiquen con precisión los factores de riesgo a través de señales de alerta analizadas de manera científica y estructurada.

Estas señales, lejos de ser meras sospechas abstractas, constituyen indicadores objetivos que guían la debida diligencia de los profesionales en libre ejercicio.



Fuente: Sànchez (2026)

- a) **Indicadores Cuantitativos:** Se centran en variables numéricas y transaccionales que se apartan del comportamiento financiero histórico o habitual del cliente. Incluyen operaciones complejas, estructuradas o en tránsito que carecen de una justificación económica visible, así como transacciones fraccionadas deliberadamente para eludir los umbrales de reporte obligatorios ante la Unidad Nacional de Inteligencia Financiera (UNIF).
- b) **Indicadores Cualitativos:** Se desprenden del perfil de la persona, su comportamiento y las características intrínsecas del negocio. Involucran situaciones donde la identidad del cliente o del beneficiario final no puede ser plenamente determinada, el uso de interpuestas personas, o la vinculación comercial con Personas Expuestas Políticamente (PEP) sin la debida autorización de la alta gerencia.

Asimismo, abarca operaciones con jurisdicciones que aplican regulaciones insuficientes contra la Legitimación de Capitales (LC) o que facilitan el secreto bancario y comercial.

c) Indicadores Derivados de Nuevas Tecnologías (Fintech y Criptoactivos):

Con el auge de las finanzas digitales, los profesionales de las Actividades y Profesiones No Financieras Designadas (APNFD) se enfrentan a riesgos emergentes caracterizados por el anonimato y la velocidad transaccional.

El uso de plataformas Fintech no reguladas, la conversión opaca de fondos tradicionales a criptoactivos mediante billeteras sin representan tipologías sofisticadas que el profesional a menudo ignora de manera negligente o intencional

En conclusión, la tipificación y el análisis sistemático de los indicadores cuantitativos, cualitativos y tecnológicos no constituyen un mero catálogo de sospechas formalistas, sino que configuran la matriz epistemológica fundamental sobre la cual se erige el Enfoque Basado en Riesgo (EBR) en el seno de las APNFD.

Desde una perspectiva analítica y axiológica, estas señales de alerta representan el estándar operativo que transforma el deber objetivo de cuidado en una praxis medible y auditable ante la Unidad Nacional de Inteligencia Financiera (UNIF).

La interacción simbiótica de estas tres dimensiones revela que la mitigación eficaz de la LC/FT/FPADM en el contexto contemporáneo venezolano exige superar el viejo paradigma del control puramente transaccional (cuantitativo), para adentrarse con agudeza en el examen del comportamiento institucional y la transparencia corporativa (cualitativo), blindando el ejercicio profesional ante las sofisticadas tipologías de opacidad que introduce la velocidad del ecosistema digital (tecnológico).

Axiológicamente, la desatención de estos indicadores trasciende la negligencia técnica para convertirse en una quiebra ética del *ethos* profesional. Quien ignora de manera intencional o displicente estas alarmas estructurales incurre en una "ceguera voluntaria" que corroe el valor de la fe pública y vulnera el principio de corresponsabilidad social.

Por lo tanto, las señales de alerta no deben ser interpretadas como una carga punitiva del Estado, sino como las herramientas de discernimiento

prudencial indispensables para salvaguardar la reserva moral de las profesiones liberales, garantizando que la técnica contable, administrativa y jurídica permanezca inequívocamente al servicio del derecho, la justicia material y el bien común.

La ceguera voluntaria omisión deliberada ante el origen de los fondos

La doctrina penal moderna describe la ceguera voluntaria o ignorancia deliberada como la postura de aquel sujeto que, estando en condiciones de sospechar que se encuentra ante una operación de carácter ilícito, prefiere "no saber" o no indagar en los detalles de la transacción para mantener el beneficio económico derivado del cliente, cerrando los ojos ante la evidencia obvia.

Para Vera y Pardo (2025)

La ignorancia deliberada supone ampliar el espectro de la tipicidad subjetiva, con el propósito de analizar comportamientos que, sin encajar en la clásica división del dolo y la culpa, pueden ser igualmente merecedores de reproche penal. En especial, en aquellos ámbitos que suponen, de forma constante, un control y supervisión de actividades generadoras de riesgo.p.226

Esta cita describe la normativización de la tipicidad subjetiva en el derecho penal económico, justificando que la ignorancia deliberada reciba un reproche penal equiparable al dolo debido a que el sujeto obligado como un abogado o contador bajo el control de la LOCDOFT toma la decisión consciente de suspender sus deberes de indagación y monitoreo ante señales de riesgo evidentes para asegurar un beneficio.

Al operar en sectores regulados que exigen por ley la gestión constante de actividades generadoras de riesgo a través de sistemas como el SIAR, la ignorancia deja de ser un simple descuido o culpa para convertirse en una estrategia de evasión deliberada.

Por lo tanto, en estos ámbitos de supervisión, el derecho penal expande sus herramientas conceptuales tradicionales para castigar penalmente a quien, sabiendo que tiene la obligación legal y los medios para conocer el origen ilícito de los fondos, prefiere "no saber", transformando su ceguera voluntaria en un comportamiento altamente reprochable.

En el marco legal venezolano, esta conducta desvirtúa la presunción de buena fe y halla una estricta delimitación en el marco sancionatorio de la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT)

Artículo 36 (LOCDOFT): Los directivos o directivas, empleados o empleadas de los sujetos obligados, que, por imprudencia, impericia, negligencia, favorezcan o contribuyan a la comisión del delito de legitimación de capitales y financiamiento al terrorismo, sin haber tomado parte en él, serán penados o penadas con prisión de tres a seis años.

Cuando un abogado, contador, administrador o economista en libre ejercicio detecta una operación inusual o sospechosa como la compraventa de bienes inmuebles o la administración de cuentas sin una lógica de mercado clara y decide omitir los mecanismos de debida diligencia previstos en la Circular N° UNIF-DG-DSU-04409, su conducta no puede ampararse en el desconocimiento

La omisión de los deberes institucionales esenciales, tales como la plena identificación de terceros intervinientes y la remisión expedita del Reporte de Actividades Sospechosas (RAS) ante la UNIF, transforma la aparente "imprudencia o negligencia" en una responsabilidad penal explícita bajo el amparo de las normas de cuidado que rigen a los sujetos obligados.

El RAS es un mecanismo protector: la propia ley estipula que su envío no constituye una denuncia penal ni acarrea responsabilidad civil, administrativa o penal para quien lo suscribe.

Por ende, preferir la ceguera frente al riesgo desplaza al profesional de la prevención a la zona de favorecimiento del delito.

A continuación, se sistematizan las obligaciones fundamentales y el marco operativo que los profesionales en libre ejercicio deben aplicar de acuerdo con la legislación y los lineamientos de la UNIF

Cuadro 1 Matriz de cumplimiento técnico para APNF Profesionales

Dimensión Operativa	Base Legal	Técnica del Deber
Sujetos Obligados	Art. 9, Numeral 9 (LOCDOFT)	Abogados, administradores, economistas y contadores públicos cuando efectúen transacciones relativas a compraventa de inmuebles, gestión de activos, cuentas bancarias u organización de empresas
Monitoreo y Detección	Art. 12 y 13 (LOCDOFT)	Obligación de establecer mecanismos internos para detectar transacciones inusuales o estructuradas, independientemente de su cuantía o aparente licitud.
Reporte (RAS)	Art. 13 (LOCDOFT)	Remisión expedita a la UNIF ante sospechas de LC/FT/FPADM. Exento de formalidades del COPP; no genera responsabilidad administrativa, civil ni penal para el suscriptor
Confidencialidad	Art. 14 (LOCDOFT)	prohibición absoluta (Tipping-off) de revelar al cliente, usuario o terceros que se ha emitido un RAS o que se examina una operación. Sanción: Multa de 1.000 a 3.000 U.T.
Conservación de Registros	Art. 10 (LOCDOFT)	Custodia obligatoria de registros físicos y digitales por un período mínimo de cinco (5) años contados desde la finalización de la relación o ejecución de la operación
Estructura del SIAR	Circular UNIF-04409	Adopción de una cultura de cumplimiento

Fuente: Sanchez (2026)

El Deber de Cuidado del Sujeto Obligado

En el ordenamiento jurídico penal, la posición de garante es la situación en la que se encuentra un sujeto que tiene el deber jurídico de impedir que se produzca un resultado delictivo, de modo que la no evitación de este equivale a su propia causación.

Bajo el esquema de la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT), este concepto se traslada de forma explícita a las Actividades y Profesiones No Financieras Designadas (APNFD) mediante la imposición de las denominadas normas de cuidado.

El Profesional en Libre Ejercicio, como los abogados, contadores, administradores y economistas no operan en un vacío regulatorio; la ley los define formalmente como sujetos obligados cuando sus servicios se vinculan a operaciones críticas como la compraventa de inmuebles, la creación de empresas o la administración de activos de clientes.

Su posición de garante no nace de un acuerdo privado con el cliente, sino de un mandato de orden público. Tienen el deber de controlar las fuentes de peligro dentro de su ámbito de actuación profesional para evitar que su labor sea instrumentalizada por organizaciones criminales.

En tal sentido, en la primera línea de contacto, el personal que interactúa directamente con el cliente (recepción, analistas, asistentes) actúa como el filtro operativo primario del riesgo. Es la encargada de aplicar los protocolos iniciales de la debida diligencia, tales como verificar plenamente la identidad del cliente y del beneficiario final.

Por tanto, la mitigación del riesgo no puede depender de esfuerzos individuales aislados; requiere la institucionalización de un Sistema Integral de Administración de Riesgos (SIAR)

El Bloque Punitivo

La vía administrativa: Multas, inhabilitaciones profesionales y revocación de licencias comerciales por deficiencias en el control interno

El ordenamiento jurídico venezolano dota a los órganos y entes de control de potestades expresas para regular, supervisar y sancionar administrativamente a los sujetos obligados que muestren deficiencias en sus estructuras de prevención.

En cuanto a las multas la LOCDOFT establece un estricto régimen de sanciones corporativas y personales tasadas en Unidades Tributarias (U.T.) ante el quebrantamiento de los deberes de cuidado.

En relación a las inhabilitaciones profesionales, en consonancia con los mandatos constitucionales de control del ejercicio profesional y las directrices de la LOCDOFT, los entes de tutela económica en coordinación con los colegios profesionales debidamente facultados pueden suspender temporal o definitivamente la licencia de ejercicio de aquellos abogados, contadores, administradores o economistas que demuestren una inobservancia sistemática del ordenamiento preventivo.

Sobre el particular, la revocación de las licencias comerciales, de acuerdo con el artículo 8 de la LOCDOFT, los órganos de control están plenamente autorizados para otorgar, denegar, suspender o cancelar las licencias, habilitaciones y permisos de operación económica de los sujetos obligados que

vulneren los estándares mínimos del SIAR, privándolos de su capacidad para operar legalmente en el mercado formal.

En este orden de ideas, la LOCDOFT y el diseño institucional de la Unidad Nacional de Inteligencia Financiera (UNIF) articulan un bloque de persecución frente a estas conductas:

Por un lado, el Rol de la UNIF concebida como el órgano desconcentrado encargado de recibir, centralizar y analizar los reportes emitidos por los sujetos obligados, depende de la celeridad y fidelidad del flujo informativo para estructurar las alertas tempranas del Estado.

Mientras que la configuración de la complicidad por omisión, prevista en el artículo 13 de la LOCDOFT estipula de forma taxativa que el RAS no constituye una denuncia penal, sino un mecanismo preventivo. Al ocultar voluntariamente una transacción sospechosa compleja o inusual, el profesional rompe la barrera de contención.

En este marco normativo el artículo 27 de la LOCDOFT establece que se consideran delitos de delincuencia organizada no solo los cometidos por grupos estructurados, sino también aquellos ejecutados por una sola persona actuando de conformidad con las definiciones de la ley.

Ello se concatena de forma directa con el artículo 36, el cual castiga con penas de prisión de tres (3) a seis (6) años a quienes por imprudencia, negligencia o impericia favorezcan o contribuyan a la legitimación de capitales. La omisión deliberada de reportar anula la condición de tercero neutral: el asesor pasa a ser un cooperador imprescindible o cómplice, dado que su silencio proporciona el blindaje operativo que la organización criminal requiere para dotar de aparente licitud a sus fondos.

El poder de fiscalización de la UNIF

El poder fiscalizador de la Unidad Nacional de Inteligencia Financiera (UNIF) sobre los profesionales en libre ejercicio (abogados, contadores) no opera necesariamente de forma reactiva o mediante una inspección física inicial.

Al procesar ese reporte, la UNIF ejerce su facultad de trazabilidad. Investiga quién preparó el contrato, quién constituyó la sociedad mercantil o

quién asesoró la estructura jurídica. Al cruzar los datos del Registro Público, las notarías y la banca, la UNIF identifica la participación del abogado o profesional.

Cuando un profesional omite una señal de alerta o no reporta una transacción sospechosa de un cliente, la UNIF suele detectarlo a través del análisis de reportes descendientes o colaterales emitidos por los sujetos obligados del sector financiero (bancos, empresas de seguros, instituciones del mercado de valores

Por consiguiente, la supervisión de la UNIF asegura que el libre ejercicio de la profesión no sea desnaturalizado. La tutela estatal garantiza que los profesionales actúen bajo el enfoque basado en riesgo (EBR), elevando el costo de operación para las estructuras criminales y protegiendo el sistema económico nacional de la infiltración de capitales de origen ilícito, el terrorismo y el financiamiento a la proliferación de armas de destrucción masiva.

Consideraciones reflexivas

El tránsito hacia la implementación efectiva del Enfoque Basado en Riesgo (EBR) en el ejercicio de la abogacía, la contaduría pública y la administración en Venezuela no representa una mera adición de cargas burocráticas, sino una reconfiguración axiológica del ejercicio liberal frente a las exigencias éticas de la modernidad.

El administrador, el contador y el abogado actúan, en consecuencia, como los ingenieros del tejido mercantil y garantes de la confianza pública. Sin una supervisión asertiva por parte de la UNIF y una profunda conciencia deontológica del sujeto obligado, los vehículos societarios corren el riesgo ontológico de ser desnaturalizados, degradándose a meros "cascarones vacíos" orientados a la fragmentación institucional y al ocultamiento del Beneficiario Final.

Por ende, la intervención fiscalizadora del Estado no debe ser interpretada desde una visión corporativista como una injerencia arbitraria a la autonomía gremial, sino como una garantía de inmunidad institucional y de justicia distributiva que preserva la licitud, la equidad y la transparencia del tráfico jurídico y mercantil de la nación.

A manera de colofón, el gran desafío contemporáneo para este bloque profesional radica en armonizar sus respectivos deberes de reserva técnica y

ética con la obligación legal y moral de prevención. Si bien el abogado se ampara en el secreto profesional para salvaguardar el valor de la inviolabilidad de la defensa, y el contador y el administrador se rigen por principios éticos de confidencialidad para proteger la seguridad del tráfico comercial, estas prerrogativas legítimas jamás pueden ser instrumentalizadas axiológicamente como una patente de corso para la opacidad o el ocultamiento del delito. El secreto profesional encuentra su límite ético infranqueable allí donde comienza la complicidad con la injusticia.

En conclusión, los abogados, contadores y administradores en Venezuela deben asumir un rol proactivo y corresponsable en la administración de riesgos, trascendiendo el paradigma del mero cumplimiento normativo formal por una auténtica ética de la responsabilidad. La adopción del Sistema Integral de Administración de Riesgos (SIAR) no constituye un menoscabo al libre ejercicio, sino el único mecanismo válido y legítimo para blindar la fe pública, garantizar la seguridad jurídica del Estado y asegurar que las ciencias jurídicas, contables y administrativas sigan siendo baluartes éticos de la legalidad en el entorno globalizado del siglo XXI.

Referencias Bibliográficas

Circular UNIF-DG-DSU-04409 de fecha 10 de noviembre 2023. Señales de alerta, Controles Internos y Directrices Relacionadas con los Reportes de Actividades Sospechosas RAS. [Documento en línea]. Disponible <https://www.unif.gob.ve/circulares/> [consulta: 2026, junio 14].

Formulario PE-UNIF-005 Reporte de Actividades Unidad de inteligencia Financiera [Documento en línea]. Disponible UNIF. [https://www.unif.gob.ve/wp-content/uploads/Circulares UNIF/UNIF DIF DAE 028.pdf](https://www.unif.gob.ve/wp-content/uploads/Circulares_UNIF/UNIF_DIF_DAE_028.pdf) [consulta: 2026, junio 10].

Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LODOFT). Gaceta Oficial N° 39.912. de fecha 30 de abril de 2012

Vera O. y Monsalve S. (Willful Blindness” Y “Compliance”: Aplicación En Colombia.) Revista Derecho Penal y Criminología volumen XLVI número 120 enero-junio de 2025 pp. 213-238. Disponible en línea <file:///C:/Users/Nelly%20Sanchez/Downloads/Dialnet-WillfulBlindnessYComplianceAplicacionEnColombia-9943908.pdf>

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR DE ECONOMÍA Y FINANZAS
ESCUELA NACIONAL DE ADMINISTRACIÓN Y HACIENDA PÚBLICA
DIRECCIÓN DE POSTGRADO Y ADIESTRAMIENTO
PROGRAMA DE-ESPECIALIZACIÓN EN GESTIÓN DE PREVENCIÓN DE
LEGITIMACIÓN DE CAPITALES Y FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR SEÑALES DE ALERTA

**Rol Del Intermediario De Seguros En La Detección De Señales De Alerta
De LC/FT Vinculadas Al Cliente.**

Autor: Juan C., Cabello M.
Facilitadora: Lic. Elizabeth Peláez
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
DIRECCIÓN DE POSTGRADO Y ADIESTRAMIENTO
PROGRAMA DE-ESPECIALIZACIÓN EN GESTIÓN DE PREVENCIÓN DE
LEGITIMACIÓN DE CAPITALES Y FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR SEÑALES DE ALERTA

**Rol del Intermediario de Seguros en la detección de señales de alerta de
LC/FT vinculadas al cliente.**

Autor (a): Juan C., Cabello M

Correo electrónico: juanc.maquinam@gmail.com

<https://orcid.org/0009-0009-7505-7398>

Resumen

El presente ensayo examina el rol fundamental e insustituible del intermediario de seguros en la República Bolivariana de Venezuela como primer eslabón de contención contra la Legitimación de Capitales y el Financiamiento al Terrorismo (LC/FT). A partir de un análisis jerárquico que abarca el orden público económico constitucional, los estándares de la Recomendación 1 y 10 del Grupo de Acción Financiera Internacional (GAFI), y las exigencias de la Providencia Administrativa N° SAA-01-0536-2024 de la Superintendencia de la Actividad Aseguradora (SUDEASEG), se fundamenta porque la detección de señales de alerta vinculadas al cliente es una obligación legal ineludible. El estudio integra datos estadísticos descriptivos de la Unidad Nacional de Inteligencia Financiera (UNIF), los cuales demuestran de forma empírica que el 68,35% de los Reportes de Actividades Sospechosas (RAS) en el país provienen de inconsistencias en el perfil financiero y operaciones sin justificación económica clara del cliente. Finalmente, se destaca la necesidad imperativa de articular una comunicación bidireccional y robusta entre el intermediario de seguros y el Oficial de Cumplimiento (O.C.) de las empresas aseguradoras, permitiendo optimizar el flujo de información y robustecer las labores de análisis estratégico que efectúa la Unidad Nacional de Inteligencia Financiera (UNIF) para la salvaguarda de la soberanía financiera del Estado venezolano.

Palabras Claves: Intermediario de Seguros, Señales de Alerta, Oficial de cumplimiento

Abstract

This essay examines the fundamental and irreplaceable role of the insurance intermediary in the Bolivarian Republic of Venezuela as the first line of defense against Money Laundering and Terrorist Financing (ML/TF). Based on a hierarchical analysis encompassing the constitutional economic public order, the standards of Financial Action Task Force (FATF) Recommendations 1 and 10, and the strict technical requirements of Administrative Provision No. SAA-01-0536-2024 issued by Superintendence of Insurance Activity (SUDEASEG), this study demonstrates why the detection of red flags linked to customers constitutes an unavoidable legal obligation. The research integrates empirical and descriptive statistical data from the National Financial Intelligence Unit (UNIF), revealing that 68.35% of the Suspicious Activity Reports (SARs) processed at the national level originate from inconsistencies between the client's financial profile and their transactions, as well as operations lacking clear economic justification. Finally, it highlights the urgent need to structure a robust, bi-directional communication channel between the insurance intermediary and the Compliance Officer (C.O.) of insurance companies. This synergy optimizes information flows and enhances the strategic analysis performed by the National Financial Intelligence Unit (UNIF) to safeguard the financial sovereignty of the Venezuelan State.

Keywords: Insurance Intermediary, Red Flags, Compliance Officer, Financial Intelligence, Risk-Based Approach.

Introducción

El dinamismo de los mercados financieros globales y la constante evolución de las tipologías delictivas empleadas por la delincuencia organizada transnacional han obligado a los Estados a reconfigurar sus mecanismos tradicionales de fiscalización y control. En este panorama, los sectores financieros no bancarios, y de manera muy particular el sector de los seguros y reaseguros, han emergido como áreas de alta vulnerabilidad estratégica. La delincuencia ya no solo busca canales de colocación primaria, sino vehículos contractuales complejos donde el fraccionamiento de capitales o la cancelación anticipada de pólizas permitan el blanqueo masivo de activos con apariencia de total licitud. Dentro de esta estructura comercial, el intermediario de seguros (agente, corredor o sociedad de corretaje), se sitúa en la posición de mayor relevancia técnico-criminológica

al ser el único actor que interactúa cara a cara con el tomador del riesgo en la fase de preventa o vinculación inicial.

Tradicionalmente, la doctrina de cumplimiento normativo ha enfrentado serias dificultades metodológicas debido a la persistencia de enfoques meramente formalistas. Autores de referencia, como Blanco Cordero (2015), advierten que los sujetos obligados suelen caer en un cumplimiento por mera verificación documental (*checklist compliance*), lo cual anula la efectividad práctica de la inteligencia financiera corporativa. En Venezuela, este diagnóstico fue validado críticamente en el último Informe de Evaluación Mutua (IEM) emitido por el Grupo de Acción Financiera del Caribe (GAFIC), evidenciando brechas significativas en la capacidad de detección analítica y temprana de inusualidades en los sectores no bancarios. Ante esta realidad, la sola recolección pasiva de documentos de identidad ya no es suficiente; se requiere que el intermediario actúe como un verdadero analista predictivo y ejerza su rol como sujeto obligado en su ámbito de actuación profesional.

El propósito central de este ensayo es analizar el rol del intermediario de seguros en la República Bolivariana de Venezuela bajo los lineamientos del Enfoque Basado en Riesgos (EBR), evaluando de qué manera la detección y el procesamiento oportuno de las señales de alerta vinculadas al cliente se transforman en insumos sustanciales para la prevención de los delitos socioeconómicos. Para lograr esto, la investigación examina la fundamentación constitucional del orden público económico, el catálogo técnico de alertas y las disposiciones normativas de la Providencia Administrativa N° SAA-01-0536-2024 de la SUDEASEG (La Providencia 0536). Adicionalmente, el estudio se adentra en dos elementos medulares del sistema preventivo: el rol del Oficial de Cumplimiento (O.C.) como canalizador y receptor del esfuerzo preventivo del intermediario, y la posterior función de inteligencia macrofinanciera realizada por la Unidad Nacional de Inteligencia Financiera (UNIF) en el análisis de los Reportes de Actividades Sospechosas (RAS). A través de esta visión integral, se busca demostrar que el cumplimiento normativo es, en esencia, una corresponsabilidad que coadyuva de manera directa a la seguridad de la Nación.

I. El marco constitucional del orden público económico y la tutela del interés general.

El análisis del rol del intermediario de seguros en la República Bolivariana de Venezuela no puede iniciarse desde una perspectiva puramente mercantil o comercial. Su fundamentación dogmática descansa sobre el ordenamiento constitucional que rige la seguridad de la Nación y el orden público económico. La **Constitución de la República Bolivariana de Venezuela (CRBV)** establece en su artículo 322 que la seguridad de la Nación es competencia esencial y responsabilidad del Estado, y su defensa es responsabilidad de todos los venezolanos y venezolanas, extendiendo este principio de corresponsabilidad al ámbito socioeconómico. Cuando la delincuencia organizada instrumentaliza las instituciones financieras para el lavado de dinero, no solo comete un delito patrimonial, sino que atenta contra la estabilidad del Estado, distorsiona los precios de los mercados y corroe la integridad de la economía nacional.

Bajo este mandato constitucional, la **Ley de Reforma del Decreto con Rango, Valor y Fuerza de Ley de la Actividad Aseguradora (Gaceta Oficial Extraordinaria N° 6.770)** transforma radicalmente la naturaleza jurídica del sector seguros. En su **Artículo 1°**, la ley establece que su objeto es regular, supervisar y vigilar la actividad aseguradora:

"...a fin de garantizar los procesos de transformación socioeconómicos que promueve el Estado, en tutela del interés general representado por los derechos y garantías de los tomadores, asegurados, beneficiarios, contratantes, usuarios y afiliados, según corresponda..."

Este concepto de **"tutela del interés general"** es la piedra angular del presente ensayo. Implica que el intermediario de seguros (definido en la ley como agente de seguros, corredor de seguros o sociedades de corretaje) deja de ser un simple mandatario comercial cuyo único fin es la captación de primas y el cobro de comisiones. El legislador lo eleva a la categoría de **Sujeto Obligado**, convirtiéndolo en un guardián del orden público económico.

Esta conceptualización de la actividad aseguradora como un bien de interés general o de orden público socioeconómico encuentra un firme asidero en la doctrina nacional. Autores como Chang y Negrón (2014) sostienen que el contrato de seguro sobrepasa la mera esfera patrimonial privada porque las reservas técnicas constituidas por los sujetos obligados representan el ahorro público de la sociedad, confiriéndole al Estado una facultad de intervención intensa para preservar la fe pública. En idéntico sentido, desde la perspectiva del Derecho Penal Económico, Bajo Fernández y Bacigalupo (2001) afirman que los delitos financieros modernos no dañan únicamente el patrimonio individual, sino que corroen el orden económico general que sostiene al Estado social. Por ende, la elevación legal del intermediario de seguros al estatus de Sujeto Obligado no es un mero capricho administrativo, sino una delegación formal del deber constitucional de coadyuvar con la seguridad económica de la República.

Por lo tanto, la detección de una señal de alerta vinculada al cliente no es una opción discrecional o un acto de cortesía burocrática hacia el supervisor; es el cumplimiento de una obligación legal y ética destinada a proteger el interés general de la sociedad frente a los flujos financieros de origen criminal. La firma del intermediario en una solicitud de póliza o en una ficha de inscripción actúa como una certificación de legitimidad, y su inobservancia acarrea severas responsabilidades administrativas, civiles y penales de carácter personalísimo y en tal sentido, vistas las consecuencias, deben prestar mayor seguimiento y atención a las funciones delegadas y conferidas por el Estado.

II. El marco internacional (GAFI) y el diagnóstico crítico del Informe De Evaluación Mutua (IEM) de Venezuela

Como ha sido costumbre en nuestros planteamientos, para comprender la urgencia o necesidad técnica en la detección de señales de alerta, es imperativo y necesario conectar la realidad local con los estándares o normas globales. Las **40 Recomendaciones del GAFI** establecen en su **Recomendación 1**, la adopción obligatoria del **Enfoque Basado en Riesgo (EBR)**, el cual exige que los países y sus instituciones financieras identifiquen, evalúen y entiendan sus

riesgos, aplicando recursos preventivos de manera proporcional a dichos riesgos. Asimismo, la **Recomendación 10** rige las medidas de **Debida Diligencia del Cliente (DDC)**, prohibiendo explícitamente la apertura de contratos anónimos o bajo nombres ficticios, e imponiendo la obligación de verificar la identidad del cliente, el beneficiario real y el origen de sus fondos.

El **Último Informe de Evaluación Mutua (IEM) de Venezuela realizado por el GAFIC**, adoptado en noviembre de 2022 y publicado a inicios de 2023, abordó con rigurosidad y precisión el nivel de cumplimiento técnico y, fundamentalmente, la *efectividad* del sistema preventivo nacional. El informe situó bajo la lupa los **Inmediatos de Efectividad (IO)**, específicamente el **IO3** (relativo a la calidad de la supervisión de las autoridades competentes) y el **IO4** (relativo a la implementación efectiva de medidas preventivas por parte de los sujetos obligados).

El GAFIC diagnosticó que, si bien el sector bancario venezolano mostraba un nivel avanzado de madurez en sus sistemas automatizados de monitoreo, los **sectores financieros no bancarios, con especial énfasis en el sector asegurador, presentaban brechas críticas en la efectividad de la detección temprana de operaciones sospechosas**. El informe técnico señaló que persistía en una parte del sector seguros una cultura de "cumplimiento formal" o *compliance ciego*, donde los intermediarios se limitaban a compilar o recabar documentos para llenar un expediente físico (cumplimiento por *checklist* o lista de chequeo), pero carecían de capacidad analítica y racional para identificar y procesar las **Señales de Alerta en la fase de vinculación del cliente**.

Doctrinariamente, la conducta descrita donde el intermediario prefiere omitir la indagación frente a alertas evidentes se enmarca en la denominada "Teoría de la Ignorancia Deliberada" o *Willful Blindness* (Ceguera voluntaria). Tal como refiere el experto penalista Blanco Cordero (2015), en la legitimación de capitales quien tiene el deber legal y contractual de conocer el perfil de su cliente y decide no hacerlo para obtener un beneficio económico, asume el resultado lesivo de su conducta bajo la figura del dolo eventual. La jurisprudencia y la dogmática penal contemporánea no admiten el desconocimiento inexcusable como

eximente cuando los indicios o señales de alerta eran palmarios. Así, el intermediario que tramita una póliza ignorando los patrones de inusualidad descritos no comete una simple falta administrativa, sino que asume de manera corresponsable los elementos del tipo objetivo penal contemplado en la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT).

Este diagnóstico es el que impulsa la severidad de las reformas normativas actuales en el país. El Informe de Evaluación Mutua (IEM) del GAFIC dejó claro que el intermediario de seguros es el "cuello de botella" del sistema: si el agente o corredor no detecta la inusualidad en el primer contacto con el cliente, el dinero de origen ilícito puede ingresar al torrente financiero con apariencia de legalidad a través del pago de primas, contaminando el reaseguro y los fondos de reserva del sector y de todo el sistema financiero venezolano.

III. La penalización de la Ceguera Voluntaria bajo la aplicación de la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT)

La inobservancia de las señales de alerta por parte del intermediario de seguros no se traduce únicamente en una sanción de carácter administrativo por parte del órgano regulador (SUDEASEG). La **Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT)** tipifica de manera taxativa las obligaciones penales sustantivas a las que se enfrenta el profesional del seguro.

El **Artículo 14 de la LOCDOFT** impone de forma expresa la obligación de reportar las operaciones sospechosas de manera directa a la Unidad Nacional de Inteligencia Financiera (UNIF). La ley define como operación sospechosa aquella transacción inusual que, no obstante estar o no en los parámetros ordinarios del cliente, despierte la sospecha de que los fondos provienen de actividades relacionadas con los delitos de delincuencia organizada, o que están dirigidos al financiamiento al terrorismo.

Si un intermediario de seguros detecta múltiples señales de alerta en un cliente (por ejemplo, un cliente que se niega a explicar el origen de un patrimonio millonario para asegurar una flota de camiones, o que exige pagar la prima a través de múltiples transferencias fraccionadas de terceras personas sin vinculación aparente) y decide "cerrar los ojos" o ignorar las alarmas con el único fin de concretar la venta y percibir su comisión, la doctrina penal moderna y la jurisprudencia venezolana bajo la LOCDOFT configuran dicha conducta bajo la figura del **Dolo Eventual**. El intermediario que ignora deliberadamente las señales de alerta no es una víctima de la astucia del delincuente; se convierte en un **facilitador necesario o colaborador** para la legitimación de capitales, exponiéndose a las penas privativas de libertad contempladas en la ley para el delito de legitimación de capitales y delincuencia organizada.

IV. Operatividad de las señales de alerta a través del Sistema Integral de Administración de Riesgos (SIAR). (Providencia Administrativa SAA-01-0536-2024)

La interpretación y desarrollo detallado de estos mandatos constitucionales, internacionales y penales a la práctica diaria del intermediario de seguros está rígidamente normada por la **Providencia Administrativa N° SAA-01-0536-2024** emitida por la SUDEASEG, la cual deroga expresamente la antigua providencia del año 2021 (SAA-08-004-2021) e impone la reingeniería total de los controles internos.

Bajo esta nueva normativa, los intermediarios deben en su condición de persona natural deben diseñar e implementar, bajo un estricto enfoque basado en riesgo (EBR), y dar cumplimiento al contenido de la Ley, con énfasis en la aplicación de la Debida diligencia del Cliente y las Sociedades de corretaje como Personas Jurídicas además deben diseñar e implementar un Sistema Integral de Administración de Riesgos (SIAR) de LC/FT/FPADM y Otros Ilícitos. Las señales de alerta no operan de forma aislada, sino que constituyen el insumo transversal que alimenta de manera viva cada una de las **cinco etapas secuenciales y obligatorias del SIAR**:

1. **Identificación de los Riesgos:** Mapeo técnico de las amenazas y vulnerabilidades antes de la suscripción.
2. **Segmentación de los Riesgos:** Clasificación del portafolio del intermediario según las características homogéneas de los factores de riesgo.
3. **Medición o Evaluación de los Riesgos:** Determinación cuantitativa y cualitativa del impacto y probabilidad de ocurrencia (Riesgo Inherente vs. Riesgo Residual).
4. **Control:** Aplicación de los mitigantes específicos aprobados por la Junta Directiva.
5. **Monitoreo:** Seguimiento continuo y en tiempo real del comportamiento del cliente durante la vigencia del contrato.

Para las carteras e intermediarios exceptuados de implementar el SIAR en su estructura corporativa completa, la Providencia 0536 es taxativa: deben mantener obligatoriamente un registro detallado de sus clientes bajo el principio riguroso de la **Debida Diligencia del Cliente (DDC)**, asegurando que ninguna transacción sea procesada de forma ciega.

V. Catálogo técnico-criminológico de señales de alerta vinculadas al cliente

Con la intención de dotar el presente ensayo de un valor operativo e inédito, presentamos de forma pormenorizada un **catálogo multidimensional de señales de alerta enfocadas estrictamente en el comportamiento, transaccionalidad y estructura del cliente**, clasificadas bajo las mejores prácticas internacionales del sector, de la siguiente manera:

A. Alertas Basadas en el Comportamiento e Identidad del Cliente

- **Resistencia a la Transparencia:** Clientes que muestran una marcada **desgana**, evasivas, renuencia o retrasos injustificados para proveer la información mínima de identificación, actualización de datos o soportes que verifiquen el origen lícito de sus fondos.
- **Inconsistencia Tecnológico-Geográfica:** Solicitud de una póliza por parte de un cliente potencial desde una ubicación geográfica distante o extranjera, sin un nexo comercial claro, cuando en las cercanías de su domicilio real podría contratar un servicio de similares características.
- **Uso de Documentación Cuestionable:** Presentación de estados financieros, referencias comerciales, actas de asambleas de accionistas desactualizadas o registros tributarios que generan una profunda incertidumbre respecto a la operación real de la empresa, su estabilidad financiera o la legitimidad de sus firmas.

B. Alertas Basadas en las Transacciones Financieras del Cliente

- **El Fenómeno del Pago en Exceso:** Primas pagadas por el cliente de forma anticipada sin justificación técnica aparente, o la realización deliberada de pagos en exceso por encima del valor correcto de la factura para, de manera inmediata, solicitar una devolución o reembolso, logrando que la aseguradora emita por un medio de pago a través de una transferencia "limpia" a su nombre.
- **Cancelación y Rescate Anómalo:** Clientes que contratan pólizas (especialmente seguros de vida o ahorro con alto valor de rescate) mostrando un absoluto desinterés por las condiciones de cobertura o los deducibles, pero exhibiendo una fijación inusual por las cláusulas de rescate anticipado, cancelando el contrato a los pocos días y aceptando penalizaciones económicas severas con tal de reintegrar el dinero al circuito financiero legal.

- **Liquidaciones Inusuales en Efectivo o Cuasi-efectivo:** Pagos de primas, subrogaciones o compras de salvamentos utilizando dinero en efectivo o instrumentos cuasi-efectivos que superan los límites ordinarios permitidos por el Banco Central, rompiendo con el perfil transaccional lógico del asegurado.

C. Alertas Basadas en los Tipos de Producto y Estructura Corporativa

- **Contratación Incoherente:** Clientes que adquieren pólizas de seguros colectivos o de ingeniería cuyos riesgos o sumas aseguradas no guardan ninguna relación con el giro del negocio, el tamaño de la organización o su objeto social declarados.
- **Siniestralidad Sospechosa:** Ocurrencia de siniestros con características idénticas de un mismo asegurado, de asegurados económicamente relacionados o que apuntan a un mismo beneficiario final dentro de un mismo ramo de seguros en un período de tiempo sospechosamente corto.
- **Opacidad Societaria:** Empresas tomadoras que carecen de una personería jurídica razonable, grupos de asegurados no homogéneos o estructuras corporativas complejas donde se impide la identificación plena de la persona natural que ostenta el control (Beneficiario Final).

VI. Sustentación jurídico-empírica basada en las estadísticas de la Unidad Nacional de Inteligencia Financiera (UNIF).

En este contexto pasamos a destacar aspectos neurálgicos del **Informe de Retroalimentación Basado en el Análisis Descriptivo de los Reportes de Actividades Sospechosas (RAS) emitido por la Unidad Nacional de Inteligencia Financiera (UNIF) anual 2025**. Los datos estadísticos oficiales consolidados por este órgano de inteligencia en Venezuela desvelan una métrica contundente que redefine las prioridades de control:

- El **50,00%** de la totalidad de los RAS procesados a nivel nacional se fundamentan taxativamente en la señal de alerta de **"Inconsistencia entre el perfil financiero y las operaciones realizadas"**.
- Al sumar este indicador con el motivo técnico de **"Operaciones sin justificación económica clara"**, el cual representa el **18,35%**, se concluye de forma categórica que **el 68,35% de todas las alertas que movilizan el sistema de justicia preventiva nacional nacen de la incongruencia del perfil del cliente.**

VII. Aspectos sustanciales del rol del intermediario de seguros en la detección de señales de alerta.

El Rol del Intermediario de Seguros en la detección de señales de alerta vinculadas al cliente constituye el núcleo protector de la actividad aseguradora contemporánea. Bajo el actual ecosistema regulatorio venezolano dictado entre 2024 y 2026, la detección oportuna de la inusualidad transmuta el cumplimiento burocrático en un acto de salvaguarda del orden público económico. El intermediario bien capacitado, respaldado por las cinco etapas que conforman **el SIAR**, el catálogo técnico de alertas y las directrices de la ONCDOFT y la UNIF, deja de ser un vendedor ciego de pólizas para convertirse en una frontera jurídica impenetrable, garantizando que su ejercicio profesional sirva a la tutela del interés general y al blindaje absoluto del Sistema Financiero Nacional venezolano frente a la lupa de la comunidad internacional.

Interpretación Criminológica Aplicada al Rol del Intermediario

Es nuestro criterio que las redes criminales no penetran el sistema asegurador mediante tipologías indetectables, sino explotando la falla más elemental e histórica de los Sujetos Obligados: **la laxitud en la ejecución de la Debida Diligencia del Cliente (DDC) y la falta de actualización periódica de sus perfiles económicos.**

La "inconsistencia de perfil" ocurre cuando el intermediario de seguros actúa como un mero transcriptor de datos en frío, omitiendo evaluar si los fondos transados guardan coherencia con la realidad del cliente. Al demostrar que casi el 70% de las alertas nacionales se concentran en esta brecha, la investigación concluirá que el rol del intermediario es insustituible: al ser el único actor que interactúa cara a cara con el tomador en la fase de preventa, tiene la obligación legal de aplicar una **DDC Intensificada**, transformando el cumplimiento formal en inteligencia financiera defensiva real para blindar su firma profesional.

VIII. Contraposición técnica con la evaluación sectorial de riesgos 2026 (ONCDOFT)

Es importante contrastar el rol del intermediario de seguros con las conclusiones técnico-metodológicas de la reciente **Evaluación Sectorial de Riesgos de LC/FT/FPADM realizada por la ONCDOFT**. Aunque este estudio del Estado se enfocó originalmente en evaluar las vulnerabilidades de los profesionales y actividades no financieras especificadas (APNFD) como abogados, contadores públicos y agentes inmobiliarios, sus hallazgos son perfectamente aplicables por analogía simétrica al intermediario de seguros.

La Evaluación Sectorial arrojó que estos profesionales operan frecuentemente como "puertas de entrada" inconscientes a la economía real debido a dos fallas críticas: la deficiente conservación de las fichas de DDC y la falta de entrenamientos dinámicos adaptados a la realidad local. Al cruzar este documento con la Providencia 0536 de la SUDEASEG, el ensayo planteará que el intermediario de seguros debe asimilar las lecciones de la Evaluación Sectorial, implementando las siguientes directrices operativas de vanguardia; a saber:

1. **Mesas de Trabajo de Adecuación Normativa:** Revisión y adecuación continua de los manuales de políticas internas de las empresas de seguros y/o de medicina prepagada con las cuales opera en coordinación con los órganos de control, asegurando que las matrices de riesgo se

adapten de forma ágil a las nuevas tipologías criminales detectadas en los ejercicios anuales del Estado.

2. **Conservación Íntegra de Soportes:** Conservar de manera rigurosa e inalterable toda la documentación de soporte (fichas de DDC, soportes de origen de fondos, contratos) por los períodos legales establecidos, garantizando que dicha información esté disponible de forma oportuna para las fiscalizaciones *extra situ e in situ* de la UNIF y la SUDEASEG.
3. **Capacitación de Simulación Práctica (Código RUF-ONCDOFT):** El Artículo 29 del Plan Operativo Anual (POA) debe cumplirse superando la capacitación netamente magistral. Se exige la inclusión de talleres de simulación basados en casos reales del contexto venezolano actual, permitiendo al intermediario y a su personal de primera línea practicar la toma de decisiones críticas y el reporte oportuno ante la aparición de señales de alerta de alto riesgo.

IX. El Rol de Enlace del Oficial de Cumplimiento y la Labor de Inteligencia Financiera de la UNIF

La efectividad del sistema preventivo en el sector asegurador venezolano depende críticamente de un canal de comunicación robusto y fluido entre el intermediario de seguros (quien detecta la señal de alerta en el campo) y el Oficial de Cumplimiento (O.C.) de la empresa de seguros. Conforme a lo establecido en la Providencia Administrativa N° SAA-01-0536-2024, el O.C. funge como el director técnico del SIAR y el nexo formal ante los órganos de control del Estado. Al respecto, autores especializados en gobernanza corporativa y *compliance* como Pieth (2014) argumentan que el Oficial de Cumplimiento no puede actuar de forma aislada en una oficina corporativa; su éxito operativo radica en su capacidad de dotar a las líneas de negocio e intermediarios externos de las herramientas analíticas necesarias para identificar inusualidades en tiempo real.

Cuando un intermediario de seguros identifica una o varias señales de alerta y recopila la documentación correspondiente mediante la Debida Diligencia del Cliente (DDC), debe remitir de inmediato estos hallazgos al Oficial de Cumplimiento de la respectiva aseguradora. El O.C. tiene la alta responsabilidad legal de evaluar dicha inusualidad a la luz de la matriz de riesgo integral de la institución. Si tras este análisis técnico-financiero se determina la ausencia de una justificación económica lógica por parte del cliente, el O.C. procederá a estructurar y transmitir de manera directa el Reporte de Actividad Sospechosa (RAS) ante la Unidad Nacional de Inteligencia Financiera (UNIF), garantizando el estricto cumplimiento del principio de confidencialidad o prohibición de revelación (*tipping-off*) fijado en el artículo 14 de la LOCDOFT.

Una vez que el RAS es recibido por la UNIF, se activa la fase más sofisticada y estratégica del sistema de prevención del delito financiero: la **inteligencia financiera**. Como bien sabemos la UNIF no es un órgano punitivo ni de persecución penal inmediata; su misión esencial, tal como la define la doctrina criminológica y los estándares internacionales de Gottschalk (2010), consiste en transformar reportes administrativos individuales en inteligencia táctica y estratégica utilizable por los órganos jurisdiccionales. La labor de la UNIF consiste en someter los RAS a un análisis descriptivo, cruzando la información reportada por las aseguradoras con bases de datos fiscales, registros inmobiliarios, movimientos del sector bancario y perfiles migratorios.

Esta visión macro y cruzada de la información financiera permite a la UNIF desvelar las complejas tramas corporativas, identificar redes transnacionales de legitimación de capitales y determinar patrones operativos de la delincuencia organizada que resultarían invisibles para una empresa de seguros o un intermediario analizados de forma aislada. La calidad de los análisis efectuados por la UNIF depende de manera directa de la rigurosidad y precisión con la que el intermediario de seguros en primera línea haya detallado la señal de alerta y documentado las inconsistencias de perfil de su cliente.

Conclusiones y Reflexiones

El análisis minucioso del ordenamiento jurídico venezolano y de la dinámica del mercado asegurador permite concluir, de manera categórica, que el rol del intermediario de seguros ha trascendido las fronteras de la mera intermediación mercantil para consolidarse como un pilar fundamental de la seguridad de la Nación y del orden público económico. Bajo el riguroso ecosistema normativo delineado en los últimos años, la detección temprana y metódica de las señales de alerta vinculadas al cliente ha dejado de ser un formalismo administrativo para convertirse en una obligación técnico-legal insustituible. Cuando un agente, corredor o sociedad de corretaje ejecuta de forma eficaz las políticas de Debida Diligencia del Cliente (DDC), no sólo mitiga riesgos corporativos, sino que provee al Estado venezolano de la materia prima indispensable para la defensa contra los flujos de dinero de procedencia ilícita.

En segundo lugar, los datos estadísticos descriptivos provistos por la Unidad Nacional de Inteligencia Financiera (UNIF) para el cierre del año 2025, constituyen una evidencia científica irrefutable: al concentrarse el 68,35% de las alertas nacionales en inconsistencias de perfil y operaciones carentes de lógica económica clara, queda demostrado que la delincuencia organizada busca penetrar el sistema financiero a través de la laxitud o ceguera voluntaria de los actores de primera línea. Esta realidad sitúa al intermediario en una disyuntiva de alta sensibilidad jurídica: ignorar de manera deliberada los patrones conductuales, transaccionales o societarios inusuales con el único propósito de concretar una venta lo convierte automáticamente en un facilitador necesario bajo la figura del dolo eventual, exponiéndolo a las graves sanciones punitivas contempladas en la LOCDOFT y en la Ley de la Actividad Aseguradora.

Finalmente, la consolidación de un sistema preventivo robusto exige optimizar la sinergia comunicacional entre los intermediarios del seguro y el Oficial de Cumplimiento de las entidades aseguradoras. La transmisión inmediata, detallada y confidencial de las inusualidades es el único mecanismo que permite al O.C. estructurar Reportes de Actividades Sospechosas (RAS) con valor analítico real. Este flujo de información es el que nutre la labor macro de

inteligencia financiera de la UNIF, permitiéndole desarticular las redes criminales complejas mediante el cruce estratégico de información. El fortalecimiento continuo del talento humano mediante capacitaciones prácticas bajo el Código RUF-ONCDOFT, la debida conservación de soportes y el abandono definitivo del *compliance* ciego son las herramientas que transformarán al sector asegurador venezolano en una frontera jurídica infranqueable e impenetrable que garantice la estabilidad socioeconómica y la tutela del interés general de la República.

Referencias Bibliográficas

- 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.
- Bajo Fernández, M., & Bacigalupo, S. (2001). Derecho penal económico. Centro de Estudios Ramón Areces.
- Blanco Cordero, I. (2015). El delito de blanqueo de capitales (4ta ed.). Editorial Aranzadi.
- Chang, J., & Negrón, M. (2014). Derecho de Seguros y Regulación Prudencial en la Actividad Aseguradora Venezolana. Editorial Buchivacoa.
- Dib Tajan, A. G. (2015). Estrategias de inversión y gestión de riesgo de fraude en el sector asegurador del municipio Maracaibo (Trabajo de grado de maestría, Universidad Rafael Urdaneta). Maracaibo, Venezuela.
- Escuela Nacional de Administración y Hacienda Pública. (2016). Manual para elaboración y presentación de trabajos académicos. ENAHP-IUT.
- Felson, M., & Boba, R. (2010). Crime and everyday life (4th ed.). SAGE Publications.
- Gottschalk, P. (2010). White-collar crime: Detection, prevention and strategy in business organizations. Universal-Publishers.

- 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). GAFI/FATF.
- Miró Llinars, F. (2012). El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. Marcial Pons.
- Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT). (2026). Evaluación Sectorial de Riesgos de LC/FT/FPADM en Profesionales y Actividades No Financieras Designadas (APNFD) en la República Bolivariana de Venezuela. MPPRIJP.
- Pieth, M. (2014). Compliance: In business and public administration. Intersentia.
- Superintendencia de la Actividad Aseguradora. (2024). Providencia SAA-01-0536-2024. Normas sobre Administración de Riesgos de LC/FT/FPADM en la Actividad Aseguradora. Gaceta Oficial de la República Bolivariana de Venezuela, 6.835 (Extraordinario), septiembre 03, 2024.
- 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.
- Zúñiga Rodríguez, L. (2019). Criminalidad organizada y derecho penal (2da ed.). Editorial Comares.

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LA ECONOMÍA Y FINANZAS
ESCUELA NACIONAL DE ADMINISTRACIÓN Y HACIENDA PÚBLICA
DIRECCIÓN DE POSTGRADO Y ADIESTRAMIENTO
ESPECIALIZACIÓN EN GESTIÓN CONTRA LA LEGITIMACIÓN DE
CAPITALES Y FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR: SEÑALES DE ALERTA

**Rol Estratégico de los Profesionales Jurídicos y Financieros en libre
ejercicio profesional: Señales de alerta, controles internos y directrices
para la prevención de LC/FT/FPADM**

Autora: Dra. Silumerany Rodríguez
Asesor de Contenido: Lic. Elizabeth Peláez
Asesor Metodológico: Dr. Mario Morales

Caracas, Julio 2026

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LA ECONOMÍA Y FINANZAS
ESCUELA NACIONAL DE ADMINISTRACIÓN Y HACIENDA PÚBLICA
DIRECCIÓN DE POSTGRADO Y ADIESTRAMIENTO
ESPECIALIZACIÓN EN GESTIÓN CONTRA LA LEGITIMACIÓN DE
CAPITALES Y FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR: SEÑALES DE ALERTA

**Rol Estratégico de los Profesionales Jurídicos y Financieros en libre
ejercicio profesional: Señales de alerta, controles internos y directrices
para la prevención de LC/FT/FPADM**

Autora: Dra. Silumerany Rodríguez ¹
Correo Electrónico: silualex913@gmail.com
^{ID} <https://orcid.org/0009-0000-7838-9720>

Resumen

El presente ensayo analiza el rol estratégico de los profesionales jurídicos y financieros en libre ejercicio como una línea de defensa económica crítica contra la Legitimación de Capitales, el Financiamiento al Terrorismo y el Financiamiento de la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM). Bajo una metodología analítico-documental, se examina la transmutación de estos sujetos obligados bajo la categoría de Actividades y Profesiones No Financieras Designadas (APNFD), conforme a las Recomendaciones 22, 23 y 28 del Grupo de Acción Financiera (GAFI) y el artículo 9 de la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT) en Venezuela. El estudio desglosa las señales de alerta cuantitativas, referidas a la opacidad en el manejo de fondos y activos, y las señales cualitativas, centradas en comportamientos atípicos y estructuras societarias complejas. Se aborda el desafío estructural de la dualidad funcional, donde el profesional independiente debe actuar simultáneamente como sujeto obligado y oficial de cumplimiento en microestructuras operativas. Asimismo, se delimita el alcance del secreto profesional como un límite legítimo que, si bien prevalece en el ejercicio de la defensa legal, no debe amparar la opacidad sobre el beneficiario final o transacciones ficticias, respetando siempre la prohibición de revelación o *tipping-off*. Se evidencia una brecha de efectividad en el sistema preventivo nacional, caracterizada por la recepción nula de reportes por parte de este sector en las estadísticas de la Unidad Nacional de Inteligencia Financiera (UNIF). El ensayo concluye que el valor estratégico de estos profesionales radica en su capacidad de neutralizar tipologías delictivas en su origen, proponiendo directrices orientadas a la adopción de una cultura de cumplimiento proporcional y personalizada, basada en un Enfoque Basado en Riesgo (EBR), la implementación de manuales a medida, el monitoreo activo de alertas y la

necesaria coordinación entre gremios profesionales y las autoridades para robustecer la seguridad socioeconómica del Estado.

Descriptores: Actividades y Profesiones no Financieras Designadas, Reporte de Actividades Sospechosas, Secreto Profesional.

Abstract

This essay analyzes the strategic role of independent legal and financial professionals as a critical line of economic defense against Money Laundering, Terrorist Financing, and the Financing of the Proliferation of Weapons of Mass Destruction (ML/TF/FPWMD). Using an analytical-documentary methodology, it examines the classification of these entities as Designated Non-Financial Businesses and Professions (DNFBPs), in accordance with FATF Recommendations 22, 23, and 28 and Article 9 of the LOCDOFT in Venezuela. The study breaks down quantitative red flags—related to opacity in the handling of funds and assets—and qualitative red flags, focusing on atypical behaviors and complex corporate structures. It addresses the structural challenge of functional duality, wherein the independent professional must simultaneously act as an obligated entity and a compliance officer within micro-operational structures. Furthermore, it defines the scope of professional privilege as a legitimate boundary; while it prevails in the exercise of legal defense, it must not shield opacity regarding the ultimate beneficial owner or fictitious transactions, while always respecting the prohibition against disclosure or tipping-off. An effectiveness gap in the national preventive system is evident, characterized by the absence of reports from this sector in the National Financial Intelligence Unit (UNIF) statistics. The essay concludes that the strategic value of these professionals lies in their ability to neutralize criminal typologies at their source, proposing guidelines aimed at adopting a culture of proportionate and tailored compliance based on a Risk-Based Approach (RBA), the implementation of customized manuals, active alert monitoring, and necessary coordination between professional associations and authorities to strengthen the State's socioeconomic security.

Descriptors: Designated Non-Financial Businesses and Professions, Suspicious Activity Report, Professional Secrecy.

Introducción

En el complejo entorno económico y legal contemporáneo, los fenómenos delictivos asociados a la Legitimación de Capitales, el Financiamiento al Terrorismo y el Financiamiento de la Proliferación de Armas de Destrucción

Masiva (LC/FT/FPADM) han dejado de ser amenazas exclusivas de los circuitos bancarios tradicionales para convertirse en riesgos sistémicos transnacionales.

A medida que los países han robustecido los controles sobre las instituciones financieras, las organizaciones de delincuencia organizada han desplazado su foco operativo hacia otros sectores vulnerables de la economía, buscando de manera sistemática el auxilio involuntario o la complicidad de asesores independientes. Es en esta coyuntura donde los profesionales jurídicos y financieros que se desempeñan en el libre ejercicio tales como abogados, contadores, administradores y economistas adquieren una relevancia fundamental y de alta sensibilidad dentro del ordenamiento legal.

A nivel internacional, el Grupo de Acción Financiera Internacional (GAFI) identificó esta vulnerabilidad y extendió formalmente sus estándares incluyendo a estos profesionales dentro de las Actividades y Profesiones No Financieras Designadas (APNFD), reconociendo que la experiencia técnica de estos asesores en la ingeniería jurídica, la constitución de empresas y la validación contable representa una codiciada puerta de acceso a la economía formal. Esta responsabilidad global se encuentra plenamente indexada en el ordenamiento jurídico venezolano a través de la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT).

El propósito fundamental de este artículo es analizar el rol estratégico que desempeñan estos profesionales como garantes de la transparencia financiera, examinando los estándares legales vigentes, las señales de alerta cuantitativas y cualitativas, los límites que el secreto profesional impone legítimamente al deber de informar, y las asimetrías institucionales en materia de supervisión, ofreciendo herramientas teóricas y operativas para fortalecer esta línea de defensa económica contra la delincuencia organizada.

Estándares Internacionales

A nivel global, las Cuarenta Recomendaciones del Grupo de Acción Financiera Internacional (GAFI) constituyen el estándar técnico de referencia en materia de prevención de LC/FT/FPADM, estructurando lineamientos que abarcan a los

sectores financiero y no financiero, así como a los mecanismos de investigación y represión penal de estos delitos.

Dentro de este marco, el sector no financiero denominado Actividades y Profesiones No Financieras Designadas (APNFD), conforme la traducción oficial realizada por el GAFILAT con autorización del GAFI, incluyen a:

- a) Casinos
- b) Agentes inmobiliarios.
- c) Comerciantes de metales preciosos.
- d) Comerciantes de piedras preciosas.
- e) **Abogados, notarios, otros profesionales jurídicos independientes y contadores - esto se refiere a los profesionales que trabajan solos, en sociedad o empleados de firmas profesionales. No se propone referirse a los profesionales 'internos' que son empleados de otros tipos de empresas, ni a los profesionales que trabajan para agencias gubernamentales, que pudieran estar sujetos ya a medidas ALA/CFT.**
- f) Proveedores de Servicios Fiduciarios y Societarios se refiere a todas las personas o actividades que no se cubren en otra parte de estas Recomendaciones, y que, como actividad comercial, prestan alguno de los siguientes servicios a terceros:
 - actuación como agente para la constitución de personas jurídicas;
 - actuación (o arreglo para que otra persona actúe) como director o apoderado de una sociedad mercantil, socio de una sociedad o desempeño de un cargo similar con respecto a otras personas jurídicas;
 - provisión de un domicilio registrado; domicilio comercial o espacio físico, domicilio postal o administrativo para una sociedad mercantil, sociedad o cualquier otra persona jurídica o estructura jurídica;
 - actuación (o arreglo para que otra persona actúe) como fiduciario de un fideicomiso expreso o que desempeñe una función equivalente para otra forma estructura jurídica;
 - actuación (o arreglo para que otra persona actúe) como accionista nominal por cuenta de otra persona. (Negrillas propias para resaltar el texto)

Las APNFD, están obligadas a implementar un Enfoque Basado en Riesgo (EBR), aplicar la Debida Diligencia del Cliente (DDC), registrar transacciones y reportar actividades sospechosas; su evaluación del cumplimiento técnico, siguiendo la metodología del GAFI, se rige por el bloque de las

Recomendaciones 22, 23 y 28 (además de los criterios específicos de las Recomendaciones 6 y 7). De este modo, la arquitectura de cumplimiento para las APNFD se articula formalmente a través de dos ejes fundamentales:

- La Recomendación 22 (Debida Diligencia y Registros): Extiende de manera vinculante los estándares de las instituciones financieras a las APNFD. Esto obliga a los sectores a adoptar las directrices sobre Debida Diligencia del Cliente (Recomendación R.) (R.10), mantenimiento de registros (R.11), seguimiento de Personas Expuestas Políticamente (R.12), mitigación de riesgos frente a Nuevas Tecnologías (R.15) y las reglas de Dependencia en terceros (R.17).
- La Recomendación 23 (Otras Medidas de Control): Exige a los profesionales jurídicos y financieros independientes la aplicación de los lineamientos de las Recomendaciones 18 a 21; esto abarca el diseño de Controles internos y gestión de filiales (R.18), la vigilancia en transacciones con Países de mayor riesgo (R.19), la obligación del Reporte de Actividades Sospechosas (R.20), y el apego estricto a las normas de Confidencialidad y prohibición de revelación o *tipping-off* (R.21).

Al respecto, cabe destacar que, si bien la Recomendación 28 del GAFI exige que los países regulen, supervisen y controlen a las APNFD para prevenir la LC y el FT, aplicando medidas preventivas estrictas, las Notas Interpretativas de las Recomendaciones 22 y 23, señalan que los Estados no requieren promulgar leyes ni mecanismos coercitivos de carácter exclusivo para las APNFD, siempre y cuando estas actividades y profesiones se encuentren plenamente integradas e indexadas dentro del marco legal preventivo general de la nación.

Específicamente, en cuanto a los profesionales jurídicos y financieros en libre ejercicio, se contempla una excepción taxativa a la obligación de reporte en virtud del secreto profesional y el privilegio legal, siempre que los datos de la

transacción se hayan obtenido dentro de las circunstancias protegidas por dicha confidencialidad.

En este sentido, corresponde a cada país determinar los asuntos específicos amparados bajo este criterio, el cual típicamente cubre la información que reciben de los clientes al momento de verificar su estatus legal, o bien, en el desempeño de su tarea de defensa y representación en procesos judiciales, administrativos, de arbitraje o mediación.

Como contraparte operativa a esta facultad, las directrices internacionales facultan a los Estados a permitir que estos profesionales independientes remitan sus Reportes de Actividades Sospechosas (RAS) a través de sus respectivas organizaciones de autorregulación, siempre que existan mecanismos adecuados de cooperación y coordinación con la Unidad de Inteligencia Financiera.

Ahora bien, puntualizando en las vulnerabilidades operativas e inherentes a los servicios prestados por estos profesionales, la *Guía dirigida al sector de APNFD para la construcción de una matriz de riesgos en prevención del lavado de activos y financiamiento al terrorismo (LA/FT)*, publicada por el GAFILAT en diciembre de 2022, contempla aspectos claves enmarcado en las funciones específicas desarrolladas:

1. Vulnerabilidades Críticas en el Ejercicio Contable y Financiero

En el ámbito de la contabilidad y la auditoría, el documento advierte que los delincuentes buscan instrumentar al profesional para dotar de una falsa apariencia de legitimidad a estructuras ilícitas. Esto se manifiesta principalmente a través de:

- Debilidades de Información: El mantenimiento de registros financieros deficientes o incompletos por parte de los clientes, lo que obstaculiza la trazabilidad real de los fondos.

- Instrumentalización de Estados Financieros: El uso indebido en la preparación y auditoría de balances para justificar capitales ilícitos o encubrir delitos fiscales y tributarios.
- Abuso de la Gestión Corporativa: La designación roles de administración, o la falsificación y el abuso de cuentas de clientes para ocultar la verdadera identidad del beneficiario final.
- Administración de Fondos de Terceros: El riesgo de desvirtuar el uso de las cuentas de clientes (diseñadas para custodiar transacciones legítimas) convirtiéndolas en canales de tránsito para el LC/FT.

2. Vulnerabilidades Críticas en el Ejercicio Jurídico y Legal

Respecto a los profesionales del derecho, la guía del GAFILAT resalta que su conocimiento técnico y su capacidad para estructurar negocios jurídicos son altamente codiciados por las organizaciones delictivas para evadir los controles del Estado. Las principales alertas se concentran en:

- Debilidades de Información: El mantenimiento de registros deficientes o incompletos por parte de los clientes.
- Operaciones Inmobiliarias: El sector de bienes raíces representa una vulnerabilidad de primer orden debido al elevado volumen de capitales que moviliza, posicionando al abogado que sustancia estas operaciones en una zona de alto riesgo.
- Diseño de Estructuras Corporativas Complejas: La creación de empresas pantalla, vehículos societarios opacos o fideicomisos orientados deliberadamente a frustrar el rastreo de la propiedad y bloquear la labor de inteligencia de las autoridades.

3. Vulnerabilidades Comunes

Además de las vulnerabilidades inherentes a cada profesión, la guía técnica unifica una serie de vulnerabilidades comunes que deben activar de forma inmediata los protocolos de sospecha y debida diligencia reforzada por parte de los asesores jurídicos y financieros:

- Opacidad Corporativa: Ejecución de operaciones con estructuras societarias complejas orientadas a simular transacciones, o con clientes cuyo beneficiario final resulte imposible de identificar.
- Inconsistencia Financiera y Operativa: Transacciones donde el origen económico o jurídico de los fondos no sea claramente determinable, o que muestren discrepancias evidentes frente a las actividades habituales y la línea de negocio declarada por el cliente.
- Irregularidades Comerciales: Operaciones con indicios de ser ficticias o que presenten desviaciones técnicas asociadas a esquemas de sobre o subfacturación.
- Riesgo Reputacional y Legal Coincidente: Conocimiento formal o indiciario de que el cliente se encuentra bajo investigación activa por delitos precedentes o vinculados directamente al LC/FT.

4. Autoevaluación y Cumplimiento: La Dimensión Operativa del Asesor Independiente

El diseño de estas directrices e indicadores plantea un desafío estructural único en el sector no financiero, ya que a diferencia de las instituciones bancarias que poseen departamentos de control dedicados solo a la labor de prevención, en el libre ejercicio es común que el profesional independiente deba asumir de forma simultánea la condición de sujeto obligado y actuar como su propio Oficial de Cumplimiento.

Esta dualidad traslada la responsabilidad directa de identificar, evaluar y comprender los riesgos de su cartera de clientes y de su práctica particular al propio profesional; convirtiendo la autoevaluación constante en un mecanismo indispensable para ejecutar un Enfoque Basado en Riesgo (EBR) verdaderamente efectivo, asegurando que la implementación de los controles internos no sea un cumplimiento plano o reactivo, sino un blindaje dinámico y proporcional a la escala de sus operaciones.

Marco Legal Nacional

El deber de reportar y la adopción de controles internos en el ordenamiento jurídico venezolano se fundamentan en la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Teirrorismo (LOCDOFT), norma que delimita de forma expresa las responsabilidades del sector de los profesionales independientes, homologándolos técnicamente con las exigencias internacionales de las APNFD.

En este sentido, el artículo 9 numeral 9 de la LOCDOFT rompe con la visión tradicional de que la prevención del delito financiero es exclusiva del sector financiero, al incorporar de forma taxativa a los abogados, administradores, economistas y contadores en el libre ejercicio de la profesión bajo la categoría de sujetos obligados, cuando ejecutan transacciones por cuenta de sus clientes relacionadas con:

- a) compraventa de bienes inmuebles;
- b) administración del dinero, valores y otros activos del cliente;
- c) administración de cuentas bancarias, de ahorro o valores;
- d) organización de aportes para la creación, operación o administración de compañías;
- e) creación, operación o administración de personas jurídicas o estructuras jurídicas, y compra y venta de entidades comerciales.

Asimismo, el núcleo operativo de la ley se distribuye entre los artículos 10 al 23, configurando un bloque normativo que asigna responsabilidades concurrentes a todos los sujetos obligados, que incluyen obligaciones y sanciones (multas) por incumplimiento y medidas de prevención, tales como:

- Obligación de conservar registros y controlar transacciones
- Obligación de identificación del cliente
- Obligación de conocer el destino de las transacciones
- Obligación del reporte de actividades sospechosas
- Obligación de confidencialidad
- Obligación de no cerrar cuentas
- Obligación de identificar a terceros intervinientes
- Obligación de reportes de transacciones en efectivo

- Obligaciones asociadas a la identificación de personas expuestas políticamente
- Medidas especiales sobre negocios y transacciones
- Medidas en las sucursales y subsidiarias de los sujetos obligados en el exterior y bancos extranjeros
- Medidas en la adquisición de participaciones en el capital de los sujetos obligados
- Obligación de declarar
- Prohibición de transporte de capitales

Es de resaltar, que además de las obligaciones señaladas, en mayo de 2021 fue publicada la Providencia Administrativa N° ONCDOFT-002-2021, que regula el Registro Unificado de Sujetos Obligados (RUSO-ONCDOFT) y tiene por objeto establecer los requisitos y procedimientos que deben cumplir los sujetos obligados cuya actividad no se encuentre regulada por una ley especial o que no estén sometidos a ningún órgano o ente de prevención, control, supervisión, fiscalización y vigilancia. No obstante, su implementación operativa por parte del órgano rector se encuentra en instrumentación.

Lineamientos Técnico-Operativos

A. Unidad Nacional de Inteligencia Financiera (UNIF)

La Unidad Nacional de Inteligencia Financiera (UNIF), emitió la circular número UNIF-DG-DSU-04409 del 10 de noviembre de 2023, referida a las señales de alerta, controles internos y directrices relacionadas con los reportes de actividades sospechosas (RAS), la cual está dirigida específicamente a abogados, administradores, economistas y contadores en el libre ejercicio de sus profesiones, y tiene como objetivo la prevención de la legitimación de capitales y el financiamiento al terrorismo mediante la vigilancia de transacciones sospechosas.

En esta circular, se detallan múltiples señales de alerta, tanto cuantitativas como cualitativas, que estos profesionales deben monitorear para detectar comportamientos atípicos en sus clientes, así como el deber de implementar

controles internos basados en riesgos e informar cualquier irregularidad a las autoridades, enfatizando la confidencialidad de los reportes y prohibiendo revelar a terceros si una actividad ha sido denunciada ante la inteligencia financiera.

Dentro de los puntos clave detallados en la circular, se encuentran los siguientes aspectos:

1. Actividades Específicas: La circular señala que estos profesionales son considerados sujetos obligados cuando realizan transacciones para un cliente relacionadas con las siguientes actividades:

- Compraventa de bienes inmuebles
- Administración del dinero, valores y otros activos del cliente;
- Administración de cuentas bancarias, de ahorro o de valores;
- Organización de aportes para la creación, operación o administración de compañías;
- Creación, operación o administración de personas jurídicas o estructuras jurídicas, así como la compraventa de entidades comerciales.
- Se indica de manera específica que no está dirigida a profesionales de planta o "internos" que sean empleados de empresas y profesionales que trabajen para instituciones gubernamentales.

2. Señales de Alerta: El documento proporciona una lista detallada de indicadores para detectar comportamientos atípicos.

Cuantitativas: Estas señales se enfocan principalmente en el manejo de fondos, la naturaleza de las transacciones y las inconsistencias financieras. Incluyen:

- Identificación y opacidad: Operaciones donde no se logra identificar al beneficiario final o se utilizan arquitecturas comerciales y societarias para brindar opacidad sobre el origen de los fondos.
- Naturaleza de la operación: Transacciones que no parecen ser resultado de las actividades habituales del cliente, operaciones ficticias o con signos

de sobre/subfacturación, e identificación de estructuras corporativas que simulan operaciones.

- Manejo de efectivo y activos: Exceso de transacciones en efectivo, realización de múltiples operaciones financieras menores en nombre de clientes (depósitos, retiros, cambios de moneda) y traspasos de propiedad que sirven como pantalla para dinero ilícito.
- Inconsistencias de perfil: Clientes con estilos de vida que no guardan relación con sus ingresos o que muestran cambios económicos repentinos sin justificación. También se incluyen discrepancias entre los ingresos declarados al banco y la operatividad financiera real.
- Criptoactivos y banca: Movimientos en cuentas bancarias o billeteras virtuales sin documentación soporte, o transacciones de criptoactivos a través de casas de intercambio que no poseen licencias de la Superintendencia Nacional de Criptoactivos (Sunacrip).
- Personas Expuestas Políticamente (PEP): Clientes categorizados como PEP que intentan evitar la debida diligencia, que no justifican el origen de sus fondos o que inician negocios sin que se conozca la procedencia de su capital.
- Otras: Registros incompletos por parte del cliente, uso de instituciones no reguladas por la Superintendencia de las Instituciones del Sector Bancario de Venezuela (SUDEBAN) para compraventa de divisas, y pagos elevados por parte de Organizaciones Sin Fines de Lucro (OSFL) que no guardan relación con su objeto social

Cualitativas: Estas señales se centran en el comportamiento del cliente, la estructura de sus negocios y el cumplimiento de normativas. Incluyen:

- Estructura y documentación: Creación de estructuras societarias complejas que dificultan conocer al cliente, uso de documentos públicos o contables falsificados, y creación de vehículos corporativos o fideicomisos complejos.

- Comportamiento del cliente: Clientes que se niegan a suministrar información económica o sobre su composición accionaria, o empresas que se niegan a cumplir con controles de revisión física de inventario.
- Irregularidades en personas jurídicas: Aparición de una persona como dueño de varias empresas en poco tiempo, domicilios fiscales en zonas residenciales que no pueden ser verificados, o cambios constantes en la junta directiva sin justificación.
- Falta de transparencia y controles: Clientes con ausencia de sistemas de administración de riesgos de LC/FT/FPADM o que presentan informes de auditoría con irregularidades en sus controles internos.
- Antecedentes y sanciones: Clientes sancionados recurrentemente por autoridades gubernamentales o cuyos miembros (accionistas, directivos, clientes) aparezcan mencionados en noticias vinculadas a delincuencia organizada o en listas de sanciones del Consejo de Seguridad de las Naciones Unidas.
- Jurisdicciones de riesgo: Operaciones regulares hacia países catalogados como centros financieros offshore, paraísos fiscales o jurisdicciones de alto riesgo según el GAFI.
- Dádivas: Clientes que constantemente ofrecen o entregan regalos, invitaciones o dádivas sin una justificación clara y razonable.

3. Controles Internos y Cultura de Cumplimiento: Respecto a los controles internos, la circular impone a los profesionales en libre ejercicio la adopción de una "cultura de cumplimiento", la cual rechaza los estándares genéricos y exige políticas de administración integral del riesgo de LC/FT/FPADM e instaurar políticas y procedimientos de administración de riesgos proporcionales a su tamaño y volumen de operaciones. Esta infraestructura de control se vertebra sobre cinco pilares estratégicos:

- a. Proporcionalidad y Personalización: El sistema de control debe diseñarse a la medida del profesional, indexando su complejidad a la naturaleza, tamaño, volumen de operaciones, ubicación geográfica, nivel de riesgo y disponibilidad tecnológica.

- b. Debida Diligencia del Cliente (DDC): Obliga a implementar sistemas de información robustos para la identificación del cliente y del beneficiario final, prohibiendo taxativamente la representación de terceros sin una validación previa.
 - c. Mitigación de Vulnerabilidades Sectores: Los controles deben corregir directamente debilidades críticas, tales como la asimetría de conocimiento técnico, las fallas en la supervisión bajo el Enfoque Basado en Riesgo (EBR), la ausencia de un Oficial de Cumplimiento y la falta de medición del riesgo en la cartera de clientes.
 - d. Medidas Intensificadas: Exige la aplicación de debida diligencia reforzada ante clientes de alto riesgo o que presenten señales de alerta, alineándose rigurosamente con los estándares internacionales del GAFI.
 - e. Suficiencia Operativa y Tecnológica: Se exige el uso de los recursos humanos, logísticos y tecnológicos necesarios para monitorear transacciones y detectar comportamientos atípicos oportunamente, robusteciendo el análisis previo al envío de cualquier reporte a la UNIF.
4. Reportes de Actividades Sospechosas (RAS): Se instruye sobre la obligación de remitir reportes a la Unidad Nacional de Inteligencia Financiera (UNIF) de manera oportuna y con calidad documental. Se enfatiza que estos reportes deben basarse en un Enfoque Basado en Riesgo (EBR).

Operativamente, esta obligación se canaliza a través del Formulario RAS DGOE-008/2024 e Instructivo para la Elaboración de los Reportes de Actividades Sospechosas (RAS), diseñados específicamente para las Actividades y Profesiones No Financieras Designadas (APNFD) y publicadas por la UNIF el 30 de agosto de 2024.

En este orden de ideas, es imperativo señalar que la UNIF publica semestralmente informes de retroalimentación en los que se desglosa, entre otros indicadores, el volumen y la distribución porcentual de los RAS remitidos

por cada sector obligado. Históricamente, estos informes reflejan una recepción nula por parte de los profesionales jurídicos y financieros en libre ejercicio.

Este preocupante escenario invita a una profunda reflexión sobre la asimetría en la cultura de cumplimiento de este sector, sobre posibles puntos críticos como tergiversaciones respecto al alcance del secreto profesional y la urgente necesidad de fortalecer la supervisión y capacitación de estos profesionales.

5. Confidencialidad y Secreto Profesional: La circular no formula una definición teórica del secreto profesional, sino que delimita su alcance y aplicación legal frente a las obligaciones de reporte de los profesionales. Por un lado, consagra la prohibición de revelación (tipping-off), alineándose con la Recomendación N° 21 del GAFI, al establecer que los sujetos obligados no deben informar al cliente ni a terceros sobre el envío de un Reporte de Actividad Sospechosa (RAS) a la UNIF. Por el otro, exceptúa taxativamente la obligación de reportar si la información relevante fue obtenida bajo amparo del secreto profesional o del privilegio legal.

El documento advierte que el secreto profesional constituye una de las vulnerabilidades identificadas en el sector, ya que puede convertirse en una debilidad para los procesos de identificación del cliente y del origen de los fondos bajo un Enfoque Basado en Riesgo (EBR). Es decir, la circular reconoce el secreto profesional como un límite legal que prevalece sobre la obligación de reportar actividades sospechosas a la UNIF, siempre que la información se haya obtenido bajo ese amparo legal.

En este contexto, conviene resaltar que la Sentencia N° 0527 de la Sala Constitucional del Tribunal Supremo de Justicia (TSJ) de Venezuela, dictada el 10 de abril de 2025, estableció que los abogados, en el ejercicio de la representación judicial, actúan exclusivamente conforme al mandato otorgado por sus clientes y no como partícipes de los hechos materia del litigio, y por tanto, no se les puede atribuir responsabilidad penal por defender a sus representados,

ya que no se les considera asociados ni beneficiarios de los resultados del proceso.

B. Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT).

La ONCDOFT publicó una Evaluación Sectorial de Riesgos 2026, enfocada en las profesiones asociadas a abogados, contadores y agentes inmobiliarios en Venezuela, donde se señala que puntualmente en relación con los contadores y abogados que, la delincuencia organizada busca integrar a ambos sectores en una estratificación coordinada, utilizando a los abogados para crear estructuras opacas y los contadores para legitimar flujos de caja mediante el aseguramiento de ingresos, simulando operaciones además mediante contratos ficticios o facturas falsa

En consecuencia, esta evaluación examina los Organismos de Autorregulación (OAR), la composición, el tamaño de cada sector, y sus riesgos asociados. Asimismo, expone conclusiones, recomendaciones y el plan de supervisión basado en riesgos, tal como se detalla a continuación:

	Abogados	Contadores
Organismos de Autorregulación	Federación de Colegios de Abogados de Venezuela (FCAV) y los Colegios Estadales, siendo obligatoria además la inscripción en el INPREABOGADO	Federación de Colegios de Contadores Públicos de Venezuela (FCCPV). Todo profesional debe poseer el número de Contador Público Colegiado (CPC) y registrarse en el Registro Único de Actuación Profesional (RUAP) para habilitar sus actuaciones técnicas
Composición	333.343 profesionales a marzo de 2026.	172.024 agremiados a febrero de 2026
Calificación de Riesgo	ALTA	MODERADA
Principales Vulnerabilidades	Es el único sector donde los riesgos críticos por uso de efectivo en montos elevados no logran ser mitigados efectivamente.	La mayor amenaza es la identificación del Beneficiario Final en estructuras jurídicas complejas.

	Se identifica una carencia estructural de mecanismos sancionatorios y falta de automatización en la debida diligencia. Existe el riesgo de ser utilizados para la constitución de estructuras corporativas opacas que fragmentan el rastro del dinero.	Exposición crítica a ser utilizados por Personas Expuestas Políticamente (PEP) a través de empresas fachada.
Secreto Profesional	Se establece un equilibrio donde los "actos neutros" (defensa técnica) no constituyen complicidad, pero esto no exime al profesional del reporte de buena fe ante actividades sospechosas	Riesgo de conflictos éticos donde el profesional podría no reportar irregularidades por temor o malinterpretación del secreto profesional
Señales de Alerta	Solicitudes para crear empresas con socios extranjeros sin actividad comercial aparente, o la firma de balances que justifican capitales para compras inmobiliarias sin soporte documental previo.	
Diagnóstico de 25 IEM del GAFIC (4ta Ronda, 2016-2025)	Abogados y contadores son catalogados frecuentemente como facilitadores estratégicos, permitiendo el ingreso de flujos ilícitos mediante estructuras legales de alta complejidad que desafían las capacidades actuales de supervisión	

Fuente propia: **Rodríguez 2026**

La evaluación presenta un Plan de Supervisión en materia de LC/FT/FPADM 2026, en relación con los sectores de Abogados y Contadores presenta una transición de un modelo de control formalista hacia una Supervisión Basada en Riesgo (SBR). Su objetivo es dirigir los recursos del Estado hacia las áreas de mayor vulnerabilidad identificadas en la evaluación sectorial. A continuación, se resumen los ejes y acciones estratégicas del plan para estos profesionales:

1. Ejes Estratégicos de Supervisión: El plan define acciones diferenciadas según el perfil de riesgo de cada profesión

Para Abogados (Sector Prioritario):

- Monitoreo In Situ: Realización de inspecciones aleatorias para auditar la calidad de los expedientes de Debida Diligencia del Cliente (DDC) y la verificación del origen de los fondos.

- Gestión de Efectivo: Supervisión estricta de los protocolos de cobro y la exigencia de la bancarización obligatoria de honorarios para mitigar el riesgo crítico del manejo de grandes sumas de dinero.

Para Contadores Públicos:

- Control Extra Situ: Ejecución de auditorías digitales sobre los registros de visado y la verificación del cumplimiento de los Reportes de Actividades Sospechosas (RAS) ante la UNIF.

Acción Común (Todos los sectores):

- Identificación del Beneficiario Final (BF): Implementación de cruces de información entre los registros mercantiles y las declaraciones de BF para romper la opacidad corporativa.

2. Marco Estratégico de Medidas Preventivas: Se establecen protocolos que los profesionales deben integrar en su práctica diaria:

- Debita Diligencia Reforzada (DDR): Obligatoria para transacciones con Personas Expuestas Políticamente (PEP) y estructuras corporativas opacas.
- Levantamiento del Velo Corporativo: Procedimiento para identificar a la persona natural que posea al menos el 25% del capital o ejerza el control efectivo de una entidad.
- Mantenimiento de Registros: Conservación de toda la documentación de soporte por un período mínimo de 5 años.
- Reporte Obligatorio: Información oportuna a la Unidad Nacional de Inteligencia Financiera (UNIF) sobre cualquier actividad sospechosa.

3. Fases de Implementación (Cronograma 2026): El plan se ejecutará en dos etapas clave durante el año 2026:

Fase I (Segundo y Tercer Trimestre):

- Sensibilización y Capacitación: Talleres de simulación de casos reales sobre DDC, identificación de PEPs y señales de alerta.
- Adecuación Normativa: Mesas de trabajo para alinear las políticas internas de los profesionales con las nuevas guías técnicas de la ONCDOFT y la UNIF.

Fase II (Cuarto Trimestre):

- Ejecución de Inspecciones: Se iniciarán las inspecciones in situ para el sector de Abogados (calificado como riesgo Alto) y supervisiones extra situ para el sector de Contadores (calificado como riesgo Moderado).

Rol Estratégico de los Profesionales Jurídicos y Financieros en el Libre Ejercicio

En el marco de la prevención de LC/FT/FPADM, la actuación del profesional independiente ya no se limita a la prestación de un servicio técnico; se constituye como una función de control delegada por el Estado. Su rol estratégico se desglosa según su área de especialidad y las operaciones de riesgo que ejecutan por cuenta de terceros, aunque en la praxis pueden existir similitud e intercambio en los roles y flujos de información y no se limiten taxativamente a ello:

1. El Abogado y Asesor Legal (Gobernanza Corporativa y Estructuras Jurídicas): Su papel estratégico radica en blindar la creación de personas jurídicas, fideicomisos y vehículos societarios complejos. Al ser el profesional encargado de redactar actas constitutivas y sustanciar la compraventa de bienes inmuebles o entidades comerciales, actúa como el primer filtro contra la opacidad corporativa.

Su deber fundamental es aplicar una estricta Debida Diligencia del Cliente (DDC) para identificar fehacientemente al beneficiario final, evitando que su conocimiento del derecho sea instrumentalizado para diseñar empresas pantalla o estructuras destinadas a frustrar la labor de inteligencia financiera.

2. El Contador Público (Trazabilidad Financiera y Transparencia Patrimonial): Su rol estratégico es asegurar la integridad de la información financiera que ingresará o circulará en el sistema económico. Al preparar, auditar y dictaminar balances o estados financieros, el contador independiente valida la realidad económica de una entidad.

Su función preventiva consiste en detectar inconsistencias operativas o transacciones ficticias que pretendan justificar capitales ilícitos o encubrir delitos tributarios, debiendo mitigar el riesgo de que su firma dote de una falsa apariencia de legitimidad a flujos de efectivo de origen desconocido.

3. El Administrador (Gestión de Recursos y Custodia de Cuentas de Terceros): Su posición estratégica se ubica en el control directo de los flujos monetarios cuando es contratado para la administración de dinero, valores, cuentas bancarias o activos de los clientes, al gestionar operativamente la tesorería de un tercero, el administrador en libre ejercicio tiene acceso directo a la trazabilidad de los fondos.

Su rol exige el monitoreo continuo de señales de alerta cuantitativas, asegurando que el uso de las cuentas de los clientes responda estrictamente al objeto civil o mercantil del negocio y no sirva como canal de tránsito para la fragmentación o el lavado de dinero.

4. El Economista (Análisis de Viabilidad y Perfil de Riesgo de Negocio): Su rol estratégico aporta una visión macro y microeconómica en la organización de aportes para la creación, operación o administración de compañías, evaluando la coherencia de los modelos de negocio y el origen de los recursos para proyectos de inversión.

Su enfoque preventivo permite analizar la razonabilidad económica de transacciones complejas y determinar si el perfil financiero declarado por el cliente es consistente con la realidad del mercado, identificando de manera temprana operaciones y esquemas que muestren desviaciones técnicas evidentes.

Conclusiones Reflexivas

La inclusión taxativa de los profesionales jurídicos y financieros en libre ejercicio como sujetos obligados consolida la realidad global y nacional de que la prevención ya no es tarea exclusiva del sector financiero. Por el contrario, estos profesionales independientes se configuran hoy como una línea de defensa crucial frente a las redes de delincuencia organizada, las cuales buscan instrumentalizar la fe pública y el conocimiento técnico para el beneficio de sus operaciones ilícitas.

El reto estructural radica en que estos profesionales en libre ejercicio se enfrentan al desafío de ser en la praxis, sujeto obligado y Oficial de Cumplimiento dentro de su propia estructura y operaciones; esta dualidad operativa exige que la autoevaluación y el Enfoque Basado en Riesgo (EBR) no se asuman como meras formalidades burocráticas, sino como un blindaje dinámico, proporcional y personalizado a la naturaleza y volumen de sus operaciones comerciales.

En lo que respecta al Secreto Profesional y Deber de Reportar, las directrices nacionales e internacionales, reconocen el secreto profesional y el privilegio legal como límites operativos legítimos frente a la obligación de emitir un Reporte de Actividades Sospechosas (RAS). No obstante, este amparo legal no debe transformarse en una patente de opacidad; ya que opera exclusivamente cuando la información se obtiene en el ejercicio genuino de la defensa legal o la verificación del estatus jurídico, quedando estrictamente prohibido su abuso para encubrir la falta de identificación del beneficiario final o transacciones manifiestamente ficticias.

Siendo así, el rol de los profesionales jurídicos y financieros en libre ejercicio ha dejado de ser meramente técnico u operativo para transformarse en una función

de co-responsabilidad y salvaguarda del orden socioeconómico, constituyéndose como la barrera ética y jurídica de acceso al circuito económico legal.

Su valor estratégico radica en que poseen la capacidad exclusiva de neutralizar las tipologías delictivas en su origen, impidiendo que las organizaciones delincuenciales utilicen la ingeniería societaria, la fe pública o la validación contable para legitimar capitales de procedencia ilícita.

No obstante, aunque estos profesionales ya tienen años siendo llamados al cumplimiento, en la praxis operativa enfrenta aún grandes retos para alcanzar los niveles de cumplimiento y efectividad esperados, debiéndose adoptar sistemáticamente una serie de lineamientos:

- Diseñar manuales y procesos de cumplimiento a la medida y no genéricos, estructurando controles internos basados en su propia realidad operativa, el perfil de su cartera de clientes y la naturaleza de los servicios prestados
- Implementar protocolos reforzados de identificación que aseguren el conocimiento real del beneficiario final, en especial cuando se trate de Personas Expuestas Políticamente (PEP) o transacciones ligadas a criptoactivos sin licencias de los reguladores competentes.
- Monitorear activamente las Señales de Alerta Cualitativas y Cuantitativas, estableciendo revisiones periódicas que evalúen la consistencia del perfil financiero del cliente frente a sus actividades realizadas, prestando especial atención a inconsistencias operativas como el uso excesivo de efectivo, domicilios fiscales no verificables o el empleo de documentación contable adecuada a lineamientos normativos de los entes de control sobre la facturación y los mecanismos de pagos, para asegurar su validez.
- Garantizar de forma estricta que, ante la detección de un comportamiento atípico calificado como sospechoso, se realice el análisis y la remisión del RAS a la UNIF, bajo el más absoluto celo profesional, estando terminantemente prohibido revelar o alertar al cliente o a terceros sobre dichas actuaciones.
- Impulsar de manera efectiva el plan de supervisión en materia de LC/FT/FPADM 2026 para abogados y contadores, presentado en la

evaluación sectorial de riesgos realizada por la Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT), instrumentando el Registro Unificado de Sujetos Obligados (RUSO-ONCDOFT), a la par que se establezcan lineamientos y criterios de cumplimiento adaptados a las microestructuras operativas de los asesores independientes.

- Impulsar canales de coordinación entre los colegios profesionales y la Unidad Nacional de Inteligencia Financiera (UNIF) para promover el envío de reportes de actividades sospechosas (cuando aplique) y establecer metodologías que robustezcan la calidad de los insumos informativos de cara a la efectividad global del sistema preventivo nacional.

Referencias

Acceso a la Justicia (10 de abril de 2025). *El defensor penal o el apoderado civil no es cómplice, socio ni corresponsable con su cliente*. <https://accesoalajusticia.org/el-defensor-penal-o-el-apoderado-civil-no-es-complice-socio-ni-corresponsable-con-su-cliente/>

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

Grupo de Acción Financiera de Latinoamérica (GAFILAT, 2022). *Guía dirigida al sector de APNFD, para la construcción de una matriz de riesgos en prevención del lavado de activos y financiamiento al terrorismo (LA/FT)*. Disponible: <https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guia-para-la-construccion-de-Matriz-de-Riesgo-para-APNFD.pdf>

Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo. Gaceta Oficial de la República Bolivariana de Venezuela Número 39.912 de fecha 30 de abril de 2012.

Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT, 2026). *Evaluación Sectorial de riesgos de LC/FT/FPADM 2026 De abogados, contadores y Agentes inmobiliarios*. Disponible: <https://biblioteca.fccpv.org/>

Unidad Nacional de Inteligencia Financiera (UNIF, 2023). *Circular UNIF-DG-DSU-04409*. Disponible en: [https://www.unif.gob.ve/wp-content/uploads/Circulares_UNIF/CC_UNIF_04409\(2023-11-10\).pdf](https://www.unif.gob.ve/wp-content/uploads/Circulares_UNIF/CC_UNIF_04409(2023-11-10).pdf)

Unidad Nacional de Inteligencia Financiera (UNIF, 2024). *Circular UNIF-DDG-DGOE-003085*. Disponible en: [https://www.unif.gob.ve/wp-content/uploads/Circulares_UNIF/CC_UNIF-DDG-DGOE-003085_\(30_08_2024\).pdf](https://www.unif.gob.ve/wp-content/uploads/Circulares_UNIF/CC_UNIF-DDG-DGOE-003085_(30_08_2024).pdf)

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR DE ECONOMÍA Y FINANZAS
ESCUELA NACIONAL DE ADMINISTRACIÓN Y HACIENDA PÚBLICA
DIRECCIÓN DE POSTGRADO Y ADIESTRAMIENTO
ESPECIALIZACIÓN EN GESTIÓN CONTRA LEGITIMACIÓN DE CAPITALS Y
FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR SEÑALES DE ALERTA

**LA ADMINISTRACIÓN DE RIESGOS DE LEGITIMACIÓN DE CAPITALS,
FINANCIAMIENTO AL TERRORISMO Y FINANCIAMIENTO A LA
PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA EN VENEZUELA
Y LA IMPORTANCIA DE LA IDENTIFICACIÓN DE SEÑALES DE ALERTA,
PARA LA CONSOLIDACIÓN DE LA INTELIGENCIA FINANCIERA
NACIONAL.**

Autor: Abg. Esp. Jesús Mora
Facilitador: Prof. Lic. Elizabeth Peláez
Asesor metodológico: Prof. 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
DIRECCIÓN DE POSTGRADO Y ADIESTRAMIENTO
ESPECIALIZACIÓN EN GESTIÓN CONTRA LEGITIMACIÓN DE CAPITAL Y
FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR SEÑALES DE ALERTA

**LA ADMINISTRACIÓN DE RIESGOS DE LEGITIMACIÓN DE CAPITAL Y
FINANCIAMIENTO AL TERRORISMO Y FINANCIAMIENTO A LA
PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA EN VENEZUELA
Y LA IMPORTANCIA DE LA IDENTIFICACIÓN DE SEÑALES DE ALERTA,
PARA LA CONSOLIDACIÓN DE LA INTELIGENCIA FINANCIERA
NACIONAL.**

Autor: Esp. Jesús Mora

<https://orcid.org/0009-0007-3413-6933>

RESUMEN

En este Ensayo se realiza el análisis del Sistema Nacional de Prevención contra la Legitimación de Capitales, Financiamiento al Terrorismo y a la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM) en Venezuela. Alineado con los estándares internacionales del Grupo de Acción Financiera Internacional (GAFI), se destaca la importancia de identificar señales de alerta mediante un Enfoque Basado en Riesgo, especialmente ante el impacto de nuevas tecnologías como los activos virtuales y las financial technology *FINTECH* (tecnología financiera). El ensayo resalta el papel crítico de la primera línea de defensa de los sujetos obligados y la necesaria autonomía del Oficial de Cumplimiento para analizar operaciones inusuales y generar Reportes de Actividades Sospechosas (RAS) técnicos y oportunos. Un análisis comparativo revela asimetrías operativas: mientras el sector bancario muestra solidez regulatoria, las Actividades Profesionales No Financieras Designadas (APNFD) tales como: abogados, contadores, Casinos, Agentes Inmobiliarios, Comerciantes de metales preciosos y piedras preciosas, presentan vulnerabilidades estructurales y una supervisión aún incipiente. Finalmente, se aborda el rol estratégico de la Unidad Nacional de Inteligencia Financiera (UNIF), proponiendo la automatización total de los procesos para eliminar la manualidad en la entrega de reportes. Se concluye que la efectividad del sistema depende de cerrar la brecha entre el marco normativo y su implementación práctica, garantizando transparencia en la identificación del beneficiario final para fortalecer la integridad financiera nacional.

Descriptores clave: Señales de Alerta, LC/FT/FPADM, Enfoque Basado en Riesgos, UNIF, APNFD, Oficial de Cumplimiento.

ABSTRACT

This essay analyzes the National System for the Prevention of Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction (ML/TF/WMD) in Venezuela. Aligned with the international standards of the Financial Action Task Force (FATF), it highlights the importance of identifying warning signs through a Risk-Based Approach, especially given the impact of new technologies such as virtual assets and financial technology (Fintech). The essay emphasizes the critical role of the first line of defense for obligated entities and the necessary autonomy of the Compliance Officer to analyze unusual transactions and generate timely and technically sound Suspicious Activity Reports (SARs). A comparative analysis reveals operational asymmetries: while the banking sector demonstrates regulatory strength, Designated Non-Financial Businesses (DNFBPs), such as lawyers, accountants, casinos, real estate agents, and precious metals and gemstone dealers, exhibit structural vulnerabilities and still-developing supervision. Finally, the strategic role of the National Financial Intelligence Unit (UNIF) is addressed, proposing the complete automation of processes to eliminate manual reporting. It is concluded that the system's effectiveness depends on closing the gap between the regulatory framework and its practical implementation, ensuring transparency in identifying beneficial owners to strengthen national financial integrity.

Keywords: Red Flags, AML/CFT/AFP/DMW, Risk-Based Approach, UNIF, DNFBPs, Compliance Officer.

INTRODUCCIÓN

La Legitimación de Capitales, el Financiamiento al Terrorismo y el de la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM) son amenazas globales que exigen un Enfoque Basado en Riesgo (EBR). Para la República Bolivariana de Venezuela, esto es un desafío estratégico tras su inclusión en la "Lista Gris" del GAFI en 2024. Aunque el marco normativo nacional —respaldado por la Constitución, la LOCDFT y la reciente Resolución 010.25 de la SUDEBAN (2025)— se ha robustecido, la aparición de activos virtuales y tecnologías Fintech obliga a los Sujetos Obligados a dinamizar la detección de señales de alerta. En este sistema, el Oficial de Cumplimiento es el eje central para proveer inteligencia financiera a la UNIF mediante los Reportes de Actividades Sospechosas (RAS). Sin embargo, persisten asimetrías críticas en sectores vulnerables como las APNFD (abogados, contadores y agentes inmobiliarios).

Frente a este panorama, este ensayo analiza críticamente los componentes del sistema preventivo venezolano, evaluando las señales de alerta tecnológicas, la autonomía del Oficial de Cumplimiento y el rol de la UNIF. Finalmente, mediante un análisis comparativo entre el sector financiero y el profesional, se identificarán las brechas operativas actuales y se formularán propuestas viables para optimizar la eficiencia del régimen común y cumplir con los estándares internacionales de integridad.

I

Identificación de Señales de Alerta y el Impacto de las Nuevas Tecnologías

Las señales de alerta son indicadores o comportamientos de clientes, empleados o transacciones que se apartan de los parámetros de normalidad y sugieren una posible vinculación con actividades ilícitas.

En Venezuela, la identificación de estas señales debe basarse en un Enfoque Basado en Riesgo (EBR), considerando cuatro factores principales: clientes, productos/servicios, zona geográfica y canales de distribución.

A. Tipos de señales de alerta por Factor:

Cliente: Inconsistencias entre el perfil financiero y las operaciones realizadas (causa principal de reportes en 2025), el uso de testaferros, Usurpación de Identidad o la negativa a revelar la condición de Persona Expuesta Políticamente (PEP).

Producto/Servicio: Cancelaciones anticipadas de pólizas en efectivo, compraventa sucesiva de un mismo inmueble por montos inconsistentes o transacciones estructuradas para eludir umbrales de reporte.

Zonas Geográficas: Operaciones vinculadas o realizadas en zonas fronterizas con alta porosidad o jurisdicciones calificadas como de alto riesgo por el GAFI.

B. Uso de nuevas tecnologías y activos virtuales

La digitalización financiera ha introducido riesgos emergentes. La Resolución 010.25 de la SUDEBAN y la ENR 2024 destacan la vulnerabilidad de las Fintech y los Proveedores de Servicios de Activos Virtuales (PSAV).

Señales de alerta:

Criptoactivos: Uso de anonimizadores de IP, rotación de IP (IP Rotation) o Proxy Swarming, pitufeo digital (Digital Smurfing) o estructuración, operaciones en la Dark Web, o la minería digital no autorizada como mecanismo para ofuscar el origen de los fondos.

Banca Digital: El auge de plataformas de pago móvil (P2P, C2P) facilita el fraccionamiento de fondos para evitar controles tradicionales.

Canales virtuales: El uso de plataformas que interactúan con exchanges no autorizadas por la Superintendencia Nacional de Criptoactivos (SUNACRIP) representa un nivel crítico de exposición.

II. Sujetos Obligados y la Estructura de la Primera Línea de Defensa

Los sujetos obligados son todas las personas naturales o jurídicas sometidas a la supervisión de un ente de control por mandato de la LOCDOFT.

- Su estructura interna es fundamental para la detección temprana.

A. Estructura y Áreas Sensibles

La normativa venezolana exige que los sujetos obligados cuenten con un Sistema Integral de Administración de Riesgos de LC/FT/FPADM (SIAR LC/FT/FPADM) que incluya:

- Junta Directiva
- Presidente
- Oficial de Cumplimiento

- Unidad de Prevención y Control (UPC y/o UAR LC/FT/FPADM y Otros Ilícitos (OI): También presta apoyo a la gestión técnica y operativa del Oficial de Cumplimiento y algunas regulaciones no consideran la obligatoriedad de conformación, siendo la Responsable del análisis de operaciones financieras y la elaboración de estadísticas.
- Responsables de Cumplimiento

Primera Línea de Defensa: Personal de taquilla, ventas y atención al cliente. Son los responsables de conocer el inicio del negocio y detectar los patrones o comportamientos derivados de información relacionada con delitos de LC/FT/FPADM/YOI y las actitudes sospechosas de forma inmediata.

Áreas Sensibles: Departamentos que manejan altos volúmenes de efectivo, transferencias internacionales o la apertura de cuentas para personas jurídicas con estructuras complejas y es el contacto inicial de la relación comercial y permite detectar actitudes, comportamientos fuera de los parámetros de normalidad y obtiene los documentos que permiten identificar al tercero, en ese lugar se debe designar un Responsable de Cumplimiento.

B. Autonomía del Oficial de Cumplimiento

El Oficial de Cumplimiento debe tener un rango de alto nivel y autonomía para decidir si una operación inusual califica como sospechosa.

- Se requiere dedicación exclusiva a la Administración de Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento a la Proliferación de Armas de Destrucción Masiva (AR/LC/FT/FPADM)
- Su criterio es determinante para evaluar si existen elementos de juicio suficientes para considerar si una transacción califica para elaborar un RAS sin interferencias de la gerencia comercial, basándose en la debida diligencia periódica y actualizada, así como la autonomía suficiente para realizar el mismo.

III. Correcta Elaboración del Reporte de Actividades Sospechosas (RAS)

El RAS no es una denuncia penal, sino una herramienta de inteligencia financiera que no genera responsabilidad penal o civil para quien la emite, siempre que actúe de buena fe.

- Criterios de calidad en la elaboración (Instructivo PE-UNIF-005)

Un RAS eficiente debe responder técnica y cronológicamente a seis interrogantes:

- ¿Quién? Identificación plena de los implicados, incluyendo beneficiarios finales y PEPs.
- ¿Qué? Descripción precisa de las técnicas, mecanismos e instrumentos financieros utilizados.
- ¿Cuándo? Fechas de advertencia y duración de la actividad.
- ¿Dónde? Sucursales o jurisdicciones extranjeras involucradas.
- ¿Por qué? Justificación cualitativa de la sospecha basada en el perfil financiero del cliente.
- ¿Cómo? Método utilizado para realizar la transacción o el conjunto de operaciones.

Se prohíbe estrictamente la revelación al cliente de que está siendo objeto de un análisis o reporte (principio de no revelación o tipping-off).

IV. Impacto de la Unidad Nacional de Inteligencia Financiera (UNIF)

La UNIF es la autoridad administrativa central en Venezuela encargada de recolectar, centralizar y analizar los RAS generados por los sujetos obligados

para detectar patrones delictivos y activar los procesos de investigación ante los órganos de seguridad del Estado.

Funciones Estratégicas

Análisis y Confirmación: Transforma los reportes crudos en inteligencia procesable para el Ministerio Público cuando existen indicios de hechos punibles.

Retroalimentación: Emite boletines y ejercicios de tipologías para educar a los sectores sobre nuevas amenazas.

Cooperación Internacional: Actúa como enlace con el Grupo Egmont y homólogos extranjeros para el seguimiento de capitales transnacionales.

Limitaciones Identificadas por Organismos Internacionales

Observadores como el Grupo de Acción Financiera del Caribe (GAFIC) y consultoras regionales han señalado que la efectividad de la UNIF se ve afectada por:

Manualidad de procesos: Muchos RAS aún se entregan físicamente en ventanilla, lo que retrasa el análisis.

Recursos limitados: La cantidad de funcionarios analistas se considera insuficiente comparada con el volumen de transacciones del país y la complejidad de los casos vinculados a la corrupción y el tráfico de drogas

V. Análisis Comparativo Sectorial y Sectores Faltantes

El sistema preventivo en Venezuela muestra niveles de madurez asimétricos entre sus diversos actores.

Sector	Fortalezas	Debilidades / Vulnerabilidades
Bancario	Sólida regulación (SUDEBAN), alta automatización y 90% de los RAS emitidos.	Exposición a remesas no reguladas y uso excesivo de efectivo.
Seguros	Nueva ley con sanciones severas basadas en el tipo de cambio de mayor valor.	Riesgo en siniestros ficticios para recuperar fondos ilícitos.
Valores	Monitoreo de títulos valores.	Bajo volumen de reportes (0,1% del total).
APNFD (Abogados/ Contadores)	Identificados como "guardianes" clave del sistema.	Alta informalidad, falta de mecanismos de visado obligatorio para identificar beneficiarios finales.
Inmobiliario	Intermediación en activos de valor estable.	Sector preferente para integrar fondos de corrupción por opacidad en la valoración.

Fuente: Mora 2026

-Sectores que requieren mayor inclusión o supervisión

Aunque la ley los menciona, existe una brecha operativa en:

- Cooperativas de servicios financieros: A menudo operan sin el mismo rigor de auditoría que la banca tradicional.
- Proveedores de servicios societarios y fiduciarios: Especialmente aquellos que proveen domicilios fiscales para empresas que pudieran ser fachada.
- Sector inmobiliario informal: Un gran número de agentes operan sin estar afiliados a la Cámara Inmobiliaria, eludiendo la supervisión.

VI. Propuestas de Mejora y Recomendaciones

Para optimizar el Sistema Nacional de Lucha contra la LC/FT/FPADM, se proponen las siguientes acciones:

Automatización Total de la UNIF: Transitar obligatoriamente hacia el reporte digital electrónico para todos los sectores, eliminando la entrega física en ventanilla para mejorar la oportunidad de la inteligencia financiera.

Fortalecimiento de las APNFD: Implementar el visado obligatorio de actuaciones profesionales (abogados y contadores) vinculado a una declaración jurada de origen de fondos, lo que permitiría a la UNIF cruzar datos de manera más eficiente.

Identificación Centralizada del Beneficiario Final: Crear un registro nacional único y digital accesible para los entes de control, rompiendo la opacidad de las empresas fachada y las sociedades espejo en el extranjero.

Capacitación Especializada en FT y FPADM para todos los sectores, que incluya a los organismos de seguridad e investigación del Estado: Dado que los reportes se centran excesivamente en LC, es vital instruir a los sujetos obligados en tipologías específicas de financiamiento al terrorismo, especialmente en zonas fronterizas y para Organizaciones Sin Fines de Lucro (OSFL).

Independencia Presupuestaria de la UNIF: Garantizar que la unidad cuente con recursos técnicos y humanos suficientes, alineados con el riesgo jurisdiccional de Venezuela (Lista Gris del GAFI), para mejorar su capacidad de investigación y persecución.

Debida Diligencia Reforzada Obligatoria para PEPs: Sin importar el monto de la transacción, cualquier operación que involucre a una persona expuesta políticamente debe ser sometida a un escrutinio intensificado automático.

Conclusiones (Reflexiones)

Desafíos y Perspectivas del Sistema Nacional de Lucha contra la LC/FT/FPADM en Venezuela.

I. El Fortalecimiento del Marco Normativo y el Compromiso Internacional

La República Bolivariana de Venezuela ha transitado por un proceso de profunda reestructuración de su marco regulatorio para alinearse con los Estándares Internacionales del GAFI. El hito más reciente y significativo en este ámbito es la promulgación de la Resolución 010.25 de la SUDEBAN (2025), la cual deroga normativas anteriores para introducir una actualización integral que incorpora de manera explícita el Financiamiento a la Proliferación de Armas de Destrucción Masiva (FPADM)

Esta resolución no sólo amplía el catálogo de definiciones, incluyendo conceptos modernos como Fintech, Activos Virtuales y Crowdfunding, sino que ratifica la obligatoriedad del Enfoque Basado en Riesgo (EBR) como eje rector de la administración de riesgos.

Paralelamente, la ejecución de la Evaluación Nacional de Riesgo (ENR 2024) representó un ejercicio de introspección estratégica que permitió identificar 44 riesgos de impacto nacional.

Este documento es fundamental, ya que permite al Estado y a los sujetos obligados comprender las amenazas reales del entorno, tales como el uso del mercado paralelo de divisas, la porosidad fronteriza y el impacto de las nuevas tecnologías.

Sin embargo, este avance normativo se produce en un contexto de alta presión internacional tras la inclusión de Venezuela en la "Lista Gris" del GAFI en junio de 2024.

Esta designación impone la necesidad de demostrar no solo el cumplimiento técnico (leyes en papel), sino la efectividad sistémica, que es el grado en que los resultados definidos se logran en la práctica.

El compromiso político de alto nivel asumido por el país busca precisamente cerrar esa brecha para mejorar la percepción de riesgo jurisdiccional.

II. La Brecha de Implementación: El Desafío de los Sectores No Financieros (APNFD)

A pesar de la solidez del marco legal en el sector bancario, el sistema preventivo venezolano presenta una asimetría operativa crítica en las Actividades Profesionales No Financieras Designadas (APNFD) tales como: abogados, contadores, Casinos, Agentes Inmobiliarios, Comerciantes de metales preciosos y piedras preciosas, identificados internacionalmente como gatekeepers o guardianes, presentan vulnerabilidades estructurales debido a la falta de una legislación de desarrollo específica.

El Informe de Evaluación Mutua (IEM) del GAFIC señala que muchos de estos profesionales no se consideran a sí mismos sujetos obligados, a pesar de estar contemplados en la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT), lo que genera vacíos jurídicos que la delincuencia organizada puede explotar para la estratificación de fondos.

En el análisis sectorial, se observa que:

Sector Inmobiliario: Es el tercer sector más vulnerado en la región. En Venezuela, se han identificado tipologías de compraventa sucesiva de inmuebles para ofuscar el rastro del dinero, representando un porcentaje significativo de los motivos de reporte.

Abogados y Contadores: Su rol es ambivalente. Si bien la Sentencia 0527-2025 protege el secreto profesional en "actos neutros", esto no los exime de la

responsabilidad de aplicar la Debida Diligencia del Cliente (DDC) y reportar actividades sospechosas de buena fe.

El riesgo en estos sectores se califica a menudo como "crítico" o "alto" debido al uso excesivo de efectivo y la dificultad para identificar al beneficiario final en estructuras corporativas opacas.

La efectividad del sistema depende de transitar hacia una Supervisión Basada en Riesgo (SBR) que sea proactiva y no meramente administrativa.

Esto implica que las inspecciones in situ deben auditar la calidad real de los controles internos y no solo la existencia de manuales documentales.

III. Modernización de la UNIF y Fortalecimiento de la Inteligencia Financiera

El tercer pilar para la efectividad sistémica radica en el fortalecimiento institucional de la UNIF. Las fuentes revelan limitaciones operativas que afectan la oportunidad de la inteligencia financiera en el país. Uno de los hallazgos más preocupantes es la manualidad de los procesos, los sujetos obligados a menudo presentan los RAS de forma impresa en ventanilla, lo que retrasa el análisis y aumenta el riesgo de manipulación de datos.

Para que Venezuela salga de la "Lista Gris", es imperativo automatizar totalmente el sistema de reportes a través de plataformas digitales seguras.

Además, la UNIF enfrenta desafíos en cuanto a recursos humanos y presupuestarios. Con una plantilla limitada de analistas para procesar miles de reportes anuales, la carga de trabajo por funcionario se considera insuficiente comparada con otras Unidades de Inteligencia Financiera de la región.

- La modernización debe incluir:

Independencia operativa y presupuestaria: Para garantizar que las decisiones de análisis financiero no se vean afectadas por influencias externas.

Capacitación especializada: Es vital formar al personal en la detección de tipologías emergentes vinculadas al Financiamiento al Terrorismo (FT) y el uso de activos virtuales, áreas donde el conocimiento nacional todavía es calificado como moderado o limitado.

Cooperación Interinstitucional: La coordinación horizontal entre la UNIF, el Ministerio Público y los órganos auxiliares como el CICPC es fundamental para transformar los reportes de inteligencia en sentencias condenatorias efectivas.

En conclusión, Venezuela posee las herramientas normativas de vanguardia (Resolución 010.25 y ENR 2024), pero el éxito del sistema nacional contra la LC/FT/FPADM se medirá por su capacidad para sincerar las evaluaciones de riesgo y demostrar resultados tangibles en la judicialización de los delitos precedentes, especialmente la corrupción y el tráfico de drogas.

Solo mediante una supervisión inteligente de las APNFD y una UNIF modernizada y robusta, el país podrá garantizar la integridad de su sistema financiero y cumplir con los estándares de seguridad y transparencia exigidos por la comunidad internacional.

Referencias

Cámara Inmobiliaria de Venezuela (CIV). (2026). Evaluación sectorial de riesgos de legitimación de capitales, financiamiento al terrorismo y financiamiento de la proliferación de armas de destrucción masiva: Sectores abogados, contadores y agentes inmobiliarios.

Gaceta Oficial de la República Bolivariana de Venezuela. (2012, 30 de abril). Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo. (Número 39.912).

Grant Thornton Venezuela. (2025). Nota informativa: Comparación de la Resolución 010.25 y la Resolución 083.18 de SUDEBAN para la administración y supervisión de los riesgos de LC/FT/FPADM.

Grupo de Acción Financiera Internacional (GAFI). (2019). Orientación para un enfoque basado en riesgos para profesionales legales.

<https://www.fatf-gafi.org/publications/documents/Guidance-EBR-legal-professionals.html>

Grupo de Acción Financiera Internacional (GAFI). (2025). Estándares internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva: Actualización a agosto de 2025. <https://www.fatf-gafi.org>

Grupo de Acción Financiera del Caribe (GAFIC). (2023). Medidas antilavado de dinero y contra la financiación del terrorismo: República Bolivariana de Venezuela, Informe de Evaluación Mutua. <https://www.fatf-gafi.org/en/countries/global-network/caribbean-financial-action-task-force--cfatf-.html>

Grupo de Acción Financiera de Latinoamérica (GAFILAT). (2022). Guía dirigida al sector de APNFD, para la construcción de una matriz de riesgos en prevención del lavado de activos y financiamiento al terrorismo (LA/FT). <https://www.gafilat.org>

Grupo de Acción Financiera de Latinoamérica (GAFILAT). (2024). Cuarta actualización del informe de amenazas regionales en materia de lavado de activos y financiamiento del terrorismo 2022-2023. <https://www.gafilat.org>

Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT). (2024). Evaluación Nacional de Riesgo (ENR) en Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva. Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz.

Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT). (2026). Informe Técnico N° 002-26: Sistematización y análisis de las observaciones de la 4ta ronda evaluaciones mutuas del Grupo de Acción Financiera del Caribe (GAFIC) / APNFD / 2016-2025. Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz.

Rodríguez, J. P., Castro, R. M., & Rueda, C. A. (2024). Venezuela incluida en la Lista Gris del GAFI: ¿Cuál es su impacto en el riesgo jurisdiccional? RICS Management.

RSM Global. (2026). The power of being understood: Regional perspectives and economic outlook for Latin America 2026. <https://www.rsm.global>

Unidad Nacional de Inteligencia Financiera (UNIF). (2019). Instructivo para la elaboración del Reporte de Actividades Sospechosas (PE-UNIF-005).

Unidad Nacional de Inteligencia Financiera (UNIF). (2025). XII Ejercicio de tipologías 2025: Informe ejecutivo. <https://www.unif.gob.ve>

Unidad Nacional de Inteligencia Financiera (UNIF). (2026). Atribuciones de la Unidad Nacional de Inteligencia Financiera. <https://www.unif.gob.ve/informacion-institucional/atribuciones/>

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 Señales de Alerta

**Áreas sensibles y gestión de riesgos: rol de los responsables de
cumplimiento en la detección de señales de alerta en el sector asegurador
y valores.**

Autora: Abog. Yabandra N. Lorca Cabeza

Facilitadora: Lic. Elizabeth Peláez

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 Señales de Alerta

Áreas sensibles y gestión de riesgos: rol de los responsables de cumplimiento en la detección de señales de alerta en el sector asegurador y valores.

Autor (a): Abog. Yabandra N. Lorca Cabeza
Correo electrónico: yabandralorca@gmail.com
<https://orcid.org/0009-0003-5803-3825>

Resumen

La gestión de riesgos de legitimación de capitales, financiamiento al terrorismo, financiamiento de la proliferación de armas de destrucción masiva (LC/FT/FPADM) en los sectores de seguros y valores en Venezuela ha evolucionado hacia un enfoque proactivo mediante el Sistema Integral de Administración de Riesgos (SIAR). La herramienta estratégica fundamental de este sistema son las **señales de alerta**, indicadores cualitativos y cuantitativos que detectan comportamientos atípicos ajenos al perfil del cliente o de las contrapartes. Como quiera que el Oficial de Cumplimiento no puede supervisar cada transacción, la normativa contempla unos actores ejecutivos, dentro de ellos se prevé una figura única de la normativa local: los **"responsables de cumplimiento"** y responsables de primera línea de contacto, en los sectores seguros y valores respectivamente, quienes actúan como la primera línea de defensa en las áreas sensibles de riesgo de los sujetos obligados. Estos responsables operativos tienen la obligación técnica y supervisora de identificar, documentar y reportar de forma mensual cualquier operación inusual. El levantamiento oportuno de estas alertas es el insumo esencial para elaborar el Reporte de Actividades Sospechosas (RAS) enviado a la Unidad de Inteligencia Financiera (UNIF), activando el ecosistema preventivo y penal, lo que permitiría una mitigación efectiva, la estructura organizativa, fundamentada en el rol efectivo de estos actores ejecutivos, fortaleciendo la malla de protección definitiva para salvaguardar la integridad y estabilidad reputacional e institucional del sujeto obligado.

Descriptor clave: Señales de Alerta, SIAR, Responsables de Cumplimiento, RAS.

Abstract

Risk management regarding money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction (ML/TF/FPWMD) in Venezuela's insurance and securities sectors has evolved toward a proactive approach through the Comprehensive Risk Management System (SIAR). The fundamental strategic tool of this system consists of "red flags"—qualitative and quantitative indicators that detect atypical behaviors inconsistent with the profiles of clients or counterparties. Since the Compliance Officer cannot oversee every transaction, the regulations provide for specific executive roles—including a figure unique to local regulations known as "compliance officers" (distinct from the chief compliance officer) and "front-line contact officers" in the insurance and securities sectors, respectively—who act as the first line of defense in high-risk areas for obligated entities. These operational officers bear the technical and supervisory obligation to identify, document, and report any unusual transaction on a monthly basis. The timely raising of these alerts serves as the essential input for generating the Suspicious Activity Report (SAR) submitted to the Financial Intelligence Unit (UNIF), thereby activating the preventive and criminal enforcement ecosystem to enable effective mitigation; the organizational structure, grounded in the active role of these executive officers, thus strengthens the ultimate protective framework safeguarding the integrity as well as the reputational and institutional stability of the obligated entity.

Key descriptors: Red Flags, SIAR, Compliance Leads, RAS.

Introducción

Las señales de alerta constituyen una herramienta estratégica fundamental en la lucha contra la delincuencia organizada para las organizaciones, al actuar como el mecanismo primario de detección temprana y mitigación ante operaciones sospechosas vinculadas a estas amenazas, permitiendo identificar y frenar a tiempo eventos de riesgos de legitimación de capitales, financiamiento al terrorismo y proliferación de armas de destrucción masiva.

La presencia de una o varias señales de alerta sirve como detonante para que el sujeto obligado inicie un seguimiento y examen más profundo de un cliente o transacción. Si bien, una sola señal puede no ser prueba de delito, la concurrencia de múltiples indicadores sin una explicación comercial lógica genera la sospecha necesaria para actuar.

La importancia de las señales de alerta radica en que constituyen la base para el Reporte de Actividades Sospechosas (RAS), que son el insumo esencial para que el Oficial de Cumplimiento y las áreas sensibles de riesgo y/o primera línea de contacto determinen la necesidad de elaborar y enviar un Reporte de Actividad Sospechosa (RAS) a la unidad de inteligencia financiera (UNIF).

Un diseño correcto del Sistema de Administración de Riesgos (SIAR) depende de la capacidad de identificar estas “señales de alerta” en cada sector.

En este sentido, el presente ensayo busca analizar el impacto de la estructura organizativa de los sujetos obligados en la correcta identificación y gestión de alertas desde las áreas sensibles y/o primera línea de contacto como se denominan en los sectores seguros y valores, respectivamente en Venezuela.

1. La administración de riesgos el nuevo paradigma en la administración de riesgos de legitimación de capitales, financiamiento al terrorismo, financiamiento de la proliferación de armas de destrucción masiva.

En el actual escenario financiero, la administración de riesgos de Legitimación de Capitales (LC), Financiamiento al Terrorismo (FT) y Financiamiento de la Proliferación de Armas de Destrucción Masiva (FPADM) ha pasado de un cumplimiento normativo reactivo para transformarse en una estrategia proactiva basada en la prevención y el control.

En este sentido, según Negrón y Chang (2021), “La estructura creada por la normativa sublegal venezolana responde a los estándares internacionales y las mejores prácticas recogidas en la materia, de donde puede señalarse que Venezuela tiene además una figura única y pocas veces observadas en otras jurisdicciones, que son los “*responsables de cumplimiento*” en cada una de las áreas sensibles de riesgo dentro de la estructura interna del sujeto obligado.

En este contexto la normativa del sector asegurador, la Providencia Administrativa N° SAA-01-536-2024, de fecha 29 de agosto de 2024, publicada en la Gaceta Oficial N° 6.835 de fecha 03 de septiembre de 2024, establece el

deber para los Sujetos Obligados de implementar un Sistema Integral de Administración de Riesgos (SIAR) de LC/FT/FPADM y Otros Ilícitos que sea capaz de identificar, medir y mitigar las amenazas delictivas.

El núcleo operativo de este sistema parte de la identificación de “áreas sensibles de riesgos”, siendo preponderante en este contexto el rol estratégico que desempeñan un eslabón de la cadena preventiva, como lo son los “*responsables de cumplimiento*”, actores ejecutivos que tienen una particularidad importante en el caso del SIAR, ya que esta figura únicamente existe en los sistemas de administración de riesgos de nuestro país, tal como bien lo sostienen Negrón y Chang supra mencionados.

Estos actores ejecutivos (responsables de cumplimiento), actúan como la primera línea de defensa en la detección de comportamientos atípicos dentro de la organización, es este caso el sector asegurador y el mercado de valores venezolano.

Por su parte en el caso del mercado de valores, la Providencia N° 025 de fecha 17 de marzo de 2025, publicada en la Gaceta Oficial N°43.096 de fecha 27 de los mismos, mes y año, integra dentro de la conformación del SIAR LC/FT/FPADM y otros ilícitos dos (2) actores ejecutivos, como lo son “*el responsable de cumplimiento designado en cada área sensible de riesgo de LC/FT/FPADM y otros ilícitos*” y “*los responsables de primera línea de contacto*”

2. Identificación de Áreas Sensibles mediante la Autoevaluación de Riesgo.

Las áreas sensibles de riesgos de LC/FT/FPADM y otros ilícitos, no son estáticas; su determinación surge del proceso de autoevaluación de riesgo, es decir, del análisis retrospectivo y prospectivo, en donde el Sujeto Obligado identifica sus propias vulnerabilidades. Este proceso permite segmentar los riesgos en niveles alto, moderado y bajo, atendiendo a factores críticos como el tipo de clientes, la naturaleza de los productos o servicios, los canales de

comercialización y las zonas geográficas donde se opera o donde están domiciliados los clientes.

Ahora bien, conforme lo señalan los instrumentos normativos supra referidos, los *“responsables de cumplimiento”* son designados precisamente en estas áreas sensibles, identificadas previamente por su mayor exposición al riesgo de ser utilizadas por la delincuencia organizada.

3. Definición y perfil del “responsable de cumplimiento.”

Dentro de la estructura del SIAR, el responsable de cumplimiento es el personal seleccionado de las áreas de riesgo o agencias que funge como enlace directo con la Unidad de Administración de Riesgos de LC/FT/FPADM y Otros Ilícitos o el Oficial de Cumplimiento, según corresponda. Su designación es obligatoria y debe ser individualizada por escrito, especificando claramente sus funciones adicionales a las propias de su cargo dentro de la institución.

Este actor debe poseer un conocimiento profundo de la normativa vigente y de la operatividad específica de su área para poder supervisar la observancia de los controles internos de manera efectiva.

En este sentido, para el sector asegurador, conforme a la Providencia Administrativa N° SAA-01-0536-2024, antes mencionada, los responsables de cumplimiento tienen funciones específicas, dentro de las cuales entre otras encontramos, la referida a la remisión a la Unidad de AR/LC/FT/FPADM y otros ilícitos y al Oficial de Cumplimiento, en la forma, tiempo y modo que se establezca, la información relacionada sobre operaciones inusuales o actividades sospechosas, o en su defecto, notificar el no haber tenido conocimiento de la realización de alguna de éstas en el mes inmediato anterior a la fecha de notificación.

En este mismo orden, la Providencia N° 025, de fecha 17 de marzo de 2025 del mercado de valores, impone el deber a los responsables de primera línea de contacto, de informar al respectivo responsable de cumplimiento, de su área o

directamente al oficial de cumplimiento las operaciones o actividades inusuales observadas en el desempeño de sus labores o en el entorno laboral, que a su juicio pudieran estar relacionadas con delitos de LC/FT/FPADM y otros ilícitos. (Artículo 31 de la providencia supra mencionada).

Esta obligación, de los responsables de cumplimiento de primera línea de contacto, es similar al contenido del artículo 18 de la Providencia Administrativa N° SAA-01-0536-2024 de seguros, con la salvedad de que esta obligación es genérica, y como bien lo prevé la norma in comento: *“Cualquier empleado debe informar a la Unidad de AR/LC/FT/FPADM y otros ilícitos o al Oficial de Cumplimiento en lo aplicable, sobre irregularidades en la observancia de las disposiciones legales y reglamentarias vigentes o derivadas del Manual de Políticas, Normas y Procedimientos en materia de AR/LC/FT/FPADM y otros ilícitos”*.

En consonancia con esto, quien escribe considera que evidentemente en el caso de los dos sectores referidos, existe un vínculo entre la operatividad y el cumplimiento, toda vez que las funciones atribuidas por la normativa para estos actores ejecutivos del SIAR es estratégica, ya que el rol de los “responsables de cumplimiento” y los “responsables de cumplimiento de primera línea de contacto” es eminentemente técnico y supervisor.

4. Detección de Señales de Alerta: El Indicador de Riesgo.

La detección de señales de alerta es un proceso continuo que abarca todo el ciclo de vida de la relación comercial: desde la vinculación contractual y el cierre del negocio, hasta el monitoreo transaccional y la actualización periódica de datos de clientes y contrapartes.

En este sentido, visto que es operativamente inviable que el Oficial de Cumplimiento supervise directamente cada interacción y transacción de las contrapartes, resulta indispensable que quienes son responsables en las áreas operativas de los sujetos obligados, (responsables de cumplimiento y los responsables de primera línea de contacto) observen e informen a este,

cualquier inusualidad que escape de los perfiles transaccionales u operacionales, es decir, que estén atentos a cualquier señal de alerta.

Las señales de alerta se definen como el conjunto de indicadores cualitativos y cuantitativos que permiten identificar oportunamente comportamientos atípicos. Sobre este particular González Quiroz (2024), define las Señales de Alerta como: “Situaciones u operaciones que escapen de la normalidad estipulada por el Sujeto Obligado. Es el conjunto de indicadores cualitativos y cuantitativos que permiten identificar oportuna y/o prospectivamente comportamientos atípicos de las variables relevantes, previamente determinadas por la entidad.

Constituyen una herramienta para que el sujeto obligado, a través del análisis del área de Compliance, pueda identificar operaciones inusuales o sospechosas.”

En este mismo sentido, la referida autora, indica que conforme lo define el Grupo de Acción Financiera de Latinoamérica (GAFILAT) “Las señales de alerta son elementos que permiten detectar la posible presencia de operaciones de “lavado de activos”. Son situaciones, operaciones, transacciones, características atípicas, distintas, que superan los patrones de normalidad que el mismo Sujeto Obligado ha estipulado”.

Estos indicadores son claves para que, en las distintas áreas sensibles de riesgos, se activen los protocolos internos del sujeto obligado para estructurar y remitir un Reporte de Actividad Sospechosa (RAS) o Reporte de Operación Sospechosa (ROS). No obstante, debemos tener en cuenta la mera presencia de una señal de alerta no es necesariamente una base para una sospecha de LC/FT/FPADM, pero podría impulsar un mayor monitoreo y examen, siendo que, en última instancia, un cliente puede suministrar una explicación que justifique las señales de alerta y los propósitos de la operación.

Ante este supuesto de que la señal de alerta arroje indicios para un RAS, tras recibirlo, la Unidad Nacional de Inteligencia Financiera (UNIF) ejecuta el análisis técnico correspondiente y, de hallar méritos, lo eleva a la categoría de Informe de Inteligencia Financiera con destino al Ministerio Público. La fiscalía evaluará la viabilidad de la acción penal y, de corroborarse los indicios de criminalidad,

esa alerta primigenia se consolidará como el detonante del proceso penal, culminando en la investigación, imputación, juicio y eventual condena del autor por el delito de lavado de activos.

Bajo esta perspectiva, en la práctica de gestión de riesgos de legitimación de capitales, financiamiento al terrorismo, financiamiento de la proliferación de armas de destrucción masiva y otros ilícitos, es evidente que las señales de alerta no son simples trámites de monitoreo automatizado, sino que constituyen una pieza del escudo preventivo, dentro de las líneas de defensa (la alerta en el sujeto obligado), por lo que si estos no detectan ni escalan de forma oportuna y con el debido sustento técnico las alertas tempranas, se genera un vacío de información que neutraliza la labor del resto de los actores del ecosistema.

Dicho esto, nos encontramos que, en los sectores asegurador y valores, estas señales pueden manifestarse en operaciones que, por su cuantía, frecuencia o naturaleza, no guardan relación con el perfil económico del cliente. Por lo que es responsabilidad ineludible del “responsable de cumplimiento” y “los responsables de cumplimiento de primera línea de contacto” remitir al Oficial de Cumplimiento cualquier operación inusual o actividad sospechosa detectada en su área, o en su defecto, notificar formalmente la ausencia de tales hallazgos al cierre de cada mes.

Partiendo de lo antes dicho, podemos indicar que los responsables de cumplimiento y los responsables de cumplimiento de primera línea de contacto, tienen el deber de levantar señales de alertas y reportarlas al Oficial de Cumplimiento, velar por la efectividad en el cumplimiento normativo interno y externo por parte de todos los colaboradores del sujeto obligado, coadyuvando así en la implementación del SIAR.

Los responsables de cumplimiento en las áreas comerciales deben prestar especial atención a los intermediarios de la actividad aseguradora, conforme lo estipula la normativa de este sector.

En este sentido, las señales de alerta, en este sector incluyen cambios repentinos en el estilo de vida del intermediario, niveles elevados de endeudamiento o un incremento desproporcionado de carteras con prima única sin justificación económica clara.

5. Indicadores de Riesgo y Señales de Alerta en Operaciones con Activos Virtuales (Criptoactivos).

El ecosistema de activos virtuales es utilizado de forma prioritaria por organizaciones criminales para la legitimación de capitales, aprovechando las brechas en la implementación global de los estándares del Grupo de Acción Financiera Internacional (GAFI), actualizados al período 2024-2025. Estas plataformas suelen ser explotadas en las fases de estratificación (superposición) e integración, buscando el anonimato y la evasión de controles transfronterizos tradicionales.

En este sentido, podemos mencionar algunas de las principales señales de alerta metodológicas que los sujetos obligados deben incorporar en sus sistemas de monitoreo automatizado y matrices de riesgo:

1. Inconsistencia en el Perfil Transaccional (Fraccionamiento y Tipologías): Alerta: Detección de operaciones recurrentes, estructuradas en montos exactos o calibradas deliberadamente justo por debajo del umbral de reporte obligatorio (*smurfing* o pitufeo), con el fin de eludir los sistemas de alerta temprana.

2. Riesgo Geográfico y Jurisdicciones No Cooperantes: Alerta: Flujos de fondos dirigidos hacia, o provenientes de, países con deficiencias estratégicas en sus sistemas Antilavado de Activos/Contra Financiamiento al Terrorismo (ALA/CFT), específicamente aquellos incluidos en las listas grises y negras del GAFI, o zonas con nula regulación sobre Proveedores de Servicios de Activos Virtuales (PSAV).

3. Vulnerabilidades en la Identificación del Cliente (Debida Diligencia / KYC): Alerta: Modificaciones atípicas y constantes en el perfil digital del usuario, presentación de documentación de identidad de dudosa legitimidad o

inconsistencias graves en los procesos de conocimiento del cliente. Esto incluye indicios de suplantación de identidad o creación de identidades sintéticas.

4. Uso de Tecnologías de Ofuscación y Anonimato: Alerta: Utilización deliberada de herramientas orientadas a romper la trazabilidad de la cadena de bloques (*blockchain*), tales como servicios de mezcla (*mixers o tumblers*), criptomonedas de alta privacidad (orientadas al anonimato), y operaciones recurrentes en plataformas *Peer-to Peer* (P2P) sin controles regulatorios.

Estas plataformas *Peer-to-peer* (P2P), o "red entre pares", es una arquitectura descentralizada donde computadoras o usuarios se conectan e interactúan directamente (de igual a igual) sin necesidad de un servidor central o intermediario. Cada nodo actúa simultáneamente como cliente y servidor, compartiendo recursos, datos o servicios.

Como es sabido, *Blockchain*, o cadena de bloques, es un libro de contabilidad digital distribuido que almacena datos de cualquier tipo. Una cadena de bloques puede registrar información sobre transacciones de criptomonedas, propiedad de *NFT* o contratos inteligentes *DeFi*.

En este mismo contexto, los mezcladores de criptomonedas, también conocidos como *tumblers* o *blenders*, son servicios que combinan y redistribuyen los cryptoactivos de múltiples usuarios para ocultar el flujo de fondos.

5. Opacidad en el Origen de los Fondos: Alerta: Negativa, resistencia o incapacidad del cliente para demostrar el origen lícito y la trazabilidad de sus cryptoactivos, especialmente cuando los fondos provienen de protocolos de Finanzas Descentralizadas (DeFi) o redes de billeteras complejas y multinivel.

6. Comportamiento Anómalo en las Billeteras (*Wallets*): Alerta: Migración repentina y sin justificación económica entre billeteras con custodia (plataformas reguladas) y billeteras sin custodia (auto-custodia), interacción con direcciones identificadas en listas de sanciones, o patrones de actividad que no coinciden con el perfil transaccional histórico del usuario.

La presencia de uno o más de estos indicadores no constituye por sí misma una prueba de delito, pero activa de forma inmediata la obligación de ejecutar una Debida Diligencia Intensificada (DDI) y, de ser el caso, procesar el Reporte de Actividad Sospechosa (RAS) ante la unidad de inteligencia financiera correspondiente.

Ahora bien, desde esta perspectiva, la gestión moderna de riesgos exige que los sistemas informáticos tengan la capacidad de detectar operaciones inusuales, señales de alerta en tiempo real por lo que, el SIAR debe contar con herramientas tecnológicas que permitan emitir reportes de concentración de productos por un mismo cliente o grupo económico.

En tal sentido, los responsables de cumplimiento, de los sectores mencionados en este ensayo deben apoyarse en estas herramientas para generar alertas tempranas, especialmente en operaciones efectuadas mediante nuevas tecnologías, *Insurtech (de insurance y technology)* lo que implica la unión entre la tecnología y el sector de los seguros, es decir, las empresas y soluciones digitales que modernizan la industria aseguradora o criptoactivos, donde el anonimato puede ser mayor y se requiere una Debida Diligencia Intensificada.

La gestión de riesgos no se limita a clientes externos. Los responsables de cumplimiento también deben vigilar la conducta del personal interno, prestando atención a señales como el rechazo a promociones o traslados, el no disfrute de vacaciones o la recepción de regalos y dádivas de clientes sin justificación

Cualquier comportamiento inusual de un empleado debe ser notificado de inmediato para su análisis, ya que las debilidades en el control interno por imprudencia o negligencia pueden favorecer la comisión de ilícitos

En conclusión, las señales de alerta constituyen la piedra angular estratégica en el ecosistema de administración de riesgos de LC/FT/FPADM y otros ilícitos, toda vez que funcionan como el “mecanismo primario de detección temprana”, que permite a los sujetos obligados identificar y mitigar operaciones sospechosas

antes de que se conviertan en daños reputacionales o legales. La presencia de uno o varios de estos indicadores actúa como el detonante que obliga a la institución a iniciar un seguimiento y examen más profundo de una transacción o cliente.

Es allí donde el rol de los responsables de cumplimiento es vital para garantizar la efectividad del SIAR de LC/FT/FPADM y otros ilícitos, toda vez que las áreas sensibles de riesgo del sujeto obligado garantizan que el flujo de información hacia el Oficial de Cumplimiento sea veraz y oportuno, permitiendo que la institución detecte y reporte actividades sospechosas antes de que se materialicen daños reputacionales o legales.

Es por ello que resulta fundamental que esta labor de los responsables de cumplimiento y de los responsables de cumplimiento de primera línea de contacto, sea respaldada por un sólido buen gobierno corporativo y herramientas tecnológicas avanzadas, constituye la malla de protección definitiva que salvaguarda la solvencia y la transparencia del sector asegurador y de valores frente a las amenazas globales de la delincuencia organizada.

En la práctica, debido a que la delincuencia organizada actualiza constantemente sus métodos, estas señales de alerta deben ser dinámicas, exigiendo un análisis sistémico permanente durante todas las etapas del delito. Además, su alcance es integral, pues cubren tipologías específicas tanto para la legitimación de capitales como para el financiamiento al terrorismo y la proliferación de armas de destrucción masiva.

Referencias

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

González Quiroz, Nahyr C. (2024). Ebook: Alerta en el Sector Financiero – Identificar y notificación de señales de alerta Lavado de Dinero en: <https://www.riskglobalconsulting.com/ebook/identificar-y-notificacion-de-senales-de-alerta-lavado-de-dinero>

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

Providencia N° 025 del 17 de marzo de 2025. Normas relativas a la Administración 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, aplicables a los sujetos obligados por la Superintendencia Nacional de Valores. Gaceta Oficial de la República Bolivariana de Venezuela. N° 43.096 de 27 de marzo de 2025.

Providencia N°SAA-01-536 del 29 de agosto de 2024, publicada en la Gaceta Oficial N° 6.835 de fecha 03 de septiembre de 2024. Normas sobre administración de riesgos de legitimación de capitales, financiamiento al terrorismo, financiamiento de la proliferación de armas de destrucción masiva y otros ilícitos en la actividad Aseguradora.

REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR DE ECONOMÍA Y FINANZAS
ESCUELA NACIONAL DE ADMINISTRACIÓN Y HACIENDA PÚBLICA
DIRECCIÓN DE POSTGRADO Y ADIESTRAMIENTO
PROGRAMA DE ESPECIALIZACIÓN EN GESTIÓN CONTRA LA
LEGITIMACIÓN DE CAPITALES Y FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR SEÑALES DE ALERTA

**DE LA DETECCIÓN TEMPRANA A LA MITIGACIÓN DEL RIESGO 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
Facilitador: Lic. Elizabeth Peláez
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
DIRECCIÓN DE POSTGRADO Y ADIESTRAMIENTO
PROGRAMA DE ESPECIALIZACIÓN EN GESTIÓN CONTRA LA
LEGITIMACIÓN DE CAPITALES Y FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR SEÑALES DE ALERTA

DE LA DETECCIÓN TEMPRANA A LA MITIGACIÓN DEL RIESGO 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
ID <https://orcid.org/0009-0003-5594-9520>
Correo electrónico: alonso.brito61@gmail.com

RESUMEN

El sector asegurador por su esencia y funcionamiento se hace apetecible para la Delincuencia Organizada, ya que con el dinero obtenido de los delitos obtienen bienes muebles e inmuebles que luego deciden ampararlos con una póliza de seguros cuya prima es cancelada con dinero ilícito; una vez emitida la póliza pueden solicitar la anulación anticipada de la misma y la empresa de seguros debe hacerles una devolución de la prima no devengada. En otro caso pueden hacer un reclamo de un siniestro, es decir, el riesgo se materializó por lo que la empresa de seguros hará un análisis del reclamo sin encontrar medios probatorios que permitan rechazarlo, por lo cual deben proceder con la indemnización. En cada uno de estos procesos se pueden detectar señales de alerta, las cuales deben ser revisadas, analizadas y de acuerdo al hecho que persista la alerta puede generarse un Reporte de actividad sospechosa que debe ser reportada a la Unidad Nacional de Inteligencia Financiera, así como también, generar las medidas de mitigación correspondientes, que permitan actuar y mantener un control y monitoreo sobre los riesgos.

DESCRIPTORES: Señales de Alerta, Detección, Mitigación, Reguladores, Sujetos Obligados, Riesgos, Sector Asegurador, Legitimación de Capitales, Financiamiento al Terrorismo, Financiamiento a la Proliferación de Armas de Destrucción Masiva.

ABSTRACT

The insurance sector, due to its essence and operation, is attractive to Organized Crime, since with the money obtained from crimes they obtain movable and

immovable property that they then decide to protect with an insurance policy whose premium is paid with illicit money; Once the policy has been issued, they can request the early cancellation of the policy and the insurance company must refund the unearned premium. In another case, they can make a claim for a claim, that is, the risk materialized, so the insurance company will make an analysis of the claim without finding evidence that allows it to be rejected, so they must proceed with compensation. In each of these processes, warning signs can be detected, which must be reviewed, analyzed and according to the fact that the alert persists, a suspicious activity report can be generated that must be reported to the National Financial Intelligence Unit, as well as generate the corresponding mitigation measures, which allow action and maintain control and monitoring of risks.

DESCRIPTORS: Warning Signs, Detection, Mitigation, Regulators, Obligated Subjects, Risks, Insurance Sector, Money Laundering, Financing of Terrorism, Financing of the Proliferation of Weapons of Mass Destruction.

INTRODUCCIÓN

La actividad aseguradora, por su propia naturaleza de dispersión de riesgos y manejo de grandes flujos de capital, se encuentra en una posición de vulnerabilidad frente a las redes de criminalidad organizada. Los delitos de Legitimación de Capitales (LC), Financiamiento al Terrorismo (FT) y el Financiamiento de la Proliferación de Armas de Destrucción Masiva (FPADM) y Otros Ilícitos, representan amenazas multidimensionales que no solo socavan la estabilidad financiera de las compañías de seguros, sino que comprometen la integridad del sistema económico global.

La estabilidad y la integridad de los sistemas financieros globales dependen, en gran medida, de la capacidad de sus ecosistemas para blindarse frente a las dinámicas delictivas del siglo XXI. En este contexto, la actividad aseguradora ha dejado de ser vista como una industria periférica para convertirse en un objetivo estratégico del crimen organizado. Los delitos de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva no solo erosionan la confianza en la Actividad Aseguradora, sino que comprometen la seguridad jurídica y financiera de los países.

El sector asegurador presenta una arquitectura de riesgos singular, caracterizada por productos de inversión a largo plazo, complejas redes de

intermediación y una multiplicidad de beneficiarios que, frecuentemente, son instrumentalizados para la integración de fondos de origen ilícito en el sistema económico formal.

Históricamente, la gestión de estos riesgos en el sector se limitaba a modelos estáticos y reactivos, centrados en el cumplimiento procedimental básico. Sin embargo, ante el perfeccionamiento de las técnicas delictivas, el paradigma actual exige una transición hacia un enfoque dinámico y proactivo, basado fundamentalmente en la identificación temprana de señales de alerta y la mitigación robusta mediante el Enfoque Basado en Riesgo, como lo señala la Recomendación N° 1 del Grupo de Acción Financiera Internacional (GAFI), es por ello que la respuesta institucional ya no depende únicamente de la detección, sino de la capacidad de las aseguradoras para articular una respuesta operativa eficaz que logre reducir el riesgo inherente a niveles residuales aceptables, sin desatender sus obligaciones de debida diligencia intensificada.

La eficacia de la prevención de LC/FT/FPADM en la actividad aseguradora no reside exclusivamente en la sofisticación tecnológica de los sistemas de monitoreo, sino en la integración sinérgica entre una cultura de cumplimiento arraigada en las empresas y un sistema integral de administración de riesgos que permita transitar, de manera fluida y coherente, desde la detección temprana de anomalías conductuales hasta la implementación de medidas de mitigación proporcionales y eficaces.

1. El Contexto del Riesgo en el Sector Asegurador

Para comprender la necesidad de una detección temprana, es fundamental identificar cómo operan estos delitos en la actividad aseguradora. A diferencia de la banca, donde las transacciones son inmediatas y de alta frecuencia, el sector asegurador ofrece capas de complejidad a través de la suscripción, emisión de pólizas, beneficiarios y devoluciones de primas por cancelaciones anticipadas.

Como señala Sarmiento (2018), el lavado de activos en el sector asegurador no busca la velocidad, sino la legitimidad a largo plazo. Al pagar una prima con

fondos ilícitos y luego cancelar la póliza o reclamar un siniestro, el delincuente recibe una indemnización mediante un cheque o transferencia de una entidad bancaria, integrando efectivamente el dinero en el torrente financiero de ese país.

Por su parte, el Financiamiento al Terrorismo y el Financiamiento a la Proliferación de Armas de Destrucción Masiva, presentan retos aún más complejos, ya que los fondos utilizados pueden ser de origen totalmente lícito, pero su destino final es el financiamiento de actividades terroristas o la adquisición de tecnologías sancionadas internacionalmente.

2. La Detección Temprana: Señales de Alerta y Debida Diligencia

La detección temprana constituye la primera línea de defensa en el Enfoque Basado en Riesgo (EBR). Consiste en la capacidad de la empresa de seguros para identificar incongruencias o comportamientos inusuales antes o durante la contratación del servicio.

El pilar fundamental de esta etapa es la Debida Diligencia del Cliente (DDC) o *Know Your Customer (KYC)*. Según el Grupo de Acción Financiera Internacional (GAFI, 2012), las instituciones deben ir más allá de la simple recopilación de documentos de identidad, deben comprender el propósito de la relación comercial y determinar el "Beneficiario Final".

Factores de Riesgo Clave

De acuerdo con las guías de supervisión de la Asociación Internacional de Supervisores de Seguros (IAIS, 2020) y la metodología para la autoevaluación de riesgos establecida en la providencia Administrativa Nro. SAA-01-0536-2024, emanada de la Superintendencia de la actividad aseguradora, la detección temprana debe segmentar el riesgo en cuatro factores esenciales:

Clientes: Identificación de Personas Expuestas Políticamente (PEP), estructuras jurídicas opacas o clientes de sectores de alta intensidad de efectivo.

Productos: Pólizas de vida individual con componente de ahorro, contratos de capitalización o pólizas de grandes riesgos comerciales con primas inusualmente elevadas.

Canales de Comercialización: Ventas a través de intermediarios (corredores o agentes) que impiden el contacto directo con el cliente, o plataformas digitales sin la debida verificación biométrica o tecnológica.

Zonas Geográficas: Operaciones vinculadas a jurisdicciones no cooperantes o sancionadas por el Consejo de Seguridad de las Naciones Unidas.

Las herramientas tecnológicas avanzadas, como los algoritmos de *Machine Learning* (Permite a las computadoras aprender de los datos y mejorar sin recibir órdenes directas) y el monitoreo transaccional automatizado, permiten a las aseguradoras establecer "señales de alerta" automatizadas. Un ejemplo de esto es el pago de primas fraccionadas por parte de terceros no relacionados, o solicitudes de reembolso dirigidas a cuentas en paraísos fiscales.

3. De la Detección a la Mitigación: El Enfoque Basado en Riesgo (EBR)

Detectar a tiempo carece de valor si la organización no cuenta con la infraestructura operativa para mitigar el impacto. La transición entre la detección y la mitigación se articula mediante el Sistema Integral de Administración del Riesgo de Legitimación de Capitales, Financiamiento al Terrorismo y el Financiamiento a la Proliferación de Armas de Destrucción Masiva y Otros Ilícitos.

Blanco (2021) enfatiza que mitigar no significa "evitar el riesgo a toda costa", sino gestionarlo de acuerdo con el apetito de riesgo de la empresa y los límites legales. Cuando la detección temprana arroja un nivel de riesgo "Alto", la mitigación exige la aplicación de una Debida Diligencia Intensificada. Esto implica:

- Obtener la aprobación de la alta gerencia para mantener la relación comercial.
- Indagar exhaustivamente sobre el origen de los fondos y el patrimonio del cliente.
- Someter la póliza y al cliente a un monitoreo continuo y estrecho.

Si los controles de mitigación no logran disipar la duda razonable sobre la licitud de la operación, o si se confirma una coincidencia con listas de sanciones internacionales restrictivas, la aseguradora, tiene la obligación ineludible de emitir de inmediato un Reporte de Actividad Sospechosa ante la Unidad Nacional de Inteligencia Financiera (UNIF).

Seguidamente se detallan los procesos metodológicos y tecnológicos más efectivos para la detección de señales de alerta en el sector asegurador:

1. Segmentación Dinámica de Clientes y Canales (EBR):

El Enfoque Basado en Riesgo (EBR) exige que las señales de alerta se configuren de acuerdo con el perfil específico del cliente. El método de segmentación consiste en agrupar a los asegurados según variables homogéneas de riesgo (edad, nacionalidad, actividad económica, origen de fondos y canales de distribución).

- **Modelado de Comportamiento Habitual:** El sistema establece una "línea base" de lo que es un comportamiento normal para un segmento específico (por ejemplo, un comerciante local que contrata una póliza de salud estándar).
- **Disparadores de Desviación (Triggers):** La señal de alerta se activa automáticamente cuando el cliente se desvía drásticamente de su segmento sin una justificación económica lógica. Por ejemplo, si ese mismo comerciante contrata repentinamente una póliza de vida con fines de inversión por una prima millonaria pagada en efectivo o desde una cuenta en el extranjero.

2. Implementación de Matrices de Riesgo Automatizadas

Las matrices de riesgo son el corazón del monitoreo preventivo. Los métodos modernos utilizan sistemas transaccionales que asignan un puntaje de riesgo (scoring) en tiempo real durante la fase de suscripción del seguro.

- **Filtros de Coincidencia Automatizados (Sanction Screening):** Es el método inmediato de detección temprana. Consiste en contrastar en tiempo real las bases de datos de la aseguradora con listas restrictivas globales de alta actualización (como las listas OFAC, las listas del Consejo de Seguridad de la ONU para FPADM, y los listados de la Unión Europea).
- **Ponderación de Variables:** La matriz no evalúa las señales de forma aislada. Si un cliente es una Persona Expuesta Políticamente (PEP) (Riesgo Medio-Alto) y contrata una póliza de seguros a través de un intermediario en una zona fronteriza de alto riesgo (Riesgo Alto) y solicita cláusulas de rescate anticipado (Riesgo Alto), el sistema consolida un score crítico que analiza el riesgo antes de la emisión de la póliza.

3. Tipificación Regulatoria y "Banderas Rojas" de Producto

Las señales de alerta deben estructurarse metodológicamente según las etapas del contrato de seguro: Suscripción, Emisión (Pago de Primas), Vigencia y Siniestro/Indemnización. A continuación, se presenta una tabla con los métodos de detección a través de "Banderas Rojas" (Red Flags) específicas para la actividad aseguradora:

Etapas del Seguro	Método de Detección / Señal de Alerta (Red Flag)	Riesgo Asociado
Suscripción	* Clientes que muestran un desinterés inusual por las condiciones de cobertura o costos, pero extrema urgencia por cerrar el contrato. * Uso de estructuras jurídicas opacas (empresas fachada) donde es imposible identificar al Beneficiario Final (Persona Natural).	LC / FT

Etapa del Seguro	Método de Detección / Señal de Alerta (Red Flag)	Riesgo Asociado
Vigencia y Pagos	* Pago de primas mediante múltiples transferencias fraccionadas por importes justo por debajo del umbral de reporte obligatorio (<i>pitufeo</i>). * Primas pagadas por terceros (personas naturales o jurídicas) que no guardan ninguna relación familiar o comercial aparente con el asegurado.	LC
Siniestro o Indemnización	* Solicitud de cancelación anticipada de pólizas de vida-inversión a los pocos días de su emisión, aceptando penalizaciones económicas severas con tal de recibir un cheque de reembolso de la aseguradora. * Siniestros reportados sospechosamente rápido tras la contratación de la póliza, o reclamaciones donde los beneficiarios están ubicados en zonas de conflicto o bajo sanciones por terrorismo, es decir, Jurisdicciones clasificadas por el GAFI.	LC / FT / FPADM
Fuente A. Brito (2026)		

4. Análisis de Datos Avanzado y Redes de Vínculos (Link Analysis)

Los métodos tradicionales de detección temprana basados en reglas fijas ("si pasa de \$X monto, alerta") suelen generar un alto volumen de falsos positivos. Por ello, los métodos avanzados incorporan tecnologías de análisis de datos complejas:

- **Minería de Datos y Machine Learning:** Permite descubrir patrones ocultos. Por ejemplo, el sistema puede detectar que diez pólizas de ramos comerciales distintos (cascos, transporte, fianzas) tienen un denominador común sutil: el mismo perito tasador, el mismo intermediario y un origen de fondos proveniente de un mismo grupo de empresas *offshore* (Compañías registradas en jurisdicciones diferentes a su domicilio o en Paraísos Fiscales).
- **Análisis de Grafos (Redes de Vínculos):** Este método mapea visual y digitalmente las conexiones entre tomadores, asegurados, beneficiarios, intermediarios y médicos. Es una herramienta indispensable para identificar

redes de delincuencia organizada que intentan diluir el rastro del dinero atomizando los contratos en diferentes ramos de la aseguradora.

5. El Factor Humano: Canales de Denuncia e Inteligencia de Intermediarios

Ninguna tecnología sustituye el criterio del personal en la primera línea de defensa. El método aquí se centra en la capacitación especializada de los intermediarios de seguros (corredores y agentes).

- **Debida Diligencia Conductual:** El intermediario es quien tiene el contacto cara a cara o digital directo con el proponente. Los manuales de cumplimiento deben entrenar al intermediario para detectar conductas evasivas, inconsistencias en el lenguaje corporal, o la incapacidad del cliente para explicar de forma coherente a qué se dedica su negocio.
- **Canales Éticos de Denuncia (*Whistleblowing*):** Mecanismos anónimos y seguros para que empleados o intermediarios reporten sospechas de complicidad interna, ya que las redes de LC/FT/FPADM y Otros Ilícitos, suelen buscar la captación de empleados de las aseguradoras para facilitar el ingreso de fondos ilícitos saltándose los controles automáticos.

Medidas de Mitigación del Riesgo de LC/FT/FPADM y Otros ilícitos en la Actividad Aseguradora

Una vez que los sistemas de detección temprana identifican un riesgo inusual o un perfil elevado, la empresa de seguros debe desplegar de inmediato medidas de mitigación operacionales, organizacionales y tecnológicas. Mitigar el riesgo en seguros no implica rechazar todo negocio complejo, sino aplicar salvaguardas que reduzcan el riesgo inherente a un nivel de riesgo residual aceptable para la organización y los reguladores.

1. Clasificación Metodológica de las Medidas de Mitigación

Las estrategias de mitigación en el sector asegurador se dividen en tres grandes dimensiones interconectadas:

A. Controles sobre la Política de Suscripción y Emisión

El diseño de los productos de seguros debe incorporar "cortafuegos" desde su origen para evitar que las tipologías criminales se materialicen:

- **Restricciones en el Uso de Efectivo:** Establecer umbrales máximos estrictos o la prohibición absoluta del cobro de primas en efectivo para todos los ramos. Las transacciones deben realizarse obligatoriamente a través del sistema bancario regulado para garantizar la trazabilidad de los fondos.
- **Políticas de Rescate y Cancelación Controladas:** Limitar las cláusulas que permitan reembolsos rápidos en efectivo o mediante cheques a favor de terceros no vinculados. En caso de cancelación anticipada de una póliza, el dinero debe ser devuelto exclusivamente a la misma cuenta bancaria de origen del tomador originario.

B. Gobierno Corporativo y Cultura de Cumplimiento

Como sostienen López y Martínez (2022), la efectividad de un sistema de mitigación no radica solo en el *software* (conjunto de programas, instrucciones y reglas para ejecutar ciertas tareas en una computadora u ordenador) de monitoreo, sino en el compromiso de la junta directiva y en la independencia del Oficial de Cumplimiento.

- **Estructura de las Tres Líneas de Defensa:** La mitigación exige que la primera línea (intermediarios y suscripción) actúe como un filtro ético; la segunda línea (el Oficial de Cumplimiento) evalúe y diseñe las metodologías; y la tercera línea (auditoría interna) verifique la efectividad real de estos controles de forma independiente.

C. Debida Diligencia Intensificada (DDI)

Cuando el cliente, el canal o la jurisdicción representan un riesgo superior a la media, se despliega la Debida Diligencia Intensificada. Esto implica un análisis

cualitativo profundo que incluye la verificación del origen de la riqueza (*Source of Wealth*) y del origen de los fondos (*Source of Funds*), asegurando que el patrimonio guarde perfecta concordancia con la actividad económica declarada por el asegurado.

2. Marco Tecnológico para la Mitigación del FPADM

La mitigación del Financiamiento de la Proliferación de Armas de Destrucción Masiva (FPADM) requiere un tratamiento diferenciado. Mientras que en la Legitimación de Capitales se mitiga evaluando el comportamiento del cliente, en el FPADM el riesgo es predominantemente binario: existe o no existe una coincidencia con las listas de sanciones internacionales.

Las medidas de mitigación técnicas incluyen:

- **Congelamiento Preventivo Inmediato:** Las aseguradoras deben poseer sistemas capaces de suspender la emisión de la póliza o retener previa orden judicial, cualquier pago de siniestro o indemnización en el mismo instante en que se detecte una coincidencia exacta (match) con las listas del Consejo de Seguridad de la Organización de las Naciones Unidas (ONU).
- **Bloqueo de Coberturas en Ramos de Grandes Riesgos:** Monitorear con especial rigurosidad los seguros de transporte marítimo, aviación y cascos, asegurándose de que las rutas, mercancías o banderas de los buques no estén vinculadas a programas nucleares o regímenes sancionados.

3. Normativa Legal Internacional y Nacional Reguladores

El sustento jurídico que obliga y define la implementación de estas medidas de mitigación se divide en el *soft law* (conjunto de normas, principios, recomendaciones y códigos de conducta que no tienen fuerza jurídica obligatoria ni vinculante, pero que poseen relevancia e influencia práctica en el mundo) internacional y la legislación local obligatoria:

Marco Internacional

- **Recomendaciones 1 y 28 del GAFI:** La Recomendación 1 establece la obligación de aplicar el Enfoque Basado en Riesgo para mitigar las amenazas detectadas. Por su parte, la Recomendación 28 detalla la regulación y supervisión específicas para el sector de los seguros.
- **Estándar de Supervisión de Seguros (ICP 22) de la IAIS:** La Asociación Internacional de Supervisores de Seguros determina en su Insurance Core Principle 22 que los supervisores locales deben exigir a las aseguradoras medidas de mitigación eficaces, proporcionales a los riesgos identificados en sus Evaluaciones Internas de Riesgo.
- **Venezuela, Superintendencia de la Actividad Aseguradora (SUDEASEG):** Regulado formalmente bajo la Providencia Administrativa N° SAA-01-0536-2024, que establece las normas relativas a la administración de los riesgos relacionados con los delitos de LC/FT/FPADM y Otros Ilícitos en la Actividad Aseguradora.

Conclusiones

La evolución de la actividad aseguradora en el escenario contemporáneo demuestra que la gestión de los riesgos de LC/FT/FPADM ha dejado de ser una obligación periférica o un mero ejercicio de verificación de listas para consolidarse como un pilar estratégico de la gobernanza corporativa.

La transición analizada a lo largo de este ensayo, que va desde el despliegue de sistemas de detección temprana hasta la ejecución de medidas de mitigación proporcionales, revela que la seguridad del sector no depende de la rigidez de sus controles, sino de su capacidad de adaptación. El Enfoque Basado en Riesgo (EBR), promovido por el GAFI y la norma prudencial emanada de la Superintendencia de la Actividad Aseguradora, ha demostrado ser el único marco metodológico capaz de conciliar la rentabilidad del negocio con la preservación de la integridad financiera global.

El primer y más apremiante reto futuro radica en la convergencia entre la transformación digital de la industria (*Insurtech*) y la sofisticación del crimen financiero transnacional. La proliferación de canales de comercialización no presenciales, la automatización extrema de la suscripción digital y el uso de contratos inteligentes (*smart contracts*) basados en tecnología *blockchain* (base de datos digital compartida y descentralizada que guarda información en bloques unidos de forma segura), que ofrecen innegables eficiencias operativas, pero simultáneamente abren nuevas ventanas de vulnerabilidad.

El desafío para las áreas de cumplimiento no será únicamente adoptar herramientas de *Machine Learning* para la detección de anomalías, sino garantizar la "explicabilidad" y la gobernanza ética de esos algoritmos, evitando sesgos que deriven en la exclusión financiera injustificada o en el debilitamiento sutil de las debidas diligencias sobre el Beneficiario Final.

Un segundo desafío de carácter geopolítico e institucional es la complejidad regulatoria en torno a la mitigación del FPADM. A diferencia del lavado de activos tradicional, donde los patrones suelen ser conductuales y financieros, el financiamiento de la proliferación de Armas de Destrucción Masiva exige un monitoreo en tiempo real de cadenas de suministro globales, rutas marítimas, seguros de cascos y mercancías de uso dual. En un mundo con tensiones geopolíticas fragmentadas, las listas de sanciones internacionales se modifican con una velocidad sin precedentes. Las aseguradoras del futuro deberán pasar de un monitoreo estático y reactivo a un modelo de inteligencia comercial predictiva, integrando datos de geolocalización satelital y análisis de redes complejas para evitar la cobertura indirecta de entidades o regímenes sancionados.

Finalmente, se concluye que el factor determinante en la efectividad de cualquier sistema de administración de riesgos seguirá siendo el capital humano y la cultura organizacional. La tecnología más avanzada resulta inocua si no está respaldada por una estructura de Gobierno Corporativo donde la alta gerencia asuma el cumplimiento como una inversión reputacional y no como un costo operativo. La verdadera resiliencia del sector asegurador frente a las amenazas

de LC/FT/FPADM no se medirá por el número de reportes de actividad sospechosa generados de forma automática, sino por la capacidad de la organización para cultivar un entorno ético transfuncional, donde la primera línea de defensa desde el Intermediarios de Seguros, hasta el suscriptor actúe con la convicción de que proteger la institución es, en última instancia, proteger la estabilidad del orden económico y social global.

Referencia Bibliográfica

- Asociación Internacional de Supervisores de Seguros (IAIS). (2020). *Application Paper on Combatting Money Laundering and Terrorist Financing*. Basilea: IAIS.
- Blanco, J. (2021). *Gestión del Riesgo y Prevención del Lavado de Activos en el Sector Financiero*. Ediciones de la U.
- Grupo de Acción Financiera Internacional (GAFI). (2012-2023). *Estándares internacionales sobre la lucha contra el lavado de activos y el financiamiento del terrorismo y la proliferación: Las Recomendaciones del GAFI*. París: GAFI.
- López, G., y Martínez, J. (2022). *Compliance 4.0 en el Sector Asegurador: Mitigación tecnológica de riesgos de lavado de dinero*. Madrid: Editorial Universitas.
- Rebolledo A. 2014. *Prevención y Control de Legitimación de Capitales y del Financiamiento al Terrorismo*.
- Sarmiento, R. (2018). *Prevención de Lavado de Activos en Seguros: Vulnerabilidades y Controles Operativos*. Bogotá: Editorial Legis.
- Superintendencia de la Actividad Aseguradora (SUDEASEG). (2024). *Providencia Administrativa Nro.SAA-01-0536-2024, Normas sobre la Administración del Riesgos de LC/FT/FPADM y Otros Ilícitos en la Actividad Aseguradora*. Caracas, Gaceta Oficial Nro. 6.835, del 03 de septiembre de 2024.
- Zúñiga, M. (2019). *El Enfoque Basado en Riesgo y la mitigación del Financiamiento de la Proliferación: Desafíos para el sector financiero y asegurador*. México: Editorial Porrúa.

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 SEÑALES DE ALERTA

**ARQUITECTURA SISTÉMICA DE LAS SEÑALES DE ALERTA PARA LA
PREVENCIÓN DE LEGITIMACIÓN DE CAPITALES Y FINANCIAMIENTO AL
TERRORISMO: UN ENFOQUE BASADO EN RIESGO E INTELIGENCIA
FINANCIERA PARA LAS INSTITUCIONES BANCARIAS**

Autor: Dr. Oscar Perdomo

Facilitadora: Dra. Elizabeth Peláez

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 SEÑALES DE ALERTA

**ARQUITECTURA SISTÉMICA DE LAS SEÑALES DE ALERTA PARA LA
PREVENCIÓN DE LEGITIMACIÓN DE CAPITALES Y FINANCIAMIENTO AL
TERRORISMO: UN ENFOQUE BASADO EN RIESGO E INTELIGENCIA
FINANCIERA PARA LAS INSTITUCIONES BANCARIAS**

Autor: Dr. Oscar Perdomo

<https://orcid.org/0009-0003-9026-9184>

Correo electrónico: oscarperdomovielma@gmail.com

RESUMEN

La presente investigación desarrolla una aproximación sistémica, transcompleja y multidimensional sobre el diseño, calibración y gestión operativa de las señales de alerta de Legitimación de Capitales y Financiamiento al Terrorismo (LC/FT) en el sector bancario. En un entorno financiero global caracterizado por la digitalización acelerada, la proliferación de criptoactivos, la arquitectura del *Open Banking* (Banca abierta) y la sofisticación de las redes criminales transnacionales, los sistemas tradicionales de control basados en reglas uniformes y umbrales rígidos resultan críticamente inefectivos. A través del Enfoque Basado en Riesgos (EBR) dictado por el Grupo de Acción Financiera Internacional (GAFI), este trabajo postula la necesidad de transitar hacia modelos predictivos dinámicos e inteligentes. Asimismo, se introduce y fundamenta el nuevo rol del Oficial de Cumplimiento como un "Hermeneuta Organizacional", un intérprete crítico capaz de desentrañar la opacidad algorítmica de la Inteligencia Artificial (IA) y preservar el juicio prudencial y ético humano en la toma de decisiones estratégicas. A partir de matrices analíticas transcomplejas, se desglosan las señales de alerta asociadas a los factores cliente, producto, canal y geografía, concluyendo con lineamientos de gobernanza corporativa y recomendaciones de políticas públicas orientadas a garantizar la efectividad práctica del sistema preventivo.

Palabras clave: Señales de Alerta, Legitimación de Capitales, Enfoque Basado en Riesgos, Hermeneuta Organizacional, Inteligencia Artificial, Sector Bancario, Efectividad.

ABSTRACT

This research develops a systemic, transcomplex, and multidimensional approach to the design, calibration, and operational management of anti-money

laundering and counter-terrorist financing (AML/CFT) warning signals in the banking sector. In a global financial environment characterized by accelerated digitalization, the proliferation of crypto assets, the architecture of Open Banking, and the sophistication of transnational criminal networks, traditional control systems based on uniform rules and rigid thresholds are critically ineffective. Through the Risk-Based Approach (RBA) dictated by the Financial Action Task Force (FATF), this work posits the need to move toward dynamic and intelligent predictive models. Furthermore, it introduces and substantiates the new role of the Compliance Officer as an "Organizational Hermeneuticist," a critical interpreter capable of unraveling the algorithmic opacity of Artificial Intelligence (AI) and preserving prudential and ethical human judgment in strategic decision-making. Using transcomplex analytical matrices, the warning signs associated with customer, product, channel, and geography factors are broken down, concluding with corporate governance guidelines and public policy recommendations aimed at ensuring the practical effectiveness of the preventative system.

Keywords: Warning Signs, Money Laundering, Risk-Based Approach, Organizational Interpreter, Artificial Intelligence, Banking Sector, Effectiveness.

INTRODUCCIÓN Y CONTEXTUALIZACIÓN

El sistema financiero contemporáneo experimenta una mutación sin precedentes inducida por la convergencia de las tecnologías emergentes y la reconfiguración de los canales de intermediación económica. Lo que históricamente se concibió como un circuito lineal de depósitos, créditos y transferencias físicas, hoy se despliega como una infraestructura viva, hiperconectada y tridimensional gobernada por códigos algorítmicos, procesamiento masivo de datos (*Big Data*) y transacciones de alta velocidad. Esta nueva arquitectura global, si bien democratiza el acceso a los servicios financieros e impulsa la inclusión socioeconómica, también dilata significativamente la superficie de ataque y exposición ante la delincuencia financiera organizada.

La legitimación de capitales y el financiamiento al terrorismo (LC/FT) han dejado de ser procesos rudimentarios únicamente de canalización física de efectivo para convertirse en sofisticadas operaciones de ingeniería financiera transnacional. Las organizaciones criminales instrumentalizan con asombrosa agilidad las debilidades estructurales de los sistemas de control interno, explotando la velocidad de las billeteras digitales, la descentralización de la tecnología

Blockchain (Cadena de Bloques), las finanzas descentralizadas (DeFi) y las asimetrías regulatorias entre jurisdicciones para fragmentar, difuminar e integrar capitales de origen ilícito en los torrentes sanguíneos de la economía formal.

En este complejo panorama, las instituciones bancarias en Venezuela emergen como un sector caracterizado por un ecosistema de alta vulnerabilidad y exposición crítica. Como integrante del sistema financiero del país, concentra la mayor representación transaccional de personas naturales y jurídicas, los flujos comerciales de mayor rotación, contemplando las sedes principales de las instituciones bancarias tanto públicas como privadas. Esta masividad genera una cantidad ingente de "ruido transaccional", un manto de operaciones cotidianas legítimas detrás del cual los legitimadores de capitales intentan mimetizar sus patrones de colocación, estratificación e integración.

El problema fundamental que aborda esta investigación radica en la obsolescencia y rigidez de los sistemas tradicionales de control de cumplimiento. Durante décadas, las instituciones bancarias estructuraron sus defensas sobre la base de reglas lógicas estáticas y umbrales fijos del efectivo: si una transacción superaba un monto determinado, el sistema encendía una luz, una señal de alerta. Sin embargo, en la era de la automatización y la incertidumbre radical, este enfoque normativo-lineal resulta doblemente lesivo. Por un lado, asfixia operativamente a las Unidades de Prevención LC/FT inundándolas con una tasa masiva de "falsos positivos" (operaciones/comportamientos que luego son descartados, que activan alarmas erróneamente), y por el otro, genera una peligrosa subprotección al ser incapaz de detectar los "falsos negativos", es decir, aquellas operaciones delictivas sofisticadas que se ejecutan por debajo de los umbrales legales mediante técnicas de fraccionamiento (*pitufeo*) o estructuración de redes complejas.

Frente a esta realidad, el Grupo de Acción Financiera Internacional (GAFI) ha sido categórico al exigir la adopción estricta de un Enfoque Basado en Riesgos (EBR), estandarizado en su Recomendación 1. El EBR postula que los recursos analíticos e institucionales de las entidades financieras deben distribuirse de manera asimétrica y proporcional a las amenazas detectadas. Por ende, la

"Señal de Alerta" constituye el núcleo operativo fundamental del sistema de prevención: es el evento disruptivo, el patrón anómalo o la desviación estadística, el patrón que rompe la normalidad conductual del cliente para exigir la intervención analítica del especialista.

La presente investigación tiene como objetivo general evaluar la arquitectura sistémica de las señales de alerta bajo el Enfoque Basado en Riesgos en el sector bancario, reflexionando sobre los lineamientos metodológicos y operativos para su optimización funcional. Científicamente, se justifica por la urgente necesidad de dotar a los profesionales de cumplimiento de un marco epistémico transcomplejo que trascienda el mero llenado formal de casillas de verificación. El Oficial de Cumplimiento contemporáneo debe evolucionar hacia un rol de "Hermeneuta Organizacional", un auditor y decodificador de lógicas matemáticas complejas que comprenda no sólo el *cuánto* de la transacción, sino el *por qué*, el *cómo* y el *quién* desde una perspectiva ética y social.

A lo largo de los capítulos de este ensayo, se analizarán los fundamentos normativos globales (GAFI, Grupo de Acción Financiera de Latinoamérica-GAFILAT, *entre otros*); se examinará la metodología técnica para diseñar y calibrar alertas utilizando herramientas de Inteligencia Artificial sin caer en los riesgos de opacidad de "caja negra" o *model drift*; se estructurarán detalladamente matrices transcomplejas de señales de alerta clasificadas por factores de riesgo; y se definirá el ciclo de vida de la alerta y su trascendencia procesal como Reporte de Actividad Sospechosa (RAS) ante la Unidad de Inteligencia Financiera. Todo esto configurará una propuesta integral orientada a robustecer la resiliencia institucional de la banca ante la incertidumbre y las amenazas delictivas del siglo XXI.

1. MARCO CONCEPTUAL, NORMATIVO Y EPISTÉMICO

1.1 Delimitación y Taxonomía de una Señal de Alerta

Para edificar una aproximación teoría de la administración de riesgos financieros, es imperativo establecer una precisión terminológica rigurosa que disipe las

ambigüedades habituales en la literatura de cumplimiento. En la práctica operativa diaria, los conceptos de "señal de alerta", "operación inusual" y "operación sospechosa" suelen utilizarse erróneamente de forma intercambiable, lo que desestructura la eficiencia de los procesos de investigación interna.

- **Señal de Alerta:** Es un indicador técnico, automatizado o manual, que se activa cuando una transacción, una conducta o un conjunto de características de un cliente colisiona con un parámetro de control preestablecido o se desvía significativamente de los patrones estadísticos considerados normales para su segmento económico. La señal de alerta no constituye en sí misma una declaración de ilegalidad; es un disparador de atención analítica, un síntoma que extrae un dato del flujo masivo para someterlo a escrutinio.
- **Operación Inusual:** Es aquella transacción o patrón de transacciones que, habiendo activado una o varias señales de alerta, no guarda aparente coherencia con el perfil financiero, la actividad económica declarada, los antecedentes históricos o el volumen de negocio normal del cliente. Toda operación inusual requiere la apertura formal de un expediente de análisis y la ejecución de un proceso de debida diligencia ampliada o reforzada para intentar identificar su justificación económica o legal.
- **Operación Sospechosa:** Es la categoría conclusiva del análisis interno. Se alcanza cuando, tras haber investigado exhaustivamente la operación inusual, el cliente no logra aportar una justificación económica lícita, razonable y comprobable, o cuando las explicaciones suministradas resultan manifiestamente falsas, inconsistentes o incongruentes. En este punto, la institución financiera adquiere la convicción —o la sospecha fundamentada— de que los fondos están vinculados de alguna manera con actividades de legitimación de capitales, delitos precedentes o financiamiento al terrorismo, lo que gatilla la obligación legal e inmediata de transmitir un Reporte de Actividad Sospechosa (RAS) a la Unidad Nacional de Inteligencia Financiera (UNIF).

La taxonomía de las señales de alerta puede clasificarse según su naturaleza metodológica en:

1. Alertas Cuantitativas de Umbral: Basadas en la transgresión de límites monetarios, transaccionales fijos establecidos por la ley o por las políticas internas de la entidad (v.g., transacciones en efectivo que rozan el límite legal de reporte).
2. Alertas Cualitativas Conductuales: Vinculadas a la actitud, el comportamiento o los atributos del cliente durante la vinculación o la ejecución de la operación (v.g., renuencia a suministrar información, nerviosismo, presentación de documentación con indicios de alteración).
3. Alertas Estadísticas de Desviación Perfilada: Activadas por algoritmos analíticos que comparan la transacción del usuario en tiempo real contra su propia media histórica de comportamiento (*desviación* intracliente) o contra la media de su grupo demográfico y comercial homogéneo (*desviación* intercliente).

1.2 El Enfoque Basado en Riesgos (EBR) como Matriz Generadora

El Enfoque Basado en Riesgos (EBR) representa el cambio de paradigma epistemológico más profundo en la historia de la prevención de delitos financieros. Su conceptualización formal se encuentra plasmada en la Recomendación 1 de las 40 Recomendaciones del GAFI, actualizada periódicamente, la cual impone a los Estados, reguladores e instituciones financieras la obligación de identificar, evaluar y entender sus riesgos específicos para aplicar recursos de mitigación de forma proporcional.

Bajo el modelo tradicional normativo-lineal, los controles se diseñaban bajo una lógica de "talla única" (*one-size-fits-all*). Este enfoque asumía que un cliente corporativo dedicado a la importación masiva de bienes compartía la misma naturaleza de riesgo que un pensionado que recibía un subsidio estatal,

aplicando procedimientos documentales idénticos. El resultado de esta rigidez era la ineficiencia sistémica: parálisis burocrática en los segmentos de bajo riesgo y vulnerabilidad crítica ante la sofisticación delictiva en los segmentos de alta exposición.

El EBR funciona como una matriz generadora hipercompleja que reconoce que el riesgo es una variable dinámica determinada por la interacción multilíneal de diversos factores de exposición:

$$\text{Riesgo} = f(\text{Cliente} \times \text{Producto} \times \text{Canal} \times \text{Geografía})$$

Al comprender el riesgo como un producto de variables interdependientes, las señales de alerta dejan de ser universales para volverse hiperespecíficas. Una misma transacción de retiro de efectivo puede ser perfectamente normal para un comercio minorista local en una región con Bajo Riesgo Relativo, pero constituirá una señal de alerta crítica e inmediata si es ejecutada por una Organización No Gubernamental (ONG) que opera en una región fronteriza de alta sensibilidad, es decir, con Alto Riesgo de Financiamiento al Terrorismo. El EBR, por lo tanto, dota al sistema de control de una plasticidad y una inteligencia contextual indispensables para sobrevivir en entornos de incertidumbre radical.

1.3 Estándares Internacionales Obligatorios y Evaluaciones de Efectividad

La adopción e implementación de un sistema robusto de señales de alerta no es una facultad discrecional de las juntas directivas bancarias, sino una exigencia obligatoria emanada del derecho internacional, estándares internacionales, mejores prácticas y de los acuerdos transfronterizos de supervisión. El Grupo de Acción Financiera de Latinoamérica (GAFILAT), en su carácter de grupo regional al estilo del GAFI, supervisa rigurosamente el cumplimiento de estos estándares a través de sus metodologías de Evaluación Mutua.

En este punto es preciso destacar que Venezuela forma parte del Grupo de Acción Financiera del Caribe (GAFIC), sin embargo, para efectos académicos y del objetivo del presente ensayo, se utilizará parte de la información obtenida del GAFILAT.

Comentado lo anterior, y continuado con el desarrollo del ensayo, a partir de la Cuarta y la actual Quinta Ronda de Evaluaciones Mutuas del GAFILAT, el enfoque de los evaluadores internacionales ha migrado drásticamente desde el cumplimiento técnico formal (evaluar si las leyes están escritas en la Gaceta Oficial o si los bancos tienen manuales impresos) hacia la medición de la Efectividad Práctica, estructurada en los denominados Resultados Inmediatos (RI). Específicamente, dos Resultados Inmediatos dependen de manera directa de la calidad del diseño y gestión de las señales de alerta:

- Resultado Inmediato 4 (Supervisión): Evalúa si los supervisores bancarios (como la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN) en Venezuela) aplican un enfoque basado en riesgos para vigilar que las entidades financieras tengan sistemas de alerta debidamente calibrados y adaptados a su materialidad operativa.
- Resultado Inmediato 5 (Medidas Preventivas): Examina directamente la capacidad del sector financiero para interceptar operaciones inusuales, mitigar riesgos y transmitir reportes de alta calidad a la Unidad Nacional de Inteligencia Financiera (UNIF). Si un banco posee un sistema de alertas obsoleto que no detecta las tipologías delictivas reales de su entorno regional, los evaluadores internacionales calificarán el sistema como "Inefectivo", lo que puede arrastrar la calificación soberana del país hacia listas de monitoreo intensificado (lista gris o negra del GAFI), con severas consecuencias para las líneas de corresponsalía bancaria internacional y el acceso al crédito global.

A este robusto entramado internacional se suman marcos normativos de vanguardia que reconfiguran las obligaciones tecnológicas del cumplimiento: la Regulación MiCA (Markets in Crypto-Assets) de la Unión Europea (2023), que impone a los Proveedores de Servicios de Activos Virtuales (VASPs) la obligación estricta de implementar señales de alerta criptográficas de alta frecuencia; y la Ley de Inteligencia Artificial de la (UE) Unión Europea (AI Act) de 2024, que cataloga formalmente a los algoritmos de scoring (o puntuación/calificación) crediticio y detección automatizada de fraudes

financieros como sistemas de "Alto Riesgo", obligando a las corporaciones a garantizar la transparencia, la explicabilidad analítica y la auditoría humana de dichos modelos.

1.4 El Oficial de Cumplimiento como Hermeneuta Organizacional en Entornos DANCE

La complejidad intrínseca de los mercados globales contemporáneos exige una profunda revisión de la dimensión ontológica del profesional de cumplimiento. Los marcos conceptuales tradicionales, de corte positivista y formalista, concebían al Oficial de Cumplimiento como un inspector burocrático cuyo horizonte laboral se limitaba a cotejar que el expediente del cliente tuviera la firma legible y la copia de la identificación vigente. Esta visión estática resulta letal en entornos caracterizados por la transcomplejidad y catalogados bajo los acrónimos VUCA (Volátil, Incierto, Complejo, Ambiguo) y DANCE (Dinámico, Ambiguo, No lineal, Complejo y Emergente).

En un entorno DANCE, considerado como un modelo de liderazgo y gestión que describe contextos caracterizados por ser dinámicos, ambiguos, no lineales y complejos, donde los flujos de datos financieros mutan de forma impredecible y los delincuentes organizados emplean IA generativa para falsificar identidades y eludir controles, el Oficial de Cumplimiento debe emerger bajo una nueva figura epistémica: el "Hermeneuta Organizacional".

La hermenéutica, entendida originalmente como la filosofía del arte de la interpretación de textos, se traslada al espacio corporativo y financiero para definir la capacidad del especialista de leer de manera crítica, contextual y profunda la "data viva" de la institución. El hermeneuta organizacional comprende que un dato transaccional aislado no posee un significado intrínseco; su verdadero sentido brota cuando se analiza a la luz de un "círculo hermenéutico" que conecta de forma permanente la parte (la transacción individual que activó la señal de alerta) con el todo (la historia de vida del cliente, el entorno macroeconómico regional, las presiones institucionales y las vulnerabilidades geopolíticas internacionales).

Donde el algoritmo calcula de forma binaria y automatizada, el hermeneuta organizacional interpreta. La Inteligencia Artificial es extraordinariamente eficiente para procesar millones de transacciones por segundo e identificar correlaciones matemáticas complejas; sin embargo, carece por completo de la capacidad de comprender el dilema ético, el contexto moral, la responsabilidad social y la intención humana detrás de la conducta financiera. El hermeneuta organizacional es el auditor de la lógica algorítmica: es quien examina la opacidad de los modelos de *Machine Learning* (Aprendizaje automático) detecta los sesgos discriminatorios institucionalizados y preserva la multidimensionalidad de la condición humana frente al reduccionismo del automatismo tecnológico. El profesional del futuro no compite con la máquina; la audita y la dota de sentido ético y legal.

2. METODOLOGÍA DE DISEÑO, CALIBRACIÓN Y AUDITORÍA DE SEÑALES DE ALERTA

2.1 Fuentes de Información y Modelación de Perfiles Transaccionales

El diseño metodológico de una arquitectura de señales de alerta de alta efectividad requiere una ingesta de datos multidimensional y una rigurosa modelación de perfiles transaccionales. Un sistema de control ciego a las particularidades de su entorno está condenado al fracaso. Por ende, la base de datos de entrenamiento del sistema preventivo debe alimentarse de tres fuentes analíticas primarias:

1. Fuentes Externas Globales y Sectoriales: Informes periódicos de tipologías delictivas publicados por el GAFI, GAFILAT, GAFIC, *Egmont Group* - Red mundial de Unidades de Inteligencia Financiera (UIF), entre otros y las tipologías de legitimación de capitales específicas emitidas por la Unidad Nacional de Inteligencia Financiera. Estos documentos proveen el mapa de ruta de las tácticas criminales de vanguardia.

2. Fuentes Internas Históricas de la Entidad: Análisis retrospectivo de los Reportes de Actividades Sospechosas (RAS) previamente confirmados por el banco, así como el estudio minucioso de la base de datos de "falsos positivos" acumulados, lo cual permite identificar qué reglas de control están mal parametrizadas y generando ruido innecesario.
3. Fuentes de Contexto Regional e Institucional: Incorporación de las dinámicas económicas propias de la zona de operación. Esto implica, por ejemplo, modelar las elevadas tasas de transacciones comerciales informales, el uso intensivo de divisas en efectivo para operaciones cotidianas y la velocidad de rotación de fondos en los principales ejes comerciales y de servicios.

A partir de esta ingesta informativa, la organización ejecuta la Modelación, Patrones de Perfiles Transaccionales (PPT), un proceso matemático-estadístico que busca establecer la línea base de normalidad de cada usuario. El perfil financiero no es una declaración estática de ingresos; es una estructura conductual predictiva dinámica construida sobre alguna de las siguientes variables clave: volumen mensual agregado esperado de transacciones, monto máximo por transacción individual, frecuencia de operaciones, origen y destino geográfico de las transferencias, y proporción de uso de canales digitales frente a canales físicos y manejo de efectivo. El cruce continuo de estas variables genera el "comportamiento esperado", sirviendo como el telón de fondo sobre el cual cualquier anomalía encenderá de forma inmediata una señal de alerta calibrada.

2.2 Lógicas de Detección: Reglas Fijas vs. Modelos Analíticos Avanzados (IA)

La infraestructura tecnológica de un banco moderno debe cohabitar con dos lógicas de detección marcadamente diferenciadas, cuyas fortalezas y debilidades deben equilibrarse de forma estratégica para garantizar la resiliencia integral:

- Reglas de Negocio Fijas e Históricas: Operan bajo la lógica condicional determinista de "*Si X, entonces Y*" (v.g., *Si el cliente realiza un depósito en efectivo superior a \$10,000 USD, activar señal de alerta*).
 - Ventajas: Alta predictibilidad, simplicidad técnica en su programación, facilidad absoluta de auditoría ante los reguladores e interpretabilidad inmediata por parte del personal de primera línea.
 - Desventajas: Rigidez estructural absoluta. Son extremadamente fáciles de evadir por los delincuentes *financieros una vez que estos descubren los umbrales de reporte (fenómeno de estructuración)*. Asimismo, *saturan las unidades de cumplimiento con tasas intolerables de falsos positivos* al no contemplar las variaciones contextuales de la transacción.
- Modelos Analíticos Avanzados basados en Inteligencia Artificial (IA) y Machine Learning (ML): Operan mediante enfoques estocásticos, algoritmos de aprendizaje supervisado (árboles de decisión, bosques aleatorios, redes neuronales) y aprendizaje no supervisado (algoritmos de agrupamiento como *K-Means* o modelos de detección de anomalías espaciales). Estos sistemas analizan simultáneamente cientos de variables transaccionales no lineales, identificando correlaciones ocultas e imperceptibles para el ojo humano.
 - Ventajas: Extraordinaria capacidad predictiva adaptativa. Identifican de forma inmediata esquemas delictivos de lavado de dinero emergentes e inéditos y reducen hasta en un 40% la tasa de falsos positivos al contextualizar dinámicamente el comportamiento del usuario.
 - Desventajas: Alta complejidad tecnológica, elevado costo de implementación, requerimiento crítico de bases de datos masivas perfectamente limpias y estructuradas, y el riesgo metodológico de la opacidad de "caja negra" (*black box*), donde el algoritmo emite una alerta, pero es incapaz de explicar de forma inteligible los pasos lógicos internos que lo llevaron a dicha conclusión.

2.3 Gestión de Riesgo de Modelo (MRM) y Combate al *Model Drift*

La adopción masiva de la Inteligencia Artificial en el ámbito preventivo ha dado nacimiento a una nueva disciplina crítica para el Hermeneuta Organizacional: la Gestión de Riesgo de Modelo (*Model Risk Management* - MRM). El riesgo de modelo se define como la posibilidad de sufrir consecuencias adversas (sanciones regulatorias, pérdidas financieras, exclusión injusta de clientes) derivadas de decisiones basadas en modelos predictivos incorrectos, mal entrenados, sesgados u obsoletos.

Para mitigar este riesgo, el Oficial de Cumplimiento debe estructurar e institucionalizar un riguroso marco de MRM sustentado en cuatro pilares metodológicos continuos:

1. Validación Independiente del Modelo: Antes de que un algoritmo analítico de detección de legitimación de capitales sea desplegado en el entorno de producción, debe someterse a una evaluación técnica exhaustiva por parte de un equipo de matemáticos y científicos de datos totalmente independientes de los desarrolladores originales. Esta validación audita la arquitectura matemática, la idoneidad de los datos de entrenamiento y la resiliencia del modelo ante escenarios extremos.
2. Combate Sistemático al *Model Drift* (Desviación del Modelo): Los modelos de IA no son estáticos; sufren un proceso natural de degradación predictiva denominado *Model Drift*. Esto ocurre principalmente por dos razones: el *Concept Drift* (cuando las tipologías y formas de legitimar capitales de las redes criminales mutan drásticamente, haciendo que el patrón aprendido por la IA quede obsoleto) y el *Data Drift* (cuando las condiciones macroeconómicas del sector cambian —v.g., un proceso de dolarización o reconversión monetaria—, alterando por completo la distribución estadística de los datos de entrada). El Hermeneuta Organizacional debe ejecutar pruebas de estrés periódicas y reentrenamientos algorítmicos continuos para garantizar que el modelo no pierda su calibración y efectividad.
3. Auditorías de Sesgo Algorítmico e Inclusión (*Bias Audits*): Un modelo de IA mal calibrado puede aprender correlaciones espurias o discriminatorias a partir de datos históricos contaminados. Por ejemplo, el sistema podría

catalogar automáticamente a todos los residentes de una determinada zona geográfica de bajos ingresos como clientes de "Alto Riesgo", generando una exclusión financiera automatizada, discriminatoria e institucionalizada. Las auditorías de sesgo recurren a pruebas de contrafácticos (modificar una variable protegida como el género o la ubicación geográfica para verificar si la alerta varía) garantizando la equidad algorítmica.

4. Explicabilidad Analítica (XAI - *Explainable AI*): En estricto alineamiento con la Ley de IA de la Unión Europea y las mejores prácticas internacionales, las instituciones bancarias deben rechazar los modelos de caja negra absoluta. La organización debe implementar herramientas de explicabilidad (como los valores de *SHAP* o *LIME*) que permitan "abrir la caja" y traducir los pesos matemáticos del algoritmo en argumentos comprensibles para los analistas humanos, los comités de ética y los inspectores reguladores estatales.

2.4 Tecnologías de Mejora de la Privacidad (PETs) en el Tratamiento de Datos

El diseño moderno de señales de alerta se enfrenta a una persistente tensión jurídica e institucional: la obligación de compartir y cruzar grandes volúmenes de datos financieros en arquitecturas de *Open Banking* para detectar redes delictivas complejas colisiona frontalmente con el derecho fundamental a la privacidad de los ciudadanos y las estrictas regulaciones de protección de datos de carácter personal (como el GDPR global).

Para resolver de manera técnica esta colisión de derechos, el ecosistema FinTech (tecnología financiera) y el sector bancario de vanguardia han adoptado las denominadas Tecnologías de Mejora de la Privacidad (PETs).

Estas herramientas matemáticas avanzadas permiten entrenar modelos analíticos y activar señales de alerta interbancarias sin necesidad de exponer, revelar o transferir datos sensibles de identificación personal (PII):

- Cifrado Homomórfico: Es una forma de criptografía avanzada que permite realizar operaciones matemáticas computacionales directamente sobre

conjuntos de datos cifrados. De este modo, los algoritmos de detección pueden analizar registros financieros y encender señales de alerta sin necesidad de descifrar la información en ningún momento del proceso, manteniendo la confidencialidad absoluta del dato origen.

- **Privacidad Diferencial:** Consiste en la inyección matemática de "ruido controlado" en las bases de datos de la institución. Este ruido difumina los registros individuales específicos impidiendo la reidentificación de un cliente en particular, pero preserva intactas las propiedades estadísticas globales del grupo, permitiendo que los modelos de Machine Learning identifiquen patrones macro de legitimación de capitales de forma segura.
- **Aprendizaje Federado (*Federated Learning*):** Es un paradigma de entrenamiento de Inteligencia Artificial totalmente descentralizado. En lugar de centralizar los datos financieros de múltiples bancos en un solo servidor central (lo que crearía un riesgo cibernético crítico y violaría la privacidad), el algoritmo se distribuye localmente a los servidores de cada entidad financiera. El modelo aprende y se calibra analizando los datos locales de cada banco y, posteriormente, envía únicamente las actualizaciones de sus pesos matemáticos hacia un servidor centralizado que consolida el aprendizaje global. Los datos financieros primarios nunca abandonan su entorno de origen.

3. TAXONOMÍA OPERATIVA DE LAS SEÑALES DE ALERTA POR FACTOR DE RIESGO (MATRICES DE ANÁLISIS TRASCOMPLEJO)

Para instrumentalizar el Enfoque Basado en Riesgos (EBR) y dotar al Hermeneuta Organizacional de una herramienta analítica exhaustiva aplicable en la realidad operativa de las instituciones bancarias, se estructuran a continuación las matrices analíticas transcomplejas de señales de alerta, categorizadas meticulosamente por factores de riesgo y articuladas con sus respectivas metodologías de mitigación y justificación técnica.

3.1 Dimensiones Vinculadas al Factor Cliente e Incoherencia Económica

Esta dimensión analítica se enfoca en alguna de las características intrínsecas, conductas y atributos del sujeto que interactúa con la institución bancaria, evaluando la coherencia existencial entre su realidad civil y comercial frente al volumen de sus flujos monetarios.

Código Alerta	Descripción Técnica de la Señal de Alerta	Vulnerabilidad Delictiva / Tipología Explotada	Nivel de Riesgo	Acción Mitigante Inmediata / Rol del Hermeneuta Organizacional
CLI-001	Incongruencia Radical Transaccional: Discrepancia severa entre los ingresos declarados en el perfil KYC y el volumen real de transacciones de fondos movilizados en un periodo mensual.	Colocación de fondos de origen ilícito; uso de cuentas personales para fines comerciales no declarados.	Alto	Bloqueo analítico preventivo: Exigir de forma inmediata soportes fiscales (declaraciones de ISLR) y estados de cuenta auditados. Auditoría de la coherencia del modelo.
CLI-002	Opacidad Corporativa Estructural: Constitución de cuentas a nombre de personas jurídicas cuyas acciones están representadas al portador, o cuyas estructuras societarias incorporan múltiples capas de empresas fachada en paraísos fiscales.	Estratificación avanzada; ocultamiento deliberado del Beneficiario Final (<i>Ultimate Beneficial Owner</i> - UBO).	Crítico	Aplicación de Debida Diligencia Reforzada (DDR): Suspensión transaccional hasta la identificación plena e ininterrumpida de las personas naturales controladoras finales bajo fe pública.
CLI-003	Instrumentalización de Clientes Vulnerables (Testaferros): Movilización de grandes sumas de capital en cuentas pertenecientes a estudiantes, desempleados, pensionados o beneficiarios de subsidios sociales.	Redes de <i>pitufeo</i> y estructuración transaccional masiva gestionada por mafias organizadas.	Alto	Validación de la huella digital e IP: Analizar la procedencia geográfica de las conexiones. Entrevistar al titular bajo un enfoque ético-hermenéutico para detectar coacción o fraude por ingeniería social.
CLI-004	Perfil PEP de Alta Exposición sin Coherencia: Personas Políticamente Expuestas (PEP) nacionales o extranjeras que registran	Corrupción administrativa, peculado de fondos públicos y cohecho internacional.	Crítico	Monitoreo continuado en tiempo real: Aprobación obligatoria de la cuenta por la Junta

Código Alerta	Descripción Técnica de la Señal de Alerta	Vulnerabilidad Delictiva / Tipología Explotada	Nivel de Riesgo	Acción Mitigante Inmediata / Rol del Hermeneuta Organizacional
	incrementos patrimoniales acelerados o reciben transferencias de contratistas del Estado.			Directiva. Auditorías de contrafacticos recurrentes y rastreo extensivo del origen de la renta.
CLI-005	Renuencia Contractual o Conducta Evasiva: Cliente que muestra marcado nerviosismo, agresividad, o que decide cancelar un trámite de apertura de producto financiero en el momento en que se le solicitan soportes de origen de fondos.	Intencionalidad delictiva directa; intento de eludir los controles básicos de identificación KYC.	Medio-Alto	Registro inmediato en base de datos interna de alertas conductuales: Monitorear si el mismo sujeto intenta ingresar a la institución a través de canales digitales o sucursales alternativas.
Fuente: elaboración propia.				

3.2 Dimensiones Vinculadas al Factor Producto y Canales de Distribución

Esta sección examina la vulnerabilidad inherente a los instrumentos financieros contratados y las autopistas digitales y físicas utilizadas por el cliente para movilizar valor, detectando alteraciones en la lógica operativa del producto.

Monitoreo de canales digitales	
Aletas de Red / IP	Alertas de dispositivos
Acceso desde VPNs	Cambios súbitos de hardware
Geolocalización imposible	Automatizaciones via bots
Coincidencia transaccional	Ataques de Deepfakes en KYC
Fuente: elaboración propia.	

Código Alerta	Descripción Técnica de la Señal de Alerta	Vulnerabilidad Delictiva / Tipología Explotada	Nivel de Riesgo	Acción Mitigante Inmediata / Rol del Hermeneuta Organizacional
PRO-001	Estructuración de Depósitos en Efectivo (<i>Pitufo</i>): Multiplicidad de depósitos en efectivo	Fase de Colocación; elusión deliberada de los formularios de	Alto	Consolidación informática agregada automatizada: Programar el sistema para agrupar

Código Alerta	Descripción Técnica de la Señal de Alerta	Vulnerabilidad Delictiva / Tipología Explotada	Nivel de Riesgo	Acción Mitigante Inmediata / Rol del Hermeneuta Organizacional
	ejecutados en diferentes agencias bancarias de la zona en un mismo día por montos que rozan el límite legal de reporte.	declaración obligatoria de efectivo.		transacciones por número de identificación en un rango ≤ 24 horas. Reportar de inmediato un RAS por estructuración.
PRO-002	Cuentas Puente de Tránsito Rápido: Cuentas corrientes corporativas que reciben transferencias electrónicas masivas e inmediatamente (en minutos) debitan la totalidad de los fondos mediante transferencias hacia terceros sin dejar saldos remanentes.	Fase de Estratificación; pulverización del rastro del dinero para dificultar el rastreo analítico de la UNIF.	Alto	Implementación de algoritmos de análisis de redes y grafos: Rastrear la procedencia y el destino final de la cadena de valor. Calibrar alertas dinámicas de permanencia temporal de fondos.
PRO-003	Conexiones Digitales Simultáneas Imposibles: Accesos a la plataforma de banca en línea desde direcciones IP ubicadas en diferentes países en un intervalo de tiempo físicamente imposible de recorrer por un ser humano.	Venta de cuentas puente en el mercado negro; uso de redes virtuales privadas (VPNs) para ocultar ubicación; fraude cibernético.	Alto	Bloqueo informático de sesión inmediato: Autenticación multifactorial forzada de contingencia y validación biométrica de vida del titular de la cuenta bancaria.
PRO-004	Suplantación en KYC Remoto mediante <i>Deepfakes</i> : Intentos de apertura de cuentas 100% digitales utilizando imágenes o videos de validación facial generados sintéticamente por Inteligencia Artificial generativa.	Usurpación de identidad a gran escala para la creación de cuentas "mula" destinadas al lavado de dinero cibernético.	Crítico	Auditoría biométrica profunda: Evaluar la resiliencia de los algoritmos de detección de vitalidad (<i>liveness detection</i>). Análisis de metadatos de archivos de imagen por analistas humanos expertos.
PRO-005	Uso Atípico de Finanzas Descentralizadas (DeFi) y Criptoactivos:	Fuga de capitales, transacciones con activos virtuales de alta	Alto	Trazabilidad criptográfica complementaria: Utilizar herramientas analíticas de

Código Alerta	Descripción Técnica de la Señal de Alerta	Vulnerabilidad Delictiva / Tipología Explotada	Nivel de Riesgo	Acción Mitigante Inmediata / Rol del Hermeneuta Organizacional
	Transferencias masivas recurrentes desde cuentas bancarias tradicionales hacia <i>Exchanges</i> de criptomonedas no regulados en jurisdicciones <i>offshore</i> .	opacidad y legitimación mediante tokens de privacidad (v.g., Monero).		Blockchain (Chainalysis/Elliptic) para auditar la billetera de destino antes de liberar los fondos bancarios retenidos.
Fuente: elaboración propia.				

3.3 Dimensiones Vinculadas al Factor Geográfico y Jurisdicciones Sensibles

Esta dimensión analiza el componente geoespacial de las transacciones, cruzando la ubicación física de las agencias de origen, las rutas de tránsito del dinero y las jurisdicciones internacionales involucradas en los flujos de capital.

Código Alerta	Descripción Técnica de la Señal de Alerta	Vulnerabilidad Delictiva / Tipología Explotada	Nivel de Riesgo	Acción Mitigante Inmediata / Rol del Hermeneuta Organizacional
GEO-001	Triangulación Transfronteriza Opaca: Transferencias internacionales originadas en países de Europa o Asia que transitan por Venezuela y tienen como destino final paraísos fiscales del Caribe sin justificación comercial.	Legitimación de capitales internacional y evasión de sanciones económicas globales mediante canales comerciales ficticios.	Crítico	Auditoría de comercio exterior: Exigir de forma mandatoria conocimientos de embarque, facturas comerciales legalizadas y manifiestos de aduana reales.
GEO-002	Flujos Masivos en Zonas Fronterizas Internas Atípicas: Movilización desproporcionada de efectivo o transferencias en agencias ubicadas en zonas fronterizas o de alta incidencia minera, gestionadas desde	Financiamiento de actividades de minería ilegal, contrabando de extracción o control territorial por parte de grupos estructurados de delincuencia organizada.	Alto	Georreferenciación de riesgos corporativos: Ajustar los techos transaccionales automáticos según el mapa de vulnerabilidades territoriales del Estado venezolano.

Código Alerta	Descripción Técnica de la Señal de Alerta	Vulnerabilidad Delictiva / Tipología Explotada	Nivel de Riesgo	Acción Mitigante Inmediata / Rol del Hermeneuta Organizacional
	sedes corporativas en Venezuela.			
GEO-003	Vínculos transaccionales con países bajo monitoreo intensificado (Lista Gris del GAFI): Emisión o recepción de órdenes de pago hacia entidades financieras constituidas en jurisdicciones catalogadas por el GAFI como deficiencias estratégicas.	Exposición a redes globales de legitimación de capitales; canalización de fondos con debilidades estructurales de control.	Alto	Escrutinio expandido obligatorio: Aplicación automática de los protocolos de la Recomendación 19 del GAFI para países de alto riesgo financiero.
GEO-004	Desviación Geográfica del Patrón Comercial Corp: Empresa con sede social principal en Venezuela que ejecuta de manera súbita operaciones comerciales masivas en localidades geográficas remotas donde carece por completo de sucursales o actividad fabril.	Creación de redes fantasma de simulación comercial para la legitimación de capitales corporativos ilícitos.	Medio-Alto	Verificación e inspección física <i>in situ</i> ocasional: Confirmar la existencia real de los establecimientos comerciales de las contrapartes declaradas en la operación.
GEO-005	Canalización de Fondos de O.N.G. hacia Regiones Geopolíticamente Inestables: Transferencias internacionales emitidas por Organizaciones No Gubernamentales sin fines de lucro destinadas a zonas de conflicto bélico o bajo el control de facciones extremistas.	Desviación de recursos con fines de Financiamiento al Terrorismo (FT) bajo la fachada de ayuda humanitaria transnacional.	Crítico	Cumplimiento estricto de la Recomendación 8 del GAFI: Auditoría forense exhaustiva de la lista de beneficiarios finales de la ayuda humanitaria y cruce automático con listas antiterroristas internacionales (OFAC/ONU).
Fuente: elaboración propia.				

4.PROTOCOLO DE GESTIÓN, ESCALAMIENTO Y VALOR PROCESAL DE LA ALERTA DETECTADA

4.1 El Ciclo de Vida de la Alerta: Triage, Investigación e Inteligencia Financiera

Una vez que el sistema analítico (sea de reglas fijas o de Inteligencia Artificial) detecta una anomalía y activa una señal de alerta, esta ingresa formalmente a su Ciclo de Vida operativo, un proceso estructurado que debe ejecutarse bajo rigurosos protocolos de tiempos y movimientos analíticos para garantizar la efectividad sistémica de la institución financiera:



1. Fase de Triage y Depuración Inicial: La alerta automatizada es recibida por analistas de cumplimiento de primera línea. Su tarea exclusiva consiste en realizar un filtrado inicial rápido para descartar errores instrumentales o inusualidades explicables de forma evidente (falsos positivos de bajo impacto). Si la alerta posee consistencia y mérito técnico, es escalada formalmente en un plazo no mayor a 24 horas hacia el equipo de investigación forense.
2. Fase de Investigación y Análisis de Inteligencia Financiera: En esta etapa, el analista senior asume el papel de Hermeneuta Organizacional. Se ejecuta una inmersión profunda en el expediente del cliente, consolidando información multidimensional: se solicita debida diligencia reforzada, se analizan los nexos corporativos en registros mercantiles públicos, se realiza análisis de grafos e interconexiones transaccionales para identificar si la cuenta está vinculada a redes de lavado previamente detectadas, y se evalúa el contexto socioeconómico real de las operaciones. Toda la

información recopilada se estructura de forma cronológica en un expediente de inteligencia financiera interno con carácter estrictamente confidencial.

3. Fase de Dictamen y Cierre de Expediente: El Oficial de Cumplimiento examina las conclusiones de la investigación. Si el cliente logró justificar plenamente la licitud y coherencia de los fondos, el expediente se archiva con una nota técnica detallada que servirá para calibrar el algoritmo en el futuro. Si persiste la inusualidad y se consolida la sospecha de criminalidad, se emite el dictamen formal de aprobación para el envío inmediato del Reporte de Actividad Sospechosa (RAS).

4.2 Gobernanza Corporativa, Mitigación de Conflictos de Interés y las Tres Líneas de Defensa

Para que la arquitectura de señales de alerta funcione con integridad absoluta, debe insertarse dentro de un modelo de Gobernanza Corporativa robusto que mitigue los persistentes conflictos de interés inherentes al negocio bancario. Las áreas comerciales de las instituciones financieras operan bajo la presión constante de metas de captación de depósitos y colocación de créditos, lo que puede generar incentivos perversos para flexibilizar los controles ante clientes de alta rentabilidad pero elevada sospecha delictiva.

La protección de la integridad bancaria se fundamenta en la implementación estricta del Modelo de las Tres Líneas de Defensa, articulado orgánicamente con los comités de gobernanza interna:

ALTA DIRECCIÓN / JUNTA DIRECTIVA		
Primera (línea de defensa)	Segunda (línea de defensa)	Tercera (línea de defensa)
Áreas comerciales	Unidad de cumplimiento	Auditoría interna
Cajeros y gerentes de sucursales	Oficial (hermeneuta)	Evaluaciones de efectividad
Captación inicial de KYC	Monitoreo e inteligencia	Validaciones del modelo (MRM)
Fuente: elaboración propia.		

- Primera Línea de Defensa: Constituida por las áreas comerciales, gerencias de sucursales, cajeros y oficiales de negocios digitales. Tienen la obligación primaria de ejecutar el KYC básico en el momento de la vinculación y estar

alertas ante señales conductuales atípicas en los puntos de contacto con el cliente.

- Segunda Línea de Defensa: Encabezada de forma exclusiva por la Unidad de Prevención y Control de Legitimación de Capitales y Financiamiento al Terrorismo (UPC-LC/FT) y el Oficial de Cumplimiento. Esta línea posee independencia funcional y jerárquica absoluta, reportando directamente a la Junta Directiva. Es la encargada de diseñar las matrices de riesgo, programar y calibrar los sistemas tecnológicos de alertamiento, ejecutar las investigaciones forenses de inteligencia financiera y dictaminar de forma autónoma el envío de los reportes sospechosos, libre de interferencias.
- Tercera Línea de Defensa: Representada por el área de Auditoría Interna. Su función primordial es auditar la efectividad de las dos primeras líneas, ejecutando revisiones periódicas sobre la calidad de las investigaciones, la vigencia de los manuales de procedimientos y liderando las auditorías independientes de riesgo de modelo (MRM) de los sistemas de Inteligencia Artificial de la entidad.

La cúspide de esta estructura está integrada por el Comité de Cumplimiento y Ética de IA, encargado de sesionar de forma ordinaria para revisar las estadísticas de alertas, evaluar la efectividad de los mitigantes, resolver expedientes de alta complejidad que involucren a Personas Políticamente Expuestas (PEP) y aprobar formalmente las actualizaciones estratégicas de los parámetros analíticos de la institución bancaria.

4.3 El Reporte de Actividades Sospechosas (RAS): Calidad, Suficiencia y Valor Probatorio

El Reporte de Actividades Sospechosas (RAS) constituye el producto final de la inteligencia financiera interna de la institución bancaria y representa el eslabón de conexión fundamental entre el sector privado y el aparato de justicia penal del Estado. El RAS no debe entenderse como una denuncia penal formal, sino como un reporte técnico confidencial de inteligencia que suministra indicios de alta

probabilidad criminal a las Unidades de Inteligencia Financiera, para que estas puedan activar sus facultades de investigación punitiva. La utilidad procesal de un RAS depende de manera absoluta de tres atributos de calidad metodológica:

1. Suficiencia Narrativa Analítica: Un reporte deficiente se limita a anexar un listado de transacciones electrónicas o depósitos en efectivo en un archivo de Excel, obligando a la UNIF a adivinar la naturaleza de la sospecha. El RAS de alta calidad debe estructurar una narrativa coherente, profunda y lógica que explique de manera inteligible el *iter delictivo* analizado: por qué la conducta del cliente es sospechosa, cuál es la incongruencia económica detectada frente a su sector comercial, qué tipología específica se presume que está ejecutando y cuáles fueron las inconsistencias detectadas durante las entrevistas presenciales o digitales de debida diligencia reforzada.
2. Oportunidad Temporal: La transmisión del reporte debe ejecutarse en los plazos perentorios dictados por las normativas prudenciales y los estándares internacionales (comúnmente de forma inmediata o en un plazo máximo de 24 a 72 horas posteriores a la consolidación interna de la sospecha). Un reporte extemporáneo enviado meses después de ejecutadas las transacciones atípicas carece de valor preventivo, permitiendo que las redes criminales vacíen las cuentas bancarias y completen con éxito la fase de integración de los capitales ilícitos en mercados internacionales.
3. Valor Probatorio e Indiciario Procesal: Si bien el RAS posee carácter estrictamente confidencial bajo reserva legal internacional para proteger la integridad de la institución financiera y de sus analistas (prohibición de revelar al cliente la existencia de la investigación o *tipping-off*), la solidez técnica de su estructura narrativa dota a los fiscales del Ministerio Público y a los jueces de la República de los elementos de convicción y mapas transaccionales necesarios para fundamentar solicitudes de congelamiento preventivo de fondos, incautación de bienes, solicitudes de asistencia mutua legal transfronteriza y la emisión de órdenes de captura internacional contra los líderes de las organizaciones criminales de legitimación de capitales.

5. CONCLUSIONES

La ejecución y análisis exhaustivo desarrollado a lo largo de la presente investigación permiten consolidar las siguientes conclusiones fundamentales de carácter teórico, metodológico y operativo:

- Las nuevas tecnologías financieras han transformado de manera irreversible las bases de la intermediación financiera, convirtiendo los sistemas de control normativo tradicionales basados en reglas uniformes y umbrales rígidos, en infraestructuras obsoletas e inefectivas frente a las tipologías contemporáneas de legitimación de capitales y financiamiento al terrorismo.
- Bajo el Enfoque Basado en Riesgos institucionalizado por el GAFI y GAFILAT, GAFIC la Señal de Alerta constituye el núcleo preventivo fundamental del sistema de cumplimiento bancario, requiriendo un diseño asimétrico e hiperespecífico calibrado según la interacción dinámica de los factores de riesgo cliente, producto, canal de distribución y geografía.
- La efectividad del sistema de prevención en áreas de alta densidad y ruido transaccional, no se mide de forma cuantitativa por el volumen bruto de alertas encendidas, sino de forma cualitativa por la capacidad de reducir los falsos positivos y erradicar los falsos negativos mediante la correcta parametrización y depuración analítica continuada de los modelos.
- La adopción de herramientas avanzadas de Inteligencia Artificial y Machine Learning resulta indispensable para la supervivencia de los controles bancarios modernos en entornos DANCE; no obstante, introduce el Riesgo de Modelo (*Model Risk Management*) y la amenaza de opacidad de caja negra, obligando a las organizaciones a garantizar la explicabilidad analítica (XAI), la equidad algorítmica y la auditoría contra el *Model Drift*.
- El Oficial de Cumplimiento del siglo XXI debe experimentar una profunda transformación ontológica, transitando desde la figura del inspector burocrático estático hacia el rol del Hermeneuta Organizacional, un

especialista con alfabetización algorítmica y pensamiento transcomplejo capaz de auditar la lógica de los datos y preservar el juicio crítico, ético y humano frente a los automatismos tecnológicos.

- El Reporte de Actividades Sospechosas (RAS) representa la traducción práctica de la inteligencia financiera corporativa en valor procesal indiciario para el Estado, requiriendo los más altos estándares de suficiencia narrativa, oportunidad y rigurosidad técnica para servir de insumo eficaz en la desarticulación de redes delictivas complejas y la preservación de la estabilidad del sistema financiero global.

6. RECOMENDACIONES ESTRATÉGICAS

Con el objetivo de operacionalizar los hallazgos de esta investigación y elevar la resiliencia y efectividad de las instituciones bancarias frente a las amenazas emergentes de LC/FT, se proponen los siguientes lineamientos y recomendaciones estratégicas de aplicación inmediata:

1. Migración hacia Modelos de Segmentación Conductual Dinámica: Reemplazar los formularios de clasificación estática de clientes por algoritmos de Machine Learning no supervisados (*K-Means/Clustering*) que agrupen a los usuarios en función de su comportamiento transaccional real diario, generando señales de alerta automatizadas y personalizadas ante desviaciones estadísticas intracliente e intercliente.
2. Institucionalización de un Marco Integral de Gestión de Riesgo de Modelo (MRM): Crear unidades técnicas independientes de Validación de Modelos predictivos dentro del área de Auditoría Interna, ejecutando auditorías de sesgos (*Bias Audits*) semestrales y pruebas de estrés continuas para combatir el *Model Drift* provocado por mutaciones socioeconómicas del sector.

3. Implementación de Tecnologías de Mejora de la Privacidad (PETs): Desarrollar proyectos piloto interbancarios de Aprendizaje Federado (*Federated Learning*) y Cifrado Homomórfico para entrenar modelos predictivos compartidos de detección de lavado de dinero de alta frecuencia, facilitando el intercambio seguro de inteligencia financiera sin vulnerar el secreto bancario ni las leyes de protección de datos personales.
4. Despliegue de Protocolos de KYC (por sus siglas en inglés, *Know Your Customer* o "Conoce a tu Cliente") Tecnológicos Avanzados: Incorporar de manera obligatoria en los canales digitales de vinculación no presencial herramientas robustas de autenticación multifactorial y algoritmos biométricos de segunda generación con detección de vitalidad certificada para repeler los ataques de suplantación de identidad ejecutados mediante técnicas de *Deepfakes* (superposición del rostro de una persona sobre el rostro de otra, simulando sus expresiones faciales) e IA generativa.
5. Actualización Curricular y Formación Hermenéutica Continua: Instar a las instituciones de postgrado de vanguardia (como la ENAHP) a incorporar en sus programas de Especialización asignaturas transversales sobre Alfabetización Algorítmica, Gobernanza de Datos, Ética de la Inteligencia Artificial y Pensamiento Transcomplejo aplicado a los Delitos Financieros, dotando a los futuros Oficiales de Cumplimiento de las herramientas conceptuales para ejercer con solvencia el rol de Hermeneutas Organizacionales.

REFERENCIAS CONSULTADAS

- Asociación de Especialistas Certificados en Antilavado de Dinero (ACAMS). (2015, 19 de mayo). *Guía orientativa de GAFI para el sector bancario en la aplicación del enfoque basado en el riesgo*. Opinión ACAMS. <https://www.acams.org/es/opinion/guia-orientativa-de-gafi>
- Banco Mundial. (2007). *Guía de referencia para el antilavado de activos y la lucha contra el financiamiento del terrorismo* (2.ª ed.). Washington, D. C.: Banco Internacional de Reconstrucción y Fomento / Banco Mundial. <https://www.mpf.gob.ar/procelac->

[lavado/files/2020/04/BancoMundial.2007.Guia-de-referencia-Antilavado.pdf](#)

Christensen, C., & Raynor, M. (2005). *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Harvard Business Review Press.

Comisión Europea. (2019). *Directrices éticas para una IA fiable*. Dirección General de Sociedad Digital. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

European Union. (2023). *Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA)*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>

European Union. (2024). *Regulation (EU) 2024/1689 on artificial intelligence (AI Act)*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Floridi, L. (2013). *The ethics of information*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199641340.001.0001>

Grupo de Acción Financiera Internacional (GAFI). (2013). *Metodología para evaluar el cumplimiento técnico con las Recomendaciones del GAFI y la efectividad de los sistemas ALA/CFT*. París, Francia: GAFI/OCDE. https://www.pld.hacienda.gob.mx/work/models/PLD/documentos/metodologia_gafi.pdf

Grupo de Acción Financiera Internacional (GAFI). (2025). *Las 40 Recomendaciones del GAFI, actualizadas a diciembre de 2025*. París, Francia: Estándares internacionales institucionales sobre el control de la legitimación de capitales y el financiamiento del terrorismo.

Grupo de Acción Financiera de Latinoamérica (GAFILAT). (2024). *Las 40 Recomendaciones de GAFILAT: Estándares de cumplimiento regional*. Buenos Aires, Argentina: Secretaría Ejecutiva de GAFILAT. <https://www.gafilat.org/index.php/es/las-40-recomendaciones>

Grupo de Acción Financiera de Latinoamérica (GAFILAT). (2025). *Recomendaciones y metodología para la quinta ronda de evaluaciones mutuas*. Buenos Aires, Argentina: Centro de Documentación y Biblioteca de GAFILAT. https://biblioteca.gafilat.org/wp-content/uploads/2025/05/Recomendaciones_Metodologia-para-la-Quinta-Ronda-de-Evaluaciones-Mutuas.pdf

Huerta Tapia, M. S. (2025). *Educación financiera y Fintech en los estudiantes de una universidad de Lima Norte, 2025*. Arandu UTIC, 12(2), 3398-3409. <https://doi.org/10.69639/arandu.v12i2.1263>

Lloreda Camacho & Asociados. (2023). *Regulación FinTech en Latinoamérica (Enero 2023)*. <https://lloedacamacho.com/wp-content/uploads/2023/02/LATAMFINTECHREGULATION-ES-230123-1.pdf>

- OECD. (2019). *OECD Principles on Artificial Intelligence*. OECD Publishing. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- OECD. (2024). *Competencia, Fintechs y Open Banking*. OECD Publishing. https://www.oecd.org/content/dam/oecd/es/publications/reports/2024/09/competition-fintechs-and-open-banking_8b85b99b/f150ac77-es
- O'Farrell. (2024). *Guía de regulación FinTech LATAM*. Estudio Ofarrell. <https://www.estudio-ofarrell.com/wp-content/uploads/2024/12/Guia-de-Regulacion-Fintech-LATAM-ES.pdf>
- SELA. (2024). *Comercio y competencia: FinTech en la región de Latinoamérica y el Caribe*. Servicio Económico Latinoamericano y del Caribe. <https://www.sela.org/wp-content/uploads/2024/08/comercio-y-competencia-fintech-en-la-region-de-latinoamerica-y-el-caribe.pdf>
- Unidad de Análisis Financiero (UAF) de Chile. (2026). *Recomendaciones del GAFI y su incorporación en los estándares nacionales ALA/CFT/CFP*. Santiago de Chile: Gobierno de Chile. <https://www.uaf.cl/es-cl/sistema-nacional-alacftcfp/estandares-internacionales/recomendaciones-del-gafi>
- Unidad de Información y Análisis Financiero (UIAF) de Colombia. (2024). *Lavado de activos y financiación del terrorismo: Conceptos esenciales y pilares del sistema nacional*. Bogotá, Colombia: Ministerio de Hacienda y Crédito Público. <https://www.uiaf.gov.co/sistema-nacional-ala-cft/lavado-de-activos-y-financiacion-del-terrorismo>



Ministerio del Poder Popular
de Economía y Finanzas



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 Señales de Alerta

**De la intuición al algoritmo: El papel del aprendizaje automático en la
detección de señales de alerta para la gestión de riesgos de delincuencia
organizada**

Autora: Kimlen Chang
Facilitadora: Lic. Elizabeth Peláez
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 Señales de Alerta

**De la intuición al algoritmo: El papel del aprendizaje automático en la
detección de señales de alerta para la gestión de riesgos de
LC/FT/FPADM/YOI**

Autor: Kimlen Chang de Negrón
[https://orcid.org/ 0009-0003-7046-9103](https://orcid.org/0009-0003-7046-9103)
Correo Electrónico: eyknegron@gmail.com

Resumen

La lucha contra la delincuencia organizada enfrenta desafíos crecientes debido al volumen exponencial de transacciones y a la sofisticación de las redes criminales. Los sistemas tradicionales basados en reglas han demostrado ser insuficientes, generando un número insostenible de falsas alarmas que saturan los recursos de cumplimiento. El aprendizaje automático a través de la inteligencia artificial (*machine learning*) emerge como una herramienta transformadora, capaz de analizar grandes volúmenes de datos, identificar patrones complejos y adaptarse a la evolución de las tipologías delictivas. La evidencia empírica respalda esta afirmación. Casos como los de Danske Bank y JPMorgan Chase demuestran reducciones significativas en falsos positivos (50%-95%) y la liberación de cientos de miles de horas de trabajo. La investigación académica complementa estos hallazgos, mostrando que modelos como minería de grafos, XGBoost ((eXtreme Gradient Boosting, es un algoritmo de machine learning que usa árboles de decisión en cadena, donde cada nuevo árbol se construye para corregir los errores del anterior). o transformadores (Tab-AML) alcanzan altos niveles de precisión y capacidad de discriminación. Los resultados sugieren que no existe un algoritmo único superior, sino que el rendimiento óptimo depende del contexto institucional. Se propone una arquitectura híbrida en tres capas: filtro rápido basado en reglas, análisis con modelos de *machine learning* (que asignan puntajes de riesgo continuos) y revisión humana experta para casos complejos. Esta arquitectura transforma al oficial de cumplimiento en un auditor estratégico de los modelos. No obstante, la adopción de estas tecnologías conlleva sus propios desafíos, la existencia de sesgos algorítmicos y discriminación involuntaria y la obligatoriedad de explicar su funcionamiento para cumplir con el marco regulatorio, la obsolescencia de los modelos (*concept drift*), riesgos de ciberseguridad y resistencia organizacional.

Superar estos desafíos requiere un diseño ético, supervisión humana rigurosa y una gobernanza de datos sólida.

Palabras clave: aprendizaje automático, arquitectura híbrida, sesgo algorítmico.

Abstract

The fight against money laundering and terrorist financing (ML/TF) faces growing challenges due to the exponential volume of transactions and the sophistication of criminal networks. Traditional rule-based systems have proven insufficient, generating an unsustainable number of false alarms that overwhelm compliance resources. Machine learning emerges as a transformative tool, capable of analyzing large volumes of data, identifying complex patterns, and adapting to the evolution of criminal typologies. Empirical evidence supports this claim. Cases such as those of Danske Bank and JPMorgan Chase demonstrate significant reductions in false positives (50%-95%) and the release of hundreds of thousands of work hours. Academic research complements these findings, showing that models such as graph mining, XGBoost, (eXtreme Gradient Boosting is a machine learning algorithm that uses decision trees in a chain, where each new tree is built to correct the errors of the previous one) or transformers (Tab-AML) achieve high levels of precision and discrimination capacity. The results suggest that there is no single superior algorithm, but rather that optimal performance depends on the institutional context. A three-layer hybrid architecture is proposed: a fast rule-based filter, analysis with machine learning models (which assign continuous risk scores), and expert human review for complex cases. This architecture transforms the compliance officer into a strategic auditor of the models. However, the adoption of these technologies entails critical challenges: algorithmic biases and unintentional discrimination, the need for explainability to comply with the regulatory framework (GDPR), model obsolescence (concept drift), cybersecurity risks, and organizational resistance. Overcoming these challenges requires ethical design, rigorous human oversight, and robust data governance.

Keywords: machine learning, hybrid architecture, explainability, algorithmic bias.

INTRODUCCIÓN

Durante décadas, la detección de operaciones inusuales ha reposado en sistemas basados en reglas explícitas y en la intuición de los oficiales de cumplimiento. Las alertas se activan cuando una transacción supera un umbral predefinido, contiene una palabra clave incluida en listas restrictivas o coincide con algún patrón que ha sido configurado previamente. Este enfoque, si bien funcional frente a tipologías simples, ha demostrado ser frágil frente a los desafíos emergentes

El objetivo general de este trabajo consiste en analizar el potencial del aprendizaje automático (supervisado y no supervisado) para mejorar la detección de señales de alerta, evaluando sus ventajas sobre los métodos tradicionales, así como sus limitaciones prácticas y éticas. Para ello, se describirán las debilidades estructurales del enfoque basado en reglas e intuición; se expondrán los fundamentos técnicos de los principales modelos de *machine learning* aplicados a la detección de anomalías; se presentará evidencia empírica mediante casos de estudio documentados; se propondrá una arquitectura híbrida de implementación gradual; y se discutirán los desafíos emergentes en materia de sesgo algorítmico como la necesidad de explicar los procesos a lo interno y frente al regulador y riesgos de ciberseguridad.¹

1. Los sistemas tradicionales de detección de señales de alerta: limitaciones estructurales

Para comprender las potencialidades del aprendizaje automático, es indispensable diagnosticar primero el estado actual de los sistemas convencionales de prevención de LC/FT/FPADM/YOI. La mayoría de las instituciones financieras y de las entidades obligadas no financieras continúan operando con motores de monitoreo basados en listas de alertas y reglas ya determinadas, complementados con listas de sancionados, palabras clave y umbrales fijos. Este modelo ha sido criticado insistentemente por los organismos reguladores internacionales debido a sus graves limitaciones.

1.1 El problema de los falsos positivos

La principal limitación de los sistemas basados en reglas es su incapacidad para distinguir contextos. Una transferencia internacional de 10.001 dólares puede ser legítima para una empresa importadora, pero atípica para un estudiante universitario; no obstante, el sistema basado en umbrales trata ambas situaciones del mismo modo, generando una alerta en ambos casos. Estudios de la industria sostienen que entre el 90% y el 95% de las alertas generadas por estos sistemas son falsos positivos, es decir, corresponden a transacciones legítimas que no revisten sospecha (Breslow, s.f.). Se estima que las grandes organizaciones generan alrededor de 950 falsas alertas por cada millón de

¹ 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, LC quien ha supervisado y corregido los resultados generados para asegurar la integridad académica del documento.

transacciones al día, una carga operativa que eleva exponencialmente los costos de cumplimiento (Oztas et al., 2022).

Los datos provenientes de jurisdicciones específicas confirman la magnitud del problema. En los Países Bajos, menos del 3,5 % de los 3,48 millones de reportes de transacciones sospechosas presentados durante 2024 fueron identificados efectivamente como sospechosos, mientras que, en Francia, la unidad de inteligencia financiera Tracfin reportó que apenas el 5 % de los reportes se consideraron procesables (Thanasas, 2025). Incluso cuando las alertas llegan a las autoridades, la tasa de conversión es extremadamente baja: en Alemania, sólo el 15 % de los reportes fueron investigados por la fiscalía, y en el 95 % de los casos derivados no se produjo condena alguna (Aziani, 2023). Este panorama sugiere que el sistema global de alertas tempranas sufre una crisis estructural de efectividad, se concentran mayoritariamente en casos que no representan un riesgo real.

1.2. El rol y los sesgos de la intuición humana

Cuando un sistema basado en reglas genera una alerta, la responsabilidad recae sobre el oficial de cumplimiento y su equipo, quien debe revisar la documentación disponible, analizar el perfil del cliente y determinar si la operación reviste sospecha suficiente para elevar un reporte a la unidad de inteligencia financiera. Este proceso, que combina reglas explícitas con intuición experta, presenta al menos tres debilidades. El primero es la fatiga por saturación: frente a cientos o miles de falsos positivos diarios, el analista tiende a minimizar la alerta o a soslayar excepciones. El segundo es la falta de consistencia entre analistas: dos profesionales pueden evaluar el mismo caso y llegar a conclusiones divergentes, lo que introduce heterogeneidad en el proceso y dificulta la calibración de criterios. El tercero es la ceguera frente a patrones novedosos: la intuición se nutre de la experiencia previa, y por lo tanto resulta ciega frente a tipologías criminales emergentes para las cuales no existe un antecedente conocido.

Estos sesgos no son atribuibles a una falta de capacidad de los oficiales de cumplimiento, ni de su personal, sino a la naturaleza del entorno operativo. Las organizaciones criminales han comprendido que moviendo capital en pequeñas porciones (*smurfing*), utilizando activos virtuales en plataformas descentralizadas sin una debida diligencia a la cliente robusta, o emitiendo *deepfakes* (falsedades profundas) para sortear los controles biométricos de identidad, pueden operar sin activar los umbrales y sin generar los patrones que el analista humano está entrenado para detectar. Los sistemas tradicionales de detección, en consecuencia, se quedan rezagados precisamente frente a las conductas más sofisticadas.

Otras limitaciones vienen dadas por la gran cantidad de trabajo que recae sobre los oficiales de cumplimiento, quienes cada vez menos, gozan del tiempo necesario para analizar nuevas tendencias de la delincuencia y realizar ajustes en la parametrización de sus sistemas.

1.3. Incapacidad de los sistemas actuales basados en reglas frente a la delincuencia organizada digitalizada

La industria del crimen financiero se ha profesionalizado. En lugar de grandes transferencias únicas, los esquemas actuales prefieren microdepósitos repetidos, transferencias encadenadas a través de múltiples jurisdicciones en lapsos inferiores a una hora, y utilización de empresas fantasma con beneficiarios reales ocultos tras complejas estructuras jurídicas. Los sistemas basados en reglas resultan incapaces de detectar estas operaciones porque han sido diseñados para identificar conductas discretas y lineales y no estas operaciones complejas, denominadas redes complejas de comportamiento distribuido.

Surge entonces la necesidad de evaluar el tránsito hacia el uso de las tecnologías para pasar de un modelo basado en reglas fijas y conocimiento humano directo hacia un modelo en el que la máquina procese las masas de datos, identifique patrones de manera autónoma y presente al analista sólo aquellos casos que verdaderamente merecen atención. Este cambio de sistema es lo que el aprendizaje automático promete materializar.

2. Fundamentos del aprendizaje automático para la detección de anomalías LC/FT/FPADM/YOI

El aprendizaje automático, rama de la inteligencia artificial, se refiere a la capacidad de los sistemas computacionales para aprender patrones a partir de datos sin haber sido programados explícitamente con reglas para cada situación. En el ámbito de la prevención de LC/FT/FPADM/YOI, los algoritmos de *machine learning* pueden analizar históricos de transacciones, identificar características asociadas a comportamientos sospechosos y, a partir de ese aprendizaje, clasificar operaciones nuevas como de alto o bajo riesgo.

Desde 2019, Alvarez-Jareño, Badal-Valero y Pavía (2019) plantearon que la detección del fraude puede abordarse mediante tres estrategias complementarias, a través del aprendizaje automático, las cuales permiten identificar irregularidades basándose en datos:

- **Identificación de anomalías:** Esta técnica funciona como un filtro de comportamiento: primero agrupa a personas o empresas que actúan de

forma similar para establecer qué es lo "normal" en ese grupo. Cuando alguien se sale de ese molde o actúa de manera distinta a los demás, el sistema lo marca automáticamente como una posible irregularidad; en el caso de los números, se utiliza la Ley de Benford² para confirmar si esas cifras son auténticas o si fueron inventadas, ya que los datos falsos casi nunca siguen el patrón natural de los datos reales. En resumen: el sistema primero aprende lo que es "normal" en el grupo y, si alguien destaca por ser diferente o sus números no siguen las reglas naturales, lo identifica inmediatamente para investigarlo.

- **Análisis de redes y vínculos:** Este enfoque examina cómo se relacionan los individuos entre sí. Al mapear estas conexiones, es posible identificar interacciones que no tienen una justificación lógica o profesional, como el contacto frecuente entre partes con intereses opuestos. Estas relaciones poco frecuentes funcionan como alertas sobre posibles acuerdos indebidos que requieren revisión.
- **Modelado predictivo:** Mediante el análisis de casos de fraude ya confirmados, se pueden extraer los rasgos comunes que los definen. Al aplicar métodos estadísticos y de aprendizaje automático, es posible crear perfiles que permiten reconocer patrones sospechosos en nuevas operaciones antes de que el daño se concrete.

Desde una perspectiva técnica, los modelos aplicables a la detección de señales de alerta se pueden clasificar en tres grandes categorías.

2.1. Aprendizaje supervisado: clasificación con datos etiquetados

El aprendizaje supervisado parte de un conjunto de datos históricos que incluye transacciones ya clasificadas como «normales» o «sospechosas». El algoritmo construye un modelo que aprende a asociar las variables de entrada con la etiqueta de salida. Una vez entrenado, puede aplicarse a nuevas transacciones para predecir la probabilidad de que sean sospechosas.

² Ley de Benford: es un principio matemático que predice con precisión la distribución de dígitos en muchos tipos de conjuntos de datos

Entre los algoritmos supervisados más utilizados en la industria financiera se encuentran la regresión logística³, los árboles de decisión⁴, los bosques aleatorios (*random forests*)⁵, *XGBoost*⁶ y las redes neuronales profundas. Los bosques aleatorios, que combinan múltiples árboles de decisión para mejorar la precisión y reducir el sobreajuste, han mostrado un desempeño particularmente robusto en el contexto de la legitimación de capitales. En el ámbito de la detección de irregularidades, las investigaciones recientes demuestran que el uso de modelos avanzados de aprendizaje automático permite identificar actividades sospechosas con una precisión muy elevada. Según el trabajo desarrollado por Camino (2020), estos sistemas logran una capacidad predictiva excepcional al clasificar correctamente las operaciones, alcanzando valores de eficacia (específicamente la métrica ROC-AUC⁷) que oscilan entre 0,945 y 0,951.

Para comprender la importancia de este dato sin entrar en tecnicismos estadísticos, podemos imaginar que el modelo actúa como un filtro inteligente: una calificación cercana a 1,0 representa un sistema que acierta casi siempre al distinguir entre una transacción legítima y una sospechosa. Por tanto, obtener valores superiores a 0,94 indica que el modelo es altamente fiable, cometiendo muy pocos errores al señalar operaciones potencialmente ilícitas o al pasar por alto casos de fraude real.

En resumen, esta precisión demuestra que la tecnología actual es capaz de aprender los patrones del delito con una eficiencia superior a la de los sistemas de reglas manuales tradicionales. Sin embargo, el aprendizaje supervisado enfrenta una dificultad mayor en el ámbito de la LC/FT/FPADM/YOI: la extrema desproporción de clases. Menos del 0,1 % de las transacciones financieras suele ser fraudulento, de modo que el conjunto de entrenamiento contiene una enorme mayoría de ejemplos normales y apenas unos pocos casos sospechosos. Bajo esta condición de desequilibrio, un modelo puede aprender que la forma más

³ La regresión logística es un método estadístico utilizado en inteligencia artificial para clasificar información, calculando la probabilidad de que algo pertenezca a una categoría específica (como clasificar una operación financiera como "sospechosa" o "normal"). A diferencia de otros métodos, este algoritmo asigna un valor entre 0 y 1 a cada caso analizado; si ese valor supera un límite predefinido, el sistema genera automáticamente una alerta para que sea revisada, funcionando, así como un filtro inteligente que distingue patrones de riesgo basándose en datos históricos.

⁴ Los árboles de decisión son un modelo de inteligencia artificial que toma decisiones siguiendo una estructura lógica similar a un diagrama de flujo o un cuestionario. El sistema parte de una pregunta inicial y, dependiendo de la respuesta (sí o no), se ramifica hacia otras preguntas hasta llegar a una conclusión final. Es una de las formas más intuitivas de procesar datos porque "imita" el proceso de razonamiento humano: divide un problema complejo en una serie de pequeñas preguntas de sí o no para llegar a una clasificación clara.

⁵ Los bosques aleatorios (Random Forests) son una evolución potente de los árboles de decisión. Si un árbol de decisión es como un solo experto tratando de resolver un problema, un bosque aleatorio es un comité de expertos trabajando juntos. En lugar de crear un único árbol, el sistema crea cientos o miles de árboles de decisión independientes. Cada uno de estos árboles analiza los datos ligeramente de forma distinta (usando subconjuntos de información al azar) y llega a su propia conclusión. Al final, el "bosque" combina todas las opiniones individuales mediante una votación: la respuesta que recibe la mayoría de los votos se convierte en la decisión final del modelo.

⁶ El *XGBoost* (*eXtreme Gradient Boosting*) es un avanzado algoritmo de aprendizaje automático que perfecciona la precisión de los modelos predictivos mediante un proceso de mejora continua. A diferencia de otros métodos que analizan los datos de forma aislada, este sistema construye múltiples árboles de decisión de manera secuencial, donde cada nuevo árbol se especializa específicamente en corregir los errores cometidos por los anteriores. Este enfoque iterativo permite al modelo aprender de sus fallos y detectar patrones de riesgo financiero extremadamente sutiles y complejos, convirtiéndolo en una de las herramientas más potentes y eficientes actualmente disponibles para la detección automatizada de anomalías en grandes volúmenes de transacciones.

⁷ ROC-AUC es una métrica estándar en machine learning para evaluar modelos de clasificación binaria. Mide la capacidad del modelo para distinguir entre clases. ROC (Curva): Es un gráfico que muestra la tasa de aciertos (verdaderos positivos) vs. la tasa de falsas alarmas (falsos positivos) para distintos umbrales. El AUC mide la probabilidad de que el modelo ordene un ejemplo positivo aleatorio por encima de uno negativo aleatorio.

sencilla de maximizar la precisión es clasificar todas las transacciones como normales, lo que lo vuelve completamente inútil en la práctica.

El mismo autor nos indica que en el proceso de entrenamiento de modelos inteligentes, surgen algunos retos: la escasez de ejemplos de fraude en comparación con el volumen masivo de operaciones legítimas. Esta disparidad dificulta que los sistemas aprendan a identificar irregularidades con precisión. Para mitigar este problema, se emplean técnicas avanzadas de sobre muestreo, como las redes generativas antagónicas condicionales (conocidas como *Conditional Tabular GANs*)⁸.

En términos sencillos, estas redes funcionan como generadores de datos que crean ejemplos sintéticos, pero altamente realistas, de transacciones sospechosas. Al "fabricar" estos casos, el modelo logra balancear su conjunto de entrenamiento, obteniendo suficiente información para estudiar el fenómeno delictivo. Gracias a este método, el sistema no depende exclusivamente de los pocos casos reales disponibles, sino que se entrena con un espectro más amplio y detallado de escenarios, lo que optimiza significativamente su capacidad para detectar patrones de fraude en entornos reales.

2.2. Aprendizaje no supervisado: detección de anomalías sin etiquetas

Cuando no se dispone de datos históricos etiquetados (lo cual es frecuente en instituciones que recién comienzan a implementar *machine learning*), el aprendizaje no supervisado ofrece una alternativa valiosa. Estos algoritmos buscan identificar patrones anómalos sin conocer de antemano qué constituye una transacción sospechosa.

Entre las técnicas más prometedoras se encuentran los *autoencoders* y los bosques de aislamiento (*isolation forests*). Los autoencoders son redes neuronales que aprenden a comprimir la información de una transacción en una representación de menor dimensionalidad y luego a reconstruirla. Cuando una transacción presenta características anómalas, la reconstrucción será defectuosa y esa diferencia indicará una posible actividad sospechosa. Los bosques de aislamiento, por su parte, segmentan los datos mediante divisiones aleatorias; los puntos anómalos son aislados con pocas divisiones (camino cortos) y, por lo tanto, más fácilmente identificables.

Existen experiencias exitosas que combinan ambas técnicas. Un estudio reciente desarrolló un esquema de detección de fraude en tiempo real que

⁸ Las **Redes Generativas Antagónicas Condicionales** (o CTGANs, por sus siglas en inglés) son una tecnología de vanguardia diseñada para crear datos sintéticos que imitan perfectamente la estructura y las relaciones estadísticas de datos reales, pero sin contener información confidencial de personas reales. Funcionan mediante una competencia entre dos redes neuronales: una "Generadora", que intenta crear datos falsos realistas, y una "Discriminadora", que intenta detectar si los datos son reales o generados. Lo "Condicional" significa que el sistema puede ser instruido para generar datos con características específicas, como "clientes de un país determinado con un perfil de riesgo alto".

consolida las ventajas de *autoencoders* y bosques de aislamiento ampliados, logrando una precisión del 99 % en conjuntos de datos transaccionales reales, superando a otros sistemas de última generación. Esta capacidad de detección de anomalías sin necesidad de datos etiquetados resulta especialmente útil para identificar tipologías desconocidas que los modelos supervisados no podrían capturar porque no han visto nunca ejemplos de ellas.

2.3. La ventaja fundamental: adaptabilidad frente a rigidez

Más allá de las diferencias entre algoritmos, la principal ventaja del *machine learning* sobre los sistemas de reglas tradicionales reside en su capacidad de adaptación. Un motor de reglas es estático: los umbrales y condiciones permanecen fijos hasta que un analista los modifica manualmente. En cambio, un modelo de aprendizaje automático puede reentrenarse periódicamente sobre nuevos datos, capturando cambios en los patrones de comportamiento sospechoso y ajustando sus predicciones en consecuencia. En un entorno en el que la delincuencia organizada muta continuamente sus mecanismos, esta propiedad de actualización continua es indispensable.

3. Evidencia empírica: casos de estudio y métricas de desempeño

De acuerdo con la visión presentada Valverde, D. (2025), la aplicación de analítica predictiva está redefiniendo el sector financiero moderno, demostrando que la transición de modelos basados en reglas hacia sistemas de aprendizaje automático no es solo una mejora tecnológica, sino una necesidad operativa. La eficacia de estas herramientas trasciende la teoría cuando se implementan en entornos de alta complejidad, como lo ilustran los siguientes casos:

1. Danske Bank. Transformación operativa en Danske Bank: Ante la ineficiencia de su sistema tradicional, el cual generaba un 99% de falsos positivos y cerca de 500.000 alertas anuales, la entidad implementó un modelo de aprendizaje profundo. Este sistema analiza perfiles de clientes, comportamientos de grupos de pares y patrones temporales, reentrenándose semanalmente para adaptarse a nuevas tipologías criminales. Los resultados tras un año fueron significativos: se redujeron los falsos positivos en un 50%, se liberaron 120.000 horas de trabajo y se logró un incremento del 220% en los reportes de actividades sospechosas elevados a las unidades de inteligencia financiera. Además, la detección de esquemas de estratificación aumentó un 30%, lo que permitió a la entidad evitar multas estimadas en 30 millones de euros.

2. JPMorgan Chase: Para gestionar un volumen superior a 300 millones de mensajes de pago diarios, el banco adoptó una plataforma de inteligencia artificial basada en aprendizaje automático y procesamiento de lenguaje natural, conocida como *COiN (Contract Intelligence)*. Esta transición permitió una

reducción del 95% en los falsos positivos y una optimización drástica de los recursos humanos, liberando 750.000 horas de trabajo anuales. Asimismo, la implementación logró acortar los tiempos de investigación en los tercios, elevando la precisión y velocidad en la identificación de casos sospechosos.

4. Modelos que tenemos en la investigación académica.

Los avances tecnológicos en la detección de fraudes financieros no solo se dan en la práctica bancaria, sino que también son objeto de rigurosa investigación académica. A continuación, se presentan varios hallazgos documentados en la literatura científica que demuestran el potencial de estas herramientas.

4.1. Precisión mediante minería de grafos

Este enfoque modela las transacciones financieras como una red, donde las cuentas bancarias son nodos y las transferencias de dinero son conexiones entre ellos. El modelo analiza la estructura de esta red para identificar subgrupos de cuentas (subgrafos) que exhiben patrones de comportamiento anómalos, como la fragmentación y agregación de fondos, típicos de la legitimación de capitales.

Un estudio publicado en 2025 en la revista *Informática* desarrolló un modelo híbrido que combina el análisis de comunidades en redes (mediante el algoritmo Louvain⁹) con técnicas de desviación estadística (*AntiBenford*¹⁰). Al probarlo con el conjunto de datos de *IBM*¹¹ para detección de operaciones de legitimación de capitales, el modelo alcanzó una precisión del 96,57%, superando a los métodos tradicionales basados en reglas y a otros enfoques de *machine learning*. Este resultado demuestra que el análisis de la topología de las transacciones es una estrategia altamente eficaz para la detección de fraudes financieros.

⁹ El algoritmo de Louvain es una técnica utilizada para la detección de comunidades en redes complejas (grafos). Su objetivo es identificar grupos de nodos que están más conectados entre sí que con el resto de la red. Funciona de manera jerárquica y optimiza una medida llamada "modularidad", que básicamente calcula qué tan buena es la agrupación: si el modularidad es alta, significa que las comunidades detectadas están bien diferenciadas y son densas internamente. Inicio: El algoritmo asigna a cada nodo (persona o cuenta) su propia comunidad individual. Optimización local: El algoritmo mueve cada nodo de una comunidad a otra para ver si mejora la modularidad global de la red. Esto se repite hasta que ya no se pueden hacer más mejoras. Agregación: Una vez estabilizadas las comunidades, el algoritmo las "colapsa" en un solo nodo grande y repite el proceso en un nivel superior (jerárquico), permitiendo descubrir estructuras tanto pequeñas como a gran escala.

¹⁰ AntiBenford: Fenómeno opuesto a la Ley de Benford, que establece que en conjuntos de datos naturales los dígitos iniciales siguen una distribución logarítmica (el 1 aparece con mayor frecuencia que el 9). La distribución AntiBenford invierte este patrón, haciendo que los dígitos mayores sean los más frecuentes. Su detección se emplea como indicador de posible manipulación o fraude en datos numéricos.

¹¹ IBM, son datos colecciones de hechos, números y observaciones en bruto. Mediante el procesamiento y análisis de datos, la empresa transforma esta información sin procesar en conocimientos (insights) valiosos que mejoran la toma de decisiones e impulsan los resultados comerciales

4.2. Capacidad de discriminación mediante XGBoost

Los algoritmos de "potenciación de gradiente" (como XGBoost) son un tipo de aprendizaje supervisado que construye de forma secuencial múltiples modelos predictivos débiles (generalmente árboles de decisión) para corregir los errores de sus predecesores. El resultado es un modelo de "conjunto" muy potente. Su capacidad para clasificar correctamente las transacciones se mide con el indicador ROC-AUC, donde un valor de 1,0 indica una discriminación perfecta entre transacciones legítimas y fraudulentas.

Una investigación enfocada en la detección de fraudes con tarjetas de crédito (Yu et al.) evaluó varios algoritmos supervisados avanzados. En sus experimentos, el modelo XGBoost ajustado logró un valor ROC-AUC de 0,99, lo que evidencia una capacidad casi perfecta para distinguir entre operaciones normales y sospechosas. Este hallazgo subraya la eficacia de los métodos de conjunto para problemas de clasificación en el sector financiero, donde la precisión es crítica.

4.3. Arquitecturas avanzadas (*Transformers*)

Los "*transformers*" son una arquitectura de deep learning que ha revolucionado el procesamiento del lenguaje natural (siendo la base de modelos como *ChatGPT*¹²). Su fortaleza reside en la capacidad para procesar secuencias de datos y aprender relaciones complejas entre ellos, lo que los hace muy adecuados para analizar el contexto de las transacciones financieras, donde el tiempo y las conexiones entre operaciones son relevantes. El modelo Tab-AML aplica esta tecnología al monitoreo de pagos.

El estudio "*Tab-AML: A Transformer Based Transaction Monitoring Model for Anti-Money Laundering*" (Oztas et al., 2025) desarrolló un modelo con un codificador *transformer* de doble máscara y capas de atención residual. Al probarlo con el conjunto de datos SAML-D, logró un ROC-AUC de 93,01, una tasa de verdaderos positivos del 98% y una tasa de falsos positivos del 51%. Estos resultados superan a otros modelos como *TabTransformer* y *XGBoost*, destacando el potencial de los *transformers* para mejorar la detección de actividades ilícitas.

4.4. Modelos híbridos y sensibilidad

Un enfoque híbrido combina diferentes programas de *machine learning* para aprovechar las fortalezas de cada uno. Por un lado, los componentes

¹² ChatGPT: Modelo de lenguaje de gran escala desarrollado por OpenAI, basado en la arquitectura Transformer. Está entrenado con grandes volúmenes de texto para generar respuestas coherentes y contextualmente relevantes a partir de entradas en lenguaje natural. Su funcionamiento se fundamenta en el aprendizaje estadístico de patrones lingüísticos, sin comprensión semántica genuina.

"supervisados" aprenden de ejemplos etiquetados de fraudes pasados. Por otro lado, los componentes "no supervisados" exploran los datos en busca de anomalías o patrones atípicos sin necesidad de ejemplos previos. Esta combinación es particularmente útil para detectar tipologías de fraude nuevas o en evolución. La "sensibilidad" (o recall) mide la proporción de transacciones fraudulentas reales que el sistema es capaz de identificar correctamente.

Una investigación (Bi et al., 2024) presenta un sistema de detección de lavado de dinero que integra un enfoque de múltiples capas con componentes supervisados y no supervisados. La evaluación experimental, realizada sobre un conjunto de datos de más de 2 millones de transacciones de 24 meses de múltiples instituciones bancarias, demostró mejoras significativas. El sistema logró un incremento del 22,3% en la sensibilidad (recall), mientras mantenía la tasa de falsos positivos por debajo del 3%, un nivel muy bajo que minimiza las alarmas innecesarias. Además, la implementación de mecanismos de umbral adaptativo y selección dinámica de características contribuyó a una mejora del 25,2% en la puntuación ROC-AUC en comparación con los métodos convencionales, validando su eficacia y escalabilidad.

En conjunto, estos hallazgos de la literatura académica señalan una conclusión importante: no existe un algoritmo único que sea el "mejor" en todas las circunstancias. El rendimiento óptimo de cada modelo depende de las características específicas del conjunto de datos (volumen, tipo de transacciones, etc.) y del contexto operativo de cada institución financiera. La evidencia sugiere que la combinación de diferentes técnicas (híbridos) y la adopción de arquitecturas avanzadas (como *transformers*) parecen ser las que ofrecen las vías más prometedoras para mejorar la eficacia y eficiencia de los sistemas de lucha contra el lavado de dinero.

5. Propuesta de arquitectura híbrida y desafíos de implementación

La evidencia de casos de estudio y la investigación académica indican que la implementación exitosa del aprendizaje automático en la detección de LC/FT/FPADM/YOI no consiste en reemplazar abruptamente los sistemas tradicionales, sino en diseñar una arquitectura híbrida que integre de forma estratégica reglas explícitas, modelos de *machine learning* y supervisión humana. Esta aproximación permite respetar los requisitos normativos y adaptarse a los distintos niveles de madurez tecnológica de las organizaciones.

5.1. Arquitectura en tres capas

Una vez revisados los documentos analizados, pareciera que lo ideal es desarrollar estas herramientas en tres capas.

1. Capa 1 (filtro rápido basado en reglas): Un motor de reglas ligero procesa inicialmente las transacciones para resolver de forma automática los casos más elementales, como la coincidencia exacta con listas de sancionados o patrones simples y bien conocidos. El objetivo es aliviar la carga de procesamiento de las capas posteriores, no reemplazar al *machine learning*.
2. Capa 2 (análisis con aprendizaje automático): Las transacciones que superan el filtro inicial son evaluadas por modelos de machine learning. En ausencia de datos históricos etiquetados, se puede emplear un enfoque no supervisado (por ejemplo, *autoencoders* combinados con bosques de aislamiento) para detectar anomalías estructurales. A medida que se acumulan casos resueltos, se puede incorporar un modelo supervisado (como XGBoost o una red neuronal) que asigne a cada operación un puntaje de riesgo continuo, acompañado de los principales factores que contribuyeron a ese puntaje.
3. Capa 3 (revisión humana experta): Solo aquellos casos con un puntaje de riesgo que supere un umbral son remitidos a un oficial de cumplimiento para su investigación. Este umbral puede ajustarse según el apetito de riesgo de la organización: un umbral más bajo implica más revisiones humanas (mayor seguridad, pero también mayor costo), mientras que un umbral más alto reduce la carga de trabajo, aunque podría dejar pasar algunos casos sospechosos.

5.2. Requisitos para una implementación exitosa

La adopción de esta arquitectura exige condiciones habilitantes fundamentales:

- Datos históricos de calidad: Disponer de al menos 12 a 18 meses de transacciones completas, depuradas y estructuradas, que incluyan la mayor cantidad posible de atributos.
- Infraestructura tecnológica: Contar con capacidad y recursos computacionales suficientes para el procesamiento en línea.
- Explicabilidad de los modelos: El uso de herramientas como SHAP o LIME es crucial para que cada alerta generada sea acompañada de los motivos

concretos que llevaron al modelo a asignar un alto puntaje de riesgo, evitando así el problema de la "caja negra" y facilitando la justificación ante los reguladores.

- **Reentrenamiento periódico:** Dada la evolución constante de los patrones delictivos, los modelos deben ser reentrenados con frecuencia (idealmente cada semana, como en el caso de Danske Bank) utilizando la retroalimentación de los casos recientemente investigados.
- **Transformación del rol del oficial de cumplimiento.** En este modelo híbrido, el oficial de cumplimiento se transforma en una figura estratégica: supervisor y auditor de modelos. Sus nuevas responsabilidades incluyen el diseño de variables de entrada, la evaluación periódica del desempeño del modelo (mediante métricas de precisión, sensibilidad y equidad), la revisión de casos de alto riesgo, el análisis de falsos negativos para identificar debilidades y el mantenimiento de una comunicación fluida con los reguladores. Lejos de reducir el valor del talento humano, esta transformación lo potencia al liberarlo de tareas repetitivas y concentrar su capacidad analítica en casos complejos y en la mejora continua del sistema.

5.3. Desafíos y riesgos del enfoque algorítmico

A pesar de su potencial, la incorporación del aprendizaje automático en la prevención de la LC/FT/FPADM/YOI conlleva riesgos significativos que requieren un enfoque crítico y precavido.

- **Sesgo algorítmico y discriminación involuntaria:** El mayor riesgo es que los modelos de inteligencia artificial repitan prejuicios del pasado. Si un sistema se entrena con datos donde ciertos grupos fueron investigados más que otros, el modelo aprenderá erróneamente a sospechar de esos grupos, aunque no exista una razón real para ello. Para evitarlo, es fundamental elegir las variables de entrada con mucho cuidado (excluyendo datos sensibles como raza o género) y realizar pruebas de equidad constantes para asegurar que el sistema trate a todos los grupos por igual. igualdad de oportunidades, y la realización de auditorías de sesgo periódicas.

- **Transparencia y derecho a una explicación:** Los reguladores y los ciudadanos necesitan saber por qué un sistema tomó una decisión. Como los modelos avanzados (como las redes neuronales) son difíciles de entender, chocan con leyes y normas sobre la protección de datos que protege a las personas frente a decisiones automáticas. Para resolverlo, se usan herramientas, que permiten "abrir la caja" y explicar claramente cómo funciona el modelo.
- **Adaptación a nuevas amenazas:** Los delincuentes cambian constantemente sus tácticas para no ser detectados, lo que hace que los modelos pierdan precisión con el tiempo. La solución es vigilar el sistema constantemente y actualizar (reentrenar) el modelo de forma regular para que siga siendo eficaz frente a nuevos riesgos.
- **Ciberseguridad:** Los modelos pueden ser engañados si alguien contamina los datos de entrenamiento o diseña transacciones específicas para confundirlos. Para protegerse, se debe garantizar la seguridad desde el principio, verificando siempre la calidad de los datos y vigilando las operaciones que el sistema procesa.
- **Resistencia al cambio:** Es normal que los equipos tradicionales desconfíen de los algoritmos. Para superarlo, es clave capacitarlos, mostrando que la tecnología no viene a reemplazarlos, sino a ayudarles a tomar mejores decisiones. Involucrar a los expertos en cumplimiento desde el diseño ayuda a que se sientan parte del proceso y confíen en la herramienta.
- **El modelo ideal (Arquitectura híbrida):** La clave del éxito no es eliminar los métodos de siempre, sino combinarlos. El mejor enfoque es crear un sistema híbrido que mezcla reglas fijas, inteligencia artificial y la supervisión de expertos humanos. Esto permite cumplir con las leyes, aprovechar la tecnología y adaptarse a la capacidad real de cada organización.

El ensayo ha sostenido que la incorporación del aprendizaje automático en los sistemas de detección de señales de alerta de LC/FT/FPADM/YOI no es una mera mejora posible, sino un cambio del estado actual de las cosas necesario para restaurar la efectividad de los mecanismos de prevención frente a una delincuencia organizada que ha acelerado su digitalización y sofisticación. Los sistemas tradicionales basados en reglas e intuición, con tasas de falsos positivos que oscilan entre el 90 % y el 95 %, generan una carga operativa insostenible y dejan pasar las conductas más elaboradas. El aprendizaje automático, mediante técnicas supervisadas y no supervisadas, ha demostrado en casos reales (Danske Bank, JPMorgan Chase) y en estudios académicos (precisión del 96 % en conjuntos de datos públicos, reducción de falsos positivos hasta el 95 %) que es posible mejorar radicalmente la precisión, reducir los costos y liberar talento humano para tareas de mayor valor agregado.

Sin embargo, este cambio tiene sus propias debilidades. El sesgo algorítmico, la falta de explicabilidad, la obsolescencia por *concept drift*, los ataques adversarios y la resistencia organizacional constituyen desafíos sustantivos que deben ser tenidos en consideración desde el diseño. El modelo híbrido en tres capas propuesto —reglas rápidas, análisis con *machine learning* y revisión humana focalizada— ofrece una ruta de implementación gradual que respeta las exigencias regulatorias de transparencia y equidad al tiempo que aprovecha el potencial de la inteligencia artificial.

Las unidades de inteligencia financiera, los supervisores bancarios y los organismos internacionales como el GAFI tienen un rol central en este proceso: deben emitir guías claras sobre estándares mínimos de transparencia y validación de modelos; promover entornos de pruebas regulatorios (*sandboxes*) que permitan experimentar con nuevas tecnologías sin riesgo de sanción y fomentar la cooperación público-privada para compartir patrones y mejores prácticas. En un entorno normativo donde la integración de la inteligencia artificial en la debida diligencia del cliente y en el monitoreo de transacciones es ya inevitable, las instituciones financieras deben prepararse para un mundo en el que la capacidad tecnológica y la obligación legal se han vuelto inseparables.

Referencias bibliográficas

- Abbassi, H., Mendili, S. E., y Gahi, Y. (2024). Real-time online banking fraud detection model by unsupervised learning fusion. *HighTech and Innovation Journal*, 5 (1), 185-199. <https://hightechjournal.org/index.php/HIJ/article/view/616>
- Adebisi, O. O., et al. (2025). Anti-money laundering compliance using feature engineering with SQL analytics, TF-IDF and oversampling: Conditional tabular generative adversarial networks. *Informática*, 36(3), 491-524. <https://www.informatica.si/index.php/informatica/article/view/8298>

- Alvarez-Jareño, J. A., Badal-Valero, E., y Pavía, J. M. (2019). Aplicación de métodos estadísticos, económicos y de aprendizaje automático para la detección de la corrupción. *Revista Encuentros Multidisciplinares*, 65. http://www.encuentros-multidisciplinares.org/revista-65/j-m-pavia_jose-a-alvarez-jareno_elena-bedal.pdf
- Aziani, A. (2023). *What do suspicious transaction reports actually capture? Evidence from Italy*. [Presentación de conferencia]. Bahamas AML Conference. <https://bahamasamlconference.centralbankbahamas.com/documents/2024-03-26-15-13-51-Aziani-Nazzari2023-What-Suspicious-Transaction-Reports-Actually-Capture.pdf>
- Bi, W., Trinh, T. K., y Fan, S. (2024). Machine learning-based pattern recognition for anti-money laundering in banking systems. *Journal of Advanced Computing Systems*, 4(11). <https://doi.org/10.69987/jacs.2024.41103>
- Breslow, S. (s.f.). *The new frontier in anti-money laundering*. McKinsey & Company. <https://www.mckinsey.de/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20new%20frontier%20in%20anti%20money%20laundering/The-new-frontier-in-anti-money-laundering.pdf>
- Cámara Nacional de la Industria de Radio y Televisión. (s.f.). *Redes criminales amplifican poder con uso de la IA; reconfiguran operaciones*. <https://cirt.mx/redes-criminales-amplifican-poder-con-uso-de-la-ia-reconfiguran-operaciones/>
- Camino, R. D. (2020). *Machine learning for anti-money laundering: An application to the detection of suspicious activities* [Tesis doctoral, Université du Luxembourg]. OrbiLU. https://orbilu.uni.lu/bitstream/10993/44939/1/PhD_Thesis.pdf
- Fintech Global. (2025, 20 de mayo). *Europe's AML overhaul demands AI for effective compliance*. IT Brief UK. <https://amlnetwork.org/aml-laws/eu/europes-aml-overhaul-demands-ai-for-effective-compliance/>
- GAFI. (2020). *Guía de Identidad Digital*. FATF. <https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Identidad-Digital.pdf>
- GAFI. (2021). *Opportunities and challenges of new technologies for AML/CFT*. FATF. <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf>
- GAFI (2022). Estado de la Efectividad y el Cumplimiento de los Estándares del GAFI.
- GAFILAT (2023) *Transformación Digital: Nuevas Tecnologías y su Implementación en materia de Supervisión ALA/CFT*. <https://biblioteca.gafilat.org/?p=666>

- Lucas, J. A., y Smith, R. T. (2025). Tab-AML: A transformer based transaction monitoring model for anti-money laundering. En *Proceedings of the 2025 IEEE Conference on Artificial Intelligence (CAI)* (pp. 161-167). IEEE. <https://staffprofiles.bournemouth.ac.uk/display/conference/403589>
- Oztas, B., Cetinkaya, D., Adedoyin, F., y Budka, M. (2022). Enhancing transaction monitoring controls to detect money laundering using machine learning. En *2022 IEEE International Conference on e-Business Engineering (ICEBE)*. [Enhancing Transaction Monitoring Controls to Detect Money Laundering Using Machine Learning | IEEE Conference Publication | IEEE Xplore](#)
- Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Dogan, H., y Aksu, G. (2025). Tab-AML: A transformer based transaction monitoring model for anti-money laundering. En *2025 IEEE Conference on Artificial Intelligence (CAI)* (pp. 161-167). IEEE. <https://doi.org/10.1109/CAI64502.2025.00033>
- Pimpalkar, A. P., Somkunwar, R. K., Chinchalkar, S. P., Katakhdound, K. M., Bhide, A. S., y Patil, Y. M. (2025). Parallelized Louvain-based community detection and AntiBenford subgraph mining for financial fraud detection in transaction networks. *Informática*, 49(4). <https://doi.org/10.31449/inf.v49i4.8298>
- PwC. (2025). *Why PRAUC is the true test of AML model performance*. Fintech Global. [Why PRAUC is the true test of AML model performance](#)
- Thanasas, G. (2025). Transforming digital accounting: Big data, IoT, and industry 4.0 technologies—A comprehensive survey. *Journal of Risk and Financial Management*, 18(1). <https://www.mdpi.com/1911-8074/19/1/92>
- ThetaRay. (2025). *Busting the bias myth: How AI is smarter and fairer than rules-based systems*. <https://thetaray.com/busting-the-bias-myth-how-ai-is-smarter-and-fairer-than-rules-based-systems/>
- X-Mol. (2024). Improving client risk classification with machine learning to increase anti-money laundering detection efficiency. *Journal of Money Laundering Control*. <https://www.emerald.com/jmlc/article-abstract/28/1/93/1239496/Improving-client-risk-classification-with-machine?redirectedFrom=fulltext>
- Yu, S., Chang, V., Huỳnh, G. L., Jesus, V., y Luo, J. (s.f.). *Advanced supervised machine learning algorithms in credit card fraud detection*. <https://www.scitepress.org/PublishedPapers/2025/134854/>

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 Legitimación de Capitales y
Financiamiento al Terrorismo
Unidad Curricular Señales de Alerta

**Luces, cámara y acción: El marketing de impacto como señal de alerta
primaria en la legitimación de capitales dentro del ecosistema Fintech**

Autora: Abg. Mercedes Mendoza Rubio

Facilitadora: Prof. Elizabeth Peláez

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 Legitimación de Capitales y
Financiamiento al Terrorismo
Unidad Curricular Señales de Alerta

Luces, cámara y acción: El marketing de impacto como señal de alerta primaria en la legitimación de capitales dentro del ecosistema Fintech

Autora: Abg. Mercedes Mendoza Rubio

<https://orcid.org/0009-0008-8752-999X>

Correo electrónico: mendozameche2@gmail.com

Resumen

El presente análisis está orientado al uso de nuevas tecnologías y estrategias de marketing digital de impacto, en la trascendencia de las actividades delictivas de las organizaciones criminales organizadas para la obtención de fondos de inversionistas bajo engaño, perfeccionando el fraude financiero y legitimación de capitales mediante el ocultamiento de los fondos percibidos. El grado de profesionalismo y preparación de los grupos estructurados se ve reflejado en la explotación de los mercados globales y valoración de factores económicos, sociales, políticos y culturales que giran en torno al ser humano, combinando la innovación tecnológica sobre la cual se desarrolla el ecosistema *Fintech* y estrategias de marketing de impacto, que comprende el uso de multicanales de comunicación, redes sociales, *influencers* y personalidades para otorgar confiabilidad a un determinado proyecto de inversión bajo promesa de altos ingresos, exponiendo un esquema de fraude Ponzi moderno, causando impacto sobre el sistema financiero individuales y colectivos. Tomando en consideración la combinación de factores que se reflejan en casos reales planteados, el presente trabajo propone algunas variables y niveles de riesgos, relacionadas con las acciones características de las estrategias de marketing de impacto, con la intención de fomentar la generación de acciones preventivas, frente a este nuevo modelo de fraude financiero y ocultamiento de fondos.

Descriptor clave: Legitimación de Capitales; fraude financiero; Fintech; marketing de impacto; influencers.

Abstract

This analysis focuses on the use of new technologies and high-impact digital marketing strategies in the context of criminal activities carried out by organized crime groups to obtain funds from investors through deception, thereby refining financial fraud and money laundering by concealing the funds received. The level of professionalism and sophistication of these structured groups is reflected in their exploitation of global markets and their assessment of economic, social, political, and cultural factors that revolve around human beings, combining the technological innovation upon which the *Fintech* ecosystem is built with high-impact *marketing* strategies—which include the use of multi-channel communication, social media, *influencers*, and public figures—to lend credibility to a specific investment project promising high returns, thereby exposing a modern Ponzi scheme that impacts both individual and collective financial systems. Taking into account the combination of factors reflected in the real-world cases presented, this paper proposes certain variables and risk levels related to the characteristic actions of high-impact marketing strategies, with the aim of promoting the development of preventive measures against this new model of financial fraud and concealment of funds.

Key descriptors: Money Laundering; Financial Fraud; Fintech; Impact Marketing; Influencers.

Introducción

El desarrollo acelerado de la sociedad moderna viene acompañado de desafíos de diversa índole, sociales, políticos y económicos que pueden convertirse en factores de cambio de crecimiento, solapando la sombra de la delincuencia organizada.

Como bien lo manifestaron en 1994 Savona y Defeo durante la Conferencia Internacional sobre Prevención y Represión del Blanqueo de Dinero y de la Utilización del Producto del Delito: Un Enfoque Mundial, en Courmayeur, Italia, citados por Blanco (2015) en las sociedades modernas, los actores sociales han aprendido a explotar los mercados globales, las economías de escala y los defectos de armonización entre las políticas preventivas y de control, siendo la complejidad de las organizaciones criminales un reflejo de las complejidades económicas y sociales, criterio nada más cerca de la realidad actual y que ha inspirado el desarrollo del presente estudio.

El carácter transnacional de las organizaciones criminales ha trascendido las actividades criminales de producción y tráfico de drogas, tráfico de armas, la trata de personas, tráfico de órganos y la legitimación de capitales, hacia nuevas estrategias del mercado, nuevas tecnologías y dinámicas económicas, que combinadas transforman la sociedad, aceleran el desequilibrio financiero e incrementan los desafíos para los organismos encargados de hacer cumplir la ley.

Sobre base tecnológica nacen las nuevas empresas tecnológico-financieras — Fintech—, contracción de la frase en inglés “Financial Technology” – “Tecnología Financiera”, innovación y digitalización inclusiva de las finanzas con mecanismos de pago, inversión y ahorro al margen de la estructura bancaria institucionalizada, acogiendo en su ecosistema a los criptoactivos como las criptomonedas calificada como un activo digital, no disponible en representación física, tenemos los *tokens* considerados activos digitales que se crean sobre otra base criptográfica y se utilizan como medio de pago o de inversión y *stablecoins* que son activos digitales cuyo valor se respalda en monedas fiat o dinero respaldado por los Estados, o en activos físicos que funcionan bajo una estructura descentralizada utilizando interfaces digitales como aplicaciones móviles, plataformas web (redes de información) y APIs (aplicaciones para el intercambio de datos o interconexión de información), que son los puentes de conexión y comunicación entre sistemas, que en esencia representan la arquitectura Fintech.

A la par del ecosistema Fintech se ha venido fortaleciendo el fraude financiero, cuya modalidad sigue siendo valerse del engaño para obtener ilegalmente una ventaja financiera sobre una persona o entidad, un esquema que se remonta a siglos, conociéndose en la era moderna como el esquema ponzi, atribuida a Charles Ponzi, inmigrante italiano que se hizo famoso a principios del siglo XX por su esquema de inversión fraudulento que consistía en un plan de inversión de alto rendimiento que prometía ganancias extraordinarias, provocando en agosto de 1920 un colapso financiero que dejó una serie advertencia sobre estos esquemas financieros que prometen grandes riquezas en corto tiempo.

El marketing de impacto es una importante estrategia para promocionar un producto financiero, conjugando acciones para maximizar los resultados promocionales a través de la ingeniería social, transmisión de un mensaje claro de los beneficios del producto financiero, fomentar la confianza mediante el uso de elementos audiovisuales, mensaje y tono de voz claro, el uso de multicanales como redes sociales, publicidad online, televisión, radio, medios impresos, testimonios de clientes y casos de éxito en la mejora de su situación financiera, el uso de *influencers* y personalidades de reconocimiento público para la promoción de activos, entre otras.

Tomando en consideración el ecosistema Fintech, su uso para el fraude financiero y las estrategias del marketing de impacto, mediante un estudio documental y descriptivo, incorporando el uso responsable de la Inteligencia Artificial como un recurso de apoyo para seleccionar doctrina y estudios relacionados, se realiza el presente análisis sobre la identificación de la combinación de estos elementos como una señal de alerta primaria en la legitimación de capitales y recomendaciones de algunas señales de alerta.

Legitimación de Capitales, fases y señales de alerta.

La legitimación de capitales comprende el movimiento de fondos derivados de actividades ilícitas, con el propósito de ocultar el origen de dichos fondos, el dinero representa la motivación para las actividades criminales, derivando en que los narcotraficantes, autores de fraudes financieros y los grupos del crimen organizado inviertan considerables esfuerzos para conferirle legitimidad a sus ganancias ilícitas para poder mantener un estilo de vida costoso.

- **Legitimación de Capitales (LC):** En la legislación nacional, la base es la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT, 2012), la cual tipifica la legitimación de capitales como un delito autónomo en su artículo 35.

“...se entiende por legitimación de capitales el proceso de esconder o dar apariencia de legalidad a capitales, bienes, haberes provenientes de actividades ilícitas.”

- **Legitimación de Capitales (LC):** El profesor Blanco (2015) citado por Gerbasi (2016) la define como:

“...Proceso en virtud del cual los bienes de origen delictivo se integran en el sistema económico legal con apariencia de haber sido obtenidos de forma lícita”.

Movimiento de fondos que se ejecuta en etapas sistematizadas y expuestas ampliamente por la Doctrina, que se han diversificado adaptándose al comportamiento del mercado y surgimiento de nuevas tecnologías, a los efectos se adopta la concepción de Gerbasi (2016).

- Colocación: Consiste en deshacerse del dinero efectivo en los bancos sin levantar sospechas y evitando que se investigue el origen de los fondos.
- Diversificación: “desligar los fondos ilícitos de su origen, generando para ello un complejo sistema de amontonamiento (*layering*) de transacciones encaminado a borrar la huella contable de tales fondos ilícitos”, Grupo de Acción Financiera Internacional (GAFI.)
- Integración: “conferir una apariencia de legalidad a un patrimonio de origen criminal” (Gerbasi, 2016, p. 84).

Mecanismos para la identificación de operaciones inusuales: Señales de alerta.

Las señales de alerta comprenden las actividades o transacciones que, por sus características o condiciones, ponen en alerta a los sujetos obligados y a los órganos de control. Dichas señales de alerta siguen los estándares del GAFI (2025) bajo un enfoque basado en riesgo (EBR) estructuradas en tres áreas de riesgo: geográfico o de país, cliente y de servicio, entre las que se mencionan:

I. Riesgo geográfico o de país

- Sanciones y Embargos: Jurisdicciones sujetas a regímenes de sanciones, embargos o contramedidas financieras.
- Regímenes débiles: Países o territorios identificados con deficiencias estratégicas en su gobernanza regulatoria.

- Criminalidad transnacional: Zonas con altos índices de criminalidad organizada, corrupción endémica, o catalogadas como rutas activas de economías ilícitas.

II. Riesgo del cliente

- Opacidad en la estructura jurídica: Dificultad para identificar al beneficiario final mediante el uso injustificado de corporaciones pantalla.
- Perfil económico inconsistente: Fondos u operaciones comerciales que resultan desproporcionados frente al perfil sociodemográfico, ocupación, edad o ingresos declarados del cliente.
- Uso de activos virtuales no regulados: Clientes que insisten en operar de manera exclusiva mediante activos virtuales o plataformas que carecen de registro o controles de LC.

III. Riesgo en el servicio / transacción

- Uso de tecnologías emergentes: Servicios o captaciones estructuradas bajo esquemas de activos virtuales, Fintech sin registro.
- Intervención de terceros: Recepción de pagos provenientes de terceros no asociados o desconocidos, bajo condiciones lógicas confusas.
- Transacciones sin propósito legítimo: Operatividad comercial o movilizaciones de fondos que carecen de una explicación legal, fiscal, financiera o de gobernanza clara.

Detectar las señales de alerta es fundamental en la lucha contra la LC, contribuyendo en la identificación temprana de actividades potencialmente sospechosas, permitiendo a los sujetos obligados ejercer acciones inmediatas para advertir las pretensiones de usar los sistemas financieros por grupos delictivos estructurados y a los organismos de regulación, actuar para evitar que se materialice la actividad delictiva.

Como se aprecia en la relación *supra*, las nuevas tecnologías financieras han sido incorporadas en las señales de alerta, sin embargo, la celeridad y creatividad que acompaña a este sistema lo impulsa a avanzar con mayor rapidez, valiéndose estratégicamente de las plataformas de comunicación masiva o redes sociales, las inestabilidades económicas y el interés social de obtener mayores rendimientos con el menor esfuerzo.

Fintech: ecosistema innovador disruptivo del sistema financiero tradicional

Fintech es un término que incluye la innovación tecnológica aplicada al diseño, entrega y eficiencia de servicios financieros. Las empresas que combinan tecnología con las finanzas se han ido incrementando, estableciendo una competencia entre las estructuras bancarias y las empresas Fintech, adoptando los criptoactivos incluyendo criptomonedas, tokens y stablecoins como medios de pago, inversión, ahorro, transacción e intercambio, en plataformas conocidas como *exchanges* o casas de intercambio, formalmente denominados por el GAFI (2018) como Activos virtuales (AV) y Proveedores de servicios de activos virtuales (PSAV).

El referido ecosistema se encuentra bajo estricta regulación de órganos de control, la Fintech por la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN) y por el otro la Superintendencia Nacional de Criptoactivos (SUNACRIP), con dos instrumentos normativos que buscan prevenir que estas innovaciones de la tecnología financiera sean utilizadas para la legitimación de capitales, como son la Resolución N° 001-21 publicada en Gaceta Oficial de la República Bolivariana de Venezuela N° 42.151 del 17 de junio de 2021, la Providencia N° 044-2021 publicada en Gaceta Oficial de la República Bolivariana de Venezuela Número 42.110 de fecha 21 de abril de 2021 respectivamente, y la Resolución N° 010.25, emanada de la Superintendencia de las instituciones del sector bancario SUDEBAN, de fecha 20 de marzo de 2025, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela N° 43.098, del 31 de marzo de 2025.

El fraude financiero en la era digital:

La dinámica del ecosistema Fintech y el anonimato para garantizar la privacidad financiera que ofrecen los criptoactivos, resultan un escenario atractivo para la delincuencia organizada, fomentando el fraude financiero.

Al respecto, la posición de Savona y Defeo (1994) citados por Blanco (2015, pág.56) sobre la separación progresiva entre las actividades criminales y la legitimación de capitales, atribuida por los autores a una mayor profesionalización de los miembros de la organización y mayor empleo de profesionales externos, inversión en recursos para el empleo de tecnología para profesionalizar el ciclo del blanqueo-inversión, resulta concordante con la doctrina de los referidos autores, indicando que en las sociedades modernas, los actores sociales han aprendido a explotar los mercados globales.

Bases teóricas que resultan cónsonas, con la canalización de recursos de las estructuras delictivas hacia sofisticadas plataformas digitales que facilitan la captación, transacción, intercambio y ocultación de activos en escenarios de bajos niveles de registro y control, preeminente anonimato, amplio alcance transfronterizo, fortaleciéndose con la persuasión y fastuosidad de una extensa y creíble estrategia de marketing.

El Fenómeno del Marketing de Impacto en el Sector Financiero.

- Marketing de impacto y de alta resonancia: En contexto de la investigación por marketing digital internacional se refiere al conjunto de estrategias dirigidas a la comunicación y comercialización en línea fuera del país de origen de productos y servicios. Katsikeas et al., (2020) citado por García et al., (2024) radicando su relevancia en la necesidad de combinar y aplicar estrategias gerenciales con las tendencias de estrategias de mercadeo, para elevar el nivel de competitividad de las empresas.

Siendo la nueva tendencia el “marketing de impacto” que es una estrategia que busca trascender las ventas hacia la generación de

cambios profundos en la sociedad, promoviendo y diseñando soluciones en beneficio de la comunidad, va más allá de la cultura comercial del consumo e impulso de ventas de determinados productos o servicios.

- La psicología de la confianza masiva: Se caracteriza por transmitir mensajes claros, directos y transparentes, a lo que agregaría también convincentes, presentación del producto como una verdadera solución a los problemas. Se enfoca en las emociones humanas y como la plantean (Loor et al., 2021): “La psicología tiene un rol muy importante en el marketing, ya que conoce cómo funciona la mente humana teniendo en cuenta los factores sociales, políticos y culturales de su entorno”.
- El rol de las redes sociales y la economía de los *influencers* en la promoción de activos: Concluye Delgado (2023) que el uso de los *influencers* como herramienta de marketing tiene como propósito conectar las marcas con las personas a través de figuras públicas que ayuden a promocionar un producto o servicios y que generan confianza a través de redes sociales que se han convertido en los nuevos medios de comunicación que llegan directo al consumidor, es decir, influyen en la decisión de los consumidores y no es necesariamente un experto en el tema, puesto que es su imagen y credibilidad lo que va a otorgar confianza en el producto o servicio que se ofrece.

Concluye García et al., (2024) que el marketing en redes sociales sigue siendo una estrategia efectiva para maximizar la experiencia del cliente y la combinación de redes sociales con otros canales digitales constituye parte del enfoque multifacético de adaptación tecnológica.

Casos Emblemáticos: La fastuosidad como estrategia de fraude y ocultación

Para los efectos, tres casos emblemáticos de criptomonedas motivaron el presente estudio y se plantean a continuación:

- **Caso OneCoin:** Un esquema internacional de inversión en criptomonedas a través del cual se estafó a inversores de todo el mundo por una cifra de más de 4 mil millones de dólares, una narrativa liderada por una profesional, la búlgara Ruja Ignatova, una empresaria de las finanzas egresada de una reconocida universidad que le otorgaba credibilidad, se subió al escenario del Wembley Arena, un estadio cubierto en Londres, frente a miles de admiradores que la ovacionaban anunció el lanzamiento de un proyecto que prometía rentabilidad a sus inversores, utilizando una supuesta plataforma de intercambio, que no contaba con el registro digital propio de las criptomonedas. Se trató de un esquema Ponzi estructurado, impulsado por una campaña de marketing de impacto global multicanal y eventos masivos de gala y la representación de una persona con elevado nivel profesional y con un mensaje claro y firme que prometía la solución económica de todos los que se unieran, garantizando grandes ganancias para sus inversores.

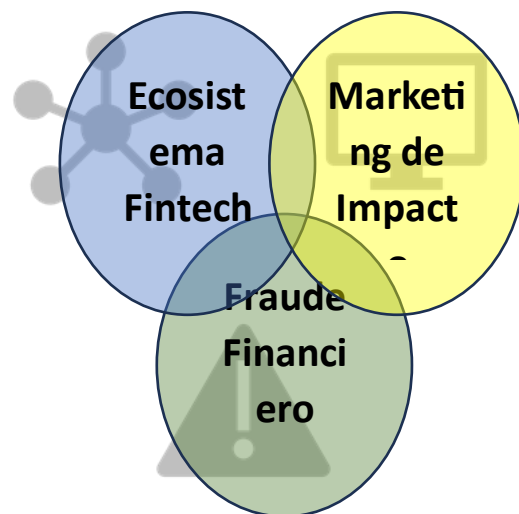
- **Caso FTX:** A través de una plataforma de intercambio de criptomonedas denominada FTX se malversaron miles de millones de dólares, estafando a inversionistas por más de 3 mil millones de dólares, su creador Samuel Bankman-Fried un genio de la tecnología, fue condenado a 25 años de prisión, declarado culpable por diversos cargos entre los que destacan fraude electrónico y conspiración para cometer lavado de dinero, entre otros. Hasta el 2022 la plataforma FTX era una de las plataformas de intercambio más grandes, empleando una agresiva campaña de marketing entre los que destacaron anuncios en el Super *Bowl* un evento de gran impacto, en el que se juega la final de la liga de fútbol norteamericana y el respaldo de celebridades. Elementos que resultan de interés como: elevado nivel profesional del actor principal, campaña de marketing que incluyó celebridades de primer nivel, patrocinios deportivos millonarios e institucionalidad ficticia.

- **Caso BitConnect:** Se trató de una plataforma de inversión en criptomonedas a través de la cual Satish Kumbhani y sus cómplices obtuvieron aproximadamente 2.400 millones de dólares de los inversores,

impulsó el aumento de la criptomoneda *BitConnet*, utilizando además dicha plataforma para ocultar los fondos obtenidos de sus inversionistas, mezclando e intercambio en diversas plataformas de intercambio, tratando de ocultar el rastro. *BitConnect* utilizó un agresivo marketing multinivel y de *influencers*, que garantizaban ganancias astronómicas. Su estrategia se basaba en la captación de novatos en criptomonedas a través de YouTube, eventos masivos, conferencias y un sistema de referidos que fomentaba la expansión piramidal, estrategias de contenido para el desvío de atención regulatoria.

Estos casos denotan las siguientes características: a) Uso de herramientas del ecosistema Fintech como una solución económica sobre la base de la tecnología financiera, que en los casos de *OneCoin* y *BitConnet* no existía el supuesto registro digital; b) Estrategias de marketing de impacto multinivel a través de redes sociales, canales de youtube, televisión, eventos masivos de gala, *influencers* y figuras públicas; c) La obtención de elevadas sumas de dinero de inversionistas que apostaban a la plataforma bajo promesa de altos índices de ganancia.

Sobre la base de los tres casos supra señalados, esta combinación de elementos representa un riesgo que amerita especial observación y evaluación, a los fines de generar señales de alerta y acciones preventivas.



Fuente: Mendoza (2026)

Recomendaciones y Conclusiones

Lo que pareciera un avance de la sociedad moderna, se convirtió en el escenario ideal para el perfeccionamiento de métodos delictivos de fraude financiero y ocultamiento de fondos obtenidos de los inversionistas. Como se evidencia de los casos precedentes, la combinación maquiavélica de importantes progresos estratégicos como el ecosistema Fintech y el Marketing de Impacto, ponen de manifiesto señales de alerta que no se deberían ignorar.

Ante el desafío que representa la supervisión de transacciones en entornos descentralizados o no regulados, aludiendo a Saldaña-Taboada (2025) es importante tomar en consideración que no es suficiente regular a las criptomonedas, siendo necesario detener el avance de estos mecanismos de fraude, que se valen de las nuevas tecnologías y estrategias de promoción altamente persuasivas con fines delictivos.

En ese sentido, la implementación de evaluación y seguimiento de campañas de marketing multinivel como mecanismo de alerta temprana, mediante herramientas que generen señales de alerta y vinculación de administradores y seguidores, enfocados en estos mercados emergentes de promoción de nuevas tecnologías financieras. A fin de detectar estructuras de fraude financiero y legitimación de capitales que utilizan el mercadeo digital como fachada para esquemas de captación de inversores, obtención de ganancias fraudulentas o legitimación de capitales.

Tomando en consideración que las señales de alerta tradicionales son reactivas, por cuanto, se activan cuando el dinero ya entró al sistema bancario, establecer mecanismos de monitoreo del marketing digital agresivo permitiría una actuación proactiva.

A continuación, se formula una propuesta de señales de alerta que conjuga las acciones de una estrategia de marketing de impacto y el nivel de riesgo que representa de las siguientes variables: 1. Intensidad de la campaña; 2. Perfil de

los promotores y 3. Estatus regulatorio, aplicando el nivel de riesgo según las particularidades de las variables.

Nivel de Riesgo	1. Intensidad de la Campaña	2. Perfil de los Promotores	3. Estatus Regulatorio
Bajo	Difusión limitada a canales propios (redes institucionales, página web), sin pauta publicitaria masiva ni eventos suntuosos.	Voceros autorizados de la empresa, directivos registrados ante SUDEBAN y personal técnico calificado.	Registro y autorización vigentes como Institución de Tecnología Financiera (ITF) ante la SUDEBAN / SUNACRIP.
Moderado	Campañas en redes sociales con presupuesto definido, segmentación de nicho y eventos de lanzamiento estándar o corporativos.	<i>Influencers</i> de nicho: creadores de contenido especializados en finanzas, economía o tecnología con audiencias medianas.	Operando bajo modalidades de prueba regulatoria o licencias provisionales en fase de evaluación técnica.
Alto a Crítico	Eventos suntuosos en hoteles de lujo, vallas en vía pública, comerciales de alta rotación en medios masivos y promesas de rendimientos extraordinarios.	Influencers o figuras públicas del entretenimiento o deportes sin conocimientos técnicos, que promueven la captación por empatía.	Operaciones al margen de la SUDEBAN (sin registro), utilizando pasarelas de pago extranjeras o promoviendo activos virtuales no regulados.

Fuente: Mendoza (2026) en colaboración con el modelo de lenguaje artificial Gemini (Google, 2026).

Referencias

- Asamblea Nacional de la República Bolivariana de Venezuela. (2012). *Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT)*. Gaceta Oficial N° 39.912.
- Blanco, I. (2015). El delito de blanqueo de capitales (4a ed.). Editorial Aranzadi.
- Departamento de Justicia. <https://www.justice.gov/usao-sdny> Consulta 23/06/2026.
- Delgado E. (2023). Marketing de Influencia: El rol de los Influencers dentro del marketing en las redes sociales. Revista Sinapsis. Vol. 1, Nro 22, junio de 2023, ISSN 1390 – 9770
- Escuela Nacional de Administración y Hacienda Pública. (2016). *Manual para elaboración y presentación de trabajos académicos*. ENAHP-IUT. Caracas.

- García, J., Zamora, M., & Ortíz, R. (2024). Estrategias de marketing digital internacional y su impacto en la experiencia del cliente: una revisión sistemática de la literatura (Prisma, 2020). *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades* 5 (5), 2651 – 2669. <https://doi.org/10.56712/latam.v5i5.2804>
- Gerbasí, G. (2016). *El tratamiento de la legitimación de capitales y el financiamiento al terrorismo en la legislación venezolana*. Alvaronora.
- Grupo de Acción Financiera Internacional. (2018). *Regulación 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*
- Grupo de Acción Financiera Internacional (GAFI). (2025). *Orientación para un enfoque basado en riesgos. Activos Virtuales y Proveedores de servicios de Activos Virtuales*.
- ROSAPARKS (2026). Comprendiendo el Marketing de Impacto. <https://rosaparks.es/blog/marketing-impacto/> Consulta 21/06/2026.
- Saldaña-Taboada, P (2025). "Criptomonedas y fraude: estafas de inversión". En *CiberData*, núm. 1, 2025, pp. 19-23.
- Lloor T., Reyna V., Silva S., y Macías O. (2021) La psicología aplicada al marketing y su influencia en las emociones del consumidor ecuatoriano. *Revista Caribeña de Ciencias Sociales* (vol 10, Nº 4 abril 2021, pp. 100-120). línea: <https://www.eumed.net/es/revistas/caribena/abril-21/psicologia-marketing>.

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 de Administración de Riesgos de
Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Señales de Alerta

**El radar bursátil: Señales de alerta, actores ocultos e inteligencia
financiera como escudo del mercado de valores venezolano**

Autora: Gianni Verasmendi

Facilitadora: Elizabeth Peláez

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 de Administración de Riesgos de
Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Señales de Alerta

**El radar bursátil: Señales de alerta, actores ocultos e inteligencia
financiera como escudo del mercado de valores venezolano**

Autora: Gianni Verasmendi

ID Orcid: 0009-0004-0873-3484

Correo electrónico: gverasmendi@gmail.com

Resumen

El mercado de valores venezolano, por su función de canalizar el ahorro hacia la inversión productiva, constituye un objetivo atractivo para la legitimación de capitales y el financiamiento al terrorismo. Este ensayo analiza, desde una perspectiva metodológica y normativa, los pilares fundamentales para una prevención efectiva en este sector. Se examina el marco jurídico aplicable, integrado por la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo, los estándares del Grupo de Acción Financiera Internacional (GAFI), la Providencia SUNAVAL N° 025 y el conjunto de circulares emitidas por la Unidad Nacional de Inteligencia Financiera (UNIF). Se desglosan las señales de alerta específicas del sector, con énfasis en la fase preoperativa de listado en bolsa y en la cadena de actores que intervienen: abogados, contadores públicos, economistas e inversionistas. Se argumenta que la debida diligencia debe trascender la verificación documental aislada para enfocarse en la coherencia sistémica entre la declaración del Impuesto sobre la Renta, los estados financieros auditados y los atestiguamientos de ingresos, pues las discrepancias entre estos documentos constituyen las señales de alerta más reveladoras. Finalmente, se proponen recomendaciones para fortalecer el radar preventivo y se reflexiona sobre la necesidad de un cambio cultural hacia la transparencia en el ecosistema bursátil.

Descriptor clave: Señales de Alerta, Debida Diligencia, Actividades Profesionales No Financieras Designadas (APNFD), Beneficiario Final, Coherencia Documental.

Abstract

The Venezuelan securities market, due to its role in channeling savings towards productive investment, constitutes an attractive target for money laundering and

terrorist financing. This essay analyzes, from a methodological and regulatory perspective, the fundamental pillars for effective prevention in this sector. The applicable legal framework is examined, including the Organic Law against Organized Crime and Terrorist Financing, the Financial Action Task Force (FATF) standards, SUNAVAL Provision No. 025, and the set of circulars issued by the National Financial Intelligence Unit (UNIF). Specific red flags for the sector are detailed, with emphasis on the pre-operational phase of stock market listing and the chain of actors involved: lawyers, public accountants, economists, and investors. It is argued that due diligence must transcend isolated document verification to focus on the systemic coherence between the Income Tax Return, audited financial statements, and income attestations, as discrepancies between these documents constitute the most revealing red flags. Finally, recommendations are proposed to strengthen the preventive radar and reflect on the need for a cultural shift towards transparency in the stock market ecosystem.

Key descriptors: Red Flags, Due Diligence, Designated Non-Financial Businesses and Professions (DNFBPs), Beneficial Ownership, Documentary Coherence.

Introducción

El mercado de valores venezolano, como cualquier plaza bursátil, cumple una función esencial en la canalización del ahorro hacia la inversión productiva. Sin embargo, esa misma función lo convierte en un objetivo apetecible para las organizaciones criminales que buscan integrar capitales de origen ilícito al circuito económico formal. La legitimación de capitales, el financiamiento al terrorismo y el financiamiento de la proliferación de armas de destrucción masiva encuentran en los mecanismos bursátiles como la emisión de títulos, la compraventa de valores, la administración de carteras en un conducto potencialmente eficaz si no se aplican controles rigurosos (Grupo de Acción Financiera Internacional GAFI, 2025, p. 7). En este contexto, las señales de alerta constituyen el primer radar que permite a los sujetos obligados del sector valores detectar operaciones inusuales o sospechosas, activando los mecanismos de reporte que alimentan la inteligencia financiera del Estado.

Ahora bien, una mirada superficial al mercado de valores podría sugerir que los únicos actores relevantes para la prevención son las casas de bolsa, los corredores públicos y las entidades emisoras. Nada más alejado de la realidad. Para que una empresa pueda listarse en bolsa y emitir títulos valores, se requiere la intervención de una cadena de profesionales cuyas actuaciones son, con frecuencia, la puerta de entrada de los capitales ilícitos o, por el contrario, la primera barrera de contención. Firmas de contadores públicos que auditan estados financieros bajo los estándares exigidos por la Superintendencia Nacional de Valores (SUNAVAL), abogados que constituyen las personas jurídicas, economistas y administradores que elaboran estudios de factibilidad y valoraciones de empresas, e incluso los propios inversionistas que presentan atestiguamientos de ingresos para justificar el origen de sus fondos: todos ellos

conforman un ecosistema en el que cada eslabón puede generar señales de alerta y, por tanto, debe estar sujeto a obligaciones de debida diligencia y reporte.

El presente ensayo aborda, desde la perspectiva de la Especialización en Gestión contra Legitimación de Capitales y Financiamiento al Terrorismo, los pilares fundamentales para una prevención efectiva en el mercado de valores venezolano. Se analiza el marco jurídico aplicable, las señales de alerta específicas del sector, incluyendo aquellas que se generan en la fase preoperativa de listado y en la fase transaccional, el papel de los sujetos obligados y de las Actividades Profesionales No Financieras Designadas (APNFD) que intervienen en el proceso, la correcta elaboración del Reporte de Actividades Sospechosas (RAS) conforme a las circulares de la Unidad Nacional de Inteligencia Financiera (UNIF), y el rol de esta última dentro de la arquitectura institucional que encabeza la Oficina Nacional contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT). Se presta especial atención a las relaciones de coherencia que deben existir entre la declaración del Impuesto Sobre la Renta (ISLR), los estados financieros auditados y los atestiguamientos de ingresos, pues es precisamente en las discrepancias entre estos documentos donde anidan algunas de las señales de alerta más reveladoras.

El marco jurídico del mercado de valores venezolano y el sistema de Administración de Riesgos de Legitimación de Capitales y Financiamiento al Terrorismo

El mercado de valores venezolano opera bajo un marco jurídico que, en materia de prevención de legitimación de capitales, no ha experimentado un proceso de actualización. La Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT), publicada en la Gaceta Oficial N° 39.912 del 30 de abril de 2012, establece la arquitectura institucional del sistema venezolano. Su artículo 6 crea la Oficina Nacional contra la Delincuencia Organizada y Financiamiento al Terrorismo (ONCDOFT) como ente rector del sistema nacional de prevención y control, mientras que su artículo 9 define a los sujetos obligados, incluyendo expresamente a las entidades que operan en el mercado de valores (Asamblea Nacional, 2012). Por su parte, la Unidad Nacional de Inteligencia Financiera (UNIF), cuyo marco legal fue actualizado mediante el Decreto con Rango, Valor y Fuerza de Ley N° 2.239 del 26 de abril de 2016, actúa como el órgano especializado encargado de recibir, analizar y diseminar los Reportes de Actividades Sospechosas (Presidencia de la República, 2016).

En el plano internacional, los estándares del GAFI constituyen una referencia ineludible. La edición de 2025 de las Recomendaciones del GAFI incorpora ajustes en materia de beneficiario final y activos virtuales que son directamente aplicables al mercado de valores (GAFI, 2025). La Metodología para la Evaluación del Cumplimiento Técnico y la Efectividad de los Sistemas LC/FT (GAFI, 2024) es el instrumento que guía la Quinta Ronda de Evaluaciones Mutuas, en la que se examina, entre otros aspectos, la efectividad con que los supervisores del mercado de valores en Venezuela, la Superintendencia

Nacional de Valores (SUNAVAL) monitorean y fiscalizan el cumplimiento de las obligaciones preventivas.

En desarrollo de este marco, la SUNAVAL emitió la Providencia N° 025, publicada en la Gaceta Oficial N° 43.096 del 27 de marzo de 2025, contentiva de las 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 (SUNAVAL, 2025). Esta providencia crea un marco normativo unificado que exige a todos los sujetos controlados casas de bolsa, corredores públicos, entidades emisoras, custodios, entre otros la implementación de un sistema integral de administración de riesgos con enfoque basado en riesgos.

Complementando este marco, la UNIF ha emitido un conjunto de normativas que, concatenado con las normas anteriores, configuran el andamiaje preventivo específico del mercado de valores. Cuatro instrumentos destacan por su relevancia y por su interacción sistemática. En primer lugar, la Circular UNIF-DDG-DSU-01563, dirigida a la SUNAVAL, que establece señales de alerta, controles internos y directrices relacionadas con los RAS para los sujetos controlados del mercado de valores (UNIF, 2023c). Esta circular es particularmente importante porque representa una intervención directa de la UNIF sobre el órgano supervisor, impartándole directrices vinculantes sobre el catálogo de señales de alerta que deben ser monitoreadas y sobre los controles internos que los sujetos obligados deben implementar.

En segundo lugar, la Circular UNIF-DDG-DSU-07210, dedicada exclusivamente a los sujetos obligados del sector valores, que profundiza en las señales de alerta, los controles internos y los procedimientos para la presentación del RAS, y que puede ser considerada como el desarrollo específico de las directrices generales contenidas en la Circular UNIF-DDG-DSU-01563 (UNIF, 2025e). Esta circular amplía el catálogo de señales de alerta operacionales y establece procedimientos detallados para la identificación del beneficiario final en el contexto bursátil.

En tercer lugar, el Instructivo UNIF-DDG-DGOE-003081 sobre señales de alerta, controles internos y directrices relacionadas con los RAS (UNIF, 2023a), que complementa a las dos circulares anteriores con lineamientos adicionales, y, en cuarto lugar, la Circular UNIF-DDG-001617 del 8 de mayo de 2024, que detalla el envío de reportes de actividades sospechosas (RAS de forma general (UNIF, 2024a). A este entramado se suma la Circular UNIF-DDG-DSU-05448 sobre identificación del beneficiario final, aplicable a todos los sectores (UNIF, 2025a).

La interacción entre estos instrumentos configura un sistema normativo de múltiples capas, la ley orgánica, providencia supervisora y circulares de la UNIF que, al menos en su diseño formal, satisface los estándares internacionales exigidos por el GAFI.

La cadena de actores en el proceso de listado en bolsa y sus señales de alerta específicas

Una de las contribuciones más importantes de un enfoque preventivo aplicado al mercado de valores es la comprensión de que el riesgo no comienza cuando un título se negocia en la rueda de la bolsa, sino mucho antes, en el momento en que una empresa decide acceder al mercado de capitales. La Circular UNIF-DDG-DSU-07210 es particularmente enfática en este punto, al señalar que los sujetos obligados del sector valores deben aplicar la debida diligencia desde el primer contacto con el cliente potencial, y no solo al momento de la transacción (UNIF, 2025e). El proceso de listado en bolsa ya sea para emitir acciones, obligaciones, papeles comerciales o cualquier otro instrumento involucra una sucesión de actores cuyas actuaciones deben estar alineadas con los más altos estándares de debida diligencia. Veamos cada uno de ellos y las señales de alerta que pueden generar, a la luz de las normativas vigentes.

El punto de partida suele ser la constitución de la persona jurídica que actuará como emisora. Aquí intervienen los abogados en libre ejercicio, quienes redactan el acta constitutiva y los estatutos sociales, definen la estructura de propiedad y establecen los mecanismos de control. La Recomendación 22 del GAFI extiende a estos profesionales las obligaciones de debida diligencia del cliente, y la Recomendación 23 les exige reportar las operaciones sospechosas (GAFI, 2025, Rec. 22 y 23). En Venezuela, la Circular UNIF-DDG-DSU-04409 de noviembre de 2023 formaliza esta obligación (UNIF, 2023b). Las señales de alerta que un abogado debe considerar en esta fase incluyen, entre otras: la utilización de testaferros o accionistas nominales que ocultan al verdadero beneficiario final, la creación de estructuras societarias excesivamente complejas e innecesarias para el giro del negocio, la constitución de empresas con capitales mínimos que no guardan relación con el volumen de la emisión prevista, el domicilio de la empresa en jurisdicciones de baja tributación sin una justificación económica plausible y la negativa del cliente a proporcionar información sobre el origen de los fondos con los que se suscribe el capital social (UNIF, 2023b; GAFI, 2023). La Circular UNIF-DDG-DSU-05448 refuerza estas exigencias al establecer directrices específicas para la identificación del beneficiario final en estructuras jurídicas (UNIF, 2025a).

Una vez constituida la empresa, el siguiente paso crítico es la preparación de los estados financieros que serán presentados ante la SUNAVAL como parte de los requisitos de listado. Aquí entran en escena los contadores públicos en libre ejercicio y las firmas de auditoría. La normativa de la SUNAVAL exige que los estados financieros de las entidades emisoras sean auditados por contadores públicos independientes, aplicando estándares que garanticen la fiabilidad de la información (SUNAVAL, 2025). La Circular UNIF-DDG-DSU-01563, en su catálogo de señales de alerta, incorpora indicadores directamente relacionados con esta fase, la presentación de estados financieros que no reflejen la situación real de la empresa, las discrepancias significativas entre los ingresos reportados

en los estados financieros y los declarados ante la administración tributaria, y la resistencia de los auditores externos a proporcionar información adicional cuando les es requerida (UNIF, 2023c). La Circular UNIF-DDG-DSU-07210 complementa este catálogo al incluir como señal de alerta específica "la presentación de estados financieros auditados por firmas que no están debidamente inscritas en el registro de la SUNAVAL o que presentan un historial de sanciones" (UNIF, 2025e). El Boletín UNIF N° 003-2024, dedicado específicamente a los contadores públicos, añade otras señales como la detección de ingresos no justificados, el uso de empresas de papel sin actividad real, la sobrevaloración o subvaloración injustificada de activos, y la presión indebida del cliente para que el auditor emita una opinión favorable sin las verificaciones correspondientes (UNIF, 2024b).

Los economistas y administradores también juegan un papel fundamental en esta fase preoperativa, pues son quienes elaboran los estudios de factibilidad económica y las valoraciones de empresas que acompañan la solicitud de listado. Las señales de alerta en este ámbito, recogidas por la Circular UNIF-DDG-DSU-07210, incluyen proyecciones de ingresos notoriamente infladas que no se sustentan en datos verificables del mercado, valoraciones que utilizan metodologías inadecuadas o que se apartan de las prácticas generalmente aceptadas sin una razón técnica válida y la omisión de riesgos materiales que cualquier analista razonable habría identificado (UNIF, 2025e).

Una vez que la empresa está listada, el foco se desplaza hacia los inversionistas que adquieren los títulos. Aquí cobran especial relevancia los atestiguamientos de ingresos, que son los documentos mediante los cuales un profesional generalmente un contador público o un administrador certifica la capacidad económica de un cliente para realizar una inversión. La coherencia entre estos atestiguamientos y otros documentos es una fuente riquísima de señales de alerta. Por ejemplo: un atestiguamiento que declara ingresos anuales significativos debe guardar una relación lógica con la declaración del ISLR del mismo período, si un inversionista presenta un atestiguamiento que refleja ingresos muy superiores a los declarados fiscalmente, se activa una señal de alerta que exige una investigación más profunda. Del mismo modo, los estados financieros de la empresa emisora deben ser consistentes con las declaraciones fiscales presentadas ante el Servicio Nacional Integrado de Administración Aduanera y Tributaria (SENIAT). Una empresa que reporta utilidades sustanciales en sus estados financieros, pero declara pérdidas o ingresos ínfimos ante el fisco está emitiendo una señal de alerta inequívoca. La Circular UNIF-DDG-DSU-07210 aborda expresamente esta problemática al incluir, dentro de su catálogo de señales de alerta, la presentación de atestiguamientos de ingresos que no guardan relación con la declaración de impuesto sobre la renta del cliente y la existencia de discrepancias significativas entre la documentación financiera, fiscal y la información proporcionada por el cliente (UNIF, 2025e). La Circular UNIF-DDG-DSU-05448, por su parte, refuerza la exigencia de que la información sobre el beneficiario final sea coherente con la documentación fiscal y financiera disponible (UNIF, 2025a).

Señales de alerta operacionales en la fase transaccional del mercado de valores

Además de las señales que se generan en la fase de listado y en la documentación preoperativa, el mercado de valores presenta un conjunto de señales de alerta operacionales que se manifiestan durante la negociación de los valores. La Circular UNIF-DDG-DSU-01563 compila un catálogo detallado de estas señales, entre las que destacan: la compra o venta de valores a precios notoriamente más altos o más bajos que las cotizaciones de mercado, lo que puede indicar un intento de transferir valor de manera artificial, las transacciones que no guardan relación con el perfil del inversionista ni con una estrategia de diversificación de riesgos, las operaciones de compra y venta sucesivas del mismo título en un corto período sin un propósito económico aparente y los movimientos frecuentes de títulos entre cuentas de una misma casa de bolsa sin justificación (UNIF, 2023c).

La Circular UNIF-DDG-DSU-07210 amplía este catálogo con señales adicionales como "la utilización de testaferros o personas interpuestas para realizar operaciones bursátiles" y "la fragmentación de órdenes de compra o venta para evadir los umbrales de reporte" (UNIF, 2025e). El Instructivo UNIF-DDG-DGOE-003081 complementa estas señales con directrices para la implementación de controles internos (UNIF, 2023a), mientras que la Providencia N° 025 de SUNAVAL exige a los sujetos controlados que incorporen todas estas señales en sus matrices de riesgo y en sus sistemas de monitoreo automatizado (SUNAVAL, 2025).

Una señal de alerta particularmente relevante en el mercado venezolano es la utilización de los títulos valores como mecanismo para burlar los controles cambiarios o para legitimar capitales provenientes de actividades ilícitas mediante la simulación de inversiones bursátiles. En estos casos, el inversionista que en realidad es un testaferro adquiere títulos con fondos de origen ilícito y luego los vende, obteniendo recursos que ya aparecen como legítimos al estar respaldados por una operación bursátil documentada. La Circular UNIF-DDG-DSU-01563 identifica esta tipología al incluir como señal de alerta las operaciones de compra y venta de títulos valores sin un propósito económico aparente y las transacciones que involucran a personas o entidades que no tienen un perfil de inversión acorde con la operación realizada (UNIF, 2023c). La Circular UNIF-DDG-DSU-07210 complementa esta identificación al señalar como sospechosas las operaciones en las que el cliente no demuestra interés por el rendimiento de la inversión sino únicamente por la rápida liquidación de los títulos (UNIF, 2025e). La detección de este tipo de esquemas requiere que el oficial de cumplimiento de la casa de bolsa cruce la información transaccional con los atestiguamientos de ingresos, las declaraciones fiscales y la información sobre el beneficiario final, identificando las inconsistencias que delaten la simulación.

La debida diligencia aplicada al mercado de valores: más allá del formulario

La Recomendación 10 del GAFI sobre Debida Diligencia del Cliente adquiere en el mercado de valores una dimensión particularmente exigente (GAFI, 2025, Rec. 10). No basta con identificar al cliente y verificar su identidad mediante la cédula de identidad o el Registro de Información Fiscal, es necesario entender la naturaleza y el propósito de la relación comercial, construir un perfil transaccional que sirva de parámetro de normalidad, y mantener un monitoreo continuo que permita detectar las desviaciones que constituyen señales de alerta. La Circular UNIF-DDG-DSU-01563 refuerza este mandato al establecer que los sujetos obligados del sector valores deben aplicar medidas de debida diligencia reforzada cuando existan dudas sobre la veracidad de la información proporcionada por el cliente o cuando el perfil de riesgo así lo amerite (UNIF, 2023c). La Circular UNIF-DDG-DSU-07210, por su parte, desarrolla este mandato con mayor detalle, exigiendo a los sujetos obligados del sector valores que implementen procedimientos de debida diligencia que incluyan, como mínimo, la verificación del origen de los fondos, la identificación del beneficiario final y el cruce de la información financiera con la documentación fiscal del cliente (UNIF, 2025e).

En el caso de un inversionista persona natural, la debida diligencia debe incluir la verificación de sus ingresos mediante el cruce de fuentes documentales: el atestiguamiento de ingresos emitido por un profesional competente, la declaración del ISLR de los últimos ejercicios fiscales, y los estados de cuenta bancarios o cualquier otra documentación que acredite el origen lícito de los fondos. La inconsistencia entre estas fuentes no es solo una señal de alerta: es un indicador que, dependiendo de su magnitud y de la ausencia de explicaciones satisfactorias, puede ameritar la presentación de un Reporte de Actividad Sospechosa (RAS). La Circular UNIF-DDG-DSU-07210 es explícita al incluir como señal de alerta la presentación de documentos de soporte inconsistentes entre sí o que no puedan ser verificados de manera independiente y la negativa del cliente a proporcionar la declaración del ISLR cuando esta es requerida para verificar la coherencia de su perfil financiero (UNIF, 2025e). En el caso de una persona jurídica que actúa como emisora o como inversionista institucional, la debida diligencia debe alcanzar al beneficiario final, desentrañando las capas de propiedad hasta identificar a la persona natural que ejerce el control efectivo, tal como lo exige la Recomendación 24 del GAFI (GAFI, 2025, Rec. 24), la Circular UNIF-DDG-DSU-05448 (UNIF, 2025a) y la propia Circular UNIF-DDG-DSU-07210 (UNIF, 2025e).

La Providencia N° 025 de SUNAVAL establece que los sujetos controlados deben implementar un enfoque basado en riesgos, lo que significa que las medidas de debida diligencia deben ser más intensas cuando el cliente, el producto o la transacción presentan un perfil de riesgo elevado (SUNAVAL, 2025). La Circular UNIF-DDG-DSU-07210 establece que los sujetos obligados del sector valores deben implementar procedimientos de debida diligencia reforzada para aquellos clientes que presenten un perfil de riesgo alto, incluyendo la verificación de la

información mediante fuentes independientes y la aprobación de la relación comercial por parte de la alta gerencia (UNIF, 2025e).

Sujetos obligados y áreas sensibles en el ecosistema bursátil

La Providencia N° 025 de SUNAVAL exige a los sujetos controlados del mercado de valores que identifiquen sus áreas sensibles, es decir, aquellas unidades operativas donde el riesgo de legitimación de capitales es más alto (SUNAVAL, 2025). La Circular UNIF-DDG-DSU-01563 complementa esta exigencia al requerir que los sujetos obligados designen oficiales de cumplimiento con la autonomía necesaria y establezcan programas de capacitación continua para el personal de las áreas sensibles (UNIF, 2023c). La Circular UNIF-DDG-DSU-07210 añade que los programas de capacitación deben incluir el estudio de casos prácticos, el análisis de tipologías delictivas y la actualización periódica sobre las nuevas señales de alerta emitidas por la UNIF y la SUNAVAL (UNIF, 2025e).

En una casa de bolsa, las áreas sensibles típicas son la tesorería, el área de finanzas corporativas y operaciones. En una entidad emisora, son sensibles las áreas de negocio, la tesorería y las relaciones con auditores externos. En todos estos casos, el personal que labora en dichas áreas debe recibir una capacitación continua y especializada que vaya más allá de la mera divulgación de las circulares, debe incluir el análisis de casos reales ocurridos en el mercado venezolano, el estudio de tipologías identificadas por la UNIF, y la realización de simulaciones que permitan desarrollar un criterio preventivo afinado.

Un aspecto que merece especial atención es la interacción entre las casas de bolsa y las APNFD que intervienen en el proceso de inversión. Cuando una casa de bolsa recibe a un nuevo cliente que presenta un atestiguamiento de ingresos firmado por un contador público, ¿verifica la casa de bolsa que dicho contador está debidamente inscrito en el colegio profesional correspondiente? ¿Cruza la información del atestiguamiento con otras fuentes? ¿Se ha establecido algún mecanismo para que la casa de bolsa alerte a la UNIF si detecta que un contador o un abogado está firmando documentos que no reflejan la realidad económica del cliente? La Circular UNIF-DDG-DSU-01563 aborda tangencialmente esta problemática al señalar que los sujetos obligados deben implementar controles que permitan verificar la autenticidad de los documentos presentados por los clientes y la idoneidad de los profesionales que los emiten (UNIF, 2023c). La Circular UNIF-DDG-DSU-07210 va un paso más allá al exigir que los sujetos obligados del sector valores verifiquen que los contadores públicos, abogados, economistas y administradores que emiten documentos de soporte para sus clientes estén debidamente inscritos en sus respectivos colegios profesionales y no presenten sanciones disciplinarias relacionadas con la legitimación de capitales (UNIF, 2025e). Sin embargo, la implementación práctica de esta exigencia sigue siendo un desafío, dada la ausencia de registros centralizados y

de canales de comunicación ágiles entre los colegios profesionales y los sujetos obligados del mercado de valores.

El Reporte de Actividades Sospechosas en el sector valores: requisitos y buenas prácticas

La Recomendación 20 del GAFI exige que los países establezcan la obligación de reportar las operaciones sospechosas a la unidad de inteligencia financiera (GAFI, 2025, Rec. 20). En Venezuela, esta obligación se materializa, para el sector valores, a través de un conjunto de instrumentos complementarios, la Circular UNIF-DDG-DSU-01563, que establece las directrices generales y el catálogo de señales de alerta que deben activar la elaboración de un RAS (UNIF, 2023c), la Circular UNIF-DDG-DSU-07210, que profundiza en las señales de alerta específicas y en los procedimientos aplicables a los sujetos obligados del sector valores (UNIF, 2025e), y la Circular UNIF-DDG-001617 del 8 de mayo de 2024, que detalla los requisitos formales y procedimentales del RAS para el sector valores (UNIF, 2024a).

Un RAS efectivo en el ámbito bursátil debe contener, conforme a estas circulares, una identificación precisa del sujeto obligado y del oficial de cumplimiento; una descripción detallada de la operación o secuencia de operaciones, con indicación de los títulos involucrados, los montos, las fechas y las partes, una fundamentación de la sospecha que vaya más allá de la enumeración de señales de alerta y que explique por qué, en el contexto del perfil del cliente, la operación es inusual, y la información disponible sobre el beneficiario final (UNIF, 2024a; UNIF, 2023c; UNIF, 2025e).

La fundamentación de la sospecha es el elemento cualitativo más importante del RAS. No es lo mismo reportar que un cliente realizó una operación por un monto elevado, que reportar que un cliente cuyo perfil indica ingresos mensuales de mil dólares según su atestiguamiento y su declaración de ISLR adquirió valores por cien mil dólares, y que al ser consultado sobre el origen de los fondos presentó una explicación vaga e inconsistente. Este segundo reporte, que incorpora el contexto del perfil y que se alinea con las señales de alerta previstas en las Circulares UNIF-DDG-DSU-01563 y UNIF-DDG-DSU-07210, es el que verdaderamente aporta valor a la inteligencia financiera. La Circular UNIF-DDG-001617 enfatiza, además, la confidencialidad del RAS y la prohibición de alertar al cliente como pilares del sistema (UNIF, 2024a), aspectos que son reiterados y reforzados por la Circular UNIF-DDG-DSU-07210 (UNIF, 2025e).

El rol de la UNIF, la ONCDOFT y la SUNAVAL en la supervisión del mercado de valores

La ONCDOFT, como ente rector del sistema, es responsable de coordinar las políticas públicas de prevención y de asegurar que todos los sectores, incluido el mercado de valores cumplan con sus obligaciones (Asamblea Nacional, 2012,

art. 6). La UNIF, por su parte, es el órgano especializado que recibe los RAS, los analiza y los cruza con otras fuentes de información para generar inteligencia financiera que pueda ser utilizada por el Ministerio Público y los órganos de investigación penal (Presidencia de la República, 2016). La SUNAVAL ejerce la supervisión directa de los sujetos controlados del mercado de valores, verificando el cumplimiento de la Providencia N° 025 y de las circulares de la UNIF, entre ellas la Circular UNIF-DDG-DSU-01563, que le está expresamente dirigida, y la Circular UNIF-DDG-DSU-07210, que desarrolla las obligaciones de los sujetos controlados.

La efectividad de esta arquitectura institucional depende, en buena medida, de la fluidez con que la información circula entre los distintos actores. Si la SUNAVAL detecta, en el curso de una inspección, que una entidad emisora ha presentado estados financieros que no guardan coherencia con sus declaraciones fiscales, esa información debe ser comunicada a la UNIF para que pueda ser cruzada con otros reportes. Si la UNIF, al analizar un RAS, identifica que un contador público ha firmado atestiguamientos de ingresos manifiestamente inconsistentes, esa información debe ser puesta en conocimiento del colegio profesional correspondiente para que se inicien las acciones disciplinarias. La Circular UNIF-DDG-DSU-07210 refuerza esta necesidad de coordinación al establecer que los sujetos obligados del sector valores deben establecer canales de comunicación con la SUNAVAL y la UNIF para el intercambio de información relacionada con operaciones sospechosas (UNIF, 2025e). La Quinta Ronda de Evaluaciones Mutuas del GAFI, y los resultados de la Plenaria de junio de 2026 celebrada en México, han subrayado la importancia de esta coordinación interinstitucional como un factor determinante de la efectividad del sistema (GAFI, 2026).

Recomendaciones para fortalecer el radar preventivo en el mercado de valores venezolano

A la luz del análisis realizado, y tomando como base las directrices contenidas en las circulares de la UNIF, particularmente las Circulares UNIF-DDG-DSU-01563 y UNIF-DDG-DSU-07210, se proponen las siguientes recomendaciones dirigidas a fortalecer la prevención de la legitimación de capitales en el mercado de valores venezolano:

En primer lugar, es necesario que la SUNAVAL, en coordinación con la UNIF, actualice y amplíe el catálogo de señales de alerta contenido en la Circular UNIF-DDG-DSU-07210 para incorporar indicadores específicos relacionados con la fase preoperativa de listado en bolsa, como son las señales vinculadas a la constitución de la empresa emisora, la auditoría de estados financieros, los estudios de factibilidad, las valoraciones de empresas y los atestiguamientos de ingresos. Esta actualización debe incluir ejemplos prácticos y criterios cuantitativos que orienten a los sujetos obligados en la detección de operaciones inusuales.

En segundo lugar, debe fortalecerse la supervisión de las APNFD que intervienen en el mercado de valores. Los colegios profesionales de abogados, contadores públicos, economistas y administradores deben asumir un rol activo en la verificación del cumplimiento de las obligaciones LC/FT, en consonancia con lo dispuesto en la Circular UNIF-DDG-DSU-04409, en los boletines N° 003-2024 y N° 005-2025 de la UNIF, y en la propia Circular UNIF-DDG-DSU-07210 (UNIF, 2023b; UNIF, 2024b; UNIF, 2025d; UNIF, 2025e).

En tercer lugar, debe crearse un protocolo formal de intercambio de información entre la SUNAVAL y el SENIAT, de modo que los supervisores del mercado de valores puedan verificar la coherencia entre los estados financieros presentados por las entidades emisoras y sus declaraciones fiscales, tal como lo sugieren las Circulares UNIF-DDG-DSU-01563 y UNIF-DDG-DSU-07210 al incluir como señal de alerta las discrepancias entre la documentación financiera y fiscal.

Finalmente, debe intensificarse la formación continua de todos los actores del ecosistema bursátil, desde los oficiales de cumplimiento hasta los profesionales en libre ejercicio, incluyendo el estudio de casos reales del mercado venezolano, la participación en ejercicios de tipologías y la simulación de escenarios de riesgo, tal como lo exige la Circular UNIF-DDG-DSU-07210.

Reflexiones Finales

El mercado de valores venezolano no es un espacio estancado dentro del sistema financiero, es un ecosistema complejo en el que convergen múltiples actores y en el que cada operación deja un rastro documental que, analizado con rigor y con una visión sistémica, puede revelar la presencia de capitales ilícitos. Las señales de alerta no deben buscarse únicamente en la fase transaccional la compraventa de títulos en la bolsa, sino también, y quizás con mayor provecho, en la fase preoperativa, en la constitución de la empresa emisora, en la auditoría de sus estados financieros, en los estudios de factibilidad que justifican la emisión, y en los atestiguamientos de ingresos que presentan los inversionistas. Las Circulares UNIF-DDG-DSU-01563 y UNIF-DDG-DSU-07210, junto con la Providencia N° 025 de SUNAVAL y la Circular UNIF-DDG-001617, proporcionan el instrumental normativo para realizar este análisis, lo que falta, en muchos casos, es la voluntad y la capacidad operativa para aplicarlo de manera consistente.

La coherencia entre la declaración del Impuesto Sobre la Renta (ISLR), los estados financieros auditados conforme a los estándares establecidos por la SUNAVAL y los atestiguamientos de ingresos trasciende un simple requisito formal; constituye una evidencia fundamental de que los recursos que ingresan al mercado de valores provienen de fuentes lícitas y de que los profesionales que participaron en su verificación actuaron con la debida diligencia. Cuando esa consistencia documental se ve afectada, surge una señal de alerta que ningún Oficial de Cumplimiento puede pasar por alto.

Tal como lo establece la Circular UNIF-DDG-DSU-07210, las señales de alerta deben evaluarse de manera integral, considerando el perfil del cliente, el contexto de la operación y la congruencia existente entre los distintos documentos y soportes presentados (UNIF, 2025e). En consecuencia, el análisis no debe limitarse a la revisión aislada de cada documento, sino orientarse a la construcción de una visión completa y razonable de la actividad económica del cliente. Solo mediante este enfoque integral es posible identificar inconsistencias, omisiones o contradicciones que puedan evidenciar la presencia de recursos de origen ilícito o la utilización del sistema financiero para fines indebidos.

Fortalecer ese radar exige, ciertamente, actualizar la normativa y perfeccionar los mecanismos de supervisión. Pero exige, sobre todo, un cambio cultural, entender que el mercado de valores no puede ser un espacio de opacidad, sino de transparencia donde cada actor el contador que audita, el abogado que estructura, el corredor que ejecuta y el inversionista que invierte asume la responsabilidad de demostrar que su actividad contribuye al desarrollo económico del país y no a su degradación.

La Circular UNIF-DDG-DSU-07210 lo resume con claridad al señalar que la prevención de la legitimación de capitales en el mercado de valores es una responsabilidad compartida que requiere el compromiso de todos los actores del ecosistema bursátil (UNIF, 2025e). Ese compromiso, más que un mandato normativo, debería ser un imperativo ético para todos los que participan en el mercado de valores venezolano.

Referencias

Asamblea Nacional de la República Bolivariana de Venezuela. (2012, 30 de abril). Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT). Gaceta Oficial N° 39.912.

Grupo de Acción Financiera Internacional [GAFI]. (2023, marzo). Guía sobre el beneficiario final de las personas jurídicas. <https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Spanish%20Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf>

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 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. París: OCDE/GAFI.

- Grupo de Acción Financiera Internacional (GAFI). (2026, junio). Resultados de la Plenaria del GAFI, México. <https://www.fatf-gafi.org/>
- Presidencia de la República Bolivariana de Venezuela. (2016, 26 de abril). Decreto con Rango, Valor y Fuerza de Ley N° 2.239, mediante el cual se dicta el Decreto de Adecuación de la Unidad Nacional de Inteligencia Financiera. Gaceta Oficial N° 40.891.
- Superintendencia Nacional de Valores (SUNAVAL). (2025, 17 de marzo). Providencia N° 025: 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 N° 43.096, 27 de marzo de 2025.
- Unidad Nacional de Inteligencia Financiera (UNIF). (2023a, 8 de mayo). Circular UNIF-DDG-DGOE-003081: Señales de alerta, controles internos y directrices relacionadas con los Reportes de Actividades Sospechosas (RAS). <https://www.unif.gob.ve/circulares/>
- Unidad Nacional de Inteligencia Financiera (UNIF). (2023b, 10 de noviembre). Circular UNIF-DDG-DSU-04409: Señales de alerta, controles internos y directrices relacionadas con los Reportes de Actividades Sospechosas (RAS) para abogados, administradores, economistas y contadores en el libre ejercicio de sus profesiones. <https://www.unif.gob.ve/circulares/>
- Unidad Nacional de Inteligencia Financiera (UNIF). (2023c). Circular UNIF-DDG-DSU-01563: Señales de alerta, controles internos y directrices relacionadas con los Reportes de Actividades Sospechosas (RAS). Superintendencia Nacional de Valores (SUNAVAL). <https://www.unif.gob.ve/circulares/>
- Unidad Nacional de Inteligencia Financiera (UNIF). (2024a, 8 de mayo). Circular UNIF-DDG-001617: Reporte de Actividad Sospechosa por parte de los Sujetos Obligados del Sector Valores. <https://www.unif.gob.ve/circulares/>
- Unidad Nacional de Inteligencia Financiera (UNIF). (2024b). Boletín UNIF N° 003-2024: Señales de alerta para contadores públicos. <https://www.unif.gob.ve/boletines/>
- Unidad Nacional de Inteligencia Financiera (UNIF). (2025a, 29 de agosto). Circular UNIF-DDG-DSU-05448: Señales de alerta y directrices respecto a la identificación, verificación y registro de datos de los beneficiarios finales de personas y estructuras jurídicas. <https://www.unif.gob.ve/circulares/>
- Unidad Nacional de Inteligencia Financiera (UNIF). (2025b, 30 de julio). Circular UNIF-DDG-DENTIF-004576: Consideraciones respecto a la inviabilidad de participación de funcionarios. <https://www.unif.gob.ve/circulares/>
- Unidad Nacional de Inteligencia Financiera (UNIF). (2025c, 3 de diciembre). Circular UNIF-DDG-DSU-07329: Guía para mitigar riesgos de

Financiamiento al Terrorismo (FT) para el subconjunto de Organizaciones Sin Fines de Lucro (OSFL). <https://www.unif.gob.ve/circulares/>

Unidad Nacional de Inteligencia Financiera (UNIF). (2025d). Boletín UNIF N° 005-2025: Refuerzo de obligaciones para APNFD. <https://www.unif.gob.ve/boletines/>

Unidad Nacional de Inteligencia Financiera (UNIF). (2025e). Circular UNIF-DDG-DSU-07210: Señales de alerta, controles internos y directrices relacionadas con los Reportes de Actividades Sospechosas (RAS) para los sujetos obligados del sector valores. <https://www.unif.gob.ve/circulares/>

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 de Administración de Riesgos de
Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Señales de Alerta

TIPOLOGÍAS DE LEGITIMACIÓN DE CAPITALS MÁS RECURRENTES EN EL CONTEXTO VENEZOLANO

Autor: Abg. Esp. Víctor Ordaz
Facilitador: Prof. Elizabeth Peláez
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 de Administración de Riesgos de
Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Señales de Alerta

TIPOLOGÍAS DE LEGITIMACIÓN DE CAPITALES MÁS RECURRENTES EN EL CONTEXTO VENEZOLANO

Autor: Abg. Esp. Víctor Ordaz
Código ORCID: 0009-0007-5234-9369
Correo electrónico: vordazccs@gmail.com

Resumen

Este ensayo analiza las tipologías de legitimación de capitales más recurrentes en Venezuela, destacando el uso de comercios, criptoactivos, minería ilegal de oro, contrataciones públicas, sector inmobiliario y actividades profesionales no financieras (APNFD). A partir de informes de organismos como el Grupo de Acción Financiera del Caribe GAFIC, Grupo de Acción Financiera de Latinoamérica GAFILAT y la Unidad Nacional de Inteligencia Financiera UNIF, se examina el marco normativo nacional y los estándares internacionales del GAFI. Aunque Venezuela posee una base legal sólida y una institucionalidad activa —evidenciada en sus ejercicios de tipologías—, las evaluaciones internacionales señalan debilidades en la efectividad de las investigaciones, la transparencia del beneficiario real y la supervisión de sectores no financieros. Finalmente, se proponen medidas estratégicas orientadas a consolidar el enfoque basado en riesgo, fortalecer la UNIF, regular los activos virtuales, optimizar la cooperación internacional y promover una cultura de cumplimiento efectiva.

Descriptor clave: Legitimación de capitales, Tipologías, Enfoque basado en riesgo, Criptoactivos, Comercio exterior (Trade-Based Money Laundering).

Abstract

This essay examines the most recurrent typologies of money laundering in Venezuela, highlighting trade-based money laundering, cryptocurrencies, illegal gold mining, public procurement, the real estate sector, and designated non-financial businesses and professions (DNFBPs). Based on reports from organizations such as CFATF, GAFATF, and Venezuela's FIU (UNIF), it reviews the national legal framework and FATF international standards. Although Venezuela has a solid legal base and active institutional mechanisms—evidenced by its typology exercises—international evaluations point out vulnerabilities in investigative effectiveness, beneficial ownership transparency, and the oversight of non-financial sectors. Finally, strategic recommendations are proposed to consolidate a risk-based approach, strengthen the FIU, regulate virtual assets, optimize international cooperation, and promote an effective compliance culture.

Key descriptors: Money laundering, Typologies, Risk-based approach, Crypto-assets, Foreign trade (Trade-Based Money Laundering)

Introducción

El presente ensayo aborda las tipologías de legitimación de capitales más recurrentes en el contexto venezolano, con un enfoque técnico y propositivo que explora oportunidades de fortalecimiento del sistema de prevención y control. A partir del análisis de informes de organismos internacionales como el Grupo de Acción Financiera del Caribe (GAFIC), el Grupo de Acción Financiera de Latinoamérica (GAFILAT) y la Unidad Nacional de Inteligencia Financiera (UNIF) de Venezuela en el que se identifican las principales modalidades utilizadas para dar apariencia de legalidad a fondos de origen ilícito. Entre ellas destacan el la Legitimación de capitales basado en el uso de comercios, el uso de criptoactivos, la explotación minera ilegal de oro, las contrataciones públicas sobrefacturadas, el sector inmobiliario, así como, la utilización de actividades y profesionales no financieros designados (APNFD). El ensayo concluye con un conjunto de recomendaciones orientadas a fortalecer el sistema nacional de prevención, mejorar la cooperación internacional y aprovechar los avances tecnológicos para una mayor efectividad en la lucha contra este flagelo.

La legitimación de capitales, conocida también como lavado de dinero en otras jurisdicciones, constituye uno de los delitos financieros de mayor impacto en la economía global. Definido como el "proceso en virtud del cual los bienes de

origen delictivo se integran en el sistema económico", este fenómeno afecta no solo la integridad del sistema financiero sino también la estabilidad macroeconómica y el desarrollo sostenible de las naciones.

Venezuela, como país con una economía históricamente dependiente de los recursos petroleros y con una posición geográfica estratégica en el norte de Suramérica, enfrenta desafíos particulares en materia de administración de Riesgos de la legitimación de capitales. Nuestro país ha sido objeto de evaluaciones periódicas por parte del Grupo de Acción Financiera del Caribe (GAFIC), organismo regional al que pertenecemos, y ha desarrollado un marco normativo e institucional para abordar esta problemática.

La Unidad Nacional de Inteligencia Financiera (UNIF) ha venido realizando ejercicios de tipologías con el propósito de "identificar y describir los métodos utilizados por las organizaciones criminales para dar apariencia de legalidad a fondos de origen ilícito". Estos ejercicios, que en 2025 alcanzaron su duodécima edición, buscan "promover el fortalecimiento de los controles, reconocer señales de alerta y cortar el circuito de financiamiento de la Delincuencia Organizada".

El propósito de este ensayo es analizar, desde una perspectiva técnica analizando las tipologías de legitimación de capitales más recurrentes en nuestro país, identificando los sectores y mecanismos más vulnerables, para luego explorar oportunidades concretas de mejora que puedan contribuir a fortalecer el sistema nacional de prevención y control o de administración de riesgos, según sea el caso. Se evidencia los esfuerzos que Venezuela ha realizado en esta materia, como lo demuestran los avances reportados por la UNIF con "una mayor cantidad de casos procesados asociados a los informes de inteligencia financiera", y se busca aportar elementos que permitan continuar mejorando dichos esfuerzos.

Definición y Etapas de la Legitimación de Capitales

La legitimación de capitales es un proceso complejo que generalmente comprende tres etapas fundamentales:

Colocación: Introducción de los fondos de origen ilícito en el sistema financiero o económico.

Procesamiento: Realización de múltiples transacciones para ocultar el origen y la propiedad de los fondos, creando capas de complejidad que dificultan su rastreo.

Integración: Reinserción de los fondos en la economía formal, con apariencia de legalidad, mediante inversiones en bienes o actividades comerciales legítimas.

Marco Normativo Venezolano

Venezuela cuenta con una base legal para la Administración de riesgos en materia de legitimación de capitales, que incluye:

Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (2012): Establece las bases para la prevención, control y represión del crimen organizado y delitos relacionados.

Normativas prudenciales de acuerdo a cada sector: Emanadas por los distintos entes de control que supervisan a los sujetos obligados, tanto del sector financiero como no financiero.

Por lo que se evidencia que nuestro país "tiene un ordenamiento jurídico necesario para llevar a cabo la prevención y corrección de los delitos de legitimación de capitales y financiamiento al terrorismo", aunque se reconoce la necesidad de que las instituciones responsables perfeccionen mecanismos y controles así como actualizar la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (2012) incluyendo aspectos como el uso de la

Inteligencia Artificial Generativa por parte de los grupos delictivos o ampliar aspectos como los criptoactivos.

Estándares Internacionales

Venezuela es miembro del Grupo de Acción Financiera del Caribe (GAFIC), un organismo intergubernamental que "han acordado implementar contramedidas comunes para abordar las políticas a fin de combatir la Legitimación de Capitales, el financiamiento del terrorismo y el financiamiento de la proliferación". Las 40 Recomendaciones del Grupo de Acción Financiera Internacional (GAFI/FATF) constituyen el estándar global en la materia.

El Informe de Evaluación Mutua de la Cuarta Ronda de Venezuela fue adoptado en noviembre de 2022, y el país ha presentado informes de seguimiento para demostrar los avances en el cumplimiento técnico de las recomendaciones.

Tipologías de Legitimación de Capitales más Recurrentes en Venezuela

A partir de la información disponible en informes de organismos nacionales e internacionales, así como de casos documentados, es posible identificar las siguientes tipologías como las más recurrentes en el contexto venezolano.

Legitimación de Capitales usando comercios (Trade-Based Money Laundering)
El Legitimación de Capitales basado en el comercio "implica la manipulación de transacciones comerciales para ocultar" el origen ilícito de los fondos. Esta modalidad es particularmente relevante en Venezuela debido a la estructura de su economía y las restricciones cambiarias históricas.

Mecanismos identificados:

Sobrevaloración o subvaloración de importaciones y exportaciones:
Manipulación de facturas y documentos de comercio exterior para transferir valor entre jurisdicciones.

Exportaciones ficticias: Declaración de operaciones de exportación que no corresponden a mercancías realmente enviadas, utilizadas para justificar la entrada de divisas al país.

Importaciones con documentación falsa: Utilización de facturas y conocimientos de embarque falsificados para canalizar fondos al exterior.

Uso de Criptoactivos

Los criptoactivos en Venezuela han evolucionado significativamente en los últimos años, y se ha convertido en un canal relevante para la legitimación de capitales. El sistema cripto venezolano "ha pasado de ser un experimento fallido de soberanía digital a ser hoy un mecanismo institucionalizado con altísimos riesgos de lavado de dinero".

Modalidades identificadas:

Transacciones de venta libre o también conocido como, *Over-The-Counter* (OTC): en el que los intermediarios que facilitan el intercambio de criptomonedas sin pasar por proveedores de servicios de activos virtuales regulados, permitiendo transacciones de gran volumen con menor supervisión.

Minería Ilegal de Oro y Comercialización del "Oro Sucio"

La minería ilegal de oro en Venezuela constituye una de las actividades ilícitas más lucrativas y con mayor vinculación con la legitimación de capitales.

Mecanismos de legitimación:

Venta de oro ilegal a cambio de criptomonedas: El oro extraído ilegalmente se intercambia por monedas estables, "proporcionando acceso a moneda líquida sin preocuparse por los embargos de activos relacionados con sanciones penales".

Exportación de oro con documentación falsificada: Declaración de oro de origen lícito cuando en realidad proviene de minería ilegal.

Modalidades identificadas:

Contratación de vivienda de interés social no ejecutada: Contratos para proyectos de vivienda que nunca se construyen, utilizados como mecanismo para extraer y legitimar fondos.

Sector Inmobiliario

El sector inmobiliario ha sido históricamente un vehículo privilegiado para la legitimación de capitales debido a la alta valoración de los activos y la relativa facilidad para ocultar la identidad del beneficiario real.

Mecanismos utilizados en Venezuela:

Compra de bienes inmuebles con fondos de origen ilícito: Adquisición de propiedades en Venezuela y en el extranjero como mecanismo de integración de capitales.

Estructuras de propiedad complejas: Utilización de "estructuras de propiedad complejas o donde el beneficiario real está ofuscado" en el que hay Participación de profesionales como la "participación de un abogado" en transacciones inmobiliarias puede ser una señal de alerta cuando se busca "anonimato real o percibido para comprar y vender bienes inmuebles con fines ilícitos".

Entre las técnicas de Legitimación de capitales utilizados en Venezuela se encuentra "la compra y venta de bienes y bienes raíces como, entre otros, fincas y ganado, y la creación de compañías de responsabilidad limitada".

Actividades y Profesionales No Financieros Designados (APNFD)

La utilización de profesionales no financieros para facilitar operaciones de legitimación de capitales es una preocupación creciente. En Venezuela, se ha

identificado que ciertos sectores profesionales presentan niveles de riesgo significativos.

Sectores de riesgo identificados:

Abogados: "Los documentos analizados determinó una calificación de riesgo alta para los profesionales del derecho", identificando como amenaza crítica "el manejo de efectivo en montos elevados sin soportes documentales que acrediten su origen lícito", los contadores públicos pueden representar un nivel de riesgo generalmente moderado.

Agentes inmobiliarios: También designados como no financieros sujetos a control.

Sectores Económicos Vulnerables

Sector Petrolero

Como principal fuente de ingresos del país, el sector petrolero representa un sector de alto riesgo para la legitimación de capitales. La complejidad de las operaciones internacionales, los múltiples intermediarios y la magnitud de los flujos financieros crean vulnerabilidades que pueden ser explotadas.

Sector de Minería

La minería, particularmente la de oro, ha sido identificada como uno de los sectores más vulnerables. La combinación de operaciones informales, falta de supervisión efectiva y el alto valor del producto la convierten en un canal atractivo para la legitimación de capitales. "La alta cotización del oro, combinada con su valor como vehículo de dinero.

Sector de Comercio Exterior

El comercio exterior, especialmente las importaciones de alimentos y otros bienes esenciales, ha sido utilizado como mecanismo para canalizar fondos. La necesidad de importar bienes ante la contracción de la producción nacional crea oportunidades para la sobrefacturación y otras manipulaciones.

Sector de Activos Virtuales

El ecosistema de activos virtuales en Venezuela, aunque emergente, presenta vulnerabilidades por las características propias de estas siendo el caso que algunas de ellas pudieran ofrecer privacidad en sus operaciones, por lo que la denominada regla de viaje en una necesidad en aras identificar de forma plena a todos los actores en una operación que involucre activos virtuales.

Evaluación del Sistema de Prevención y Control

Fortalezas Identificadas

A pesar de los desafíos, el sistema venezolano de prevención de legitimación de capitales presenta fortalezas que merecen ser reconocidas:

Marco legal establecido: Venezuela cuenta con la legislación necesaria para la prevención y sanción de estos delitos.

Existencia de la UNIF: La Unidad Nacional de Inteligencia Financiera cumple funciones de recepción, análisis y transmisión de información sobre operaciones sospechosas.

Ejercicios de tipologías regulares: La realización del XII Ejercicio de Tipologías en 2025 demuestra el compromiso con la identificación de nuevas modalidades y el fortalecimiento del sistema.

Participación multisectorial: La inclusión de "oficiales de cumplimiento de Instituciones Financieras y No Financieras" en los ejercicios de tipologías evidencia un enfoque integral.

Entes de control sectoriales: La existencia de múltiples entes de control que supervisan a los sujetos obligados.

Áreas de Mejora Identificadas por Organismos Internacionales

Las evaluaciones de organismos internacionales han señalado áreas que requieren atención:

Baja efectividad general: Se ha identificado "baja efectividad general en la mayoría de las áreas de lucha contra el Legitimación de Capitales, incluyendo investigaciones, enjuiciamientos y recuperación de activos".

Brechas en la transparencia del beneficiario real: "Brechas importantes en la transparencia del beneficiario real, exponiendo el sistema financiero a mal uso".

Supervisión débil de sectores no financieros: "Supervisión débil de sectores no financieros como las APNFD".

Oportunidades de Mejora para nuestro país

Con base en el análisis de las tipologías identificadas y las áreas de mejora señaladas, se presentan oportunidades concretas para fortalecer el sistema venezolano de prevención y control de la legitimación de capitales.

Fortalecimiento del Enfoque Basado en Riesgo

La implementación efectiva de un enfoque basado en riesgo, alineado con la Recomendación 1 del GAFI, permitiría:

Identificar y priorizar sectores de mayor vulnerabilidad: Asignar recursos de supervisión e inspección a los sectores con mayor exposición al riesgo de legitimación de capitales.

Adaptar los controles a la realidad nacional: Desarrollar medidas preventivas proporcionales a los riesgos identificados, evitando cargas regulatorias excesivas en sectores de bajo riesgo.

Actualizar periódicamente la evaluación de riesgos: Mantener una comprensión dinámica de las amenazas emergentes, como el uso de criptomonedas y las nuevas modalidades de legitimación usando el comercio.

Mejora de la Supervisión de Sectores No Financieros

La supervisión de los Profesionales y Actividades No Financieras Designadas (APNFD) requiere atención prioritaria:

Ampliar la cobertura supervisora: Asegurar que todos los sectores designados como APNFD estén sujetos a medidas de prevención y supervisión efectiva.

Desarrollar guías sectoriales específicas: Crear orientaciones adaptadas a cada sector (abogados, contadores, agentes inmobiliarios, casinos) que consideren sus particularidades operativas, como se ha realizado en el sector asegurador venezolano, en donde se han dirigido esfuerzos en realizar una guía sectorial sobre el tratamiento a las APNFD.

Fortalecer la capacitación: Implementar programas de formación continua para profesionales no financieros sobre sus obligaciones en materia de prevención.

Transparencia del Beneficiario Final

La mejora en la transparencia del beneficiario final es fundamental para prevenir el uso indebido del sistema financiero:

Crear un registro central de beneficiarios final: Establecer un sistema que permita identificar a las personas naturales que en última instancia poseen o controlan personas jurídicas y estructuras legales.

Exigir verificación de beneficiario final en todas las transacciones relevantes: Incorporar esta obligación en los procedimientos de debida diligencia de todas las instituciones financieras y no financieras.

Facilitar el acceso a la información: Asegurar que las autoridades competentes tengan acceso oportuno y efectivo a la información sobre beneficiarios reales.

Fortalecimiento de la Unidad de Inteligencia Financiera

La UNIF, como pieza central del sistema de prevención, puede beneficiarse de:

Mayor capacidad analítica: Incrementar los recursos técnicos y humanos para el análisis de inteligencia financiera, especialmente en áreas emergentes como criptomonedas.

Mejora en el intercambio de información: Fortalecer los mecanismos de cooperación interinstitucional para compartir inteligencia financiera entre las distintas autoridades.

Uso de tecnología avanzada: Implementar herramientas de análisis de datos e inteligencia artificial para identificar patrones y señales de alerta de manera más efectiva.

Regulación y Supervisión de Activos Virtuales

Dado el creciente uso de criptomonedas como vehículo de legitimación de capitales, se requiere:

Fortalecer un marco regulatorio específico: Establecer normas claras para los Proveedores de Servicios de Activos Virtuales (VASP), incluyendo requisitos de registro, debida diligencia y reporte de operaciones sospechosas.

Fortalecimiento de la Cooperación Internacional

La naturaleza transfronteriza de la legitimación de capitales exige una cooperación internacional robusta:

Ampliar acuerdos de intercambio de información: Establecer y fortalecer acuerdos bilaterales y multilaterales para el intercambio de inteligencia financiera.

Participación activa en redes internacionales: Mantener y profundizar la participación en el GAFIC y otras redes de unidades de inteligencia financiera.

Cooperación en investigaciones y recuperación de activos: Facilitar la cooperación en investigaciones transfronterizas y la recuperación de activos ilícitos en el extranjero.

Mejora de la Capacidad Investigativa y de Enjuiciamiento

Para aumentar la efectividad en la lucha contra la legitimación de capitales:

Especialización de fiscales y jueces: Desarrollar programas de formación especializada en delitos financieros complejos.

Fortalecimiento de unidades de investigación financiera: Dotar a las unidades de investigación de recursos y herramientas técnicas adecuadas.

Agilización de procesos de recuperación de activos: Establecer procedimientos más eficientes para la identificación, congelamiento y decomiso de activos vinculados a la legitimación de capitales.

Promoción de la Cultura de Cumplimiento

El fortalecimiento del sistema de prevención requiere un cambio cultural:

- Sensibilización del sector privado: Promover entre las empresas y profesionales la comprensión de los riesgos y la importancia del cumplimiento.
- Incentivos para el cumplimiento voluntario: Desarrollar mecanismos que incentiven la implementación voluntaria de medidas de prevención más allá de los requisitos mínimos.
- Educación financiera: Incluir contenidos sobre prevención del lavado de dinero en programas de educación financiera para la población en general.

Conclusiones

La legitimación de capitales en Venezuela presenta características particulares que reflejan la estructura económica del país y los desafíos que enfrenta. Las tipologías más recurrentes identificadas Legitimación de capitales usado estructuras jurídicas complejas, uso de criptoactivos, contrataciones públicas, sector inmobiliario y utilización de profesionales no financieros evidencian la diversidad de mecanismos empleados para dar apariencia de legalidad a fondos de origen ilícito.

El sistema venezolano de administración de riesgos en esta materia ha avanzado en el establecimiento de un marco normativo e institucional, con el fortalecimiento de la Unidad Nacional de Inteligencia Financiera, la realización de ejercicios de tipologías y la existencia de múltiples entes de control sectoriales. Sin embargo, las evaluaciones de organismos internacionales señalan áreas que requieren fortalecimiento, particularmente en la supervisión de sectores no financieros, la transparencia del beneficiario real y la efectividad en investigaciones y enjuiciamientos.

Las oportunidades de mejora identificadas apuntan hacia un fortalecimiento integral del sistema: desde la implementación efectiva del enfoque basado en riesgo, pasando por la mejora de la supervisión de sectores no financieros, hasta el desarrollo de capacidades técnicas para abordar los desafíos emergentes como las criptoactivos. La cooperación internacional y el fortalecimiento de la cultura de cumplimiento son elementos transversales que potenciarán estos esfuerzos.

Venezuela tiene la oportunidad de transformar los desafíos en catalizadores para la modernización de su sistema de administración de riesgos o prevención de legitimación de capitales. El fortalecimiento de este sistema no solo contribuirá a la integridad del sistema financiero nacional, sino también ayudará a la atracción de inversiones y promoviendo el desarrollo económico sostenible. La voluntad política, la cooperación entre sectores y el compromiso con los estándares internacionales serán determinantes para lograr estos objetivos.

Referencias

- Corrochano, L. M. (s.f.). El delito de legitimación de capitales en la Ley Orgánica contra la Delincuencia Organizada. Servicio BC de la UC.
- Arroyo, H. S. (s.f.). El delito de legitimación de capitales a la luz del derecho comparado. Perso UNIFR.
- Unidad Nacional de Inteligencia Financiera (UNIF). (2025, 16 de noviembre). La UNIF realiza el XII Ejercicio de Tipologías centrado en el fortalecimiento del Sistema de Prevención de Legitimación de Capitales. UNIF.
- Grupo de Acción Financiera del Caribe (GAFIC). (2025). Tercer Informe de Seguimiento Mejorado y reclasificación del Cumplimiento Técnico de la República Bolivariana de Venezuela. GAFIC.
- Grupo de Acción Financiera de Latinoamérica (GAFILAT). (2025). Informe de Tipologías Regionales de LA/FT 2025. Biblioteca GAFILAT.
- Financial Action Task Force (FATF). (2022). Anti-Money Laundering and Counter-Terrorist Financing Measures in the Bolivarian Republic of Venezuela – CFATF. FATF-GAFI.
- Financial Action Task Force (FATF). (2024). Venezuela incluida en la Lista Gris del GAFI. RICS Management.

- Andrade, J. M. M. (2023). Legitimación de Capitales: riesgos y consecuencias en la economía local. Redalyc/Dialnet.
- Transparencia Venezuela. (2025). La opacidad y la debilidad institucional facilitan el lavado de dinero. Transparencia Venezuela.
- TRM Labs. (2026). Venezuelan Money Laundering Case Study via OTC Crypto Brokers. LinkedIn.
- Transparencia Venezuela. (2025). Criptomonedas, la nueva forma de lavado y corrupción de Venezuela para el mundo. Transparencia Venezuela.
- GI-TOC. (2026). Stablecoins Have 'Increasing Relevance' in Illicit Amazon Gold Trade. Bitget News.
- Steptoe. (2026). Illicit Gold Mining in Venezuela: Reform or Regression? Steptoe.
- U.S. Department of Justice. (2026). Homeland Security Task Force Arrests Maduro Regime Ally Alex Saab on Money Laundering Charges. Justice.gov.
- KPMG. (2026). Normativas y entes de control en Venezuela que regulan la LC/FT/FPADM. KPMG.
- FATF. (2026). FATF Updates Jurisdiction Classifications. LinkedIn/Kabungo Chishiba.
- CFATF-GAFIC. (2022). Deficiency 2 - Venezuelan State Legislation. CFATF.
- K2 Integrity. (2026). Venezuela Update: Political Transition and Sanctions and AML Risk Overview. K2 Integrity.
- FATF. (2026). Venezuela's measures to combat money laundering and terrorist financing. FATF-GAFI.
- Simon Baker. (2025). AML/CFT Spotlight: Venezuela Under Increased Monitoring. LinkedIn.

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 de Administración de Riesgos de
Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Señales de Alerta

**¿Son las Señales de Alerta de Legitimación de Capitales Financiamiento al
Terrorismo y Financiamiento a la Proliferación de Armas de Destrucción Masiva,
un elemento estratégico para el Enfoque Basado en Riesgo?**

Autora: Lexssy Y. López H.

Facilitador: Elizabeth Peláez

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 de Administración de Riesgos de
Legitimación de Capitales y Financiamiento al Terrorismo
Unidad Curricular Señales de Alerta

¿Son las Señales de Alerta de Legitimación de Capitales Financiamiento al Terrorismo y Financiamiento a la Proliferación de Armas de Destrucción Masiva, un elemento estratégico para el Enfoque Basado en Riesgo

Autora: Lexssy Y. López
ID Orcid: 0009-0008-1954-5306
Correo electrónico: lyh1529@gmail.com

Resumen

La prevención de los delitos de legitimación de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva (LC/FT/FPADM) han enfrentado una significativa evolución, ha pasado de modelos tradicionales enfocados al cumplimiento normativo hacia esquemas completos basados en la gestión del riesgo. En este contexto, las señales de alerta de LC/FT/FPADM representan herramientas fundamentales dentro de los sistemas preventivos; sin embargo, su interpretación tradicional ha sido como mecanismos exclusivamente operativos de detección lo que limita su verdadero potencial. Las señales de alerta de LC/FT/FPADM pudiesen concebirse como indicadores estratégicos de riesgo, ya que su función trasciende la simple identificación de operaciones inusuales y se orientan a fortalecer la toma de decisiones, la asignación eficiente de recursos y la eficacia de los sistemas de prevención basado en riesgo. Es importante analizar si existe la posibilidad de comprender que las señales de alerta de LC/FT/FPADM pueden ser utilizadas como indicadores estratégicos de riesgo, capaces de generar información relevante para la anticipación, evaluación y tratamiento de los riesgos asociados a los delitos de LC/FT/FPADM. Mediante un análisis conceptual se plantea que una señal de alerta de LC/FT/FPADM reduce la incertidumbre del riesgo, y esta adquiere valor estratégico cuando es analizada y utilizada como insumo para la toma de decisiones. La transformación de las señales de alerta de LC/FT/FPADM en fuentes de inteligencia preventiva fortalece la capacidad organizacional para anticipar amenazas, optimizar recursos y consolidar sistemas de prevención más dinámicos, adaptativos y orientados a la gestión efectiva del riesgo optimizando así el Enfoque Basado en Riesgo (EBR).

Descriptor clave: señales de alerta de LC/FT/FPADM; gestión del riesgo; LC/FT/FPADM; indicadores estratégicos de riesgo; sistema de prevención

Abstract

Efforts to prevent money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction (ML/TF/PF) have undergone significant evolution, shifting from traditional models focused on regulatory compliance to comprehensive frameworks based on risk management. In this context, ML/TF/PF red flags serve as fundamental tools within preventive systems; however, their traditional interpretation as purely operational detection mechanisms limits their true potential. These red flags can be viewed as strategic risk indicators, as their function extends beyond the mere identification of unusual transactions to support decision-making, efficient resource allocation, and the effectiveness of risk-based prevention systems. It is important to consider the potential for using ML/TF/PF red flags as strategic risk indicators capable of generating relevant information for anticipating, assessing, and managing risks associated with ML/TF/PF. A conceptual analysis suggests that an ML/TF/PF red flag reduces risk uncertainty and gains strategic value when analyzed and used as an input for decision-making. Transforming ML/TF/PF red flags into sources of preventive intelligence strengthens organizational capacity to anticipate threats, optimize resources, and consolidate prevention systems that are more dynamic, adaptive, and focused on effective risk management, thereby optimizing the Risk-Based Approach (RBA).

Key descriptors: ML/TF/PF red flags; risk management; ML/TF/PF; strategic risk indicators; prevention system

Introducción

Durante las últimas décadas, la prevención de la legitimación de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva (en lo adelante LC/FT/FPADM) ha evolucionado desde un modelo enfocado en el cumplimiento formal de obligaciones regulatorias hacia un enfoque sustentado en la gestión integral del riesgo. Esta transformación ha sido impulsada por los estándares internacionales, que reconocen que las amenazas asociadas a estos delitos son dinámicas y requieren mecanismos de identificación, evaluación y mitigación proporcionales al nivel de exposición de cada organización. En este contexto, el enfoque basado en riesgos se ha consolidado como el eje rector de los sistemas modernos de prevención, al privilegiar la comprensión del riesgo sobre la aplicación uniforme de controles.

Las señales de alerta han ocupado históricamente un lugar preponderante dentro de los programas preventivos de cumplimiento, generalmente han sido

definidas como circunstancias, comportamientos o patrones transaccionales que podrían sugerir la existencia de una operación inusual o potencialmente vinculada con actividades ilícitas. No obstante, esta concepción, aunque técnicamente correcta, pudiese resultar insuficiente para explicar el verdadero papel que desempeñan dentro de los modelos modernos de administración del riesgo.

Desde esta perspectiva, surge la incógnita que se presenta dentro del ensayo, y en concordancia con la necesidad de verificar que su importancia no radica únicamente en advertir sobre la posible existencia de operaciones sospechosas, sino en proporcionar información relevante que puede priorizar los controles, fortaleciendo la toma de decisiones dentro de los sistemas de prevención.

Se requiere constatar si las señales de alerta LC/FT/FPADM, pueden ser concebidas como indicadores estratégicos, comprobando que permite integrarlas al proceso de identificación, evaluación, monitoreo y tratamiento del riesgo, favoreciendo una asignación más eficiente de los recursos de control y una supervisión proporcional a los niveles de exposición. Esta visión es consistente con el enfoque basado en riesgos promovido por el Grupo de Acción Financiera Internacional (GAFI), y los Órganos de Control, que exigen que las organizaciones adopten modelos preventivos más dinámicos, analíticos y orientados a la gestión estratégica del riesgo.

El propósito del siguiente ensayo es analizar el papel de las señales de alerta de LC/FT/FPADM dentro de los sistemas de prevención de LC/FT/FPADM, planteando que su verdadero valor estratégico surge cuando son transformadas en fuentes de información para la identificación de tendencias, la evaluación de exposición al riesgo y la toma de decisiones organizacionales. Para ello, se examina la evolución del paradigma del sistema preventivo desde el cumplimiento normativo hacia la gestión estratégica del riesgo, se analizan las conceptualizaciones necesarias para discernir las discrepancias que pueden existir dentro de estos elementos del sistema preventivo, plasmando una visión donde las señales de alerta pueden actuar como elementos generadores de inteligencia preventiva.

1. Un cambio del paradigma de las señales de alerta dentro del sistema de cumplimiento.

La evolución presente en el enfoque preventivo de los delitos de LC/FT/FPADM, ha obligado a las organizaciones a pasar de un modelo basado en el cumplimiento normativo hacia una gestión integral del riesgo, en este sentido, Blanco, (2015) señala que los sistemas modernos de prevención del lavado de activos requieren superar una visión exclusivamente formalista y orientarse hacia la comprensión de los riesgos asociados a las operaciones económicas.

Es evidente que debe existir una transición que responda a la evolución que viene ocurriendo dentro de los sistemas de cumplimiento, las organizaciones no deben limitarse a verificar exigencias establecidas en las normativas y comenzar a desarrollar sistemas orientados a identificar y gestionar riesgos específicos.

En este mismo contexto, la prevención de los delitos de LC/FT/FPADM, se caracterizaban por un enfoque eminentemente normativo, en el que el principal objetivo consistía en demostrar el cumplimiento de las obligaciones legales vigentes mediante la implementación de controles estandarizado, el éxito de un sistema de prevención se medía, principalmente, por el grado de observancia de las disposiciones legales y reglamentarias existentes. Esto respondía a una realidad en la que los mecanismos utilizados por las organizaciones criminales eran menos complejos y los sistemas financieros operaban en un entorno con menor interconexión internacional. Sin embargo, el incremento de las operaciones transfronterizas, el desarrollo de nuevas tecnologías financieras, la digitalización de los servicios y la sofisticación de las estructuras utilizadas para ocultar el origen ilícito evidenciaron las limitaciones de un modelo basado exclusivamente en el cumplimiento formal.

La consolidación del Enfoque Basado en Riesgos (EBR) constituye uno de los cambios más relevantes en la evolución de los sistemas internacionales de prevención de LC/FT/FPADM. Este enfoque fue impulsado por el Grupo de Acción Financiera Internacional (GAFI), que establece que los países, las

autoridades competentes y los sujetos obligados deben identificar, evaluar, comprender y mitigar los riesgos de lavado de capitales, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva de manera proporcional a su nivel de exposición (GAFI, 2025).

La Recomendación 1 del Grupo de Acción Financiera Internacional (GAFI) constituye el fundamento de este principio al establecer que la asignación de recursos y la intensidad de los controles deben guardar proporción con los riesgos identificados. Dentro de esta lógica, las organizaciones no están llamadas a aplicar idénticas medidas a todos sus clientes o productos y servicios, sino a diseñar controles diferenciados que respondan a las características particulares de cada escenario de riesgo. Este principio de proporcionalidad permite optimizar los recursos institucionales y concentrar los esfuerzos de prevención en aquellas áreas donde la exposición resulta significativamente mayor.

De acuerdo a lo anterior, el EBR representa, un cambio de paradigma que trasciende el cumplimiento regulatorio. Su propósito no consiste únicamente en satisfacer exigencias legales, sino en incorporar la gestión del riesgo como un elemento permanente dentro de la estrategia organizacional. En consecuencia, la eficacia de un sistema de prevención deja de medirse por la cantidad de procedimientos implementados y comienza a evaluarse por su capacidad para identificar oportunamente amenazas, comprender su impacto potencial y adoptar decisiones proporcionales para reducir su probabilidad de materialización.

En función a lo expuesto, las organizaciones deben consolidar EBR, y modificar la manera en la que se interpretan las señales de alerta. El GAFI igualmente indica sobre la eficacia de un sistema de prevención depende de la capacidad de las instituciones para identificar, evaluar y comprender los riesgos a los cuales se encuentran expuestas, aplicando medidas de mitigación proporcionales a dichos riesgos. Esto se debe interpretar en que las señales de alerta deben dejar de ser simples herramientas de identificación de operaciones inusuales para convertirse en insumos estratégicos para alimentar los procesos de evaluación del riesgo institucional.

Se debe considerar, que es un error muy frecuente, atribuir a las señales de alerta un carácter probatorio que excede su verdadera naturaleza jurídica y operativa. En realidad, representan indicios cuya utilidad depende de su interpretación dentro del contexto específico del cliente, del producto y servicio financiero, del canal de distribución, de la actividad económica desarrollada y del entorno geográfico donde se ejecutan las operaciones, una misma conducta puede constituir una señal de alerta para un cliente y resultar un comportamiento completamente razonable para otro, razón por la cual esto se debe sustentar en un análisis con criterios objetivos y en una adecuada comprensión del perfil de riesgo previamente definido.

El cambio del enfoque, en donde se pasa de señales de alerta utilizadas como simples herramientas de identificación de operaciones inusuales para convertirse en insumos estratégicos, exige una transformación conceptual importante, los modelos tradicionales conciben las señales de alerta como mecanismos reactivos orientados a detectar posibles irregularidades una vez ocurridas las operaciones, siendo estas capaces de ser utilizadas como instrumentos prospectivos que permiten anticipar escenarios de mayor exposición y fortalecer en la toma de decisiones. En otras palabras, su valor no reside exclusivamente en identificar comportamientos atípicos, estas pueden generar información para facilitar la gestión integral del riesgo antes de su materialización.

Esto puede resultar particularmente relevante dentro de las señales de alerta, si el objetivo de un sistema preventivo es anticipar escenarios de riesgo y asignar los recursos de manera proporcional, entonces las señales de alerta no pueden seguir interpretándose exclusivamente como listas de comportamientos atípicos o criterios operativos para el monitoreo transaccional. Su verdadera utilidad puede radicar en la información estratégica que aportan para comprender la evolución del riesgo y fortalecer la capacidad preventiva de las organizaciones.

Esta transformación supone un cambio profundo en la lógica de los sistemas de prevención. La prioridad ya no consiste únicamente en identificar operaciones sospechosas, sino en comprender las condiciones que favorecen su aparición,

las señales de alerta pueden ser comprendidas como indicadores estratégicos de riesgo y no únicamente como instrumentos operativos de detección.

No obstante, como se viene mencionando, se puede considerar que el verdadero valor de las señales de alerta de LC/FT/FPADM, no reside únicamente en su capacidad de la información proporcionada, sino que apoya decisiones oportunas y ajustadas al nivel de riesgo identificado, situación acorde con el GAFI, quienes destacan sobre el enfoque basado en riesgos el cual permite utilizar los recursos de manera más eficiente, concentrando las medidas reforzadas en los escenarios de mayor exposición y aplicando medidas simplificadas cuando el riesgo es menor.

2. Discrepancias entre señal de alerta, operación inusual, operación sospechosa e indicador de riesgo

Uno de los principales desafíos para las personas que manejan los sistemas de prevención de los delitos de LC/FT/FPADM, consiste en diferenciar adecuadamente algunos conceptos que, aunque están relacionados entre sí, cumplen funciones distintas dentro del sistema. La falta de claridad conceptual puede generar interpretaciones inadecuadas, ocasionando que aspectos como las señales de alerta sean consideradas como evidencia de una conducta ilícita o, por el contrario, que pierdan relevancia al ser tratadas únicamente como eventos rutinarios dentro de un sistema de monitoreo.

De acuerdo a lo planteado, resulta relevante dejar claro algunos aspectos claros, en cuanto al término correspondiente a señal de alerta este ha sido ampliamente utilizada en la normativa, en las guías emitidas por organismos internacionales, nacionales y en los manuales internos de prevención de LC/FT/FPADM, establecidos por los Sujetos Obligados, para describir aquellos hechos, conductas o características que se salen de lo normal en un cliente. En términos generales, una señal de alerta de LC/FT/FPADM constituye un elemento de información que llama la atención sobre una situación particular y, por sí misma, no demuestra la existencia de una actividad delictiva ni justifica automáticamente la presentación de un reporte de operación sospechosa. Su función consiste en

motivar un análisis más profundo por parte de los sujetos obligados, quienes deberán valorar el contexto integral de la operación antes de adoptar una decisión.

En este mismo contexto, es importante mencionar que de acuerdo a las Normas Relativas a la Administración y Supervisión de los Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo Financiamiento y Financiamiento a la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM), aplicables a las Instituciones del Sector Bancario, indica para la definición de “**Señal de Alerta**: Es el conjunto de indicadores cualitativos y cuantitativos, que permiten identificar oportuna y/o prospectivamente comportamientos atípicos, de las variables relevantes previamente determinadas por el Sujeto Obligado”. (Resolución 010.25; 2025)

Es preciso indicar que, Zabala (2019) plasma lo siguiente con respecto al mismo concepto:

Señales de Alerta: son todas aquellas situaciones que han sido definidos por la empresa como posible eventos generadores de riesgos relacionados con el AL/FT por ser anormales. Estos pueden ser hechos, eventos, cuantías, situaciones o indicadores cuantitativos y cualitativos que la entidad ha determinado como alarma para iniciar seguimiento y aplicación de controles preventivos. (pg. 11)

De acuerdo a lo planteado por la autora antes citada, cuando menciona “situaciones o indicadores cuantitativos y cualitativos”, se puede deducir que las señales de alerta pueden presentarse, de tipo transaccional, el cual involucra el movimiento de recursos (dinero), y con base al conocimiento que se tenga del cliente se puede establecer que hay una anomalía en aspectos como cantidad, medio de pago, beneficiario, etc., relacionado con toda actividad que se pueda cuantificar.

Asimismo, lo cualitativo se refiere a las actividades no transaccional, el cual tiene verifica comportamientos anómalos que se pudieran presentar, y se pueden identificar a través de una entrevista, una llamada telefónica, una visita a la oficina o sede principal o cualquier interacción o contacto directo o indirecto relacionado con esta.

Desde una perspectiva preventiva, una señal de alerta representa un elemento inicial de advertencia el cual indica la posible existencia de una situación y demanda un análisis adicional. No constituye una conclusión sobre la existencia de una actividad delictiva, sino un factor que incrementa la necesidad de comprender mejor una determinada conducta, operación o relación comercial.

En este mismo contexto, es importante conocer los conceptos relativos a operación inusual y operación sospechosa, vistos dentro de las señales de alerta y que suelen ser mal interpretados.

En cuanto a la operación inusual, es el primer acontecimiento de detección cuando se identifica un comportamiento atípico, es una operación irregular que por su cantidad o características, no es acorde con la actividad económica del cliente o se sale de los parámetros normales, suelen originarse a partir de una “Señal de Alerta”, como ejemplo, un incremento brusco en depósitos sin causa aparente.

En cuanto a la operación sospechosa, se entiende como la conclusión de un análisis técnico donde se determina que no hay transparencia en la operación, se asocia directamente con indicios con algún tipo de delito, es obligatorio al confirmarse la sospecha, el sujeto obligado debe emitir de forma inmediata un Reporte de Actividad Sospechosa (RAS) ante la autoridad competente, en el caso de Venezuela Unidad Nacional de Inteligencia Financiera (UNIF).

De acuerdo a la Ley Orgánica Contra la Delincuencia Organizada (2012), indica que una

Operación Sospechosa: aquellas operaciones no convencionales, compleja, en tránsito o estructurada, que después de analizada haga presumir que involucra fondos derivados de una actividad ilícita, o se ha conducido o intentado efectuar con el propósito de esconder o disimular fondos o bienes derivados de actividades ilícitas. (LOCDOFT; 2012)

En este mismo orden de ideas, se establece dentro de las Normas Relativas a la Administración y Supervisión de los Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo Financiamiento y Financiamiento a la Proliferación

de Armas de Destrucción Masiva (LC/FT/FPADM), aplicables a las Instituciones del Sector Bancario, (Resolución 010.25), las siguientes definiciones:

...**Operaciones Inusuales:** Transacción cuya cuantía o característica no guarda relación con la actividad económica del cliente o las transacciones que realiza habitualmente.

...

Actividad Sospechosa: Operación inusual, no convencional, compleja en tránsito o estructurada; que después de analizada, se presume que involucra fondos o bienes derivados de una actividad ilegal, incluyendo aquellas que se han intentado efectuar con el propósito de ocultar el origen de los fondos para violar una norma contra la LC/FT/FPADM, o evitar el reporte a la Unidad Nacional de Inteligencia Financiera (UNIF).

La diferencia fundamental entre una operación inusual y una operación sospechosa radica en la capacidad de justificación y el proceso de análisis al verificar los movimientos sobre la transacción. Mientras lo inusual es un comportamiento el cual se aparta de lo “normal”, lo sospechoso es aquello que, tras ser analizado, no tiene explicación razonable”

Cabe resaltar, sobre una operación que aparentemente resulta inusual puede tener una explicación legítima cuando se analiza el perfil económico, la actividad desarrollada por el cliente, su comportamiento histórico y la naturaleza de la relación comercial. En consecuencia, la señal de alerta funciona como un punto de partida para el análisis, no como una conclusión definitiva.

Otro aspecto fundamental, con gran relevancia son los indicadores de riesgo, (también conocidos como Key Risk Indicators o KRIs), estos son un conjunto de características específicas que permiten conocer y evaluar cómo y en qué medida un sujeto u organización se encuentra expuesto a un riesgo determinado, como los delitos de LC/FT/FPADM, estos explican el “cómo” y el “cuándo” de la exposición al riesgo para cada uno de los elementos de riesgo (como clientes, productos y servicios, áreas geográficas y canales de distribución).

Los indicadores de riesgo permiten determinar un mayor o menor índice de riesgo para un elemento en cuestión y define la forma en la que este será medido, esto sugiere la probabilidad de ocurrencia de una actividad inusual o sospechosa, dando lugar a un mayor seguimiento y análisis.

Cabe destacar, los indicadores de riesgos son un componente técnico esencial y obligatorio dentro del Enfoque Basado en Riesgo (EBR), ya que permite operativizar la identificación y medición de las amenazas y vulnerabilidades, de acuerdo a las Normas Sobre Administración de Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo, Financiamiento a la Proliferación de Armas de Destrucción Masiva y Otros Ilícitos en la Actividad Aseguradora instituyen lo siguiente:

Enfoque Basado en Riesgo (EBR): Principio que permite identificar, evaluar y entender los riesgos de los delitos LC/FT/FPADM y otros ilícitos, a los que se está expuesto los Sujetos Obligados y adoptar las medidas adecuadas para mitigar de manera efectiva dichos riesgos.

Es importante señalar; sin los indicadores de riesgo, el EBR carecería de la base técnica necesaria para realizar juicios fundamentados sobre el riesgo inherente y residual, imposibilitando la asignación eficiente de recursos exigido por el estándar internacional y normativas en la materia. El EBR permite que los indicadores se expresen de diversas formas para adaptarse a la complejidad de la organización, pueden ser cualitativos los cuales reflejan atributos descriptivos, y cuantitativos, miden datos numéricos.

Asimismo, en cuanto a los eventos de riesgos estos son el resultado de revisar cada segmento y la incidencia posible de riesgo de LC/FT/FPADM de manera permanente, teniendo en cuenta que los eventos corresponden a hechos ocurridos, o que pudiesen ocurrir en la organización.

Por otra parte, la diferencia entre una señal de alerta y un indicador de riesgo requieren especial atención, mientras una señal de alerta tradicionalmente identifica una circunstancia específica que requiere revisión, un indicador de riesgo tiene una función más amplia: permite observar tendencias, medir niveles de exposición y apoyar decisiones estratégicas. En otras palabras, la señal de alerta corresponde a la existencia de una situación la cual requiere de atención, mientras un indicador de riesgo es el análisis de la situación, con la finalidad de verificar lo proporcionado por la situación y la medida en la que pueda afectar la valoración del riesgo a fin de tomar la decisiones deberían adoptarse.

Podemos indicar, la señal de alerta es la manifestación específica o el disparador que ocurre cuando uno de esos indicadores se comporta de manera atípica para un cliente en específico, esta se genera de una suposición y posee un carácter principalmente particular y subjetivo relacionado con la persona al realiza la transacción, está obliga a realizar un análisis particular para poder desestimar la sospecha.

En cuanto al indicador de riesgo, se refiere específicamente a variables o criterios generales que se utilizan para segmentar y evaluar el nivel de riesgo de una contraparte o transacción, esto permite analizar el riesgo de forma transversal, estas suelen ser métricas utilizadas para medir el nivel de exposición al riesgo de manera estructurada.

Una señal de alerta no constituye una prueba de actividad ilícita, sino un elemento que requiere análisis adicional los mecanismos de prevención debe fundamentarse en la evaluación del riesgo y no en la presunción automática de ilicitud frente a determinados comportamientos.

Esta diferencia representa una transición desde una visión operativa hacia una visión estratégica. Cuando una organización analiza una señal de alerta únicamente como un evento aislado, limita su capacidad preventiva. En cambio, cuando integra esa información dentro de un modelo de gestión del riesgo, la señal puede convertirse en un elemento que contribuye a comprender patrones, identificar tendencias y fortalecer la asignación de recursos.

Esta distinción resulta fundamental porque uno de los errores más frecuentes consiste en asumir que la aparición de una señal equivale automáticamente a la existencia de una operación sospechosa. Tal interpretación contradice la lógica del enfoque basado en riesgos, debido a que elimina la necesidad del análisis contextual y transforma un mecanismo preventivo en un procedimiento meramente automático.

Siguiendo esta línea de ideas, conviene precisar que, si bien las señales y los indicadores de riesgo suelen estar vinculados e incluso emplearse como sinónimos, ambos poseen matices técnicos distintos dentro de los sistemas de prevención.

En consecuencia, la interpretación de una señal requiere una visión integral que combine datos internos, información externa y conocimiento especializado esta depende de la forma en que son interpretadas por la organización. Si permanecen limitadas a una función operativa, serán únicamente mecanismos de detección. Si son incorporadas dentro de un modelo estratégico de gestión del riesgo, pueden convertirse en herramientas capaces de aportar inteligencia preventiva y fortalecer la capacidad institucional para enfrentar amenazas asociadas a la LC/FT/FPADM.

En este sentido, el enfoque tradicional presenta una limitación conceptual, trata la señal de alerta como un punto final del análisis, cuando en realidad debería constituir un punto de inicio para la generación de conocimiento sobre el riesgo. La alerta no debería cerrar el proceso preventivo mediante una clasificación automática, sino abrir una etapa de evaluación que permita comprender las razones por las cuales determinado comportamiento modifica el perfil de exposición de un cliente o de una relación comercial. Esto significaría el cambio de perspectiva, transformando completamente el papel de las señales de alerta. Pasando de ser mecanismos de detección, a fuentes de información que pueden contribuir a la inteligencia preventiva de la organización.

Desde la perspectiva del marco de gestión Integral del Riesgo Empresarial, Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) (2017) sostiene que la información relevante constituye un componente fundamental para identificar, evaluar y responder ante incertidumbres que puedan afectar el cumplimiento de los objetivos organizacionales. Aplicado al ámbito del LC/FT/FPADM, este principio permite comprender que las señales de alerta poseen un valor estratégico cuando son utilizadas para mejorar la capacidad institucional de anticipación y respuesta.

3. La transformación de las Señales de Alerta, de una función de control a una función estratégica

La finalidad de la transformación de una función de control a una función estratégica, requiere abandonar la visión tradicional que limita a las señales de alerta a un mecanismo de detección de operaciones inusuales. Como se ha mencionado anteriormente, una señal de alerta no constituye una prueba de actividad ilícita ni genera automáticamente la obligación de reportar una operación sospechosa, su función consiste en advertir sobre circunstancias que modifican el nivel de exposición al riesgo y que, por tanto, requieren un análisis más profundo.

Es preciso señalar, que dicha característica vincula las señales de alerta con los indicadores estratégicos de riesgo: ambas herramientas aportan información temprana respecto a situaciones con potencial de impactar en la exposición organizacional al riesgo de LC/FT/FPADM. Si bien su presencia no confirma un evento adverso, advierte sobre transformaciones que demandan medidas proporcionales.

Por ejemplo, un incremento repentino en las transferencias internacionales de un cliente con actividad económica históricamente limitada al mercado local no constituye, por sí solo, evidencia de legitimación de capitales; no obstante, representa una variación relevante que altera su perfil de riesgo. Desde el ámbito operativo, este hallazgo exige una revisión; desde el estratégico, aporta información clave para evaluar la actualización de la categoría de riesgo del cliente, revisar la suficiencia de la debida diligencia y determinar la necesidad de implementar controles adicionales.

Esto evidencia el verdadero aporte de la señal de alerta no consiste únicamente en identificar una operación distinta al patrón esperado, sino en suministrar información lo cual reduce la incertidumbre sobre la evolución del riesgo. En otras palabras, la alerta adquiere valor estratégico porque permite comprender mejor el comportamiento del riesgo antes de generar un evento que pueda afectar a la organización.

Es importante destacar que la función de cumplimiento actualmente requiere de la participación activa, se debe identificar evaluar y tratar los riesgos que puedan afectar la sostenibilidad y reputación de la organización. Esta evolución implica pasar de un modelo reactivo, centrado en revisar incumplimientos o analizar operaciones sospechosas, hacia un modelo estratégico donde la información generada por los sistemas preventivos contribuya a la toma de decisiones institucionales.

Dentro de este nuevo escenario, las señales de alerta adquieren un valor estratégico porque proporcionan información que permite a la organización comprender cómo evolucionan sus riesgos. La función del área de cumplimiento no consiste únicamente en administrar alertas individuales, sino en interpretar los patrones que esas alertas revelan y traducirlos en conocimiento útil para la dirección.

Tradicionalmente, la información relacionada con alertas y operaciones inusuales permanecía concentrada en niveles operativos, llegando a los órganos de dirección únicamente cuando existían casos relevantes o situaciones críticas. Este modelo limita la capacidad preventiva de la organización porque desaprovecha información valiosa sobre tendencias y cambios en los niveles de exposición al riesgo.

Una gestión moderna del riesgo plantea que los sujetos obligados deben recibir información suficiente, oportuna y relevante para orientar sus decisiones. Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) señala que la información relacionada con riesgos debe fluir hacia los niveles adecuados de autoridad, permitiendo una respuesta proporcional y alineada con los objetivos institucionales (COSO, 2017).

La información proveniente de las alertas deja entonces de ser exclusiva del área operativa y se transformaría en un elemento relevante para la dirección estratégica.

La incorporación de las señales de alerta como indicadores estratégicos también genera implicaciones directas en los modelos de evaluación del riesgo. Las matrices de riesgo utilizadas para LC/FT/FPADM se construyen considerando factores como clientes, productos y servicios, canales de distribución y zonas geográficas. Si bien estos elementos continúan siendo esenciales, la incorporación de información proveniente de señales de alerta permite enriquecer la evaluación mediante evidencia obtenida del comportamiento real de las relaciones comerciales.

Esto significa e implica que la matriz de riesgo deja de ser un instrumento estático y comienza a funcionar como un modelo dinámico capaz de incorporar cambios derivados del comportamiento observado.

La Organización Internacional de Normalización (ISO 31000:2018), destaca que la gestión del riesgo debe ser dinámica y adaptarse a cambios internos y externos que puedan modificar la naturaleza de las amenazas enfrentadas por una organización (ISO, 2018).

Conclusión

A partir del análisis expuesto, se concluye que la conversión de las señales de alerta en indicadores de riesgo por parte de los Órganos de Control y los Sujetos Obligados representa una de las transformaciones más trascendentales en la evolución de los sistemas de prevención de LC/FT/FPADM, lo que permite consolidar de forma efectiva el Enfoque Basado en Riesgo (EBR).

Es importante señalar que una institución orientada al fortalecimiento de su Enfoque Basado en Riesgo, puede utilizar sus señales de alertas para comprender cómo evoluciona su exposición al riesgo y no únicamente para identificar casos individuales; esto en concordancia con lo establecido con el análisis expuesto, en donde se deja claro que las señales de alerta alcanza su verdadera dimensión estratégica cuando deja de ser vista como un instrumento de control dentro de un proceso operativo y comienza a ser interpretada como una fuente de conocimiento institucional.

El análisis evidencia que las señales de alerta cumplen una doble función: operativa, al identificar de manera oportuna desviaciones que exigen una revisión puntual, y estratégica, al transformar esos eventos en inteligencia accionable para comprender, anticipar y gestionar los riesgos institucionales. Esto permite inferir que las señales trascienden el mero rol de detonadores de procesos reactivos; evaluadas bajo el Enfoque Basado en Riesgo (EBR), potencian sustancialmente la capacidad de prospectiva de la organización. En consecuencia, esta evolución redefine la función del área de cumplimiento —que pasa de ser un centro de control reactivo a un aliado estratégico— y consolida sistemas preventivos más dinámicos, eficientes y adaptados a las complejas dinámicas del entorno financiero y la delincuencia organizada

Referencias

- Asamblea Nacional de la República Bolivariana de Venezuela.** (2012). *Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT)*. Gaceta Oficial N° 39.912.
- Asamblea Nacional de la República Bolivariana de Venezuela.** (2025). Normas Relativas a la Administración y Supervisión de los Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo Financiamiento y Financiamiento a la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM), aplicables a las Instituciones del Sector Bancario. Gaceta Oficial N° 43.098.
- Asamblea Nacional de la República Bolivariana de Venezuela.** (2024). Normas Sobre Administración de Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo, Financiamiento a la Proliferación de Armas de Destrucción Masiva y Otros Ilícitos en la Actividad Aseguradora. Gaceta Oficial N° 6.835.
- Blanco Cordero, I.** (2015), "El Delito de Blanqueo de Capitales", Editorial Aranzadi, Pamplona,
- Committee of Sponsoring Organizations of the Treadway Commission** (2017). *Gestión del riesgo empresarial: Integración con la estrategia y el desempeño* [Enterprise risk management: Integrating with strategy and performance]. COSO.

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*

International Organization for Standardization (ISO). (2018). *ISO 31000:2018 Gestión del riesgo: Directrices ISO 31000:2018*

Zabala Leal, T (2019), *Mitigación del riesgo de lavado de activos y financiamiento del terrorismo*, Editorial Politecnico Grancolombino

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 SEÑALES DE ALERTA

**LA EVOLUCIÓN DEL AZAR: SEÑALES DE ALERTA PARA MITIGAR
RIESGOS DE LC/FT EN LAS RIFAS DIGITALES EN VENEZUELA**

Autor: Abg. Esp. Yeixon Santaella Bernal

Facilitador: Lcda. Elizabeth Pelaez

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 SEÑALES DE ALERTA

**LA EVOLUCIÓN DEL AZAR: SEÑALES DE ALERTA PARA MITIGAR
RIESGOS DE LC/FT EN LAS RIFAS DIGITALES EN VENEZUELA**

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

Resumen

El presente ensayo analiza la mutación del riesgo de Legitimación de Capitales (LC) en el sector de juegos de azar en Venezuela, impulsado por la irrupción de las rifas digitales organizadas por creadores de contenido en redes sociales. Este fenómeno ha gestado un ecosistema caracterizado por la masividad telemática, la opacidad de los fondos y la exhibición injustificada de premios ostentosos, desbordando las matrices de riesgo tradicionales. Se examina la forma de obrar de estas operaciones, las cuales instrumentalizan la avalancha de pequeñas transacciones para mezclar e integrar capitales ilícitos bajo la apariencia de sorteos. En respuesta a las vulnerabilidades de los controles preventivos anclados en el uso de efectivo físico, se propone una actualización estratégica al catálogo de señales de alerta emitido por la Unidad Nacional de Inteligencia Financiera (UNIF), enfocada en el pitufeo digital, la incongruencia en el incremento patrimonial y la triangulación de cuentas. Finalmente, se reafirma con rigor dogmático que el Reporte de Actividades Sospechosas (RAS) que resulta del análisis, funciona estrictamente como un insumo analítico de inteligencia financiera, desprovisto de carácter probatorio o de convicción penal, preservando la naturaleza procesal del sistema preventivo nacional.

Descriptor clave: Rifas digitales; Señales de alerta; Inteligencia Financiera; Influencer; Reporte de Actividades Sospechosas

Abstract

This essay analyzes the evolving risk of money laundering (ML) in Venezuela's gambling sector, driven by the rise of digital raffles organized by social media content creators. This phenomenon has fostered an ecosystem characterized by massive online participation, opaque funds, and the unjustified display of

extravagant prizes, overwhelming traditional risk matrices. The essay examines how these operations function, leveraging the flood of small transactions to mix and integrate illicit funds under the guise of raffles. In response to the vulnerabilities of preventive controls based on the use of physical cash, a strategic update to the catalog of red flags issued by the National Financial Intelligence Unit (UNIF) is proposed, focusing on digital smurfing, discrepancies in asset growth, and account triangulation. Finally, it is rigorously reaffirmed that the Suspicious Activity Report (SAR) resulting from the analysis functions strictly as an analytical input for financial intelligence, devoid of probative or criminal conviction character, preserving the procedural nature of the national preventive system.

Keywords: Digital raffles; Warning signs; Financial intelligence; Influencer; Suspicious Activity Report.

La suerte del crimen organizado

La mutación constante de la criminalidad organizada exige una revisión continua de los mecanismos y medidas de prevención y control asumidos por las instituciones que conforman el sistema financiero y no financiero venezolano, con el propósito de evitar la proliferación de la delincuencia organizada. Tradicionalmente, el sector de juegos de envite y azar ha sido catalogado como una actividad de alto riesgo para la Legitimación de Capitales y el Financiamiento al Terrorismo (LC/FT), operando bajo estrictos esquemas de supervisión.

Sin embargo, la irrupción de las plataformas digitales y la economía de los creadores de contenido –quienes recurren a la recomendación de marcas logrando así monetizar sus redes sociales– han gestado un ecosistema paralelo, trasladando las rifas tradicionales a plataformas digitales sin autorización del órgano supervisor. Este fenómeno, caracterizado por su masividad, transfronterización y la opacidad en el origen de los fondos, ha generado desafíos para la elaboración de matrices de riesgo convencionales y generación para el rastreo de alertas.

Recientes actuaciones de los órganos de investigación penal han visibilizado las vulnerabilidades del sector de las loterías, donde la fachada de un sorteo digital puede ser instrumentalizada para justificar la integración de capitales ilícitos en el sistema financiero nacional.

La captación masiva de fondos a través de microtransacciones no reguladas y la exhibición de bienes de alto valor sin una justificación económica lícita aparente, representan un desafío mayúsculo tanto para los sujetos obligados como para las autoridades reguladoras.

Un caso emblemático que pone en evidencia esta afirmación, es el ocurrido en Brasil donde el *influencer* Chrys Dias fue capturado bajo la operación *Narco Fluxo*, en abril de 2018, junto a 36 personas que conformaban un grupo de delincuencia organizada que operaban desde Río de Janeiro y Sao Paulo ofertando rifas de propiedades de alto valor en redes sociales, según reseñó el portal *InSight Crime*¹³ en un artículo web.

Pero no solo en Brasil se han realizado esfuerzos para impedir la proliferación de esta tipología, también en México la Unidad de Inteligencia Financiera (UIF) en la actualidad investiga a más de 64 *influencer* de ese país “por utilizar rifas y contratos publicitarios en redes sociales para lavar dinero de redes criminales como el Cártel de Sinaloa”, refiere el mismo artículo

En este sentido, el presente ensayo tiene como propósito analizar la evolución de estas modalidades de sorteos digitales y proponer un catálogo actualizado de señales de alerta.

Asimismo, proporcionar herramientas técnicas que permitan a las instituciones financieras y demás actores del sistema, detectar oportunamente comportamientos inusuales, facilitando la generación de insumos de inteligencia financiera de alta calidad, entendiendo siempre que dichas alertas operan como elementos de análisis estratégico y no como presupuestos de convicción penal.

Todo ello, para contribuir al robustecimiento del sistema preventivo nacional, cerrando las brechas operativas frente a las nuevas tipologías de la delincuencia organizada.

Organización Sin Fines de Lucro dedicada a la investigación para profundizar y enriquecer el debate sobre el crimen organizado y la seguridad ciudadana en América Latina y el Caribe

1. De la lotería tradicional a la rifa digital

Históricamente, los juegos de envite y azar en Venezuela han operado bajo un marco de supervisión vertical, donde las instituciones oficiales de beneficencia pública actúan como garantes de un ecosistema que, por su naturaleza intensiva en efectivo y su volatilidad, presenta vulnerabilidades inherentes frente al riesgo de LC/FT.

En este modelo tradicional, la trazabilidad financiera recae sobre plataformas tecnológicas centralizadas, auditables y sujetas a estrictas normativas tributarias y de reporte.

En los últimos años, ha emergido un mercado paralelo y altamente líquido que presenta una evolución de este sector y se trata de las rifas digitales. En este nuevo entorno, las plataformas de interacción social sustituyen a las agencias de lotería tradicionales, y la figura del operador digital se erige como un promotor independiente de juegos de azar que capta fondos de forma masiva, directa y transfronteriza.

Este ecosistema digital se caracteriza por una convergencia de factores de riesgo crítico, un alto grado de pseudoanonimato comercial, una velocidad instantánea en la recepción de fondos como el uso intensivo de la red de pagos interbancarios en tiempo real, y una preocupante opacidad respecto a la procedencia lícita de los premios de alto valor (que pudieran existir o no), ofertados para atraer rápidamente a los participantes.

La debilidad regulatoria inicial frente a este fenómeno facilitó un escenario donde se pudo instrumentalizar el alcance digital para la integración y estratificación de capitales ilícitos, simulando un origen económico legítimo mediante la aparente comercialización de boletos.

Frente a esta mutación del riesgo, la respuesta institucional venezolana se materializó a través de la Comisión Nacional de Lotería (CONALOT), promoviendo la regularización de la actividad a través de la Providencia

Administrativa 2025-001, la cual en su artículo 1 establece que su principal objeto es “establecer las normas, procedimientos, regulaciones y condiciones que regirán la explotación, organización, administración, y operación del juego de lotería en su tipología de Rifa en todas sus modalidades y variantes”.

Esta misma norma también define claramente lo que son las rifas virtuales o en línea, en su artículo 6, literal b, donde aclara que son aquellas que “sigue esquemas simulados de manera digital a través de internet; y donde el evento no tiene lugar físicamente presente”.

Dicha normativa exige a los popularmente denominados riferos, la figura del Registro Único Nacional de Loterías (RUNLOT) como licencia indispensable para operar en cualquiera de las modalidades de rifas.

También, la norma exige la demostración documental sobre el origen lícito de los bienes a rifar, en cumplimiento de la Providencia Administrativa N° CNL/DP/2016-0029 de fecha 04 de abril de 2016, publicada en Gaceta Oficial N°40.952 del 26 de julio de 2016, contentiva de las Normas sobre prevención, Control y Fiscalización de los Delitos de Legitimación de Capitales y el Financiamiento al Terrorismo en la actividad de Juegos de Lotería.

No obstante, desde la óptica dogmática y operativa del sistema preventivo de LC/FT, la responsabilidad de mitigar estas vulnerabilidades trasciende al ente regulador del juego y compromete directamente la diligencia de los sujetos obligados del sector financiero.

Este nivel de exigencia frente a la innovación operativa no es una inferencia académica, sino un mandato taxativo de los estándares internacionales. La urgencia de adaptar las matrices de riesgo a esta disrupción digital encuentra su asidero normativo en el marco del Grupo de Acción Financiera (GAFI) específicamente en su Recomendación 15 sobre Nuevas tecnologías, el cual advierte de forma explícita que:

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.

Es imperativo, por tanto, que el sistema de prevención y control venezolano no se limite a la simple verificación administrativa de permisos operacionales, sino que desarrolle una comprensión profunda del comportamiento transaccional subyacente de estos operadores digitales.

Solo al decodificar la mecánica de esta migración tecnológica, las unidades de administración de riesgos de LC/FT podrán detectar oportunamente las señales de alerta y generar análisis financiero útil, marcando la diferencia entre una actividad promocional lícita y un esquema estructurado de LC/FT.

2. Las rifas criminales en Venezuela

Durante el primer semestre del año 2026, el país fue testigo de una serie de procedimientos judiciales, administrativos y policiales sin precedentes dirigidos a desarticular el ecosistema irregular de las rifas en redes sociales.

Estos operativos, que resultaron en investigaciones y detenciones preventivas de figuras de alto perfil mediático en el entorno digital —tales como Brayan Lucena, Cruzangelo Pasquale y Yeimmy Rodríguez—, expusieron la materialización de un esquema complejo de LC que operaba al margen de la supervisión financiera tradicional.

Lejos de tratarse de simples infracciones administrativas por evasión de tributos o falta de permisos ante la CONALOT, las autoridades competentes visibilizaron este fenómeno como una tipología emergente de LC. El *modus operandi* (Modo de operar) identificado en estos esquemas devela una estructura financiera sofisticada que instrumentaliza el alcance de los *influencers*¹⁴ para vulnerar los controles de los sujetos obligados.

A partir del análisis de los resultados de las investigaciones publicadas, la mecánica de esta actividad ilícita se articula en tres fases fundamentales, que

Persona con presencia en redes sociales que es capaz de influir a otros en opiniones, estilo de vida o adquisición de productos y/o servicios

permitirían a efectos de este ensayo, analizar los elementos para obtener una serie de señales de alertas que, en los capítulos siguientes, se analizarán con las señales ya ofrecidas por la Unidad Nacional de Inteligencia Financiera (UNIF).

La primera fase del esquema delictivo inicia con el creador de contenido, quien funge como operador no regulado. Este individuo oferta de manera súbita premios de altísimo valor que presentan una desconexión total con su perfil económico y su actividad financiera histórica. Se promocionan bienes suntuosos como apartamentos en zonas exclusivas, flotas de vehículos último modelo o motocicletas de alta cilindrada, entre otros.

El riesgo radica en que la procedencia de estos activos es incierta; no existe una trazabilidad bancaria previa que justifique su adquisición lícita, convirtiendo la exhibición del bien en la herramienta necesaria para justificar el posterior ingreso masivo de liquidez al sistema.

Como segunda fase se presenta lo que se puede considerar como el núcleo de la tipología, la cual se ejecuta mediante la venta masiva de boletos a costos ínfimos (por ejemplo, tickets entre 1 y 10 dólares). Al aprovechar una audiencia cautiva de millones de seguidores, se genera una avalancha de microtransacciones hacia las cuentas bancarias del organizador.

En este punto de saturación ocurre la verdadera legitimación, ya que las organizaciones criminales utilizan este canal masivo para inyectar su propio dinero ilícito mediante la autocompra ficticia de millares de boletos. Así, el capital de origen ilícito se mezcla con los aportes lícitos de los participantes reales que, por seguir a su *influencer* favorito, no duda de la veracidad del premio. Y es que en ningún momento hay farsa en el premio, la farsa no es contra el comprador de la rifa sino contra el Estado y el sistema financiero.

Este mecanismo fue explicado y denunciado públicamente en marzo de 2026 por el Gobierno Nacional a través de los medios de comunicación social. El diario El Nacional, a través de un artículo publicado, detalló la captación de estos

creadores de contenido por parte de redes estructuradas, explicando la proporción del esquema, según declaraciones de la creadora de contenido Michi Marín, quien presuntamente fue contactada para participar en este entramado y relató parte del entramado.

En esa cuenta bancaria va a entrar todo el dinero de los 100.000 tickets supuestamente que tú vendiste, y de ahí entonces el dinero ya está limpio porque entró al banco. 'Nosotros te damos el 10%'. A ver, si ellos dicen que se vendieron 100.000 tickets a 10 dólares, es 1 millón de dólares. El 10% son 100.000 dólares. Entonces esos *influencers* se están ganando 100.000 dólares sucios, aprovechándose de la gente.

Finalmente, para otorgar una apariencia de licitud definitiva y cerrar el ciclo, la tercera fase describe a los operadores que realizan sorteos telemáticos que carecen del escrutinio de auditores independientes o de la fe pública de un notario.

El mismo *modus operandi* advierte sobre el alto riesgo que estos bienes terminen presuntamente adjudicados a ganadores simulados, interpuestas personas o miembros periféricos de la misma red criminal, logrando que, de esta manera, tanto el organizador (que retiene su porcentaje como comisión) como la organización criminal (que recupera el bien o el dinero ya bancarizado) logran integrar el patrimonio al sistema formal bajo la falsa justificación legal de un premio de lotería.

Este es el método que se ha logrado visualizar en Venezuela. Sin embargo, en países como Colombia, Brasil y México existen otras formas para legitimar capitales a través de las rifas digitales. Así refiere el abogado Joao Paulo Martinelli, en una entrevista al portal *InSight Crime* al señalar que:

El lavado de dinero puede darse cuando una persona u organización vinculada a actividades criminales entrega dinero a un influencer bajo la apariencia de donaciones, y este lo devuelve mediante premios de rifas (...) Los *influencers* pueden recibir múltiples pagos de bajo monto por concepto de donaciones o de publicidad que, al no superar los topes establecidos por las entidades financieras, evitan que sean reportados como operaciones sospechosas. Estas transacciones incluso pueden realizarse con criptomonedas y billeteras virtuales, lo que complica aún más su trazabilidad. (2026).

Estas formas de proceder demuestran que las evaluaciones estáticas realizadas por los sujetos obligados son insuficientes. Las instituciones bancarias, al

enfrentar este comportamiento, pueden interpretar la avalancha de pagos móviles y transferencias como el éxito comercial o la viralidad de un cliente, fracasando en la identificación de la tipología de pitufeo digital a gran escala.

Por consiguiente, resulta imperativo fortalecer el catálogo de señales de alerta suministrado por la UNIF, que detecte la instrumentalización de la banca en estas etapas críticas, a fin de generar reportes tempranos que sirvan de auténtico insumo de inteligencia financiera.

3. Señales de alerta identificables para los juegos de lotería

Según lo establecido en el glosario de términos de la Unidad Nacional de Inteligencia Financiera (UNIF), una señal de alerta es el “conjunto de indicadores cualitativos y cuantitativos que permiten identificar oportuna y/o prospectivamente comportamientos atípicos de las variables relevantes, previamente determinadas”.

En este contexto, es menester reconocer que la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (2012) establece en su artículo 12 que:

Los sujetos obligados por esta Ley deberán establecer mecanismos que permitan detectar cualquier transacción inusual o sospechosa, aun cuando éstas tengan una justificación económica aparente o visible, así como también las transacciones en tránsito o aquellas cuya cuantía u otra característica lo amerite a juicio de la institución o según lo establezca el Ejecutivo Nacional.

Por otra parte, cada sector financiero y no financiero que cuenta con normativa prudencial, exige a los sujetos obligados a dar fiel cumplimiento a este mandato legal e insta a estar atento a la aparición de señales de alerta en las operaciones de sus clientes y relacionados.

Precisamente para fortalecer la acción de identificación y conocimiento de las señales de alerta en el sector de loterías y juegos en línea, la UNIF, en el marco de sus competencias, emitió la Circular N° UNIF-DDG-DSU-000830, de fecha 26 de febrero de 2025, la cual consagra un catálogo formal de señales de alerta cuantitativas y cualitativas.

Entre estas señales, el organismo de inteligencia financiera tipifica escenarios de riesgo fundamentales como la variedad, frecuencia y cantidad de las transacciones en efectivo, el cambio de beneficiarios en los tickets o billetes ganadores, por personas no vinculadas al jugador, y la solicitud de realizar pagos por montos elevados a través de medios electrónicos o activos virtuales con proveedores de servicios no autorizados.

Asimismo, el ente advierte expresamente sobre personas naturales y jurídicas relacionadas con operaciones superiores a su perfil de ingresos y aquellos ganadores que solicitan fraccionar el valor del premio en montos estructurados de menor cuantía o a nombre de terceras personas, entre otras.

Sin embargo, al contrastar estos indicadores con la fenomenología delictiva de los creadores de contenido observada en la reciente casuística nacional, se hace evidente la necesidad de fortalecer y adaptar dichas señales de alerta.

Las alertas vigentes de la UNIF mantienen un enfoque operacional primordialmente anclado en la dinámica de la lotería física tradicional, con un énfasis marcado en el flujo de dinero en papel moneda, la alteración de billetes impresos y la estructura presencial de los centros de apuestas.

En contraposición, el modo de proceder para la legitimación en redes sociales prescinde casi en su totalidad del efectivo físico, operando en un entorno de hiper-digitalización donde la figura del *influencer* actúa como vehículo corporativo de opacidad.

Por consiguiente, se propone la incorporación de las señales de alerta para complementar la normativa vigente y detectar la intrusión de capitales ilícitos en el ecosistema particular de los sorteos digitales:

- a. Desfase patrimonial mediático injustificado de creadores de contenido en redes sociales: si bien la UNIF alerta sobre operaciones que superan el perfil de ingresos, en el entorno de las redes sociales esto se materializa cuando un cliente, cuya actividad económica histórica es de baja

transaccionalidad, inicia campañas virales asumiendo el rol de organizador de sorteos y exhibiendo repentinamente un estilo de vida de alta gama que carece de asidero en su expediente bancario tradicional.

- b. Uso instrumental de cuentas jurídicas constituidas con objetos sociales diametralmente opuestos a los juegos de azar (por ejemplo, firmas de marketing o empresas de comercio minorista) para centralizar la recaudación masiva de boletos telemáticos.
- c. Recepción masiva de transferencias interbancarias de muy bajo importe (equivalentes a transacciones entre \$1 y \$10 mediante la red de Pago Móvil), que saturan la operatividad de la cuenta en lapsos de horas o días, sin justificar la venta de un bien tangible.
- d. Vaciado inmediato de la liquidez masivamente recaudada hacia un entramado de cuentas de terceros o su inyección rápida en plataformas de intercambio de criptoactivos con el fin de romper la trazabilidad de forma cuasi instantánea.
- e. Oferta pública de un evento donde el creador de contenido direcciona a su audiencia a efectuar los pagos a instrumentos financieros (cuentas o teléfonos afiliados a pago móvil) que no se encuentran a su nombre, utilizando a familiares o colaboradores periféricos para distanciar su identidad del rastro transaccional.
- f. Recepción atípica de transferencias de montos significativamente elevados provenientes de un grupo muy reducido de actores que simulan ser patrocinadores o compradores mayoristas de tickets digitales, siendo este el mecanismo medular para mezclar el capital sucio con los micro-aportes lícitos de los seguidores.
- g. Egresos de capital destinados a la compra de vehículos de concesionario, motocicletas de alto cilindraje o inmuebles de lujo (los premios a rifar), sin

que el promotor cuente con un flujo de caja lícito previo que demuestre su capacidad para realizar dicha inversión inicial de forma legítima.

- h. Ruptura de trazabilidad del beneficiario final: De manera homóloga a la alerta de la UNIF sobre el cambio de beneficiarios en tickets físicos, en el entorno digital el organizador justifica salidas de dinero alegando el pago de los premios o la entrega de bienes, pero fracasa al intentar demostrar documentalmente ante el banco la identidad real y verificable del ganador telemático, elevando la sospecha de que el activo fue retornado a la propia red ilícita.

La identificación temprana y la debida sustentación de estos indicadores constituyen la piedra angular del sistema de prevención y control, no solo de los sujetos obligados del sector loterías sino de los otros sectores que, como el bancario, participa en la actividad.

Es fundamental reiterar dogmáticamente que la consolidación de estas alertas en un Reporte de Actividad Sospechosa (RAS) remitido a la autoridad competente, tiene como naturaleza jurídica servir como un insumo estratégico de inteligencia financiera, desprovisto de carácter probatorio y sin constituirse como un elemento de convicción penal contra el individuo reportado.

4. Del monitoreo a la inteligencia financiera

La parametrización de nuevas tipologías y la detección de las señales de alerta propuestas anteriormente carecerían de eficacia si no se materializan en un flujo de información eficiente y dogmáticamente correcto. Se debe crear una normativa que contemple la identificación de estas personas e incluso ambicionar y quizá incorporarlos como sujetos obligados de la categoría de Actividades y Profesiones No Financieras Designadas (APNFD).

Cuando un sujeto obligado, en el ejercicio de su debida diligencia intensificada, detecta que un creador de contenido está incurriendo en un fraccionamiento digital masivo o exhibiendo una riqueza inconmensurable sin justificación

documental frente a la promoción de una rifa, el paso siguiente es la elaboración de un Reporte de Actividades Sospechosas (RAS).

Es en este punto de inflexión donde la gestión preventiva del riesgo se entrelaza con las capacidades investigativas. Sin embargo, para que el sistema funcione armónicamente, es imperativo establecer con rigor académico la naturaleza jurídica y el alcance procedimental de este reporte.

A nivel global, el destino de estas alertas está claramente delimitado por los estándares del GAFI, específicamente en su Recomendación 29, la cual dictamina de manera literal el rol del ente receptor, que en el caso venezolano es la UNIF:

Los países deben establecer una Unidad de Inteligencia Financiera (UIF) que sirva como un centro nacional para la recepción y análisis de: (a) reportes de transacciones sospechosas; y (b) otra información relevante al lavado de activos, delitos determinantes asociados y el financiamiento del terrorismo, y para la comunicación de los resultados de ese análisis.

En estricto apego a este estándar internacional y a la legislación venezolana vigente, el flujo del reporte exige comprender que el RAS remitido opera en una esfera puramente analítica. Existe una delgada línea técnica que el analista de prevención no debe cruzar y es el equiparar la emisión de un RAS con la formulación de una denuncia.

Estos reportes no ostentan estatus criminal ni constituyen, por sí mismos, elementos de convicción probatoria. Por el contrario, su función es servir estrictamente como insumos de inteligencia financiera.

Solo en el escenario donde este análisis técnico determine la presunción fundamentada de un esquema de legitimación de capitales subyacente en la rifa, la UNIF procederá a diseminar el producto de inteligencia (Informe de Inteligencia Financiera) resultante hacia el Ministerio Público.

Es esta institución, como titular de la acción penal y directora de la investigación, la única facultada para ordenar las diligencias correspondientes y transformar los

indicios financieros en verdaderos elementos de convicción que sustenten un eventual proceso judicial.

Mantener clara esta distinción procesal es vital para proteger el debido proceso y garantizar que los sujetos obligados cumplan su rol preventivo sin arrogarse funciones persecutorias que no les corresponden.

5. Reflexiones finales

La mutación de la legitimación de capitales hacia el ecosistema de las rifas digitales representa mucho más que un desafío regulatorio, constituye una profunda transgresión ética y social.

La influencia mediática y la confianza del público son instrumentalizadas por redes criminales para enmascarar la integración de capitales ilícitos, pervirtiendo la naturaleza lúdica del azar para convertirla en un vehículo de opacidad.

La respuesta del Estado venezolano no puede limitarse a una simple actualización burocrática de normativas, sino que debe asumir una postura moral activa e inquebrantable en la defensa de la integridad del sistema financiero venezolano.

La actualización de las señales de alerta propuestas en este ensayo es un imperativo profesional ineludible, ya que el Oficial de Cumplimiento moderno no debe ser un espectador pasivo ante la saturación de microtransacciones o la ostentación patrimonial injustificada en redes sociales.

Es por ende que, los analistas de prevención son considerados como los verdaderos guardianes del orden económico frente a estas nuevas amenazas, y la labor de escrutinio ante el pitufeo digital es vital para evitar que la impunidad se disfraze de viralidad.

La tecnología y las plataformas de interacción social no pueden seguir operando como un escudo que exima de responsabilidad a quienes promueven ecosistemas financieros paralelos.

Finalmente, la eficacia de la inteligencia financiera debe convivir armónicamente con la dogmática jurídica y el respeto irrestricto al debido proceso. Los RAS derivados de la detección de estas nuevas tipologías deben concebirse, indiscutiblemente, como un insumo analítico de inteligencia superior y jamás como una condena anticipada que subvierta los roles procesales.

En este sentido, la verdadera fortaleza del sistema preventivo radicará en la capacidad de desenmascarar el fraude cibernético con suma agudeza técnica, pero actuando siempre subordinados a los valores supremos de la justicia, la racionalidad y el Estado de Derecho.

Referencias

Asamblea Nacional de la República Bolivariana de Venezuela. (2012). *Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT)*. Gaceta Oficial N° 39.912.

Comisión Nacional de Loterías (CONALOT). (2016). *Providencia Administrativa N° CNL/DP/2016-0029 contentiva de las Normas sobre prevención, Control y Fiscalización de los Delitos de Legitimación de Capitales y el Financiamiento al Terrorismo en la actividad de Juegos de Lotería*. Gaceta Oficial N°40.952 del 26 de julio de 2016.

Comisión Nacional de Loterías (CONALOT). (2025). *Providencia Administrativa N° CONALOT/P/2025-001 contentiva de las Normas relativas a la administración, operación, control, inspección, fiscalización, regulación y supervisión de los procedimientos de juegos de lotería en su tipología de rifa en el territorio nacional*. Disponible en la URL: <https://www.conalot.gob.ve/wp-content/uploads/2026/03/Prov-001.pdf>

El Nacional. (2026). *Diosdado Cabello acusa a tiktokers de lavar dinero con rifas: “Estamos investigando”*. Artículo periodístico, disponible en la URL: <https://www.elnacional.com/2026/03/diosdado-cabello-acusa-a-tiktokers-de-lavar-dinero-con-rifas-estamos-investigando/>

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

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*.

InSight Crime (2026). *¿Cómo pueden los influencers facilitar el lavado de dinero de redes criminales?* Disponible en la URL: <https://insightcrime.org/es/noticias/como-pueden-influencers-facilitar-lavado-dinero-redes-criminales/>

Unidad Nacional de Inteligencia Financiera (UNIF). (2025). *Circular sobre señales de alerta, controles internos y directrices relacionadas con los Reportes de Actividades Sospechosas (RAS) del sector Loterías*. Fecha 26 de febrero de 2025. Disponible en URL: [https://www.unif.gob.ve/wp-content/uploads/Circulares_UNIF/CC_UNIF_DD_G_DSU_000830_\(2025_02_26\).pdf](https://www.unif.gob.ve/wp-content/uploads/Circulares_UNIF/CC_UNIF_DD_G_DSU_000830_(2025_02_26).pdf)

Unidad Nacional de Inteligencia Financiera (UNIF). (2026). *Glosario. Definición de Señales de Alerta*. Disponible en URL: <https://www.unif.gob.ve/glosario/>



Gobierno Bolivariano
de Venezuela

Ministerio del Poder Popular
de Economía y Finanzas



REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR DE ECONOMÍA Y FINANZAS
ESCUELA NACIONAL DE ADMINISTRACIÓN Y HACIENDA PÚBLICA
DIRECCIÓN DE POSTGRADO Y ADIESTRAMIENTO
ESPECIALIZACIÓN EN GESTIÓN CONTRA LEGITIMACIÓN DE CAPITALES
Y FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR SEÑALES DE ALERTA

**ABORDAJE DE LA SEÑAL DE ALERTA COMO INSTRUMENTO QUE
SEÑALA COMPORTAMIENTOS ATÍPICOS CUYA INTERPRETACIÓN
MUESTRA EL GRADO DE DESVIACIÓN CON RELACIÓN AL
CUMPLIMIENTO DE LA NORMA EN MATERIA DE LEGITIMACIÓN DE
CAPITALES, FINANCIAMIENTO AL TERRORISMO, EL FINANCIAMIENTO
DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA Y OTROS
ILÍCITOS**

Autor : Dr. Juan Jesús Arevalo

Facilitadora: Elizabeth Pelaez

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
DIRECCIÓN DE POSTGRADO Y ADIESTRAMIENTO
ESPECIALIZACIÓN EN GESTIÓN CONTRA LEGITIMACIÓN DE CAPITALES
Y FINANCIAMIENTO AL TERRORISMO
UNIDAD CURRICULAR SEÑALES DE ALERTA

**ABORDAJE DE LA SEÑAL DE ALERTA COMO INSTRUMENTO QUE
SEÑALA COMPORTAMIENTOS ATÍPICOS CUYA INTERPRETACIÓN
MUESTRA EL GRADO DE DESVIACIÓN CON RELACIÓN AL
CUMPLIMIENTO DE LA NORMA EN MATERIA DE LEGITIMACIÓN DE
CAPITALES, FINANCIAMIENTO AL TERRORISMO, EL FINANCIAMIENTO
DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA Y OTROS
ILÍCITOS**

Autor (a): Dr. Juan Jesús Arevalo González
[https://orcid.org/ 0009-0009-1160-046X](https://orcid.org/0009-0009-1160-046X)
Correo electrónico: Jaregon5@gmail.com

RESUMEN

El abordaje apropiado de una señal de alerta nos conduce a la interpretación de un comportamiento, el cual nos permite establecer la existencia o no de la desviación con relación al cumplimiento de una norma, es la advertencia sobre posibles riesgos (financieros, de seguridad, educativos o de salud) antes de que estos se materialicen. Su incidencia nos permite iniciar el proceso de mitigación y combate de la comisión de los delitos relativos a Legitimación de Capitales, el Financiamiento al Terrorismo, el Financiamiento de la Proliferación de Armas de Destrucción Masiva (LC/FT/FPADM), y otros ilícitos, estableciendo impedir la utilización de las Instituciones Financieras como vehículos, para la realización del delito principalmente por organizaciones criminales de carácter transnacional. Dicha Investigación tiene un carácter descriptivo, bajo un diseño documental. Principalmente la recolección de información se realizó mediante la observación documental y el resumen analítico, para producir un análisis crítico, apoyado en la herramienta fundamental denominada señales de alerta. Si bien existe todo un marco normativo, así como ejercicios de tipologías que les agrupan, así como existen marcos normativos con diferencias fundamentales en cada nación, su confección así como la realización de ejercicios, talleres y evaluaciones mutuas, está fundamentado principalmente por las recomendaciones del GAFI, las cuales están fundamentadas por el enfoque basado en riesgos, e implementadas de manera muy formal, evidenciando debilidades en la periodicidad de su actualización, y en la inclusión de importantísimas variables macroeconómicas típicas de cada país y acordes a su realidad político administrativa. Esta forzosa implementación requiere de diversas variables que aseguren la implementación exitosa del instrumento. Este

instrumento de carácter dinámico, preventivo y sistemático fundamental fortalece la adopción de medidas que garantizan la mitigación adecuada del ilícito financiero por parte de los sujetos obligados.

Descriptores: Señales de alerta, Señal de alerta, LC/FT/FPADM, GAFI, Enfoque Basado en Riesgos, Crimen Transnacional.

ABSTRACT

The appropriate approach to a warning sign leads us to the interpretation of a behavior, allowing us to establish whether or not a deviation exists in relation to compliance with a norm. It is a warning about potential risks (financial, security, educational, or health-related) before they materialize. Its impact allows us to initiate the process of mitigating and combating the commission of crimes related to Money Laundering, Terrorist Financing, Financing the Proliferation of Weapons of Mass Destruction (ML/TF/WMD), and other illicit activities, preventing the use of Financial Institutions as vehicles for committing crimes, primarily by transnational criminal organizations. This research is descriptive in nature, with a documentary design. Information was primarily gathered through documentary observation and analytical summarization to produce a critical analysis, supported by the fundamental tool known as warning signs. While a comprehensive regulatory framework exists, along with typologies that group these activities, and while regulatory frameworks differ fundamentally from nation to nation, their development, as well as the implementation of exercises, workshops, and mutual evaluations, are primarily based on the recommendations of the Financial Action Task Force (FATF). These recommendations are grounded in a risk-based approach and implemented in a very formal manner, revealing weaknesses in the frequency of their updates and in the inclusion of crucial macroeconomic variables specific to each country and aligned with its political and administrative reality. This mandatory implementation requires various factors to ensure the instrument's successful application. This dynamic, preventive, and fundamentally systematic instrument strengthens the adoption of measures that guarantee the adequate mitigation of financial crimes by obligated entities.

Descriptors: Warning signs, Risk matrix, AML/CFT/AFD/DMW, FATF, Risk-based approach, Transnational crime. Introducción

INTRODUCCIÓN

La existencia de variados instrumentos, en torno al combate del flagelo de la legitimación de capitales, requiere de un mínimo de conocimientos en la materia de carácter formal, la academia en los últimos años ha desarrollado diseños curriculares que si bien no establecen la eficiencia en el desempeño profesional de estos individuos cursantes de estos diseños curriculares, podríamos inferir que si incide en el discernimiento de las situaciones que establecen la comisión

del acto ilícito, las señales de alerta son la piedra angular de la activación del sistema integral de administración de riesgos en materia de Legitimación de Capitales, financiamiento al terrorismo, financiamiento a la proliferación de armas de destrucción masiva y otros ilícitos, las prenombradas señales establecen fundamentalmente el inicio de las acciones orientadas a la mitigación del fenómeno señalado, pero estas requieren de una formulación adecuada al contexto político administrativo donde estas suceden, razón por la cual se requiere de un estudio constante y dinámico para establecer metodologías y tipologías correctas y continuas

La particularidad político-administrativa de cada país, establecen como pilar fundamental para el afianzamiento de la consecución de las habilidades financieras para el logro de los objetivos financieros. Aparecen nuevas y diversas metodologías de trabajo con el consecuente replanteamiento de la administración y la incorporación de procesos productivos a través de la auto supervisión, autoevaluación, para producir una propuesta de eficiencia financiera, en un entorno de altísima volatilidad, típico de los países en vías de desarrollo.

El Sistema Financiero de nuestro país, al igual que otras naciones en el mundo, está conformado principalmente por Instituciones Financieras, donde se encuentran: los Bancos Centrales, bancos comerciales, cajas de ahorro, compañías de seguros y fondos de pensiones, entre otras, cuyas labores principales son las gestiones del ahorro y el crédito. Estas instituciones tienen como punto de encuentro, los Mercados Financieros: representado por aquellos espacios, o lugares, físicos o virtuales, en los cuales se intercambian activos. Estos Mercados Financieros Incluyen el mercado de capitales (bolsas de valores), mercados de dinero y mercados de divisas: también son componentes, del sistema financiero, los medios para financiar, como lo son, los Instrumentos Financieros, que son los Activos que permiten la financiación, como acciones, bonos, pagarés y derivados.

Todos ellos funcionando bajo los lineamientos de un Marco Regulatorio y de Supervisión, representado por el Marco Legal, y Normativas que determinan su

funcionamiento; la investidura como Autoridades monetarias (Bancos Centrales), que son los organismos reguladores que supervisan la estabilidad y transparencia del sistema (políticas monetarias, emisión de la moneda, entre otras funciones importantes), y en el ambiente de las actividades propias de cada negocio, como por ejemplo: en las instituciones bancarias, supervisadas por la Superintendencia de Las Instituciones del Sector Bancario (SUDEBAN), en las instituciones aseguradoras y de reaseguros, la Superintendencia de La Actividad Aseguradora (SUDEASEG), en los entes del mercado de valores, la Superintendencia Nacional de Valores (SUNAVAL), todas ellas reguladoras de las actividades de sus agremiados.

El Sistema Financiero representa el medio para las inversiones, depósitos de dinero, fluidez de los capitales, financiamientos, inversiones, comercio nacional e internacional, las grandes transacciones de negocios, por lo tanto, es el que mueve las economías mundiales, esta internacionalización hace que todos los componentes del Sistema Financiero sean muy vulnerables, ante la cada vez más compleja e ingeniosa incursión de las redes de delincuencia organizada, quienes continuamente intentan, por todos los medios, ingresar el dinero producto de delitos graves reconocidos (narcotráfico, trata de personas, tráfico de minerales y joyas, pedofilia, robos, corrupción, entre otros), y hacerlos pasar como de origen legal.

Al integrar el cumplimiento normativo (Compliance) con la metodología de gestión de riesgos, la perspectiva cambia de lo financiero puro a lo preventivo y regulatorio. Por lo cual, el buen uso de una herramienta tan importante como lo es la Señal de alerta, esta apoya la labor, pues permitirá un correcto enfoque de la situación, definir aquellos aspectos (riesgos) que pueden afectar la consecución de actividades y objetivos de la institución, dando pie a un diseño apropiado de las decisiones y estrategias de gestión orientadas a administrar el riesgo y la consecuente medida de prevenir, mitigar, o evitar, de manera de cumplir con la Normativa legal vigente, establecida por nuestro país.

No obstante, la señal de alerta debe usarse de una manera dinámica, ello debido a que los cambios de metodologías, y actuaciones de los delincuentes resultan

que probablemente los riesgos varíen, lo cual se traduce en un cambio en la clasificación de los hechos previamente identificados.

Las señales de alerta son indicadores tempranos, comportamientos atípicos o condiciones inusuales que se desvían de la normalidad. Su identificación oportuna permite evaluar riesgos, prevenir accidentes, evitar fraudes y tomar decisiones preventivas antes de que se materialice una crisis o daño mayor.

Estas atienden a diversos propósitos y clasificaciones, cuyo objetivo principal de estos indicios es llamar la atención rápidamente sobre posibles peligros. En diferentes contextos, se manifiestan de distintas maneras. En el entorno corporativo y financiero, estimulan la identificación de una situación fuera de lo común que podrían estar vinculadas al lavado de activos o al financiamiento del terrorismo. Para profundizar en estas tipologías, puedes consultar los ejercicios de tipologías realizados cada Año por la Unidad de Inteligencia Financiera, UNIF organismo especializado en la materia, para la detección de cambios repentinos, aislamiento o actitudes inusuales en Personas naturales o jurídicas permitiendo al Oficial de Cumplimiento administrar el riesgo de manera oportuna y objetiva.

Desde la perspectiva de los sujetos obligados, la situación es completamente distinta de acuerdo a las particularidades de cada sector, siendo el sector financiero el de mayor vulnerabilidad al considerar la existente instrumentalización de la legitimación de capitales, como consecuencia de la posibilidad de recopilar y acceder a fondos a través de los productos ofrecidos al público en general, así como la posibilidad de transferirlos a otras jurisdicciones y su consecuente carácter global. Es muy importante señalar que el riesgo de legitimación de capitales es sumamente dinámico, la falta de asertividad en el diseño de los productos y políticas preventivas puede ser aprovechado por delincuentes que buscan dar apariencia de legitimidad a sus fondos.

A continuación, una recopilación de señales de alerta especializada las cuales, dejan entrever indicios de los delitos precedentes de los que pueden proceder los fondos utilizados, como comúnmente sucede con las estafas o los fraudes

fiscales. Estas señales de alerta permiten a los sujetos obligados someter a escrutinio sus sistemas de prevención, a modo de mejorar su eficacia; y también al momento de estructurar nuevos servicios o colocar nuevos productos al mercado, con el fin de dotarlos de medidas suficientemente robustas y que estén a tono con los esfuerzos de cumplimiento implementados por la entidad.

Es importante destacar que los ejercicios de tipología conllevan en su actualización cierta dosis de creatividad la cual por sí sola no genera valor agregado, es importante la participación en otros procesos cognitivos, para poder convertir dicho proceso creativo en ideas, llevarlas a estrategia y a su vez en acciones concretas, ejecutables y medibles como gestión. Ahora bien, esta Nueva dimensión andragógica y porqué no de autorregulación nos permite el funcionamiento constante de un escenario capaz de mejorar el escudo contra la utilización de la empresa como vehículo de los delitos de LC/FT/FPADM

Señales de alerta en el sector financiero:

Empresas y comerciantes individuales que contratan servicios profesionales de contabilidad para registrar y clasificar información comercial y financiera que es reconocida parcialmente por sus contratantes. Flujos monetarios por actividades comerciales y financieras no reconocidas contablemente que se ingresan a las cuentas bancarias que superan los ingresos reportados en el Estado de Resultados, Declaración del Impuesto sobre la Renta y Declaración del Impuesto al Valor Agregado (IVA). Cantidades dinerarias que ingresan en las cuentas bancarias, que superan las utilidades del ejercicio registradas en el estado de resultados, sin justificación alguna. Reconocimiento de ingresos en el estado de resultados, superiores a los ingresos reales y los declarados ante el fisco.

Disminución de costos y gastos, para aparentar la generación de utilidades y de esa forma aumentar la rentabilidad de un determinado negocio. Cliente es propietario de entidades corporativas domiciliadas en jurisdicciones *off shore* consideradas de alto riesgo, con el aparente propósito de evadir obligaciones fiscales. El marco de supervisión de LC/FT/FPADM es catalogado como débil o inexistente en la jurisdicción desde donde proceden o hacia dónde se dirigen los

fondos. Traslado de fondos entre cuentas en bancos del sistema financiero nacional, para su concentración en una o dos de ellas y su posterior envío por transferencias hacia el extranjero. El Cliente solicita que el pago de rendimientos por productos financieros se realice a una cuenta en jurisdicción poco o no cooperante en la prevención del LC sin un motivo razonable.

Fondos que proceden o se dirigen a una jurisdicción catalogada como de alto riesgo por los altos índices de corrupción o la poca transparencia con la que se manejan fondos públicos. El país al que se dirigen o del que proceden los fondos ha sido catalogado por la Organización para la Cooperación y Desarrollo Económico (OCDE) como un régimen fiscal preferencial nocivo.

Cliente que recibe cuantiosas transferencias de empresas transmisoras de dinero o procesadoras de pagos en línea que no recopilan información suficiente sobre el remitente. Pagos mediante transferencias internacionales que difieren significativamente de los patrones normales para el tipo de negocio. Pagos que se envían o se reciben en elevadas cantidades exactas, en sectores en los que dicha transaccionalidad es inusual. Cliente que ocupa diversos instrumentos financieros para pagar, sin que esto tenga una justificación razonable. Alto volumen de depósitos en efectivo que exceden el perfil transaccional declarado del cliente comerciante, inconsistente con las declaraciones de impuestos, con mayor énfasis en los que realizan importación de vehículos usados o productos perecederos.

Pago en efectivo de préstamos de manera anticipada o abonos en el mismo medio superiores a la cuota establecida, cuando la procedencia de los fondos no es justificada. Recepción de fondos de billeteras digitales procedentes de conversión de criptoactivos en anonimato. Incremento repentino de transacciones y su sistemático cambio a criptoactivos. Cuentas con requisitos simplificados para apertura reflejan repentinamente alta transaccionalidad por depósitos de múltiples cuentas. Cliente realiza transacciones con billeteras digitales asociadas a esquemas de fraude, extorsión entre otros. Existe una constante rotación del titular del producto o servicio sin una explicación razonable. Beneficiario de remesa o depósito se niega a identificarse o presentan

documentos que son de difícil verificación por ser extranjeros. Adquisición y venta de valores sin una explicación coherente con el tipo de inversiones o con esquemas de inversión no razonables.

Abonos a tarjetas de crédito con dinero en efectivo generando un saldo a favor, que posteriormente es utilizado por el cliente. Cliente que inicialmente invierte en productos a largo plazo, pero de forma casi instantánea solicita la cancelación del producto y se dispone al pago de la cláusula penal. Múltiples clientes toman préstamos con la misma u otra institución bancaria para depositar esos montos en cuentas del potencial estafador. Un cliente busca acceder a un crédito o a fondos propios, pero bajo alguna condición a plazo, y al cancelar su cláusula penal expresa que lo hace por una oportunidad de inversión cuyas condiciones de rentabilidad exceden irrazonablemente a las vigentes del mercado. Cuentas bancarias que reciben múltiples depósitos de varias personas, sin una relación aparente, acumulan grandes montos que luego comienzan a ser movidos o convertidos a criptoactivos.

Cuentas de depósitos a la vista aperturadas con antigüedad no superior de tres meses, que reciben depósitos de múltiples depositantes sin relación alguna, y que no son consistentes con los movimientos proyectados en la declaración jurada. Retiros de fondos de forma inmediata a la recepción de los depósitos. Retiros de fondos mediante cajeros automáticos (ATM) internacionales, especialmente en países de Europa, África y Asia (Emiratos Árabes Unidos), utilizando tarjeta de débito, y que no son consistentes con el perfil del cliente. Funcionarios o empleados públicos que llevan un estilo de vida lujoso o tienen bienes y activos que exceden significativamente sus ingresos declarados. Vínculos cercanos entre funcionarios públicos y empresarios que podrían indicar un posible conflicto de intereses o relaciones de favoritismo indebido. Empresa recibe contratos públicos de forma recurrente sin que existan garantías que existió un proceso de licitación real. Transferencias de dinero o recursos de partidas presupuestarias gubernamentales hacia cuentas de empresas en el país o el extranjero sin una justificación clara. Persona Expuesta Políticamente procede de un país identificado como de alto riesgo por sus niveles de corrupción.

Señales de alerta indicativos de uso ilícito de activos virtuales

Ciente que realiza una operación de cambio entre dinero fiat y activos virtuales que implique una pérdida. Transacciones entre cuentas de activos virtuales y tarjetas bancarias vinculadas a fraudes, compra y venta de ilícitos en el mercado negro o extorsión. El Cliente hace un préstamo o cancela un depósito a plazo justificando que invertirá en una Oferta Inicial de Activos Digitales (ICO, por sus siglas en inglés) que le propone una rentabilidad que excede irrazonablemente la oferta promedio. Cuenta de activos virtuales que se fondean a través de múltiples depósitos efectuados por diversas tarjetas bancarias. Empresas recién constituídas generan alta transaccionalidad que sistemáticamente convierten en criptoactivos. Cliente que compra cuantiosas cantidades de activos virtuales que no se corresponden con su perfil transaccional declarado. Cliente recibe dinero fiat que procede de la conversión de activos virtuales que potencian el anonimato.

Desviaciones en el uso de activos virtuales

Comúnmente se hace hincapié en los riesgos que el uso ilícito de los criptoactivos genera con relación al LC/FT/FPADM debido al potencial anonimato de remitentes y destinatarios, rapidez transfronteriza de las transacciones o la dificultad de detección e investigación de la actividad criminal que su uso plantea; a ello se suma el tipo atroz de delitos precedentes al que se han vinculado los fondos cuya legitimación se pretende a través de este medio: trata de personas, pornografía infantil, migración ilegal y compra de objetos ilícitos en la red oscura. Sin embargo, es poco el énfasis que se hace en el hecho que una adecuada comprensión de este entorno y un abordaje congruente de los riesgos puede aportar un alto grado de seguridad a usuarios y proveedores de estos servicios en general.

La obligación de entender los riesgos de LC/FT/FPADM, a los que estamos expuestos, implícita en el mismo Enfoque Basado en Riesgos, impone la necesidad de entender cuáles características de los criptoactivos pueden ser

explotadas para potenciar el anonimato de quienes envían o reciben fondos, o para poner recursos a disposición de terroristas o proliferadores. En ese entendido, las señales de alerta aquí presentadas, buscan brindar algunos insumos para valorar las conductas transaccionales indicativas de LC/FT/FPADM en el uso de activos virtuales; pero su correcta aplicación también dependerá de la constante actualización a la que los sujetos obligados se sometan en la terminología del sector, y las herramientas o mecanismos de búsqueda de las que eche mano para mitigar los riesgos aquí tratados, a continuación señales de alerta en el uso de activos virtuales.

Otras señales de alerta en el uso de activos virtuales.

Alto flujo de fondos provenientes de wallet externas. Alto flujo de fondos provenientes de terceros sin tener relación aparente y a un usuario en común. Incremento repentino en el comportamiento transaccional. Rápido movimiento de flujo de ingresos y egresos. Renuencia del titular de la billetera para documentar transacciones y/o actualizar información. Cuentas que se fondean con múltiples depósitos por medio de tarjetas bancarias. Retiro de fondos a wallet externas. Transaccionalidad con plataformas involucradas con noticias negativas. Realizar cambios de criptoactivos a moneda fiat con una pérdida potencial. Transferir un activo virtual que opera en una blockchain pública y transparente e intercambiarlo inmediatamente a una criptomonedas de anonimato.

Vulnerabilidades que se presentan como desviaciones y señales de alerta para el sector APFND

Las Actividades y Profesiones No Financieras Designadas (APFND) se refiere a aquellas ocupaciones que por la naturaleza de las labores que desempeñan, son especialmente vulnerables para ser instrumentalizadas en la Legitimación de Capitales. Esto debido a los servicios que algunos prestan, que pueden ser asimilados a aquellos de carácter financiero; los productos que ofrecen, que

suelen ser unidades de resguardo de alto valor con características ideales para quienes buscan legitimar capitales de procedencia ilícita; o por el rol que tales profesionales desempeñan en la efectiva aplicación de las obligaciones normativas de prevención del Lavado de Dinero y Activos.

Consecuencia de ello, las APNFD están sujetas a la obligación de implementación de un catálogo de medidas preventivas de LC acordes a la naturaleza de la actividad que desarrollan; y tanto las vulnerabilidades comunes como las señales de alerta aquí presentadas deben ser tomadas en cuenta como insumos para fortalecer sus mecanismos de identificación, abordaje y seguimiento de clientes, proveedores y empleados; ajuste de los controles aplicados por los productos o servicios que ofrecen y desarrollo de capacidades de interpretación de situaciones que puedan indicar que una transacción se pretende realizar con fondos cuyo origen se encuentre en delitos precedentes.

Vulnerabilidades regionales y desviaciones más comunes para el sector de casinos y bingos

Ausencia de controles idóneos para monitorear las operaciones en efectivo por parte de clientes. Segmento en el que los clientes son esporádicos y renuentes a brindar información personal. Falta de capacitación de sujetos obligados y acompañamiento adecuado en sistemas o materia tecnológica. No hay procesos de identificación de clientes para una debida diligencia, pues está generalmente se aplica únicamente a quienes cobran premios. Poca comprensión de la aplicación del EBR a los servicios que presta el casino. No suele haber controles de volumen de apuestas acumuladas de un mismo apostador cuando este juega con montos bajos. No se suele aplicar el EBR en la selección y monitoreo del personal. Solo a ganadores de premios superiores se les exige estar bancarizados.

Señales de alerta para el sector de casinos y bingos

Conversión de fondos que se blanquean de efectivo a cheques, haciendo uso del crédito del casino. El cliente intenta intervenir en juegos de azar a través del

uso de elevadas sumas de efectivo. Cliente solicita que el casino emita un cheque a nombre de terceros o sin un beneficiario específico. El Cliente compra fichas en efectivo en pequeñas cantidades, realiza un juego mínimo y luego solicita un cheque del casino por las fichas presentadas. Cliente juega en máquina de casino que acepte dinero en efectivo, al que ingresa sumas de dinero que luego de un tiempo de juego mínimo, reclama en forma de ticket para ser redimido por cheque o transferencia del casino (bill stuffing).

Apostadores que se comunican discretamente entre sí con la finalidad de hacer juego estructurado. Cliente hace demasiadas preguntas sobre umbrales de reportería. Un jugador plantea apuestas por ambos extremos en aquellos juegos donde se admiten dos posibilidades (ejemplo: rojo/negro).

Vulnerabilidades regionales y desviaciones más comunes para el sector de agentes inmobiliarios.

Dificultad para definir al beneficiario final y necesidad de una mayor conciencia de la importancia de conocerlo. Alto uso de efectivo en algunas operaciones. Compradores y vendedores no concientizados sobre riesgos de LC en transacciones. Sector no ha comprendido a cabalidad la aplicación del EBR en el diseño y aplicación de controles. Ausencia de un supervisor o regulador que brinde pautas concretas. Falta de formación profesional de intermediarios, tramitadores y asesores, con una comprensión deficiente del alcance de los deberes preventivos. Ausencia de herramientas de acceso abierto que coadyuven a realizar una debida diligencia del cliente (DDC) efectiva. Falta de estandarización de normas preventivas de LC/FT/FPADM el sector. Facilidad de ofuscación de clientes o beneficiarios finales detrás de estructuras corporativas complejas.

Pago de un inmueble de alto valor en efectivo, sin justificación del origen de los fondos. Cliente que se encuentra designado en listas de cautela nacionales o internacionales. Compras realizadas para terceros, con el propósito de ocultar la identidad del verdadero comprador. Cliente que es PEP realiza compras de inmuebles que están fuera de lo habitual con su comportamiento transaccional previo a asumir la función pública. Cliente que adquiere distintos bienes

inmuebles sin mostrar interés en los detalles o defectos que estos tengan. Compra de bienes inmuebles realizados en forma sucesiva para transferir a distintas personas, sin un motivo razonable. Adquisición de inmuebles con pagos hechos por terceras personas. Incompatibilidad entre la naturaleza de los inmuebles adquiridos y las actividades declaradas de un cliente o vendedor.

Vulnerabilidades regionales y desviaciones más comunes para comerciantes de metales preciosos y piedras preciosas

Dificultad para detectar operaciones y transacciones sospechosas. Cultura sectorial de evasión de controles fiscales y soborno a autoridades aduanales. Sector no ha comprendido a cabalidad la aplicación del EBR en el diseño y aplicación de controles. Ausencia de un supervisor o regulador que brinde pautas concretas. Alto uso de dinero en efectivo. Producción y exportación ilegal de piedras y metales preciosos desde zonas de alto riesgo de minería ilegal. Poca o nula bancarización de actividades asociadas con extracción y comercialización de metales y piedras preciosas. Falta de pautas para la correcta identificación de clientes, proveedores y beneficiarios finales de artículos adquiridos.

Señales de alerta para el sector de comerciantes de metales y piedras preciosas

Operaciones fraccionadas realizadas a fin de evitar el Reporte de Operaciones Sospechosas. Compra de metales y piedras preciosos con distintos tipos de divisas. Personas que recurren frecuentemente a intermediarios para realizar las operaciones comerciales. Cliente está siendo investigado o procesado por delitos precedentes del Lavado de Dinero y de Activos. El cliente de manera inusual utiliza o pretende utilizar efectivo como único medio de pago. Cliente que realiza frecuentemente operaciones por sumas de dinero que exceden lo generado según sus ingresos y ocupación declarados. Proveedores están ubicados en jurisdicciones con alto riesgo de minería ilegal, y sus canales de transacción suelen eludir los controles propios del sistema financiero.

Vulnerabilidades regionales comunes para abogados, notarios, contadores y auditores

Diversidad de estructuras societarias, comerciales y financieras que pueden ser utilizadas para legitimar capitales. Dificultades para identificar al beneficiario final. Deficiente comprensión del EBR y su aplicación a las actividades concretas. Grupos minoritarios de profesionales que concentran gran parte de la actividad. Alto uso de dinero en efectivo. No se ha incluido de manera explícita o puntual las temáticas de prevención de LC dentro del marco regulatorio de la actividad notarial. Desarrollo defectuoso de los controles de debida diligencia. Normativa relacionada con la prevención de LC es aún de implementación reciente. Sector que presenta pocos RAS y de calidad precaria.

Señales de alerta para el sector de abogados, notarios, contadores y auditores

Cliente renuente a suministrar información. Los movimientos de dinero para operaciones no son acordes al perfil económico declarado por el cliente. Personas jurídicas recientemente creadas con capital mínimo realizan grandes inversiones. Cliente está siendo investigado o procesado por delitos precedentes del Lavado de Dinero y de Activos. Solicitud de pagos a terceros sin justificación de negocios plausible. El cliente de manera inusual utiliza o pretende utilizar efectivo como único medio de pago. Bien ofrecido como garantía de pago de una obligación se encuentra en una jurisdicción de alto riesgo. Operaciones ficticias o con indicaciones de valores incompatibles con los actuales del mercado. Cliente interesado en crear estructuras de propiedad complejas sin un motivo comercial razonable.

Introducción a vulnerabilidades y señales de alerta para el sector de las organizaciones sin fines de lucro (OSFL).

Tal como lo ha reconocido el GAFI, las OSFL han sido objeto de abuso por grupos terroristas e instrumentalizadas para enmascarar sus actividades, particularmente aquellas en regiones de conflicto, debido a que normalmente estas se dedican a la recaudación y desembolso de fondos para cumplir con

propósitos benéficos. esta acepción es aplicable tanto para aquellas osfl de carácter internacional, cuyas operaciones suceden en jurisdicciones con alto riesgo de financiación del terrorismo; así como a nivel nacional, con aquellas que conducen acciones benéficas en lugares o situaciones donde la amenaza de terrorismo es más patente.

Vale aclarar que a pesar del hecho que la financiación del terrorismo es un aspecto esencialmente distinto al lavado de dinero y de activos, existe bastante afinidad en el tipo de medidas a implementar desde su ámbito preventivo. así, la obligación legal de registro y reporte de transacciones con determinadas características; la identificación de clientes, contrapartes y beneficiarios finales; la adopción de un enfoque basado en riesgo o el deber de resguardo de documentación son algunos de los ejemplos de la afinidad de estos fenómenos delictivos desde el campo preventivo.

Vulnerabilidades regionales comunes para OSFL.

Gobernanza de organizaciones carentes de orientación hacia la prevención del FT. Uso no generalizado del sistema financiero formal para recaudación y consecución de actividades. Deficiente aplicación de medidas de debida diligencia para conocer a beneficiarios, donantes, empleados y patronato de organización. Cultura de displicencia hacia la instauración de deberes preventivos de FT. Alto uso de dinero en efectivo. Exclusión financiera como resultado de percepción de mayor riesgo en las actividades de algunas organizaciones, y que pueda desalentar sus actividades. Movimientos de fondos hacia diversos países sin el debido archivo de documentación de respaldo. No todas las organizaciones llevan una adecuada contabilidad, apta para demostrar coherencia entre sus actividades de beneficencia y el destino dado a los fondos recaudados.

Señales de alerta para el sector OSFL.

Recepción de donaciones por parte de personas u organizaciones que están involucradas o apoyan el terrorismo. Transacciones con contrapartes

involucradas o señaladas de financiar terrorismo. Miembros fundadores o apicales tienen vínculos con actividad terrorista. Las actividades de ayuda de OSFL se llevan a cabo en jurisdicciones con elevada actividad terrorista. Labores de asistencia humanitaria se encaminan exclusivamente en el auxilio de grupos terroristas. Donante condiciona aporte de fondos a un destino específico vinculado con personas o grupos terroristas. Beneficiarios renuentes a bancarizarse y, sin un motivo razonable, solicitan donaciones únicamente en efectivo. Empleados de la organización presentan afinidad o simpatía a organizaciones terroristas.

Desviación de señales de alerta generales para el FT.

Es un error considerar que el riesgo de Financiación del Terrorismo es de carácter secundario o exclusivo para Organizaciones Sin Fines de Lucro, ya que los grupos terroristas están constantemente innovando los mecanismos que les permitan disponer de los fondos necesarios para llevar a cabo sus actividades. Si se adopta esa percepción, se corre el riesgo de parcializar el sistema de prevención y menoscabar su efectividad, dejando expuesta a la persona a servir como canal para favorecer a personas o entidades terroristas. Resulta entonces de vital importancia concientizar sobre estos riesgos a los sujetos obligados y su personal, haciéndoles entender cuáles son sus similitudes y diferencias con el Lavado de Dinero y de Activos y cómo puede la organización ser vulnerada para estos fines. Asimismo, las siguientes señales de alerta permiten entender que la prevención de estos riesgos trasciende del mero cotejo con listas de cautela, que, si bien es importante, solamente cubre una parte del riesgo a mitigar; pero es necesario también integrar controles relacionados a la conducta del cliente, tendencias en uso de productos, servicios o en los medios de pago.

Señales de alerta generales para el fFT

Solicitudes de pago se hace a billeteras de activos virtuales o enlaces virtuales de transferencias que se ha identificado están vinculadas a actividad terrorista. Persona envía o recibe fondos de jurisdicciones con alto riesgo de terrorismo por supuestos pagos de materia prima, pero en tales países no existe actividad industrial que genere esa materia. Cuentas que se utilizan para acopio de fondos

y que luego son canalizados hacia algunos beneficiarios en territorios no cooperantes. Existencia de noticias que vinculan a un cliente, proveedor u organización a la que se hacen donaciones con una persona o grupo terrorista. Persona procedente de jurisdicciones de alto riesgo que se niega a dar un motivo razonable de su presencia en el país y de la fuente de la que obtiene los fondos de su subsistencia. Empleados de la organización muestran simpatía con causas relacionadas al terrorismo y por su función en la entidad pueden disponer del destino de fondos o bienes.

Señales de alerta generales para el FPADM.

La proliferación no estatal de armas de destrucción masiva ha sido reconocida como una amenaza para la paz y seguridad internacional por la Organización de las Naciones Unidas. Por ese motivo, el 28 de octubre de 2004, el Consejo de Seguridad de la ONU aprobó la Resolución 1540, cuyo cometido primordial es que los Estados parte se abstengan de apoyar a actores no estatales en el desarrollo, adquisición, fabricación, posesión, transporte, transferencia o uso de armas nucleares, químicas o biológicas y sus vectores; que adopten y hagan cumplir normativa tendiente a dicha finalidad y que se implementen controles internos aptos para prevención de la proliferación de estas armas.

La Recomendación 7 del GAFI recoge la resolución en comento y las resoluciones sucesoras futuras, a través de las que se demanda la aplicación de medidas y sanciones financieras dirigidas para asegurarse que ningún fondo o activo se ponga a disposición de los proliferadores o la proliferación de este tipo de armas. Reconociendo que, si bien es un ámbito bastante específico en el que se puede dar la FPADM, el esfuerzo por evitarlo sí es de incumbencia general y atañe a todos aquellos sujetos que puedan ser instrumentalizados para su consecución.

Señales de alerta generales para el FPADM.

El pedido de bienes es realizado por empresas o personas de países extranjeros que no sean el país del usuario final indicado. Una empresa de transporte

aparece como destino final del producto. La transacción involucra posibles compañías pantalla. La transacción implica el envío de mercancías incompatibles con el nivel técnico del país al que se envía. Uso de dinero en efectivo para la compra de bienes industriales. La descripción de los bienes en la documentación comercial o financiera es poco específica o engañosa. La transacción de financiamiento comercial involucra una ruta de envío a través de un país con leyes débiles de control de exportaciones. La transacción involucra a personas o compañías ubicadas en países con leyes débiles de control de exportaciones o aplicación débil de esas leyes. La transacción involucra a una persona o entidad en un país extranjero de interés de desviación.

Aun cuando en las distintas leyes, normas, providencias los lineamientos operativos están estandarizados, se sugiere aplicar variables adicionales de riesgos en caso de ser necesario, relacionadas con las particularidades de cada sociedad, que le permitan fortalecer las estrategias de prevención de LC/FT/FPADM. En La República Bolivariana de Venezuela encontramos un mercado financiero relativamente pequeño, y muy subdesarrollado, con una gran carencia de adecuaciones tecnológicas, pero la dinamización del aparato económico es evidente.

El futuro de los ejercicios de tipologías y las señales de alerta.

El reto del estudio de tipologías se encuentra en el estudio del incremento de empresas emergentes se caracterizan por su tamaño, son pequeñas y de reciente creación, con alto potencial innovador y tecnológico, de modelo escalable, de posibilidades de expansión acelerada, es decir de crecimiento exponencial y por ende de rápido aumento de su valor, estas son poseedoras de varios elementos que explican su naturaleza definida por Carla Hernández Cuellar:

1) La empresa emergente como organización tiene un carácter limitado. Es decir, hace alusión a la emergencia de una compañía que finaliza con su conversión en negocio estable. En otros casos, el final es precisamente lo opuesto. Es decir, desaparecen (no son pocas el startup que fracasan).

2) **Carácter novedoso:** La innovación es la esencia de todo startup. A menudo referida a su fuerte vinculación con las nuevas tecnologías y el mundo internet. Una novedad que supone siempre una ventaja competitiva frente a otras compañías. Y que, además, también puede aplicarse al carácter diferencial de su negocio o de los procesos productivos que emplea.

3) **Costes reducidos:** Su asociación con las TIC (Tecnologías de la Información y la Comunicación) hace de estas jóvenes empresas un negocio muy atractivo. En sus etapas iniciales no exige grandes cantidades de dinero para su puesta en marcha. A diferencia, claro está, de las compañías que operan en otros ámbitos.

4) **Financiación externa:** Aunque los costes de arranque son mínimos, a medio plazo las ganancias del startup son considerables. A consecuencia de este crecimiento acelerado muchos inversores externos se sienten atraídos. A estos inversores se les conoce como Inversores Ángel (Business Angel). Aportan una pequeña financiación a cambio de acciones o participaciones en la empresa.

5) **Objetivo y riesgos:** El startup asume un fuerte riesgo ya que su objetivo es dominar un nicho de mercado (a menudo poco explorado) en el que trabajan a base de hipótesis. Este ámbito de incertidumbre requiere una gran capacidad de adaptación a los cambios. La meta, por tanto, consiste en hacer que esas hipótesis funcionen, que los productos o servicios ofertados sean aceptados por sus clientes, manteniendo unas ganancias elevadas que le permitan retornar la inversión (garantizando la escalabilidad del negocio).

Muchas de estas compañías emergentes desaparecen al poco tiempo de vida o son vendidas antes de encontrar un modelo de negocio estable. Sin embargo, existen notables ejemplos de compañías que han prosperado, convirtiéndose en negocios de referencia (sería el caso de Google, Facebook, etc.) Aunque la cuestión está sujeta a fuertes controversias, para muchos la transición de una empresa emergente hacia un modelo de negocio repetible y escalable significa el fin del startup en sí misma, que pasa a convertirse en la empresa clásica tal y como la conocemos.

Esta dinámica de la mutación como elemento incorporado a la realidad de los negocios tiene como catalizador el uso intensivo de las tecnologías de la información y la comunicación (TIC's), con un modelo de negocio escalable que nos proporciona un crecimiento rápido y sostenido en el tiempo. El reto en el futuro radica en establecer la dinámica de cambios en los ejercicios de tipología del delito ralentizados al incorporar el análisis de la participación de las *starups* y las TICs, lo cual complica la descripción del hecho delictivo.

Para finalizar hay que señalar responsablemente que todo proceso de cambio y ajuste requerirá de la sensibilización necesaria y de un flujo de información apropiado que señale las virtudes y ventajas del cambio en ciernes, para efectuar los ajustes, acciones o actividades necesarias para preservar la interpretación de la tipología de manera adecuada y eficiente, y así a la compleja dinámica del desafío, la realidad de cada empresa es tan particular que el modelo esperado de Señal de alerta difícilmente coincida con la realidad de emprendimientos de un mismo sector cada quien se adapta de acuerdo a la realidad de su sector.

CONCLUSIONES

Con respecto a Situación actual de la aplicación y uso de la Señal de alerta en los análisis y evaluaciones de los riesgos asociados con la LC/FT/FPADM y otros ilícitos se puede concluir que:

La aplicación de la señal de alerta en los entes bajo la supervisión de los diversos órganos de control presenta un nivel de implementación formal, sustentado en el cumplimiento de la normativa vigente. No obstante, se evidencian debilidades relacionadas con la actualización periódica, y la consideración o inclusión de nuevas variables de riesgos asociados con el sujeto obligado, lo cual refuerza la integración efectiva del enfoque basado en riesgos en los procesos internos, la correcta valoración del impacto, y la frecuencia de los eventos de riesgo asociados a la LC/FT/FPADM, impulsando y orientando efectivas estrategias de prevención.

En cuanto a los elementos teóricos, normativos y prácticos, tanto nacionales como internacionales, vinculados con el uso de las señales de alerta para establecer su incidencia en los riesgos relacionados con LC/FT/FPADM, se puede concluir que:

Existen sólidos fundamentos teóricos y normativos que respaldan el uso de la señal de alerta como instrumento esencial dentro del enfoque basado en riesgos. A nivel internacional, las recomendaciones y estándares promueven la identificación, evaluación y comprensión de los riesgos de LC/FT/FPADM, mientras que, a nivel nacional, el marco legal venezolano y los lineamientos regulatorios establecen la obligatoriedad de implementar la señal de alerta como gatillo de los procesos desarrollados por el Oficial de Cumplimiento y su sistemas de Administración integral de Riesgo. Estos elementos permiten afirmar que la señal de alerta no solo constituye una exigencia normativa, sino una herramienta técnica que fortalece la toma de decisiones y el cumplimiento regulatorio.

Los sujetos obligados, deben fortalecer la aplicación de la Señal de alerta, asegurando la actualización de su autoevaluación de riesgo periódica (anual), incluyendo variables macroeconómicas acordes y representativas de la realidad de la situación país, y la importancia que ello representa para su integración efectiva en los procesos de toma de decisiones.

Dados los cambios geopolíticos, y dinámica de productos financieros mundiales, es importante que se actualice periódicamente la capacitación del personal responsable, incluido el responsable de la administración de riesgos, también conocido como Oficial de Cumplimiento, de la gestión de riesgos en materia de LC/FT/FPADM, con el fin de fomentar el dinamismo conveniente y pertinente en el área de cada uno de los sujetos obligados del sector financiero, promueva una correcta identificación oportuna, valoración, y mitigación de los riesgos.

REFERENCIAS

ARIAS, F. (2012). El proyecto de investigación: Introducción a la metodología científica. (6ª. Ed.). Caracas, Venezuela: Episteme.

CONSTITUCIÓN DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA. (1999). Gaceta Oficial de la República Bolivariana de Venezuela, 5.908 (Extraordinaria), 19 de febrero de 2009.

GARCIA (2021), Eficacia de los controles LC/FT en el sector valores venezolano, para optar al grado de Especialista en Mercado de Valores, en la Universidad Católica Andrés Bello (UCAB).

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL. (s.f.). Recomendaciones del [GAFI.fatf-gafi.org](https://www.gafi.org/).

HURTADO DE B., J. (2010). El proyecto de investigación. (6ª. Ed.). Caracas, Venezuela: SYPAL.

COMITÉ INTERAMERICANO CONTRA EL TERRORISMO, ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. “Guía práctica de prevención, detección y represión del financiamiento del terrorismo”. CICTE-OEA, 2007.

GAFI. “Estándares internacionales sobre la lucha contra el Lavado de Activos, el Financiamiento del Terrorismo, y el Financiamiento de la Proliferación de Armas de Destrucción Masiva”. París, Francia. Año 2023.

GAFILAT. “Mejores prácticas. Lucha contra el abuso de organizaciones sin fines de lucro (recomendación 8). París.

GAFILAT. “Guía dirigida al sector de APNFD, para la construcción de una matriz de riesgos en prevención del lavado de activos y financiamiento al terrorismo (LA/FT)”. GAFILAT. Buenos Aires. 2022.

GARCÍA (2021), realizó un estudio titulado Eficacia de los controles LC/FT en el sector valores venezolano, para optar al grado de Especialista en Mercado de Valores, en la Universidad Católica Andrés Bello (UCAB).

INFORME DE EVALUACIÓN SECTORIAL DE RIESGOS (ESR) del Mercado de Valores 2024- 2025. Publicada en agosto de 2025. <https://globalseguridadintegral.es/blog/como-detectar-senales-de-alerta-en-situaciones-de-riesgo/>