RNPS: 2496

ANTILAVADO DE ACTIVOS

Boletín mensual / No. 108
31 de julio de 2025 / Año VII

Elaborado por:
Inteligencia Financiera de Cuba, BCC

sumario

PALABRAS A LOS LECTORES.....2

ANÁLISIS TEMÁTICO.....5

Algunas orientaciones metodológicas sobre los Reportes de Operaciones Sospechosas para los Sujetos Obligados. 5

EXPERIENCIAS DE TRABAJO ANTILAVADO DE ACTIVOS Y CONTRA EL FINANCIAMIENTO AL TERRORISMO.....8

Se realiza en El Salvador el 51 Pleno de Representantes del Grupo de Acción Financiera de Latinoamérica 8

SECCIÓN INFORMATIVA SOBRE LA PREVENCIÓN Y EL ENFRENTAMIENTO AL LAVADO DE ACTIVOS.....9

Los delincuentes se han vuelto más expertos en tecnología: ¿cómo pueden los bancos detenerlos?.....9

EVENTO.....12

Plenario de Egmont 2025, Luxemburgo – Declaración de los copresidentes.....12

Cuba participa en Luxemburgo en foro sobre Inteligencia Financiera 16

NOTICIAS.....17

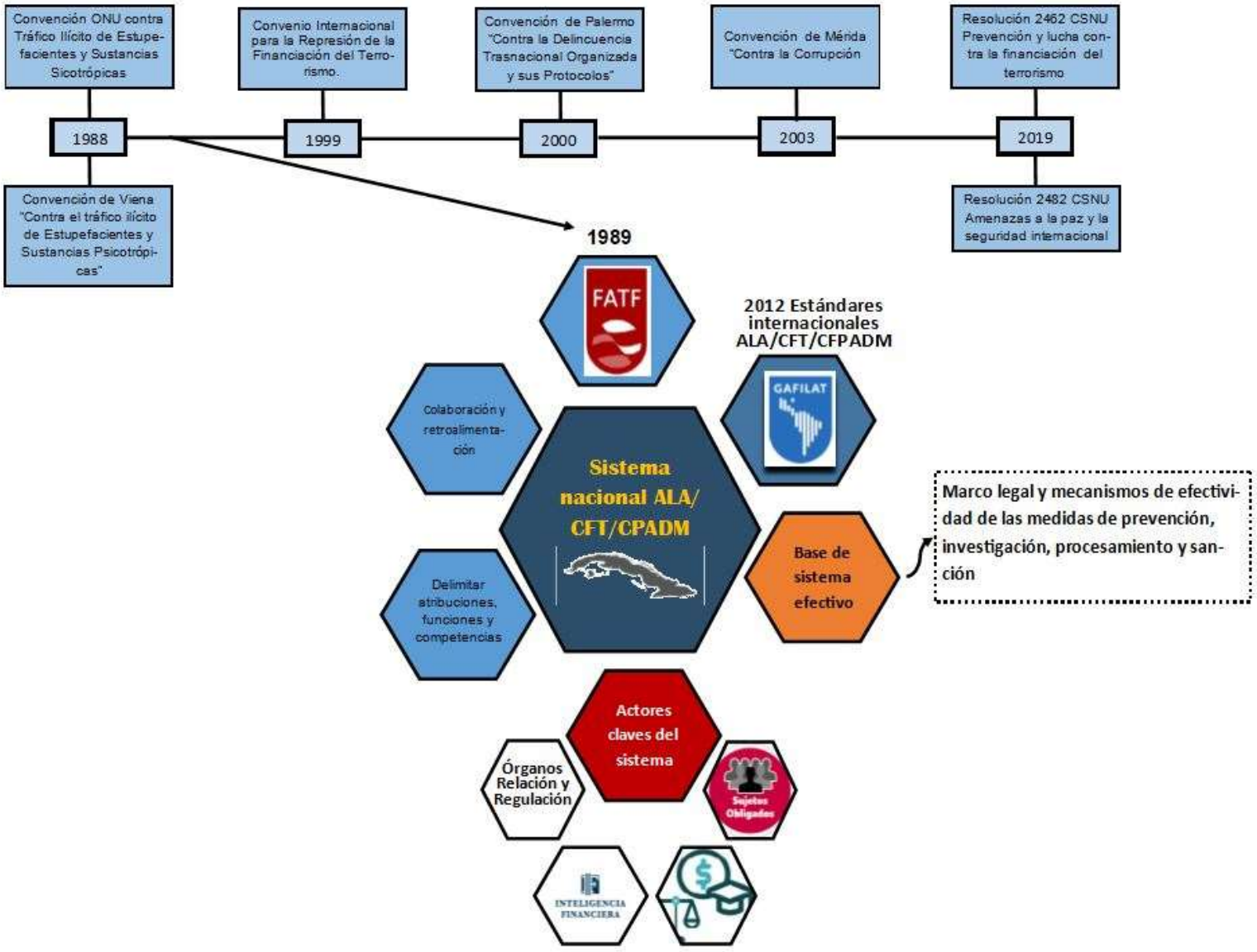
Caso Eclipse: Red familiar de alto exfuncionario de la UAFE fue sentenciada por lavado de activos.....17

La amenaza silenciosa del lavado de activos. 18

ESTIMADOS LECTORES:

Enfocados en reforzar aspectos esenciales de la prevención y el enfrentamiento lavado de activos, el financiamiento al terrorismo y a la proliferación de armas de destrucción masiva, exponemos en esta sección infografías intencionadas que resumen en imágenes explícitas la linea del tiempo, en el espacio global y en la dinámica social, que determinan nuestro sistema de mitigación de estos flagelos. Esta acción se corresponde con el propósito de contribuir a la mayor comprensión del asunto, enmarcada en la preparación de Cuba para la Evaluación Mutua de la Quinta Ronda de GAFI que inicia en el segundo semestre de 2025.

Fundamentos sobre el Sistema nacional ALA/CFT/CFPADM.



Comité Coordinador para la prevención y enfrentamiento. Órgano consultivo Ad Hoc del Sistema nacional ALA/CFT/CFPADM

Línea de tiempo que grafica los pasos a seguir en la Evaluación Mutua de Cuba

ANÁLISIS TEMÁTICO

Algunas orientaciones metodológicas sobre los Reportes de Operaciones Sospechosas para los Sujetos Obligados.

En la emisión anterior incorporamos un artículo referente a algunas señales de alerta de lavado de activos en diferentes áreas, con ejemplos reales para ayudarle a reforzar su vigilancia antilavado. Las señales por sí solas no suelen ser un indicador definitivo de la comisión de lavado de activos, pero indican algo mucho mayor y combinadas permiten desencadenar el sistema de prevención y enfrentamiento del país a estos flagelos a partir del envío a las Unidades de Inteligencia Financiera (UIF) de los Reportes de Operaciones Sospechosas.

Los Sujetos Obligados del Sistema Nacional Antilavado de Activos tienen la responsabilidad de identificar y reportar operaciones inusuales o sospechosas a la Unidad de Inteligencia Financiera a partir de la detección y recopilación de información referente a una operación sospechosa, que no es más que cualquier transacción, acto u omisión que, por sus características, monto, frecuencia o naturaleza, no tenga una justificación económica o lógica aparente, o que pueda estar relacionada con el financiamiento del terrorismo, lavado de activos, o delitos precedentes de este.

Entre los ejemplos de situaciones sospechosas más frecuentes solemos encontrar operaciones con fondos de origen desconocido o sin justificación económica, movimientos inusuales en cuentas (depósitos/retiros fuera del perfil del cliente), uso de estructuras complejas para ocultar beneficiarios reales, clientes que evaden identificarse o proveen información falsa y transacciones fragmentadas para evitar límites de reporte, entre otras.

Los Sujetos Obligados deben realizar monitoreo continuo de sus clientes y la operatoria de sus cuentas para identificar operaciones sospechosas, luego analizar si la operación carece de explicación razonable, para lo cual deben hacer la recopilación y análisis primario de la información complementaria y reportar a la UIF en un breve plazo desde la detección del evento inusual o sospechoso.

Para garantizar la calidad de los reportes y que ganen en efectividad, es imprescindible mantener al personal de cumplimiento capacitado en la detección de señales de alerta, mantener registros del análisis y las decisiones tomadas en ese nivel, mantener actualizadas las políticas internas conforme a las normativas operantes, así como una adecuada retroalimentación y guía metodológica de la UIF para conocer las tendencias delictivas detectadas en el enfrentamiento que luego se podrán traducir en señales de alerta.

Con este objetivo presente, la redacción de un Reporte de Operación Sospechosa para la Unidad de Inteligencia Financiera debe ser clara, concisa y basada en hechos objetivos que recreen el contexto en el cual se identifican las señales de alerta.

A pesar de las diferencias entre países en las normativas al respecto, existe una estructura recomendada para los reportes de estas operaciones que incluyen los datos del o Sujeto Obligado, datos del cliente o persona involucrada, descripción en detalle de la Operación Sospechosa (fecha y lugar donde ocurrió la operación, monnto exacto, tipo de operación, producto o servicio involucrado, motivo de sospecha como incongruencias en la información, intento de evadir límites, operaciones inusuales para el perfil del cliente), hechos que generan sospecha, medidas tomadas y anexos como copia de documentos, imágenes de transacciones, comunicaciones relevantes, etc.

Tenemos a bien incorporar en el artículo algunas recomendaciones claves a tener en cuenta para la correcta redacción del Reporte de Operaciones Sospechosas y elevar su calidad y aprovechamiento por parte de las Unidades de Inteligencia financieras.

En la descripción de la operación o hechos que generan sospechas evita utilizar opiniones subjetivas, en cambio usa frases como “se observa que…”, “el cliente declaró que…”. Sé específico, incluye fechas, montos exactos y detalles técnicos. No obviemos la relevancia de la confidencialidad, no se debe notifiquer al cliente sobre el reporte. Respeta los plazos de entrega establecidos y el formato establecido oficialmente.

Pongamos un breve ejemplo de narrativa: “El 15/10/2023, el cliente Juan Pérez Martínez depositó $9,800 USD en efectivo en sucursal, alegando que corresponden a la venta de un vehículo. Sin embargo, no presentó comprobante de la transacción y su perfil laboral (empleado con salario mensual de $10,000 CUP) no coincide con el monto declarado. Adicionalmente, el cliente intentó realizar otro depósito por $9,500 USD al día siguiente.”

Los operadores jurídicos (abogados, notarios, consultores jurídicos, etc.) tienen un papel crucial en la prevención del lavado de activos y el financiamiento del terrorismo. Al redactar un Reporte de Operación Sospechosa, sería conveniente enfocarse en algunos aspectos claves extras a los mencionados con anterioridad.

Además de la identificación de señales de alerta propias de la actividad, estos operadores jurídicos deben estar atentos a situaciones tales como clientes que evaden información, datos incompletos, contradicciones en su identidad u origen de los fondos. También a las operaciones inusuales, transacciones sin justificación económica o legal como la compraventa de bienes con sobreprecio o subprecio, por ejemplo. Estructuras complejas que reflejan el uso de sociedades opacas, fiduciarias o paraísos fiscales sin razón aparente. Modificaciones sospechosas de contratos que contemplan cambios repentinos en poderes, testamentos o escrituras que beneficien a terceros no vinculados. Por último, prestar atención a señales de presión para eludir controles, clientes que insisten en acelerar trámites sin cumplir requisitos legales.

Veamos un ejemplo de enfoque práctico para estos operadores del Derecho: Un notario recibe una solicitud para formalizar la venta de un inmueble valuado en $1 millón, pero el comprador desea pagar $200,000 en efectivo y el resto mediante transferencias de cuentas en el extranjero sin explicación clara. El Reporte debería detallar como mínimo

la inconsistencia en el valor de mercado contra el precio pactado, la falta de justificación para el uso de efectivo y la procedencia no declarada de los fondos internacionales.

Desde el punto de vista contable, los Sujetos Obligados que realizan esta profesión en general, deben reportar atendiendo al nivel de riesgo principalmente sobre las empresas con actividades de alto riesgo, las operaciones inusuales o sospechosas como movimientos sin justificación económica, transacciones fragmentadas para evadir umbrales, operaciones en efectivo superiores al límite legal, inconsistencias en registros contables, facturas falsas, sobrevaloración de activos, omisiones, operaciones de clientes de alto riesgo como las Personas Expuestas Públicamente o negocios sin sustento económico claro.

Los reportes suelen incluir los datos del cliente (nombre, identificación, actividad económica), detalles de la operación (monto, fecha, método de pago), indicios de riesgo (por qué es sospechosa) y el soporte documental (facturas, contratos, libros contables) que sustentan la operación.

Para todos los sujetos obligados podemos incorporar buenas prácticas adicionales que agregan valor a la cadena de prevención y enfrentamiento al lavado de activos y financiamiento al terrorismo. El enfoque debe ser preventivo y proactivo, priorizando el análisis de riesgo sobre las operaciones atípicas. La calidad del reporte es vital para que las Unidades de Inteligencia Financiera puedan investigar eficazmente.

-Documentación interna: Mantener registros de las investigaciones realizadas antes del reporte.

-Capacitación continua: Actualizarse en indicadores de riesgo y nuevas modalidades delictivas.

-Colaboración con autoridades: Proporcionar información adicional si es requerida.

En el caso cubano, el Decreto-Ley No. 317, de fecha 7 de diciembre de 2013, estipula al Banco Central de Cuba como autoridad rectora para establecer las directrices que resulten necesarias con el objetivo de prevenir el uso del Sistema Bancario y Financiero cubano para la legitimación de activos provenientes de actividades ilícitas, incluido el lavado de activos, el financiamiento al terrorismo, a la proliferación de armas y otras relacionadas de similar gravedad.

Entre otros aspectos ampara la obligación de los Sujetos Obligados a reportar operaciones sospechosas a la Dirección General de Investigación de Operaciones Financieras (DGIOF) en término y formato específicos. Con estos fines, la DGIOF en calidad de Unidad de Inteligencia Financiera recibe, centraliza y analiza los Reportes de Operaciones Sospechosas, solicita información adicional, así como disemina Informes de Inteligencia Financiera a las autoridades competentes por vías protegidas, cuando los mismos involucren activos sobre cuya procedencia existan sospechas de ilicitud.

Para ello, la DGIOF implementa la Plataforma segura de Captación Automatizada del Reporte de Operación Sospechosa (CAROS), diseñada para la captación web de los reportes provenientes de los Sujetos Obligados, de manera estandarizada, e introducirlos digitalmente y de modo seguro al proceso de análisis.

La información complementaria del reporte se recibe cifrada a través de la herramienta ARCANO, debiendo especificar en el nombre del fichero adjunto, el número del reporte y el sujeto obligado que lo envía.

Se recomienda consultar el instructivo para el uso del Sistema Informático CAROS para facilitarles el correcto registro de los datos en el formulario de reportes, en concordancia con las normas establecidas conocidas por las diferentes instituciones. Podrá encontrarlo publicado junto al presente número de este boletín en el sitio web del Banco Central de Cuba en la sección publicaciones-boletines-Antilavado de Activos (https://www.bc.gob.cu).

Fuente: *Dirección General de Investigación de Operaciones Financieras*

EXPERIENCIAS DE TRABAJO ANTILAVADO DE ACTIVOS Y CONTRA EL FINANCIAMIENTO AL TERRORISMO

Se realiza en El Salvador el 51 Pleno de Representantes del Grupo de Acción Financiera de Latinoamérica.

Se desarrolla en El Salvador, durante esta semana del 28 al 31 de julio de 2025, las reuniones de los grupos de trabajo y el LI Pleno de Representantes del Grupo de Acción Financiera de Latinoamérica (GAFILAT) con la presencia de sus 18 países miembros de América del Sur, Centroamérica y América del Norte y observadores del organismo comprometidos con el fortalecimiento de los sistemas antilavado de activos y contra el financiamiento del terrorismo.

Los progresos en la implementación de políticas de prevención de lavado de activos, financiamiento del terrorismo y proliferación de armas de destrucción masiva, será uno de los temas priorizados en este encuentro, así como el inicio de la 5ta. ronda de evaluaciones mutuas, lo que representa una gran expectativa para todos los países porque todos van a ser evaluados bajo una nueva metodología.

Durante esta reunión se abordarán, también, en cinco grupos de trabajo (grupo de trabajo de evaluaciones mutuas, grupo de análisis operativo, grupo de financiamiento de terrorismo, grupo de cooperación y desarrollo y grupo de análisis de riesgo) diversas directrices que son muy importantes para la región, entre las cuales resaltan:

- Riesgos emergentes relacionados con el lavado de dinero y el financiamiento del terrorismo.
- Esfuerzos que se están realizando para prevenir y reprimir este tipo de delitos.

- Herramientas de formación y difusión de políticas de prevención.
- Nuevos sistemas de Capacitación en estos temas.

Es importante destacar que El Salvador acoge por primera vez la sede del encuentro aportando lo necesario para que a nivel latinoamericano se cumplan con los estándares que dicta GAFILAT.

La delegación cubana que participa está compuesta por la Coordinadora Nacional de Cuba ante GAFILAT, Irma M. Martínez Castrillón, el Director General de Investigación de Operaciones Financieras (DGIOF) del Banco Central de Cuba, Fernando Luís Camejo de la Rosa, la Intendente del Banco Central de Cuba, Idania Torre Toledo, la directiva del Ministerio de Relaciones Exteriores, Yilian Gómez Sardiñas, el Coronel del Ministerio del Interior, Marcos Rodríguez y la Fiscal Martha Gómez del Sol, invitada a participar en el Taller sobre Investigaciones Financiera Paralelas, entre otros.

En el próximo Boletín ampliaremos otras informaciones sobre este Pleno.

Fuente: *Dirección General de Investigación de Operaciones Financieras*

SECCIÓN INFORMATIVA SOBRE LA PREVENCIÓN Y EL ENFRENTAMIENTO AL LAVADO DE ACTIVOS

Los delincuentes se han vuelto más expertos en tecnología: ¿cómo pueden los bancos detenerlos?

Joe Biddle, director de mercado del Reino Unido, comparte sus experiencias sobre cómo las empresas pueden protegerse mejor a sí mismas y a sus clientes contra las amenazas de delitos financieros.

El crimen organizado plantea un desafío importante para las instituciones financieras en el Reino Unido (y en todo el mundo), ya que puede ganar influencia rápidamente y amenazar la integridad del sistema financiero.

Los delincuentes pueden acceder fácilmente a mecanismos de delitos financieros, como datos comprometidos encontrados en la red oscura o herramientas de inteligencia artificial y falsificaciones profundas utilizadas para engañar y hacerse pasar por víctimas.

Entonces, **¿qué pueden hacer los bancos y otras instituciones financieras para minimizar los riesgos del crimen organizado?**

En este artículo, Joe Biddle, Director de Mercado del Reino Unido, comparte su experiencia sobre cómo las empresas pueden protegerse mejor a sí mismas y a sus clientes. Ha trabajado en todas las agencias de crédito del Reino Unido, centrándose en los mercados financieros regulados.

1. Aprovechar el conocimiento humano con soluciones tecnológicas emergentes:

Ahora es sabido que las instituciones financieras necesitan tecnología avanzada más que nunca para combatir eficazmente los delitos financieros. Los delincuentes ya están al día con las últimas tecnologías, en concreto, la IA generativa y los deepfakes. Sin embargo, a menudo existe una brecha entre la teoría y la práctica, ya que los bancos se quedan atrás en la adopción de las innovaciones tecnológicas más recientes.

Por ejemplo, en el Reino Unido, sólo 1 de cada 5 empresas de servicios financieros comprueban sistemáticamente si los nuevos clientes están sujetos a sanciones o son Personas Políticamente Expuestas (PEP).

Esta situación puede dejar a las personas más vulnerables a los grupos del crimen organizado sancionados por las autoridades nacionales e internacionales, así como a las personas políticamente expuestas (PEP) de alto riesgo a quienes las organizaciones criminales pueden presionar.

El crimen organizado suele centrarse en objetivos específicos, a menudo individuos con un alto patrimonio neto u organizaciones con dificultades financieras que pueden ser más susceptibles a la cooptación o el chantaje. La solución es sencilla: implementar herramientas para automatizar este proceso de selección y garantizar que se realice periódicamente.

La lucha contra el crimen organizado en el ámbito financiero requiere un enfoque multifacético que también aproveche otras tecnologías avanzadas. Estas incluyen el big data y el análisis predictivo, el cifrado de datos, el análisis de redes, la geolocalización y el geofencing, la autenticación biométrica, la autenticación multifactor y el software de reconocimiento de voz, afirma Joe Biddle.

2. Llevar a cabo una diligencia debida reforzada contra posibles actores maliciosos:

Cuando surgen sospechas sobre un actor potencial, las instituciones financieras deben realizar más investigaciones de conocimiento del cliente (KYC) para detectar una posible actividad delictiva.

Sin embargo, este paso a menudo falta en el KYC de las organizaciones, ya que el proceso se trata como "uno solo y listo" y no logra conectar diferentes fuentes de datos y comportamientos para comprender los niveles de riesgo de los clientes.

Una visión holística del cliente requiere integrar nuevas fuentes de información para detectar a los actores maliciosos. Las instituciones financieras deben contar con expertos en la lucha contra delitos financieros que puedan obtener la información correcta,

analizarla exhaustivamente y contrastarla con otras fuentes de datos para determinar la actividad sospechosa de los clientes, y utilizar la IA para facilitar el análisis de patrones.

Las sofisticadas estafas románticas en línea, conocidas como redes de "matanza de cerdos", muestran lo que sucede cuando los bancos y otras instituciones financieras carecen de información. Incluso cuando se gestionan principalmente desde otro país, estas redes suelen utilizar el Reino Unido como base, en parte debido al laxo proceso de registro de empresas del país. Las autoridades británicas suelen tener conocimiento del uso ilícito de propiedades específicas para dirigir estas empresas delictivas, pero no se toman las medidas necesarias para responder.

Las instituciones pueden protegerse, por ejemplo, obteniendo datos empresariales que ayuden a identificar si una empresa es una sociedad fantasma. Otro elemento de diligencia debida reforzada entra en juego cuando una empresa o un particular puede ser víctima de chantaje. Las instituciones financieras pueden determinar si los clientes atraviesan dificultades financieras y, por ejemplo, si depositan mucho más dinero del que estiman que ganan.

3. Mejorar la colaboración en la industria:

La falta de cooperación entre las instituciones financieras es un enorme obstáculo para la lucha contra el crimen organizado.

Lo ideal sería que las instituciones financieras se reunieran para compartir mejores prácticas, permitir canales seguros de denuncia o compartir información que las instituciones individuales no pueden reunir por sí solas.

Esto podría incluir información que pueda ayudar a detectar patrones de modus operandi por parte de grupos organizados o cruzar datos con bases de datos y listas negras para descubrir actores criminales conocidos.

Aunque a menudo se considera que compartir información es imposible de realizar debido a las estrictas leyes de protección de datos y de secreto bancario, en realidad es factible: un gran ejemplo es la industria de seguros del Reino Unido.

En los últimos años, el sector asegurador del Reino Unido se ha vuelto mucho más colaborativo en lo que respecta al intercambio de datos y la prevención del fraude. Si una empresa incluye a un estafador conocido en el Registro de Fraude en Seguros (IFR) del sector, el 80 % del mercado asegurador lo incluye automáticamente en la lista negra.

Los bancos e instituciones pueden empezar por organizar sus propios datos. A menudo, la información interna se almacena en varios sistemas heredados desconectados. Migrar a un proveedor de plataforma bancaria integral e iniciar una transición de datos puede permitir a los bancos analizar mejor sus datos internamente y en colaboración con otras instituciones.

En conclusión: Ya sea crimen organizado, estafas románticas o estafadores individuales, contamos con una impresionante variedad de recursos para contrarrestarlos. Pero debemos ser conscientes de la urgencia y ponerlos en práctica.

Fuente: *https://www.trapets.com/resources/blog/criminals-have-become-more-tech-savvy-how-can-banks-stop-them.*

EVENTO

Plenario de Egmont 2025, Luxemburgo – Declaración de los copresidentes.

Del 27 al 30 Luxemburgo – Con motivo del 30.º aniversario del Grupo Egmont de Unidades de Inteligencia Financiera, la sesión plenaria anual del Grupo Egmont se celebró del 6 al 11 de julio de 2025. Este evento histórico contó con la asistencia de alrededor de seiscientos delegados de las UIF miembros del Grupo Egmont, socios internacionales y observadores de todo el mundo, quienes participaron y contribuyeron a las reuniones y a la sesión plenaria en Luxemburgo, organizada por la Cellule de Renseignement Financier (CRF).

El Grupo Egmont tuvo el honor de contar con la presencia de líderes internacionales en este evento histórico como oradores: Elisa de Anda Madrazo, Presidenta del GAFI; Bruna Szego, presidenta de AMLA; Juan Manuel Vega Serrano, Vicepresidente de AMLA; Laura Codruta Kovesi, fiscal jefe europea y jefa de la Fiscalía Europea; Brigitte Strobel-Shaw, en representación de la ONUDD.

El Grupo Egmont también se complace en presentar que ahora cuenta con 181 miembros tras la aceptación de las UIF de Mozambique, Gambia, Guinea Ecuatorial y Sierra Leona como miembros de la organización. El GE continúa fortaleciendo su membresía a través de esfuerzos de alcance en regiones geográficas de enfoque estratégico, incluyendo África, Asia y el Pacífico, y el Medio Oriente y África del Norte.

Durante el evento, las UIF miembros firmaron 47 Memorandos de Entendimiento, fortaleciendo las oportunidades para el intercambio de inteligencia financiera en asuntos de LA/FT. Además, se firmó una Carta de Acuerdo entre el Grupo Egmont y el Servicio de Monitoreo Financiero de la República de Azerbaiyán, formalizando su colaboración bajo el Programa de Certificación del Centro Egmont de Excelencia y Liderazgo de UIF (ECOFEL) y subrayando el compromiso de Azerbaiyán con el desarrollo de capacidades internacionales y el intercambio de conocimiento.

Los Jefes de UIF se reunieron para impulsar una serie de iniciativas estratégicas destinadas a reforzar el papel de las Unidades de Inteligencia Financiera dentro del marco global de ALD/CFT.

Reconociendo la importancia de la autonomía y la independencia operativa para posicionar a las Unidades de Inteligencia Financiera (UIF) como impulsores clave de la eficacia dentro de sus sistemas nacionales de ALA/CFT, los Jefes de UIF (HoFIU) aprobaron una propuesta para elevar estos principios , previamente descritos en directrices internas, al nivel de expectativas formales para todos los miembros, convirtiéndolos en parte de los requisitos fundamentales del Grupo Egmont. Esta medida refleja nuestro compromiso colectivo con la protección de la integridad y la eficacia de la red global de UIF.

Además, en línea con nuestro compromiso permanente de fortalecer la colaboración segura entre jurisdicciones, la HoFIU acordó buscar mejoras del ESW que mejorarán la capacidad de identificar y conectar información relevante para el análisis ALD/CFT, entre jurisdicciones, de manera oportuna y eficaz, al tiempo que se mantienen estrictas salvaguardas en torno a la confidencialidad de los datos y el control de acceso.

Reconociendo la importancia de la capacitación y de contar con sólidas capacidades en el panorama actual de la inteligencia financiera, la HoFIU decidió fortalecer su programa insignia de desarrollo de capacidades, ECOFEL , mediante la aprobación de un nuevo enfoque de financiamiento para garantizar su desarrollo continuo y sostenibilidad. Esta decisión refleja el compromiso compartido de fortalecer la comunidad global de UIF mediante apoyo específico y planificación a largo plazo, alineándose con las prioridades cambiantes y la disponibilidad de recursos.

Los siguientes proyectos recibieron la aprobación final de HoFIU : Revisión de los Principios del Grupo Egmont para el Intercambio de Información entre UIF (proyecto conjunto con PPWG); Cooperación internacional informal eficaz (proyecto conjunto con el GAFI, Interpol y la ONUDD); Aumentar la eficacia de las UIF en el proceso de recuperación de activos; El papel de las UIF en la lucha contra los delitos ambientales; Integración de datos optimizada para cuestionarios de FIU (SDIFQ).

La organización seleccionó al Sr. Daniel Thelesklaf, Director de FIU Alemania , como nuevo Vicepresidente del Grupo de Expertos por un período de dos años. Se une a la Sra. Elzbieta Franków-Jaśkiewicz , Presidenta, y al Sr. Mohammed Shahid Ahmed , Vicepresidente, en el equipo directivo de nuestra organización.

A lo largo de la semana, se seleccionaron roles importantes adicionales para un período de dos años que finaliza después de la Plenaria del GE de 2027, incluidos:

-Ilit Ostrovitch Levi, FIU Israel, fue seleccionado como Presidente del Grupo de Trabajo de Intercambio de Información.

-Michelle Morales, FinCEN-FIU USA, fue seleccionada como Vicepresidenta del Grupo de Trabajo de Intercambio de Información.

-Fuad Aliyev, de la UIF de Azerbaiyán, fue seleccionado como Presidente del Grupo de Trabajo sobre Membresía, Apoyo y Cumplimiento.

-Carl Ramagge, FIU Gibraltar, fue seleccionado como Vicepresidente del Grupo de Trabajo de Políticas y Procedimientos.

-RJ Berry, FIU Islas Caimán , fue seleccionado como Vicepresidente del Grupo de Trabajo de Asistencia Técnica y Capacitación.

-Derly Lavertu, FINTRAC, fue seleccionado como Representante Regional para el Grupo Regional de las Américas.

-Shanmuga Priya, de FIU India, fue seleccionada como Representante Regional de Asia y el Pacífico.

-Eftasthios Tsirmpas, FIU Grecia, fue seleccionado como Representante Regional para el Grupo Regional Europa I.

-Ghizlane Dadyou, FIU Mónaco, fue seleccionada como Representante Regional para el Grupo Regional Europa II.

-Mohammad Al Muhanna, FIU Arabia Saudita , fue seleccionado como Representante Regional para Medio Oriente y África del Norte.

La organización también seleccionó a tres miembros de la junta directiva de Egmont Secure Web que cumplirán un mandato de dos años, hasta el final de la Plenaria del Grupo Egmont de 2027: Roberto Edmundo Mendoza López, UIF El Salvador, Muhammad Jiya, FIU Nigeria y Turki Mohammed Aljandal, UIF Arabia Saudita.

Se unirán al Sr. Max Braun, FIU Luxemburgo, la Sra. Hennie Verbeek-Kusters, FIU Países Bajos y el Sr. Vikas Aswal, FIU India en la Junta Directiva de ESW.

El Consejo Antilavado de Dinero (UIF Filipinas) fue elegido ganador del BECA de este año con un caso que obtuvo reconocimiento por su volumen, complejidad, métodos innovadores de inteligencia financiera y la sólida red de cooperación internacional. La Unidad de Inteligencia Financiera de India (UIF India), finalista del BECA 2025, recibió una mención honorífica por su exitosa contribución al caso.

La Plenaria de 2025 marca un hito importante: el 30.º aniversario del Grupo Egmont. Para conmemorar esta ocasión, la HoFIU decidió designar el 9 de junio como el Día Internacional de la FIU . Esta fecha conmemora la fundación del Grupo Egmont en el Palacio Egmont de Bruselas en 1995. La HoFIU aprobó formalmente la declaración

durante la semana de la Plenaria, y las celebraciones comenzarán anualmente a partir de 2026.

Otros aspectos destacados de la sesión plenaria del 30º aniversario de Egmont incluyen:

Muchos delegados participaron en el Taller del Premio al Mejor Caso Egmont (BECA) , así como en sesiones de capacitación operativa, incluido el Taller ECOFEL , el Taller de Web Segura de Egmont y la Capacitación Operativa de los Grupos de Trabajo Conjuntos de Intercambio de Información/Asistencia Técnica y Capacitación .

Entre otros resultados, durante la sesión conjunta, IEWG y TATWG presentaron un interesante video sobre el tema del abuso de activos virtuales con fines de financiamiento del terrorismo.

Además de los grupos de trabajo, las reuniones y las sesiones de capacitación que se organizan tradicionalmente durante la semana plenaria, la UIF anfitriona, Cellule de Renseignement Financier (CRF), ofreció talleres temáticos adicionales a lo largo de la semana. El objetivo de estos talleres temáticos fue brindar un espacio para la reflexión y el debate sobre temas más operativos, e incluyó: Taller sobre Asociaciones Público-Privadas Operacionales; Cinco talleres sobre análisis de datos: Herramientas de TI; Análisis operativo; Análisis estratégico; Análisis conjunto y un taller en francés. Taller sobre recuperación de activos (del Consejo de Europa)

El Grupo Egmont agradece a sus observadores y socios internacionales su continuo apoyo y cooperación, incluyendo las valiosas presentaciones y actualizaciones de la Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), la Comisión Europea, la Asociación Público-Privada de Inteligencia Financiera de EUROPOL (EFIPPP), el Grupo de Acción Financiera Internacional (GAFI), el GAFILAT, el Instituto de las Naciones Unidas para Formación Profesional e Investigaciones (UNITAR), la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), incluyendo una actualización de la Red GlobE, y la Organización Mundial de Aduanas (OMA), compartidas durante las reuniones. Agradecemos especialmente también a la UNODC y a INTERPOL por su apoyo durante las sesiones de capacitación.

El Grupo Egmont agradece a FIU Luxemburgo por su cálida bienvenida como anfitriones de la Sesión Plenaria del 30.º Aniversario de Egmont en Luxemburgo. El Grupo Egmont agradece el tiempo y el esfuerzo invertidos en la planificación del evento y se complace con el éxito alcanzado este año. ¡Felicitaciones al Director de FIU Luxemburgo, Max Braun, y a su equipo por la exitosa organización del evento!

Las UIF son indispensables en la lucha contra los delitos financieros. Su capacidad para recopilar, analizar y compartir inteligencia financiera las convierte en un pilar fundamental de los regímenes eficaces de lucha contra el lavado de dinero y la financiación del terrorismo en todo el mundo. Agradecemos a nuestras UIF miembros su compromiso y

dedicación para garantizar un entorno financiero más seguro y protegido, donde las actividades ilícitas se detecten, se disuadan y se interrumpan, salvaguardando así la integridad del sistema financiero global en beneficio de todos.

Fuente: https://egmontgroup.org/news/2025-egmont-plenary-luxembourg-co-chairs-statement/

Cuba participa en Luxemburgo en foro sobre Inteligencia Financiera

Ciudad de Luxemburgo, 10 jul (Prensa Latina). Cuba comparte sus experiencias y resultados en el ámbito de la inteligencia financiera en la trigésima primera plenaria del Grupo de Egmont, foro que sesiona esta semana en Luxemburgo, resaltó hoy la delegación de la isla.

El evento marca el aniversario 30 de la creación de un organismo internacional integrado por 170 países de gran relevancia como herramienta en el combate contra el terrorismo, el narcotráfico y otros flagelos.

La nación antillana está representada aquí por el subdirector general de la Dirección General de Investigación de Operaciones Financieras del Banco Central de Cuba, Armando Torres, y la gerente de Gestión del Conocimiento de la propia entidad, Yasmary Rodríguez.

En esta ocasión, la plenaria abarca tres sesiones principales, dedicadas a la autonomía e independencia operativa de las Unidades de Inteligencia Financiera, los recursos para el enfrentamiento a las finanzas ilícitas y el futuro de la web segura de Egmont.

Durante el foro, la isla expone sus acciones para potenciar el intercambio de información, la capacitación del personal, la cooperación y el soporte normativo. Asimismo, ratifica su compromiso en la prevención y lucha contra el lavado de activos, la financiación al terrorismo y el narcotráfico, la corrupción y el crimen transnacional organizado.

Cuba es signataria de los instrumentos multilaterales para el combate a estos flagelos y forma parte desde diciembre del 2012 del sistema del Grupo de Acción Financiera Internacional (GAFI), como miembro pleno del Grupo de Acción Financiera de Latinoamérica (Gafilat).

Fuente: https://www.prensa-latina.cu/2025/07/10/cuba-participa-en-luxemburgo-en-foro-sobre-inteligencia-financiera/

NOTICIAS

Caso Eclipse: Red familiar de alto exfuncionario de la UAFE fue sentenciada por lavado de activos.

Publicado en El Comercio, 14 de julio del 2025

Sudáfrica, Un Tribunal sentenció este lunes 14 de julio de 2025 a una red familiar de un alto exfuncionario de la UAFE, Diego Iván J.T., por lavado de activos, en el denominado caso Eclipse. La Fiscalía probó que la red, compuesta por los familiares de Diego Iván J.T., lavó alrededor de 6.1 millones de dólares en el sistema financiero nacional.

El 11 de julio, en su alegato de cierre, la Fiscalía General del Estado demostró ante el Tribunal de Garantías Penales la existencia del delito de lavado de activos por más de 6 millones de dólares.

El delito se habría cometido entre los años 2016 y 2024, por un grupo delictivo conformado por personas naturales y jurídicas: cuatro hermanos, la madre y dos empresas creadas por ellos. Evidenció cómo los procesados habrían introducido dinero de origen ilícito en el Sistema Financiero Nacional, simulando operaciones legales mediante el uso de una empresa ya existente y la creación de una nueva.

Los autores: Los principales responsables serían Édgar J. T., Ángel J. T. y Diego Iván J., con vínculos familiares y laborales.

Édgar J. T., autor directo, habría movilizado más de 1,1 millones de dólares mediante su empresa MEGAGIROS Cía. Ltda., usada para dar apariencia de legalidad a activos ilícitos. Ángel J. T. habría lavado más de 2 millones de dólares y creó la sociedad CAMBIOSCORP S. A., sin actividad real, para ocultar fondos.

En tanto, Diego Iván J., para las fechas de los hechos funcionario de la UAFE, presuntamente accedió de manera ilegal a información reservada, asesoró al grupo, manipuló alertas internas y facilitó la destrucción de evidencia. Fiscalía también demostró la responsabilidad penal de las personas jurídicas.

MEGAGIROS habría movilizado casi 2 millones de dólares sin respaldo económico; y CAMBIOSCORP, hoy disuelta, recibió más de 700 mil dólares de personas sin perfil financiero. Ambas incurrieron en operaciones típicas de lavado: depósitos fraccionados, uso de cuentas espejo, criptoactivos y cobro de cheques.

Los cómplices: Como cómplices, se identificó a Roberto Z., contador, habría estructurado la contabilidad ficticia y cobró decenas de cheques a nombre de MEGAGIROS. Marcial J., que retiró dinero ilícito y ocultó documentación clave.

Cómo operaba la red familiar del caso Eclipse: Todos ellos facilitaron el ingreso, la circulación y el ocultamiento del dinero, contribuyendo al encubrimiento del origen ilícito

de los fondos. El grupo habría utilizado remesadoras legales para ingresar montos inferiores al umbral de control. Luego, los fondos eran estratificados mediante transferencias y cheques, y finalmente convertidos en efectivo, simulando legalidad. Las operaciones se extendieron por Quito, Guayaquil y zonas fronterizas como Tulcán.

Fiscalía solicitó pena agravada: Tras concluir el alegato de cierre, Fiscalía solicitó una pena agravada de 13 años para los autores directos, multas del triple del monto lavado y el comiso de los bienes adquiridos ilícitamente.

Fuente: https://www.elcomercio.com/actualidad/seguridad/caso-eclipse-red-familiar-alto-exfuncionario-uafe-sentenciada-lavado-activos/

La amenaza silenciosa del lavado de activos.

Publicado en Al momento, 13 de julio del 2025

En las sombras del Caribe se mueve un enemigo invisible que no dispara, pero destruye, «el lavado de activos». República Dominicana, con su pujante economía turística y su posición estratégica, se ha convertido en un objetivo clave para los carteles internacionales

Aunque las autoridades nieguen la presencia formal de estructuras de los del narcotráfico, la realidad es que con sus capitales operan con sofisticación y bajo perfiles legales. Lo más preocupante es que estas operaciones suelen pasar desapercibidas, escondidas tras fachadas legales y una narrativa de crecimiento económico.

La globalización financiera, la expansión del turismo y la debilidad institucional hacen del país un terreno fértil para el blanqueo de dinero. El sistema inmobiliario, los negocios informales, las casas de cambio y algunas zonas francas son canales perfectos para inyectar dinero ilícito en la economía legal.

El lavado no solo enriquece a delincuentes, sino que distorsiona mercados, encarece la vida y debilita la competencia honesta. Esta distorsión también afecta la credibilidad del país ante inversionistas legítimos, que temen operar en un ambiente poco transparente.

Los carteles no necesitan presencia militar para conquistar un territorio, les basta el control económico. Comprar propiedades, financiar campañas políticas, crear empresas fachadas o infiltrar sectores estratégicos como puertos o aduanas son formas efectivas de colonización criminal. En este contexto, la democracia se convierte en un teatro, mientras el verdadero poder se ejerce tras bastidores. La influencia silenciosa del narcotráfico es capaz de condicionar leyes, postergar reformas y moldear decisiones públicas que benefician sus intereses.

Turismo: El turismo, orgullo nacional y motor económico, también se ve afectado. La llegada de capitales oscuros a zonas como Punta Cana, Bávaro o Samaná altera los precios, fomenta la informalidad y atrae un turismo de lujo ligado al crimen.

Esto desplaza la inversión ética y desnaturaliza el modelo sostenible que el país necesita proyectar al mundo. Además, crea una cultura de impunidad donde el lujo sin origen claro se vuelve aspiracional. El turismo, entonces, deja de ser desarrollo y se convierte en escaparate del crimen organizado. Los puertos dominicanos representan otro eslabón vulnerable en la cadena del crimen. La baja inspección de contenedores, la complicidad de funcionarios y la falta de trazabilidad en las mercancías crean una brecha crítica.

El narcotráfico se beneficia de estas debilidades para enviar drogas, lavar dinero y operar sin ser detectado. Las autoridades aduanales, muchas veces limitadas en recursos, no cuentan con tecnología adecuada ni procesos de control integrados. Esto deja al país expuesto al tráfico internacional de sustancias y capitales.

Frente a estas amenazas, la inteligencia artificial podría ser un aliado crucial. El uso de escáneres inteligentes, algoritmos de riesgo, blockchain aduanal y drones de vigilancia permitiría anticipar operaciones ilegales.

Pero se necesita inversión, voluntad política y cooperación internacional. La implementación de estas herramientas también requiere personal capacitado y una cultura institucional comprometida con la legalidad. No basta con adquirir la tecnología, hay que saber usarla para que funcione como escudo y no como ornamento.

Sin embargo, la tecnología es insuficiente sin una justicia funcional. La reforma judicial en la República Dominicana debe ser estructural: meritocracia, independencia, fiscalización y digitalización de los procesos son pilares clave. Mientras los casos de lavado prescriben o se archivan sin consecuencias, el crimen sigue avanzando. La impunidad es el combustible del crimen organizado, y sin castigo ejemplar, se normaliza la ilegalidad. Los jueces y fiscales deben estar protegidos del chantaje, la presión política o la amenaza directa de las mafias

La democracia dominicana también debe blindarse políticamente. Se requieren leyes que limiten el financiamiento electoral opaco, auditorías patrimoniales obligatorias y una ciudadanía vigilante. El narcotráfico se infiltra silenciosamente cuando se tolera la impunidad y se premia el dinero fácil, sin importar su origen. La ética pública debe recuperar su centralidad en el ejercicio del poder. Solo así se podrá recuperar la confianza social y proteger la legitimidad democrática frente al poder del dinero sucio.

En las economías en desarrollo, el lavado de activos distorsiona toda lógica financiera. Genera inflación artificial, encarece bienes raíces, expulsa a los empresarios legítimos y crea burbujas de inversión. Esto afecta a la clase media, reduce el empleo formal y debilita la soberanía económica del país. Además, deteriora la confianza en la moneda nacional y favorece la informalidad. La desigualdad se incrementa, y los más pobres terminan pagando las consecuencias de un sistema contaminado.

El impacto institucional también es grave. La captura de jueces, fiscales, alcaldes o legisladores por redes criminales impide que el Estado cumpla su rol. Cuando las

decisiones públicas responden al crimen, la democracia se transforma en simulacro. Lo que parece legal, muchas veces es solo una fachada delictiva. Esta corrupción estructural erosiona el contrato social y hace que la ley deje de ser referencia moral. El sistema entra en crisis, no por falta de normas, sino por ausencia de voluntad para hacerlas cumplir.

Combatir el lavado de activos requiere una respuesta integral. No se trata solo de operativos policiales, sino de educación ciudadana, vigilancia social, cooperación transnacional y voluntad real de limpiar las instituciones. El crimen organizado no se combate con discursos, sino con acción coordinada y firmeza ética. La sociedad civil, el sector privado y la prensa tienen un rol clave. Se requiere una cultura de legalidad que atraviese la administración pública y la vida cotidiana.

La República Dominicana está a tiempo de actuar. Posee el talento, las leyes y el apoyo internacional necesario. Pero sin transparencia, justicia y control efectivo, el país corre el riesgo de convertirse en un paraíso turístico… también para el crimen. El silencio no es neutralidad, es complicidad. La historia muestra que los países que no enfrentan este problema terminan devorados por él. Es ahora o nunca, la lucha contra el lavado es la lucha por el futuro del país.

Fuente: https://almomento.net/la-amenaza-silenciosa-del-lavado-de-activos/

DIRECTIVA DEL COMITÉ EDITORIAL:
PRESIDENTE: Fernando Luis Camejo de la Rosa
VICEPRESIDENTE: Armando Torres Aguirre
COORDINADOR GENERAL: Sergio Lázaro Medina Basso
EDITORA: Yasmary Rodríguez Alonso
DIRECCIÓN GENERAL DE INVESTIGACIÓN DE OPERACIONES FINANCIERAS
BANCO CENTRAL DE CUBA.
CORREO ELECTRÓNICO: dgiof@dgiof.gob.cu
Para esta y más información Ud. puede acceder al:
Portal del BCC en Internet: http://www.bc.gob.cu