



Instituto Mexicano de
Contadores Públicos

En congruencia con los objetivos estratégicos del IMCP, la Comisión de Prevención de Lavado de Dinero y Anticorrupción elabora este boletín informativo con el propósito de mantenerlos actualizados en materia de Prevención de Lavado de Dinero y Anticorrupción.

Boletín de la Comisión de Prevención de Lavado de Dinero y Anticorrupción

REPORTE SOBRE FRAUDE CIBERNÉTICO

DIGITALIZACIÓN Y RIESGOS DE LAVADO DE DINERO, FINANCIAMIENTO AL TERRORISMO Y A LA PROLIFERACIÓN

C.P.C., PCPLD, PCFL, PLDA y LD Silvia Rosa Matus de la Cruz
Vicepresidenta de Práctica Externa del IMCP

Directorio

Dra. y PCCAG Ludivina Leija Rodríguez
Presidenta del Comité Ejecutivo Nacional
2025-2026

C.P.C. y PCPLD Silvia Rosa Matus de la Cruz
Vicepresidenta de Práctica Externa

P.C.P., PCPLD y L.D. Angélica María Ruiz López
Presidenta de la Comisión de Prevención de
Lavado de Dinero y Anticorrupción

C.P.C., P.C.CG y M.A. Juan José Rosado Robledo
Coordinador responsable

INTRODUCCIÓN

Este documento del Grupo de Acción Financiera Internacional (GAFI) analiza el alarmante incremento del **fraude cibernético** y su relación con el **lavado de dinero** y el financiamiento del terrorismo. La organización destaca cómo la **innovación digital** y la inteligencia artificial han permitido a las redes criminales operar a gran escala, utilizando **activos virtuales** y centros de estafa transnacionales.

Para enfrentar esta amenaza, el informe propone fortalecer los estándares de **transparencia en los pagos** y mejorar la identificación de los beneficiarios finales de las empresas.

Asimismo, se subraya la necesidad de una **cooperación internacional** más ágil y el uso de tecnologías avanzadas para rastrear y recuperar fondos de manera efectiva.

El objetivo final es movilizar una respuesta global coordinada que proteja la integridad del **sistema financiero** frente a estos delitos digitales en constante evolución.

FRAUDE FACILITADO POR LA TECNOLOGÍA CIBERNÉTICA: DIGITALIZACIÓN Y RIESGOS DE LA/FT/FP

El Grupo de Acción Financiera Internacional (GAFI/FATF) identifica el fraude facilitado por la tecnología cibernética (CEF, por sus siglas en inglés) como una de las formas más extendidas y dañinas de criminalidad motivada por el lucro a escala global.

A febrero de 2026, 90% de las jurisdicciones evaluadas identifican el fraude como un riesgo mayor de lavado de dinero.

Marzo de 2026
Número 174

Nota aclaratoria

Las noticias de PLD y Anticorrupción no reflejan necesariamente la opinión del IMCP, de la Comisión de Prevención de Lavado de Dinero y Anticorrupción, y/o alguno de sus integrantes.

La responsabilidad corresponde exclusivamente a la fuente y/o el autor del artículo o comentario en particular.

Consulta el archivo histórico de noticias en:

<https://imcp.org.mx/publicaciones/vicepresidencia-practica-externa/>

twitter.com/imcp

imcp.org.mx/facebook



La rápida adopción de innovaciones digitales tras la pandemia de COVID-19 ha acelerado este fenómeno, permitiendo movimientos de fondos más rápidos y esquemas de ingeniería social altamente sofisticados.

PUNTOS CRÍTICOS IDENTIFICADOS

- **Crecimiento exponencial.** En jurisdicciones como el Reino Unido, el fraude representa más de 40% de todos los delitos, mientras que en Singapur los casos aumentaron 61% en solo dos años.
- **Convergencia criminal.** Los esquemas de fraude a gran escala están vinculados a grupos de crimen organizado transnacional que operan "centros de estafas", donde convergen delitos como la trata de personas, el tráfico de drogas y servicios profesionales de lavado de dinero.
- **Desafíos tecnológicos.** El uso de Inteligencia Artificial (IA) y *deepfakes* ha masificado el alcance de los ataques, mientras que los activos virtuales y los pagos instantáneos dificultan la recuperación de activos si no se interviene de manera inmediata.
- **Respuesta del GAFI.** Se están reforzando los estándares globales en transparencia de pagos, recuperación de activos, regulación de Proveedores de Servicios de Activos Virtuales (VASP) y el uso de tecnología avanzada (*Machine Learning*) para la detección proactiva.

MAGNITUD Y ALCANCE DE LA AMENAZA

El fraude cibernético ha aumentado de forma alarmante, adaptándose a las particularidades regionales y aprovechando las vulnerabilidades de la infraestructura financiera digital.



ESTADÍSTICAS DE IMPACTO GLOBAL

INDICADOR	DATO RELEVANTE
Jurisdicciones afectadas	156 países (90% de los evaluados) lo ven como riesgo mayor de lavado de dinero.
Crecimiento en Singapur	Incremento de 61% en casos de fraude cibernético en dos años.
Incidencia en Reino Unido	El fraude constituye más de 40% de la criminalidad total.
Tasa de victimización	Hasta 15% de la población adulta en varios países ha sido víctima.
Pérdidas económicas	Decenas de miles de millones de dólares anuales tan solo en EE. UU.

EL ECOSISTEMA DE LOS "CENTROS DE ESTAFAS"

El informe destaca la existencia de complejos o centros dedicados exclusivamente a la ejecución de fraudes. Estos centros no operan de forma aislada, sino que están integrados en ecosistemas criminales más amplios:

- **Vínculos delictivos.** Convergencia con la trata de personas y abusos a los derechos humanos, tráfico de drogas y lavado de dinero profesional.
- **Mecanismos de lavado integrados.** Los esquemas integran desde el inicio el uso de cuentas de testaferros (*nominee accounts*), redes de mulas bancarias y el comercio de cuentas de intercambio para mover fondos rápidamente a través de plataformas *fintech*.

FACILITADORES DEL FRAUDE CIBERNÉTICO

La innovación tecnológica, si bien impulsa el progreso económico, ha proporcionado herramientas que reducen las barreras de entrada para los criminales y permiten escalar sus operaciones.

- **Tecnologías emergentes.** La IA y los *deepfakes* potencian la efectividad de correos de *phishing*, sitios web falsos y publicidad engañosa en redes sociales, permitiendo estafas remotas a escala masiva.
- **Infraestructura financiera:**



- **Pagos instantáneos.** La velocidad de las transacciones supera la capacidad de respuesta de las autoridades.
- **Activos virtuales.** Los criminales solicitan pagos directamente en criptoactivos o convierten rápidamente el dinero fiduciario para evadir el rastreo y la recuperación de fondos.
- **Limitaciones operativas.** Los delincuentes actúan en tiempo real mientras que las autoridades competentes enfrentan restricciones legales, procedimentales y jurisdiccionales para compartir información internacionalmente.

FORTALECIMIENTO DE LOS ESTÁNDARES DEL GAFI

Para combatir esta epidemia, el GAFI ha actualizado y promovido la implementación de diversas medidas dentro de su marco global de ALA/CFT/CFP (Anti-Lavado de Activos, Contra el Financiamiento al Terrorismo y Contra el Financiamiento a la Proliferación).

TRANSPARENCIA Y RECUPERACIÓN DE ACTIVOS

- **Mecanismos de confirmación.** Fomento de mecanismos de "confirmación del beneficiario" para mejorar la trazabilidad de los fondos.
- **Suspensión rápida de pagos.** Los estándares revisados exigen que los países establezcan sistemas de congelación y suspensión de pagos acelerados para evitar que los fondos salgan de la jurisdicción.
- **Confiscación sin condena.** Requerimiento de regímenes de confiscación más robustos y cooperación internacional informal más rápida.

REGULACIÓN DE ACTIVOS VIRTUALES Y BENEFICIARIO CONTROLADOR

- **VASP.** Desde 2019, el GAFI introdujo estándares globales para los Proveedores de Servicios de Activos Virtuales, incluyendo la identificación de clientes y el rastreo de transacciones (regla de viaje).
- **Transparencia de personas jurídicas.** En marzo de 2022, se revisaron los estándares sobre el Beneficiario Controlador (BO) para obligar a los países a adoptar enfoques basados en riesgos que impidan el uso de empresas fantasma para ocultar ganancias ilícitas.

ALIANZAS Y SOLUCIONES TECNOLÓGICAS

- **Colaboración público-privada.** Establecimiento de centros nacionales antifraude que comparten atributos con los centros de coordinación de ALA.
- **Uso de tecnología avanzada.** Implementación de modelos de *Machine Learning* y sistemas de puntuación de riesgo en tiempo real por parte de Unidades de Inteligencia Financiera (UIF) y bancos para detectar anomalías en grandes conjuntos de datos de transacciones.





CONCLUSIÓN

El fraude facilitado por la tecnología cibernética ha dejado de ser una amenaza focalizada para convertirse en un problema global que afecta a casi todas las personas en el mundo.

El GAFI ha reafirmado su compromiso de priorizar el combate a este delito en los próximos años, enfocándose en la movilización de su "caja de herramientas" para fortalecer la cooperación internacional y la recuperación de activos.

La respuesta global coordinada, por medio de una red de más de 200 jurisdicciones, es esencial para prevenir que el capital llegue a manos de los estafadores y asegurar su recuperación cuando el fraude ya ha ocurrido.

LINK

<https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/cyber-enabled-fraud-digitalisation-ml-tf-pf-risks.html>

