



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.

Abril de 2026
Número 181

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

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

EVALUACIÓN DE LA AMENAZA DE FRAUDE FINANCIERO GLOBAL DE INTERPOL (EDICIÓN 2026)

C.P. y PCPLD Genaro Eliseo Gómez Muñoz
Integrante de la Comisión de Prevención de Lavado de Dinero y Anticorrupción del IMCP

INTRODUCCIÓN

La segunda edición de la Evaluación de la Amenaza de Fraude Financiero Global de INTERPOL (marzo de 2026) revela una crisis de escala sin precedentes.

El fraude financiero se ha consolidado como una de las **cinco principales amenazas globales**, equiparándose en peligrosidad al tráfico de drogas y al lavado de dinero.

En 2025, las pérdidas globales se estimaron en **442 mil millones de USD**, con un impacto profundo no solo en la estabilidad económica, sino también en el tejido social y la seguridad internacional.

Los hallazgos clave subrayan tres vectores de transformación:

- **Tecnología e Inteligencia Artificial:** La IA actúa como un "multiplicador de fuerza", industrializando el fraude mediante el uso de "IA agéntica" y herramientas de *deepfake*, lo que aumenta la rentabilidad de los esquemas en un 450%.
- **Policriminalización y Centros de Estafa:** El modelo de "doble víctima" se ha expandido globalmente; personas de casi 80 nacionalidades son traficadas para trabajar forzosamente en centros de estafa en línea.
- **Policriminalidad:** El fraude financia ahora directamente otras actividades graves, incluyendo el terrorismo (especialmente en África) y el crimen organizado transnacional.

INTERPOL evalúa el riesgo global de fraude financiero para los próximos tres a cinco años como **alto**, proyectando una escalada significativa debido a las bajas barreras de entrada tecnológicas y la sofisticación de las redes criminales.

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/>



PANORAMA GLOBAL Y DINÁMICAS DEL DELITO

Desde 2024, el fraude financiero ha experimentado un crecimiento acelerado tanto en volumen como en complejidad. El 77% de los líderes empresariales globales reportaron un aumento de este delito en 2025, mientras que el 73% ha sido afectado personalmente o mediante su red profesional.

INCREMENTO DE AVISOS Y DIFUSIONES (2024-2025)

La colaboración policial ha resultado en un aumento del 54% global en la emisión de avisos y difusiones relacionados con fraude. El desglose regional del incremento es el siguiente:

REGIÓN	INCREMENTO EN AVISOS/DIFUSIONES
África	+60%
Europa	+69%
Asia-Pacífico	+47%
Américas y el Caribe	+40%
Medio Oriente y Norte de África (MENA)	+17%

Durante este periodo, el Centro de Crimen Financiero y Anti-Corrupción de INTERPOL (IFCACC) apoyó en más de 1,500 casos transnacionales, recuperando o rastreando activos valorados en 1.1 mil millones de dólares.

TIPOLOGÍAS DE FRAUDE Y TENDENCIAS EMERGENTES

El informe identifica una diversificación en los métodos de engaño, con un giro hacia tácticas híbridas y tecnológicas.

- **Compromiso de Correo Electrónico Empresarial (BEC).** Sigue siendo el tipo de fraude más informado. Ha evolucionado de suplantaciones simples a ataques sofisticados de múltiples etapas impulsados por la IA y algún programa maligno especializado.



- **Fraude de inversión.** Genera las mayores pérdidas financieras individuales. Los criminales utilizan aplicaciones de trading falsas y criptomonedas, a menudo empleando un modelo de "ganancia inicial" para generar confianza antes de sustraer la inversión total.
- **Fraude de identidad sintética y de menores.** La IA permite crear identidades "nuevas" mezclando datos reales y falsos. Es particularmente preocupante el robo de identidad de menores basado en fotos y datos compartidos involuntariamente por padres en redes sociales, lo que suele pasar desapercibido hasta que la víctima alcanza la mayoría de edad.
- **Quishing.** El uso de códigos QR maliciosos para redirigir a víctimas a sitios de *phishing* o descargar un programa maligno, eludiendo las medidas de seguridad tradicionales de correo electrónico.
- **Sextorsión híbrida.** Una tendencia al alza donde los estafadores integran la sextorsión dentro de esquemas de fraude romántico o de inversión. Si el engaño financiero falla, recurren al chantaje con contenido explícito real o generado por IA.

LA INTELIGENCIA ARTIFICIAL COMO MULTIPLICADOR DE FUERZA

La tecnología digital ha reducido drásticamente las barreras de entrada al crimen financiero, transformándolo en una industria eficiente y global.

Avances tecnológicos en el crimen:

- **IA Agentic.** Agentes de IA que pueden planificar y ejecutar campañas de fraude de forma autónoma, desde la selección de víctimas hasta la generación de notas de rescate psicológicamente adaptadas.
- **Clonación de voz y *deepfakes*.** Los delincuentes requieren solo 10 segundos de audio genuino para crear clones digitales convincentes que pueden eludir



sistemas de autenticación biométrica y suplantar a familiares en "secuestros falsos".

- **Fraude como Servicio (FaaS).** Mercados en la *Dark Web* ofrecen *kits* de identidad sintética, herramientas de *phishing* y plataformas de *trading* falsas, permitiendo que actores con pocas habilidades técnicas ejecuten ataques complejos.

LA EXPANSIÓN GLOBAL DE LOS CENTROS DE ESTAFA

Lo que comenzó como un fenómeno regional en el Sudeste Asiático se ha convertido en una infraestructura criminal global.

- **Tráfico humano para fraude forzado.** Centenas de miles de personas son atraídas con ofertas de trabajo falsas y retenidas en complejos donde son obligadas a cometer estafas.
- **Expansión geográfica.** Se han descubierto centros en América Central, África Occidental y la región MENA. Las víctimas proceden de diversas regiones, incluyendo América del Sur y Europa Occidental.
- **Modelos de reclutamiento en África.** En África Occidental y Central, las redes operan bajo la apariencia de empresas de Marketing Multinivel (MLM). Las víctimas son coaccionadas para reclutar a sus propios parientes, explotando la confianza comunitaria y familiar.

NEXO ENTRE FRAUDE, TERRORISMO Y CRIMEN ORGANIZADO

El informe destaca una convergencia peligrosa entre el fraude financiero y otras formas de delincuencia grave.

- **Financiación del terrorismo.** La *Operation Catalyst* de INTERPOL reveló que esquemas Ponzi basados en criptomonedas en África (Camerún, Kenia, Nigeria) han sido utilizados para generar recursos para grupos terroristas.



- **Lavado de dinero especializado.** Las redes de fraude colaboran con grupos dedicados exclusivamente al lavado de activos, utilizando sistemas informales y criptomonedas para ocultar el rastro de los fondos.
- **Sofisticación en Sudamérica.** Se reportan operaciones que utilizan equipos láser para falsificar huellas dactilares e interceptar códigos de autenticación de dos factores, demostrando una alta capacidad técnica organizacional.

IMPACTO HUMANO Y COSTO SOCIAL

El daño causado por el fraude trasciende lo económico. Las víctimas sufren un impacto psicológico profundo que incluye:

- Vergüenza, estigma y humillación.
- Aislamiento social y pérdida de dignidad.
- Trauma psicológico grave; en casos extremos, se han reportado suicidios.

La cultura de "culpabilización de la víctima" y el juicio social disuaden la denuncia de estos delitos, lo que genera un subregistro significativo de las estadísticas reales y dificulta la acción de las autoridades.

PROYECCIONES DE RIESGO (TRES A CINCO AÑOS)

INTERPOL ha categorizado el riesgo futuro mediante una metodología ponderada:

DOMINIO	NIVEL DE RIESGO PROYECTADO
Riesgo general global	Alto
Económico	Alto
Seguridad	Alto
Social	Alto
Gobernanza	Moderado
Salud	Moderado



OPERACIONES POLICIALES DE IMPACTO

INTERPOL continúa coordinando esfuerzos internacionales para dismantelar estas estructuras:

- **Operación Liberterra III.** Resultó en más de 3,700 arrestos y la identificación de 4,414 víctimas de trata vinculadas a centros de estafa.
- **Operación Serengeti 2.0 (África).** 1,209 detenciones y 97.4 millones de USD recuperados.
- **Operación Tarjeta Roja 2.0.** Dirigida contra infraestructuras de fraude de alto rendimiento en 16 países africanos.

CONCLUSIÓN

El fraude financiero ya no es un delito aislado, sino un componente central de la poli criminalidad moderna impulsada por la tecnología. La respuesta global requiere una cooperación internacional sin precedentes, el intercambio de inteligencia en tiempo real y la adopción de mecanismos de defensa adaptativos impulsados por IA para contrarrestar las infraestructuras criminales que amenazan la seguridad económica y social a escala mundial.

LINK

www.interpol.int



Interpol Amenaza de Fruada 2026.pdf