Instituto Mexicano de
Contadores Públicos

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

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.

Junio de 2026
Número 192

## Directorio



## Nota aclaratoria



# Detección y disrupción del financiamiento al terrorismo en las redes sociales

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

## Introducción

A medida que las amenazas de Financiamiento al Terrorismo evolucionan con el desarrollo de nuevas tecnologías y plataformas digitales, el Grupo de Acción Financiera Internacional (GAFI) ha publicado un nuevo documento para concienciar sobre las principales tendencias y tipologías mediante las cuales se abusa de las redes sociales, las aplicaciones de mensajería instantánea y las plataformas de *streaming* para financiar actividades terroristas.

El informe nos presenta cómo los terroristas hacen un mal uso de estas tecnologías y sobre cómo detectar e interrumpir estas actividades, incluso mediante una mayor cooperación entre los sectores público y privado.

La presidenta del GAFI, Elisa de Anda Madrazo, declaró:

> El Financiamiento al Terrorismo se ha digitalizado y, con ello, la capacidad de llegar a miles de millones de personas y amplificar el impacto de los ataques nunca ha sido mayor. Ninguna jurisdicción ni autoridad puede abordar esta amenaza por sí sola, por lo que debemos trabajar en estrecha colaboración para evitar que los delincuentes hagan un mal uso de estas plataformas para causar daño en todo el mundo.
>
> Celebro la colaboración constructiva que hemos mantenido hasta ahora con las empresas de tecnología y redes sociales para hacer frente a esta amenaza, y espero que esta continúe para la seguridad de las personas en todo el mundo.

## Mensajería instantánea y plataformas de streaming

El ecosistema de redes sociales, aplicaciones de mensajería instantánea y plataformas de *streaming* (SMSP, por sus siglas en inglés) ha evolucionado de ser herramientas de comunicación a complejos entornos digitales que integran servicios financieros y flujos de ingresos.

Esta transformación ha permitido que organizaciones terroristas y actores individuales exploten estas plataformas para recaudar, mover, almacenar y gastar fondos de manera global.

El Grupo de Acción Financiera Internacional (GAFI) identifica que la capacidad de estos actores para abusar del sistema financiero internacional depende cada vez más de su acceso a tecnologías emergentes y de la capacidad de adaptar sus métodos a las funcionalidades de pago integradas en las interfaces de las SMSP.

Los desafíos principales radican en la distinción entre el uso de plataformas para propaganda o reclutamiento y su uso específico para el Financiamiento al Terrorismo (FT), así como en el monitoreo de comunicaciones cifradas y transacciones pequeñas y frecuentes. El documento subraya la necesidad de una respuesta coordinada que incluya la aclaración del alcance regulatorio bajo los estándares del GAFI, el fortalecimiento de las asociaciones público-privadas (APP) y la integración de la inteligencia digital con la financiera para mitigar riesgos que actualmente se reportan como altos o muy altos en zonas de conflicto.

## El ecosistema de las SMSP y su exposición al riesgo de FT

Las SMSP están diseñadas para la accesibilidad y la escalabilidad, extendiéndose desde redes sociales convencionales hasta aplicaciones de mensajería cifrada. Su evolución ha desdibujado las fronteras regulatorias tradicionales al integrar funcionalidades de pago directamente en la interfaz de usuario o mediante socios comerciales externos.

### Características fundamentales que impactan el riesgo

El impacto de estas plataformas en el panorama del riesgo de FT se debe a cuatro factores clave:

1. Alcance transnacional: Acceso global que permite operaciones transfronterizas.
2. Base de usuarios masiva: Una adopción generalizada que facilita el camuflaje de actividades ilícitas.
3. Velocidad de intercambio: Rapidez en la recopilación y transferencia de información y fondos.
4. Sistemas de filtrado y algoritmos: Uso de IA para recomendar contenido, lo cual puede ser explotado para aumentar el alcance de las campañas de recaudación.

### Desafíos en la detección

Existe una brecha significativa en la capacidad de detección de las autoridades. Menos del 30% de las jurisdicciones cubren los riesgos de FT por medio de SMSP en sus evaluaciones nacionales de riesgo.

La dificultad principal es separar el uso ideológico del transaccional

| Naturaleza del abuso | Uso para fines terroristas | Uso para Financiamiento al Terrorismo (FT) |
|---|---|---|
| Objetivo primario | Difundir propaganda, reclutar y coordinar actos terroristas. | Recaudar, mover y ocultar fondos para actividades operativas. |
| Actividades clave | Diseminación de contenido, planificación operativa cifrada. | *Crowdfunding*, transferencias P2P, uso de sistemas de pago integrados. |
| Características explotadas | Viralidad, anonimato, cifrado. | Debilidad en la Debida Diligencia del Cliente (CDD), Activos Virtuales (AV). |
| Desafío de Detección | Monitoreo de comunicaciones y moderación de contenido. | Rastreo de transacciones pequeñas, frecuentes y transferencias informales. |

## Tipologías identificadas de financiamiento al terrorismo

Los actores terroristas demuestran una alta adaptabilidad, ajustando sus métodos según las funciones de la plataforma y las medidas regulatorias.

Métodos de recaudación y movimiento de fondos:

- ***Crowdfunding* con fachada humanitaria:** Uso de redes sociales para solicitar fondos mediante apelaciones fraudulentas a la caridad, dirigidas a diásporas y confiando en micro donaciones.
- **Uso multimodal y multiplataforma:** La recaudación comienza en plataformas públicas y se traslada a mensajería cifrada para compartir instrucciones de pago privadas.
- **Explotación de la "economía del creador":** Generación de ingresos mediante herramientas de monetización como *livestreaming*, propinas digitales y suscripciones, desdibujando la línea entre ingresos legítimos y fondos extremistas.
- **Uso de Activos Virtuales (AV):** Integración de billeteras de AV y códigos QR para transferencias transfronterizas, a menudo utilizando direcciones rotativas para evadir la trazabilidad.
- **Camuflaje y lenguaje cifrado:** Uso de emojis, números y referencias internas para señalar actividades de recaudación sin activar los filtros de detección.
- **Actividad comercial disfrazada:** Los fondos se disfrazan como ventas en línea, listados en mercados digitales o eventos con boletos.
- **Factores contextuales como catalizadores:** Aprovechamiento de crisis humanitarias o conflictos para lanzar campañas de recaudación urgentes antes de que se apliquen contramedidas.

## Marcos regulatorios y responsabilidades

De acuerdo con los estándares del GAFI, las SMSP no suelen estar sujetas directamente a obligaciones de Prevención de Lavado de Dinero y Financiamiento al Terrorismo (PLD/CFT) a menos que realicen funciones de Instituciones Financieras (IF) o Proveedores de Servicios de Activos Virtuales (PSAV).

### Funciones financieras integradas

Las SMSP pueden facilitar flujos financieros mediante diversos modelos:

- **Plataforma neutral:** La SMSP actúa solo como infraestructura técnica para que terceros regulados ofrezcan servicios.

- **Entidad regulada funcional:** La SMSP ofrece, controla o influye materialmente en servicios financieros (custodia, transferencia o intercambio de fondos/AV), lo que la convierte en una IF o PSAV.

### Mecanismos de monetización en el ecosistema

- **Compras en la aplicación:** Entrada para micro transacciones y bienes virtuales.
- **Transferencias P2P:** Pagos directos entre usuarios intermediados por Proveedores de Servicios de Pago (PSP).
- **Pagos a creadores:** Mecanismos críticos para sostener las economías de creadores mediante transferencias bancarias o billeteras.
- **Billeteras en la aplicación:** Cuentas de valor almacenado para pagos rápidos o propinas.

## Respuesta operativa y el papel del sector privado

La detección efectiva depende de un enfoque coordinado y multicapa que involucre a Unidades de Inteligencia Financiera (UIF), fuerzas del orden y supervisores.

### Necesidades operativas críticas

- **Establecimiento de canales bilaterales:** Comunicación fluida con las SMSP para el intercambio de información y preservación de datos.
- **Uso de Inteligencia de Fuentes Abiertas (OSINT):** Aplicación de análisis de redes y técnicas de monitoreo avanzado.
- **Vinculación de inteligencia digital y financiera:** Capacidad para conectar el comportamiento en línea con las transacciones financieras subyacentes.

### El sector privado como primera línea de defensa

Las SMSP tienen la capacidad de desarrollar herramientas de detección basadas en IA para identificar actividades de FT en etapas tempranas. La cooperación permite que las autoridades obtengan señales de alta calidad y que la industria diseñe algoritmos más efectivos para prevenir el abuso sin afectar las operaciones comerciales legítimas.

## Recomendaciones estratégicas

Para fortalecer la resiliencia global ante el uso de SMSP para el FT, el GAFI propone las siguientes acciones:

- **Clarificar el alcance regulatorio:** Identificar qué funcionalidades de las SMSP entran en los estándares del GAFI y aplicar las obligaciones PLD/CFT correspondientes.
- **Evaluar riesgos de tecnologías emergentes:** Incorporar experiencia del sector privado para entender riesgos en IA, finanzas descentralizadas (DeFi) y comunicaciones cifradas.
- **Fortalecer el diálogo estructurado:** Crear marcos legales para el intercambio de datos seguro y oportuno entre SMSP, IF, PSAV y autoridades competentes.
- **Aumentar la capacidad operativa:** Proporcionar herramientas especializadas y capacitación para investigar ecosistemas digitales.
- **Cooperación internacional:** Agilizar el acceso transfronterizo a evidencia electrónica y mecanismos de cooperación legal.
- **Desarrollar indicadores específicos:** Expandir las señales de alerta (*red flags*) que incluyan el uso de lenguaje codificado y herramientas de monetización de plataformas de *streaming*.

## Link

*www.fatf-gafi.org*