



En congruencia con los objetivos estratégicos del IMCP, la COMISIÓN DE PREVENCIÓN DE LAVADO DE DINERO Y ANTICORRUPCIÓN prepara este boletín informativo con la finalidad de mantenerlos actualizados en materia de Prevención de Lavado de Dinero y Anticorrupción.

Directorio

C.P. PCFI Héctor Amaya Estrella
Presidente del Comité Ejecutivo Nacional
2023-2025

C.P. y PCCAG Ludivina Leija Rodríguez
Vicepresidente General

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

C.P.C., 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

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.

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

EVALUACIÓN DE INTERPOL SOBRE EL FRAUDE FINANCIERO UNA AMENAZA GLOBAL IMPULSADA POR LA TECNOLOGÍA

C.P. Y PCLD GENARO ELISEO GÓMEZ MUÑOZ
INTEGRANTE DE LA COMISIÓN NACIONAL DE PREVENCIÓN DE LAVADO DE DINERO Y
ANTICORRUPCIÓN DEL IMCP

Una nueva evaluación de la INTERPOL sobre el fraude financiero mundial se acaba de publicar recientemente, en la cual se destaca el uso de la tecnología, la cual está permitiendo a los grupos del crimen organizado atacar mejor a sus víctimas en todo el mundo.

El uso de la Inteligencia Artificial (IA), los grandes modelos de lenguaje y criptomonedas combinados con los modelos de negocios de *phishing* y *ransomware* como servicio han resultado en fraudes más sofisticados y profesionales sin la necesidad de habilidades técnicas avanzadas y a un costo relativamente bajo.

El análisis detrás de la Evaluación Global del Fraude Financiero de la INTERPOL también señala la expansión global de la trata de personas con fines de criminalidad forzada en los centros de llamadas, en particular para llevar a cabo estafas de "sacrificio de cerdos", un esquema híbrido que combina fraudes que se tornan en un modelo bien elaborado, romántico y de inversión, utilizando las criptomonedas.

Los tipos de fraude detallados en este informe se destacan de otros, **la suplantación de identidad**, el romance, el soporte técnico, el pago por adelantado y los fraudes de telecomunicaciones, fraudes de inversión en línea, el *phishing*, así como el compromiso del correo electrónico empresarial (Bussines Email Compromise; BEC, por sus siglas en inglés).

Abril de 2024

Número 91

Consulta el archivo histórico de Prevención de Lavado de Dinero y Anticorrupción en:
<http://imcp.org.mx/noticiaspldft>



El secretario general de la INTERPOL, Jürgen Stock, afirmó:

Nos enfrentamos a una epidemia en el crecimiento del fraude financiero, que lleva a que individuos, a menudo personas vulnerables, y empresas sean defraudados a escala masiva y global.

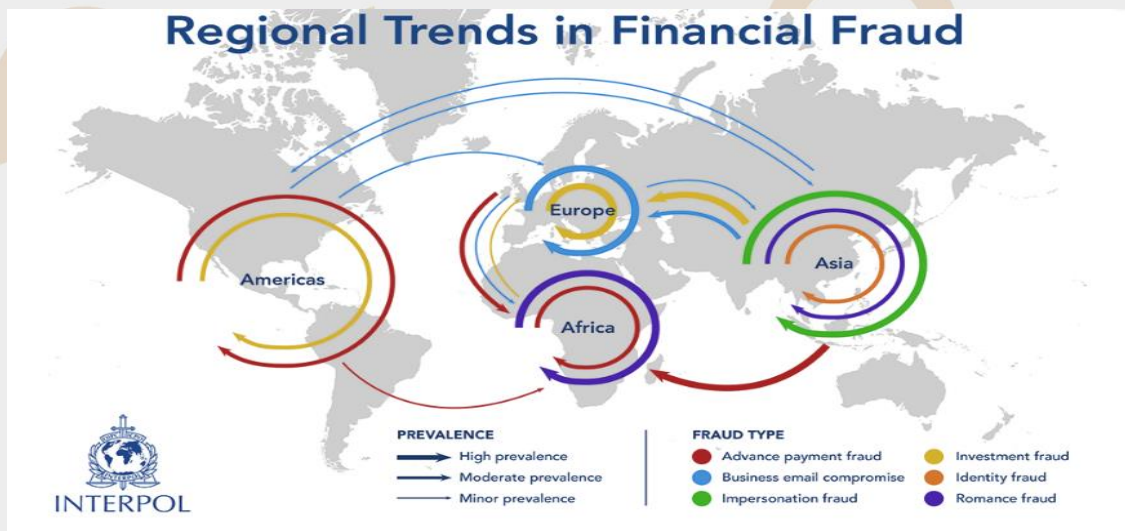
Los cambios en la tecnología y el rápido aumento en la escala y el volumen del crimen organizado han impulsado la creación de una variedad de nuevas formas de defraudar a personas inocentes, empresas e incluso gobiernos.

Con el desarrollo de la IA y las criptomonedas, la situación sólo empeorará si no se toman medidas urgentes.

Es importante que no existan refugios seguros para que operen los defraudadores financieros.

Debemos cerrar las brechas existentes y garantizar que el intercambio de información entre sectores y a través de fronteras sea la norma, no la excepción.

También debemos fomentar una mayor denuncia de delitos financieros, así como invertir en el desarrollo de capacidades y capacitación para que las fuerzas del orden con el objetivo de desarrollar una respuesta más efectiva y verdaderamente global.





HALLAZGOS CLAVE

- Las tendencias globales que más prevalecen son el fraude en inversiones, el fraude en pagos anticipados, el fraude romántico (por así llamarlo) y la vulneración del correo electrónico empresarial.
- El fraude financiero lo lleva a cabo con mayor frecuencia una red de coautores, que varía desde muy estructurada hasta poco afiliada.
- Una necesidad urgente de fortalecer la recopilación y el análisis de datos para desarrollar estrategias de defensa más informadas y efectivas.

Para abordar eficazmente esta escalada delictiva a escala mundial y cerrar brechas de información cruciales, una de las recomendaciones del informe es la necesidad de crear **asociaciones público-privadas (tema que la nueva presidenta del GAFI ha encabezado en los últimos años)** de múltiples partes interesadas para rastrear y recuperar fondos perdidos por fraude financiero. Desde el lanzamiento del mecanismo de suspensión de pagos de INTERPOL de Intervención Rápida Mundial (I-GRIP) en 2022, la organización ha ayudado a los países miembros a interceptar más de 500 millones de dólares en ingresos delictivos, procedentes en gran medida de fraudes cibernéticos.

TENDENCIAS REGIONALES EN FRAUDE FINANCIERO

ÁFRICA

El compromiso del correo electrónico empresarial sigue siendo una de las tendencias más frecuentes en África; sin embargo, hay un uso cada vez mayor del fraude en la matanza de cerdos. Se han identificado casos de este tipo de fraude en África occidental y meridional dirigidos a víctimas en otras jurisdicciones fuera del continente.



Ciertos grupos criminales de África occidental, incluidos Black Axe (Nigeria), Airlords y Supreme Eiyee, continúan creciendo a escala transnacional y se sabe que tienen amplias habilidades en fraude financiero en línea, como fraude romántico, fraude de inversiones, fraude de pagos por adelantado y fraude de criptomonedas.

AMÉRICA

Los tipos de fraude más comunes en América son la **suplantación de identidad**, el romance, el soporte técnico, el pago por adelantado y los fraudes de telecomunicaciones.

El fraude impulsado por la trata de personas sigue siendo un fenómeno delictivo en aumento.

La operación coordinada por INTERPOL, Operación Turquesa V, reveló que cientos de víctimas fueron sacadas de la región tras ser atraídas a través de aplicaciones de mensajería y plataformas de redes sociales y coaccionadas a cometer fraudes, incluidos fraudes en inversiones y *pig butchering* (matanza de cerdos, el cual **consiste en manipular a una persona emocionalmente para que realice inversiones en falsas plataformas de comercio**).

Cada vez hay más pruebas de que los grupos criminales latinoamericanos como Comando Vermelho (Brasil), Primeiro Comando da Capital (PCC) (Brasil) y Cartel Jalisco Nueva Generación (CJNG) (México) también están involucrados en la comisión de fraude financiero.

ASIA

Los esquemas de fraude en la matanza de cerdos se iniciaron en Asia en 2019 y se expandieron durante la pandemia de COVID-19. Posteriormente,



Asia surgió como un punto focal, y las organizaciones criminales de los países más pobres de la región emplean estructuras de tipo empresarial.

Otro tipo de fraude que ha experimentado un aumento en los últimos años en Asia es un tipo de fraude de telecomunicaciones en el que los perpetradores se hacen pasar por agentes del orden o funcionarios bancarios para engañar a las víctimas para que revelen sus credenciales de tarjeta de crédito o cuenta bancaria o para que entreguen grandes cantidades de dinero.

EUROPA

Los fraudes de inversión en línea, el *phishing* y otros esquemas de fraude financiero en línea se han intensificado hacia objetivos cuidadosamente seleccionados para maximizar las ganancias. Las aplicaciones para teléfonos móviles también están en el punto de mira de los ciberdelincuentes.

Las redes criminales involucradas en estos esquemas en línea a menudo exhiben modos de operación sofisticados y complejos, que generalmente son una combinación de diferentes tipos de fraude.

También está aumentando la matanza de cerdos, que se lleva a cabo predominantemente en centros de llamadas en el Sudeste Asiático.

LINK

Para conocer el reporte completo:

<https://www.interpol.int/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology>

Para conocer la operación Turquesa V:

<https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2023/Americas-detencion-de-257-sospechosos-de-trafico-de-migrantes-y-trata-de-personas>