UIF
EL SALVADOR
1999

COMPILACIÓN DE TIPOLOGÍAS RELACIONADAS AL USO DE ACTIVOS VIRTUALES

OCTUBRE 2025

COMPILACIÓN DE TIPOLOGÍAS RELACIONADAS AL USO DE ACTIVOS VIRTUALES

Unidad de Investigación Financiera UIF

CONTENIDO

INTRODUCCIÓN

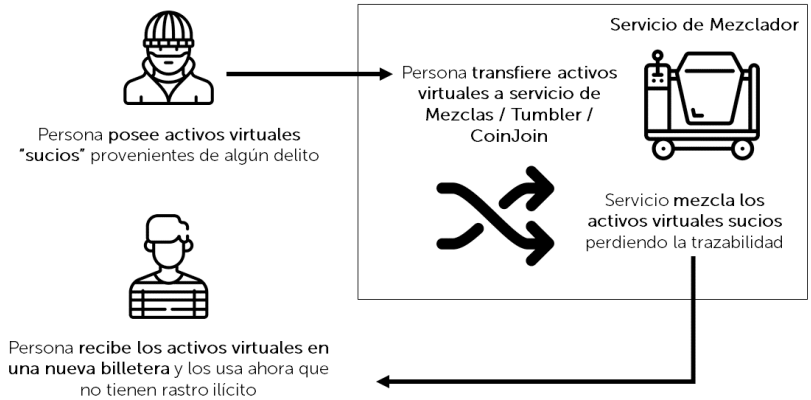
El presente documento ha sido elaborado para el uso y consulta de la Unidad de Investigación Financiera (UIF), las autoridades competentes y los sujetos obligados. Su contenido reúne diez tipologías vinculadas al uso de activos virtuales en esquemas asociados al Lavado de Dinero y de Activos (LA/FT), identificadas a partir de patrones y conductas identificadas por organismos internacionales.

El objetivo principal de este compendio es fortalecer la capacidad de detección y prevención del lavado de activos mediante activos virtuales, brindando herramientas que permitan reconocer con mayor precisión las conductas, operaciones y patrones transaccionales que caracterizan estos esquemas. Con ello, se busca apoyar a las instituciones públicas y privadas en el diseño y ajuste de mecanismos de control, así como en la mejora de sus señales de alerta, contribuyendo al esfuerzo nacional para proteger al país frente a los riesgos derivados del uso indebido de nuevas tecnologías financieras.

Las metodologías, descripciones y ejemplos presentados en este documento se basan en hechos reales y tipologías reconocidas por organismos internacionales, adaptadas al contexto nacional. No obstante, se han modificado los elementos identificatorios a fin de preservar la confidencialidad de personas, instituciones y lugares, evitando cualquier perjuicio o señalamiento directo.

Finalmente, debe entenderse que las conductas descritas no constituyen un juicio de responsabilidad penal, sino que representan tendencias analíticas destinadas a comprender los riesgos emergentes dentro del ecosistema de activos virtuales y su posible utilización con fines ilícitos.

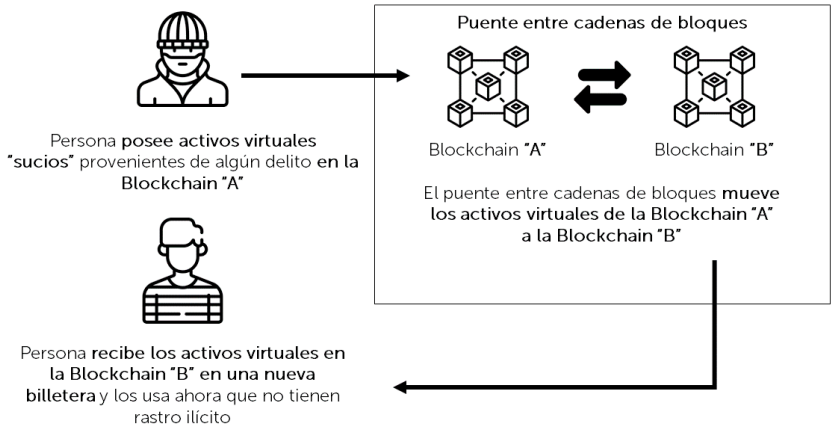
TIPOLOGÍAS ASOCIADAS A ACTIVOS VIRTUALES Y LAVADO DE DINERO Y ACTIVOS:

Nombre de la Tipología:	*Mixers* **/** *CoinJoin* **(servicios de mezcla)**
Descripción:	Uso de servicios que agrupan fondos de múltiples usuarios y devuelven cantidades "mezcladas" para romper la trazabilidad entre origen y destino. Estos servicios buscan esconder el rastro de las transacciones en la *blockchain*, dificultando la identificación del beneficiario final. Existen tanto mezcladores centralizados como técnicas descentralizadas (*CoinJoin*[1]*, coin-swapping*[2]), los cuales han sido ampliamente utilizados por actores criminales para el encubrimiento de transacciones a través de distintas capas de fondos.
Sector vulnerado:	Proveedores de servicios de activos virtuales (PSAV), intercambios, custodios, fuerzas de investigación.
Señales de alerta:	Salidas a *mixers*[3] tras recepción de fondos ilícitos; múltiples pequeñas entradas desde direcciones desconocidas y salida en lotes; uso simultáneo de mezcladores e intercambios para *'cash-out'*.
Fuente:	FATF, Europol, AUSTRAC.
Diagrama ilustrativo:	

1 CoinJoin: técnica que combina transacciones de varios usuarios en una sola, ocultando el vínculo entre origen y destino de los fondos.

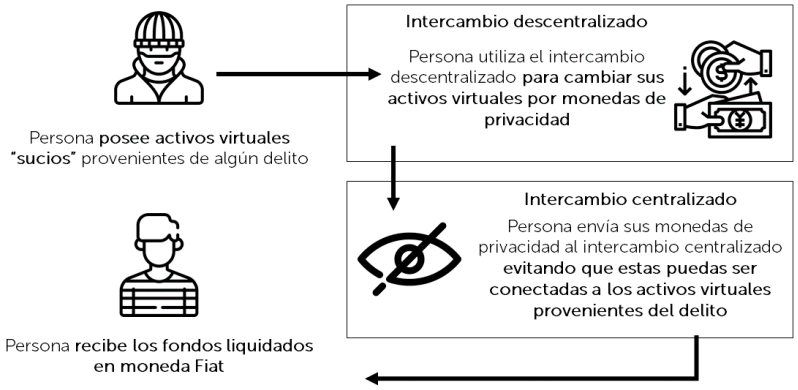
2 Coin-swapping: intercambio directo de una criptomoneda a otra, sin hacer uso de un intercambio regulado. Principalmente utilizado para dificultar la trazabilidad.

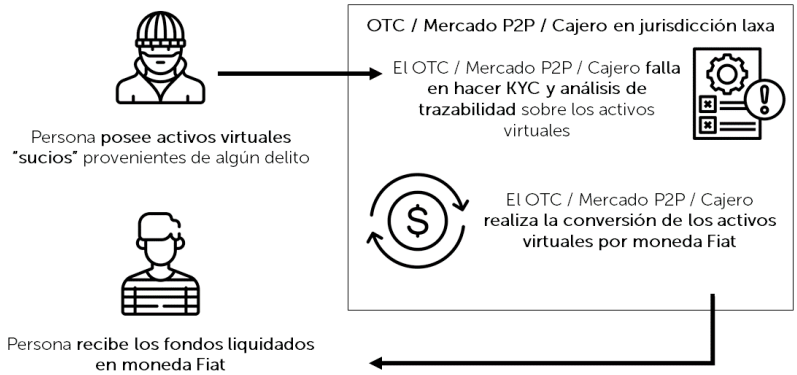
3 Mixers: servicios que mezclan fondos de distintos usuarios para romper la trazabilidad y ocultar el origen de los activos.

Nombre de la Tipología:	**Saltos de cadena (*chain-hopping*[4]) y puentes entre Blockchains (*cross-chain bridges*[5])**
Descripción:	Consiste en transferir valor de forma rápida entre diferentes *blockchains* (por ejemplo, BTC → ETH → BSC → Solana), aprovechando las diferencias en niveles de trazabilidad y controles de cumplimiento. El uso de puentes inter-cadena y *swaps* atómicos permite ocultar el rastro de los fondos, haciendo más compleja la labor de trazar los flujos ilícitos. Esta tipología es cada vez más común en operaciones transnacionales
Sector vulnerado:	Plataformas de finanzas descentralizadas, puentes inter-cadena, DEX (intercambio descentralizado)
Señales de alerta:	Movimientos en cadena múltiples en ventanas muy cortas; uso de puentes con baja gobernanza o sin *KYC* (Conoce tu cliente); actividad hacia/desde cadenas con anonimato relativo.
Fuente:	FATF, Europol.
Diagrama ilustrativo:	

4 Chain-hopping: movimiento rápido de fondos entre diferentes blockchains para dificultar su trazabilidad.

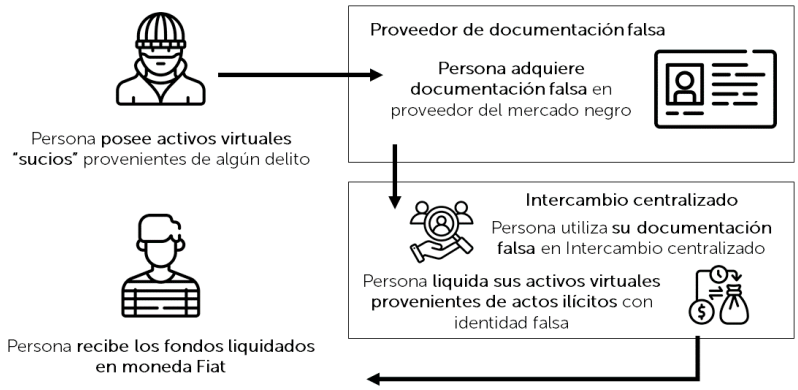
5 Cross-chain bridges: herramientas que permiten transferir activos entre distintas blockchains, facilitando la conversión y el movimiento de valor.

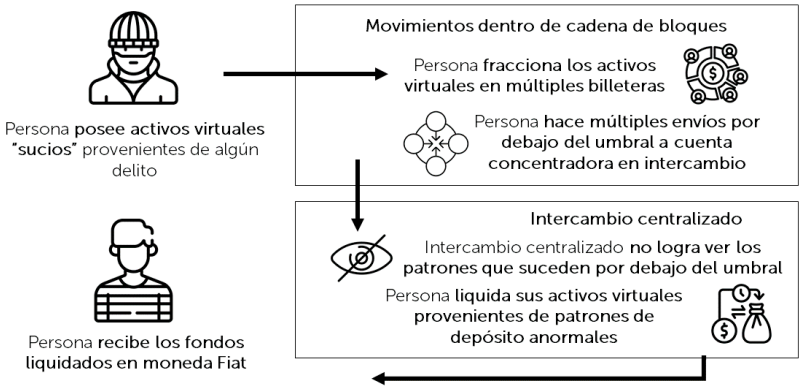
Nombre de la Tipología:	**Monedas de privacidad y herramientas de anonimización**
Descripción:	Empleo de criptomonedas con altos niveles de privacidad (como Monero o Zcash) o herramientas avanzadas de anonimización (tecnologías de conocimiento cero, *zk-techniques*). Estas monedas fueron diseñadas con el objetivo legítimo de proteger la privacidad de los usuarios, pero han sido aprovechadas por grupos criminales para evadir sanciones, ocultar flujos de ganancias ilícitas, y dificultar la trazabilidad en investigaciones.
Sector vulnerado:	PSAV, redes de corresponsalía, controles de sanciones.
Señales de alerta:	Transferencias repetidas hacia/desde direcciones asociadas a privacidad; uso de rutas mixtas (monedas privadas →intercambio) antes del retiro; falta de datos de contraparte.
Fuente:	FATF, Egmont Group.
Diagrama ilustrativo:	

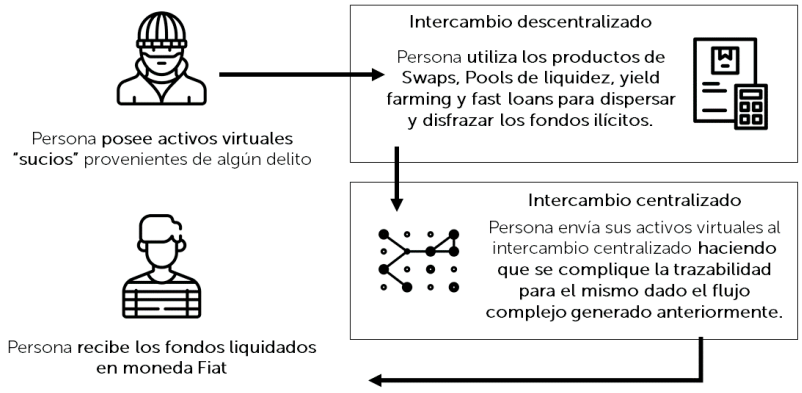
Nombre de la Tipología:	**OTC / Mercados P2P y cajeros**
Descripción:	Venta directa *peer-to-peer*[6] (P2P) o a través de corredores *Over The Counter* (OTC)[7] y uso de cajeros automáticos de criptomonedas para retirar efectivo sin suficientes controles de debida diligencia. Estos mecanismos permiten que fondos ilícitos se conviertan en dinero fiat sin pasar por plataformas reguladas, aprovechando las lagunas normativas en algunos países.
Sector vulnerado:	Proveedores OTC, mercados P2P, operadores de cajeros.
Señales de alerta:	Grandes ventas en OTC por nuevos usuarios; instrucciones de pago en efectivo; uso recurrente de cajeros en jurisdicciones con estándares regulatorios limitados; referencias a 'no *KYC*'.
Fuente:	AUSTRAC, FinCEN.
Diagrama ilustrativo:	

6 Peer-to-peer (P2P): operaciones directas entre usuarios para comprar o vender activos virtuales sin intermediarios ni controles de debida diligencia.

7 Over the Counter (OTC): intercambio privado de grandes volúmenes de activos virtuales fuera de plataformas públicas o reguladas.

Nombre de la Tipología:	**Exchanges centralizados y apertura de cuentas con documentación falsa**
Descripción:	Apertura de cuentas en intercambios con documentación falsa o uso de 'mulas' financieras que prestan su identidad para introducir fondos en entidades reguladas. Este esquema permite a los delincuentes aprovechar la infraestructura regulada y acceder rápidamente a conversiones entre cripto y fiat.
Sector vulnerado:	Intercambios centralizados, servicios de verificación de identidad, corresponsales bancarios.
Señales de alerta:	Depósitos altos de activos virtuales y retiros inmediatos en *fiat*; múltiples cuentas con patrones iguales (misma IP o dispositivo); discrepancias entre perfil del cliente y comportamiento transaccional.
Fuente:	FATF, FinCEN.
Diagrama ilustrativo:	

Nombre de la Tipología:	**Estructuración con múltiples transferencias**
Descripción:	Fragmentación de montos ilícitos en varias micro-transacciones realizadas a través de numerosas direcciones o billeteras, para evadir los umbrales de reporte y dificultar la detección de patrones. Posteriormente, los fondos se consolidan en una cuenta mayor para su conversión o *cash-out*.
Sector vulnerado:	PSAV, servicios de monitoreo, intercambios con reglas de umbral rígidas.
Señales de alerta:	Grandes volúmenes de micro-transacciones seguidos de consolidación; patrones temporales regulares (ej. diarios).
Fuente:	AUSTRAC, Europol.
Diagrama ilustrativo:	

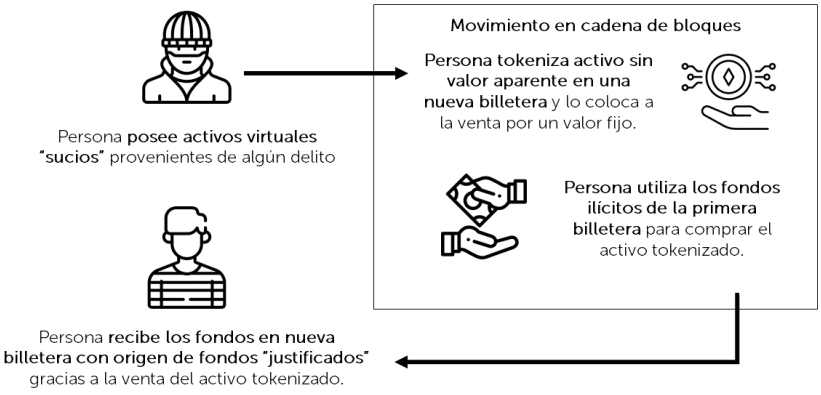
Nombre de la Tipología:	**Encubrimiento mediante Finanzas descentralizadas**
Descripción:	Uso de protocolos descentralizados de finanzas (DeFi) para dispersar y disfrazar fondos ilícitos mediante múltiples *swaps*[8], inversión en pools de liquidez[9] o uso de préstamos flash[10]. Estos mecanismos permiten crear rutas complejas y anónimas sin necesidad de intermediarios centralizados.
Sector vulnerado:	Plataformas DeFi, custodios de claves privadas, proveedores de oráculos[11].
Señales de alerta:	*Swaps* complejos en intercambios centralizados sin actividad económica legítima; uso de *tokens* de baja liquidez; transacciones en contratos nuevos o poco auditados.
Fuente:	FATF, Europol.
Diagrama ilustrativo:	

8 Multiple swaps: serie de intercambios sucesivos entre distintos criptoactivos, generalmente en plataformas DeFi, para ocultar el rastro de los fondos.

9 Pools de liquidez: fondos colectivos en plataformas DeFi donde los usuarios depositan criptoactivos para facilitar intercambios o generar rendimientos.

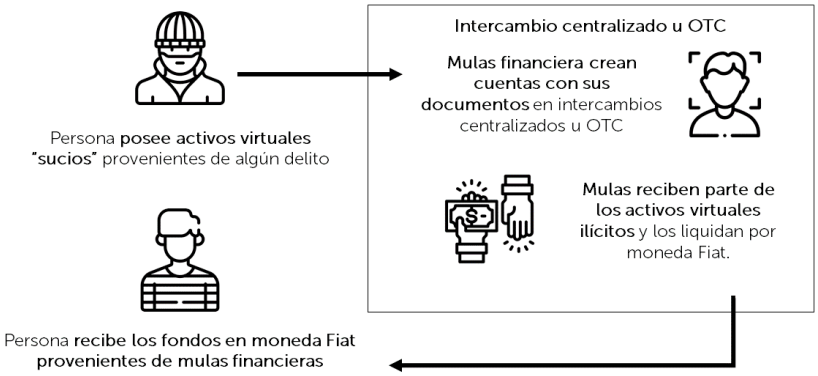
10 Préstamos flash (flash loans): *préstamos* instantáneos sin garantía, ejecutados y devueltos dentro de una misma transacción blo*ckchain*.

11 Proveedor de oráculos: entidad o servicio que suministra datos externos a contratos inteligentes, esenciales para ejecutar operaciones automáticas en DeFi.

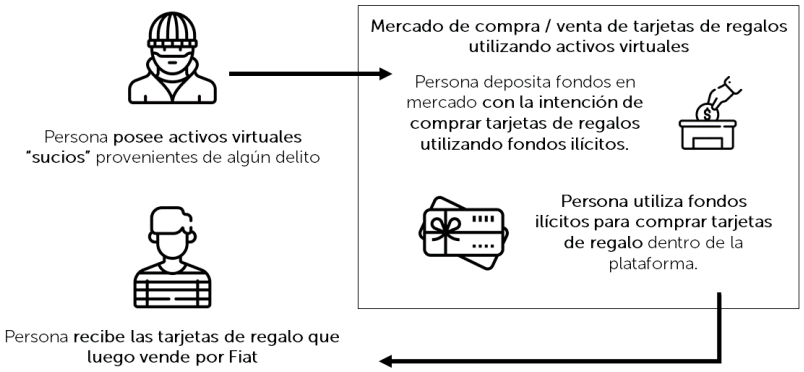
Nombre de la Tipología:	**Uso de NFTs y mercados tokenizados**
Descripción:	Compra-venta artificial de NFTs[12] a precios inflados o ficticios para justificar transferencias de valor ilícitas. Los criminales también tokenizan activos ficticios y realizan ventas coordinadas para dar apariencia de legitimidad, haciendo posteriormente *cash-out* en intercambios.
Sector vulnerado:	Mercados virtuales de NFT, plataformas de subastas, servicios de custodia.
Señales de alerta:	Ventas rápidas entre direcciones vinculadas; patrones de *wash-trading*[13]; discrepancia entre precios y mercado; retiros inmediatos tras ventas.
Fuente:	FATF, Europol.
Diagrama ilustrativo:	

12 NFT (Non-Fungible Token): activo digital único registrado en blockchain que representa la propiedad o autenticidad de un bien digital o físico.

13 Wash-trading: práctica de compra y venta simultánea del mismo activo para simular volumen o inflar artificialmente su valor.

Nombre de la Tipología:	**Redes de mulas y estafas en línea**
Descripción:	Estafadores cobran en activos virtuales (ej. esquemas de inversión fraudulenta, estafas románticas, *phishing*). Posteriormente utilizan redes de mulas financieras y conversiones a *fiat*[14] a través de negociaciones *Over The Counter* (OTC) o intercambios lo que dispersa los fondos y complica la trazabilidad.
Sector vulnerado:	PSAV, plataformas de pago, redes sociales/*marketplaces.*
Señales de alerta:	Clientes que envían fondos bajo presión o instrucciones de terceros; cuentas que actúan repetidamente como intermediarias; cobros por 'recuperación de fondos'.
Fuente:	FinCEN, Egmont Group.
Diagrama ilustrativo:	

14 Fiat: moneda de curso legal emitida por un Estado o banco central, como el dólar estadounidense o el euro.

Nombre de la Tipología:	**Uso de instrumentos prepagados, tarjetas y plataformas de juego**
Descripción:	Conversión de activos virtuales en tarjetas prepago, vales electrónicos o créditos de juegos en línea, que luego pueden ser revendidos o retirados como efectivo. También se observa en casinos en línea y cripto-casinos, donde los fondos ilícitos se introducen como apuestas y luego, se retiran como ganancias aparentemente legítimas.
Sector vulnerado:	Comercios electrónicos, plataformas de juego, emisores de tarjetas prepago, casinos en línea.
Señales de alerta:	Depósitos cripto convertidos en créditos de juego y retiros en cuentas bancarias no relacionadas; compras recurrentes de tarjetas prepago; fraccionamiento de valores.
Fuente:	FATF, Europol, AUSTRAC.
Diagrama ilustrativo:	

FUENTES CONSULTADAS:

FATF — Virtual assets: red flag indicators of Money Laundering and Terrorist Financing (fatf-gafi.org).

AUSTRAC — Indicators of suspicious activity for the digital currency (cryptocurrency) sector (austrac.gov.au).

Europol — Cryptocurrencies: tracing the evolution of criminal finances (Europol).

Egmont Group — Report on abuse of Virtual Assets for Terrorist Financing Purposes (egmontgroup.org).

FinCEN — FinCEN issues notice on the use of convertible virtual currency kiosks for scam payments and other illicit activity (FinCEN.gov).

COMPILACIÓN DE TIPOLOGÍAS RELACIONADAS AL USO DE ACTIVOS VIRTUALES

OCTUBRE 2025