



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:.....	4
Tipologías relacionadas al uso de activos virtuales	5
Mixers / CoinJoin (servicios de mezcla)	5
Saltos de cadena (chain-hopping) y puentes entre Blockchains (cross-chain bridges)	6
Monedas de privacidad y herramientas de anonimización	7
OTC / Mercados P2P y cajeros.....	8
Exchanges centralizados y apertura de cuentas con documentación falsa	9
Estructuración con múltiples transferencias.....	10
Encubrimiento mediante Finanzas descentralizadas	11
Uso de NFTs y mercados tokenizados	12
Redes de mulas y estafas en línea	13
Uso de instrumentos prepagados, tarjetas y plataformas de juego	14
Fuentes consultadas	15

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.

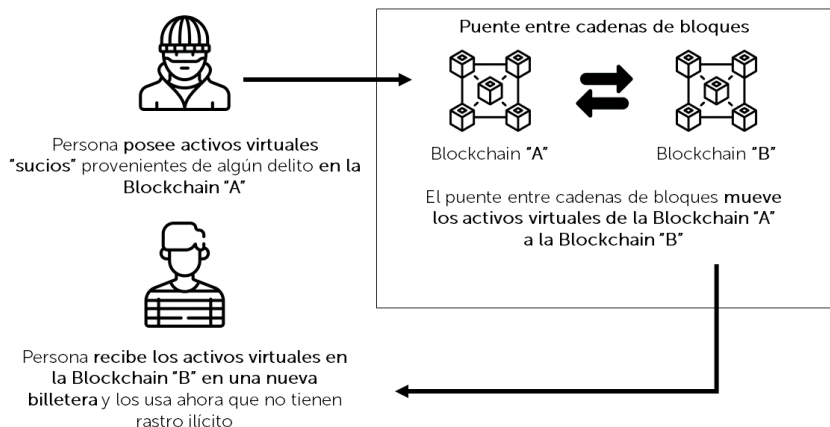
TIPOLOGÍAS ASOCIADAS A ACTIVOS VIRTUALES Y LAVADO DE DINERO Y ACTIVOS:

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 <i>blockchain</i>, dificultando la identificación del beneficiario final. Existen tanto mezcladores centralizados como técnicas descentralizadas (<i>CoinJoin</i>¹, <i>coin-swapping</i>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 <i>mixers</i> 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, AUSTAC.
Diagrama ilustrativo:	<pre> graph LR A[Persona posee activos virtuales "sucios" provenientes de algún delito] --> B[Persona transfiere activos virtuales a servicio de Mezclas / Tumbler / CoinJoin] B --> C[Servicio de Mezclador] C --> D[Servicio mezcla los activos virtuales sucios perdiendo la trazabilidad] D --> E[Persona recibe los activos virtuales en una nueva billetera y los usa ahora que no tienen rastro ilícito] </pre>

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

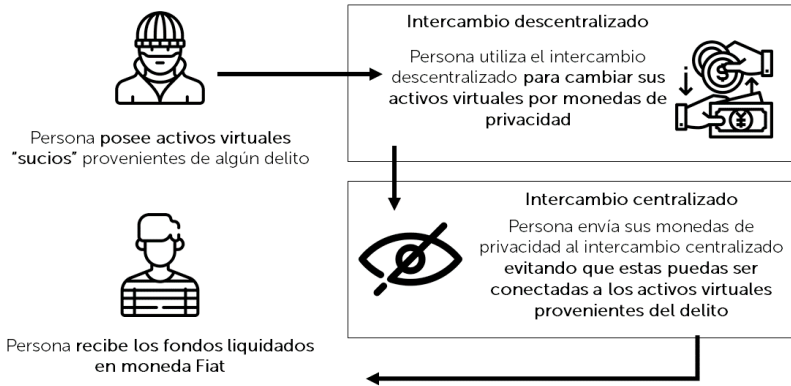
2 Coin-swapping: intercambio directo de una criptomoneda a otra, sin hacer uso de un intercambio regulado. Principalmente utilizado para dificultar la trazabilidad.

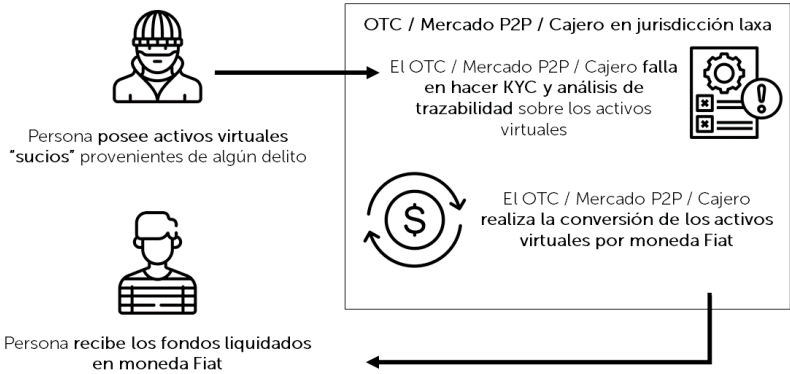
3 Mixers: servicios que mezclan fondos de distintos usuarios para romper la trazabilidad y ocultar el origen de los activos.

Nombre de la Tipología:	Salto de cadena (<i>chain-hopping</i>⁴) y puentes entre Blockchains (<i>cross-chain bridges</i>⁵)
Descripción:	Consiste en transferir valor de forma rápida entre diferentes <i>blockchains</i> (por ejemplo, BTC → ETH → BSC → Solana), aprovechando las diferencias en niveles de trazabilidad y controles de cumplimiento. El uso de puentes inter-cadena y <i>swaps</i> 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:	 El diagrama ilustra el proceso de salto de cadena y el uso de puentes entre blockchains. A la izquierda, una persona con un casco (representando un actor ilícito) posee activos virtuales "sucios" en la Blockchain "A". Estos activos se transfieren a un "Punto de conexión entre cadenas de bloques" (puente) que conecta Blockchain "A" y Blockchain "B". El puente mueve los activos virtuales de Blockchain "A" a Blockchain "B". Finalmente, la persona recibe los activos virtuales en Blockchain "B" en una nueva billetera, lo que oculta el rastro ilícito original.

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

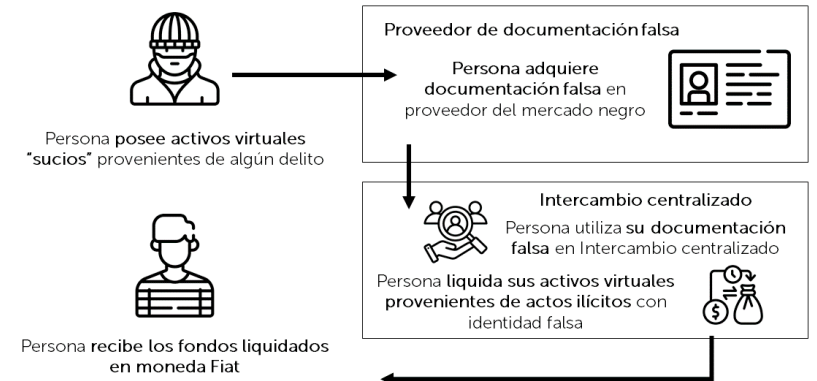
5 Cross-chain bridges: herramientas que permiten transferir activos entre distintas blockchains, facilitando la conversión y el movimiento de valor.

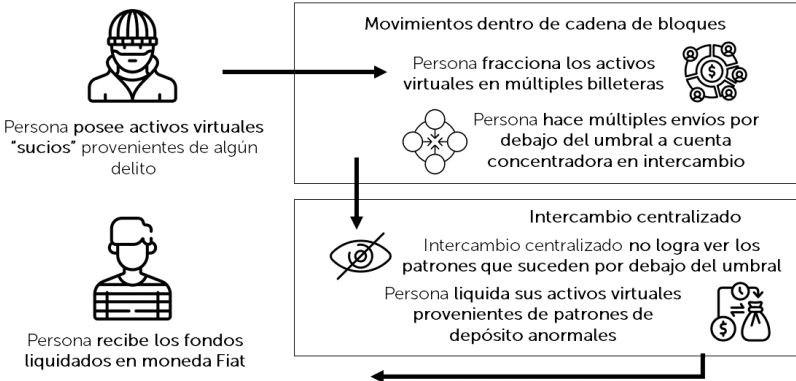
Nombre de la Tipología:	Monedas de privacidad y herramientas de anonimización
Descripción:	Empleo de criptomonedas con altos niveles de privacidad (como Monero o Zcash) o herramientas avanzadas de anonimización (tecnologías de conocimiento cero, <i>zk-techniques</i>). Estas monedas fueron diseñadas con 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 corresponsalia, 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:	 El diagrama ilustra el flujo de dinero desde activos virtuales 'sucios' hasta moneda fiat. Comienza con una persona que posee activos virtuales 'sucios' provenientes de algún delito. Esta persona utiliza un intercambio descentralizado para cambiar sus activos virtuales por monedas de privacidad. Luego, estas monedas de privacidad son enviadas a un intercambio centralizado, donde se evitan ser conectadas a los activos virtuales provenientes del delito. Finalmente, la persona recibe los fondos liquidados en moneda fiat. <pre> graph TD A[Persona posee activos virtuales "sucios" provenientes de algún delito] --> B[Intercambio descentralizado Persona utiliza el intercambio descentralizado para cambiar sus activos virtuales por monedas de privacidad] B --> C[Intercambio centralizado Persona envía sus monedas de privacidad al intercambio centralizado evitando que estas puedan ser conectadas a los activos virtuales provenientes del delito] C --> D[Persona recibe los fondos liquidados en moneda Fiat] </pre>

Nombre de la Tipología:	OTC / Mercados P2P y cajeros
Descripción:	Venta directa <i>peer-to-peer</i> ⁶ (P2P) o a través de corredores <i>Over The Counter</i> (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:	 El diagrama ilustra el flujo de fondos ilícitos desde una persona que posee activos virtuales 'sucios' (representada por un icono de un hombre con un casco) a un OTC / Mercado P2P / Cajero en jurisdicción laxa. En esta entidad, se falla en hacer KYC y análisis de trazabilidad sobre los activos virtuales (representado por un icono de una computadora con un signo de exclamación). Posteriormente, se realiza la conversión de los activos virtuales por moneda Fiat (representado por un icono de una moneda con un signo de dólar). Finalmente, la persona recibe los fondos liquidados en moneda Fiat (representado por un icono de un hombre con una pila de dinero).

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 <i>fiat</i> ; múltiples cuentas con patrones iguales (misma IP o dispositivo); discrepancias entre perfil del cliente y comportamiento transaccional.
Fuente:	FATF, FinCEN.
Diagrama ilustrativo:	 El diagrama ilustra el flujo de un esquema de lavado de dinero a través de un exchange centralizado. Comienza con una persona que posee activos virtuales 'sucios' provenientes de un delito. Esta persona adquiere documentación falsa de un proveedor del mercado negro. Luego, utiliza esta documentación falsa para abrir una cuenta en un intercambio centralizado. Finalmente, liquida sus activos virtuales en moneda fiat, recibiendo los fondos. <pre> graph TD A[Persona posee activos virtuales "sucios" provenientes de algún delito] --> B[Proveedor de documentación falsa Persona adquiere documentación falsa en proveedor del mercado negro] B --> C[Intercambio centralizado Persona utiliza su documentación falsa en Intercambio centralizado Persona liquida sus activos virtuales provenientes de actos ilícitos con identidad falsa] C --> D[Persona recibe los fondos liquidados en moneda Fiat] </pre>

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 <i>cash-out</i> .
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:	 El diagrama ilustra el proceso de estructuración con múltiples transferencias. Comienza con una persona que posee activos virtuales "sucios" provenientes de algún delito. Estos activos se fragmentan en múltiples billeteras y se envían por debajo del umbral a una cuenta concentradora en un intercambio. El intercambio centralizado no logra ver los patrones que suceden por debajo del umbral. Finalmente, la persona liquida sus activos virtuales provenientes de patrones de depósito anormales, recibiendo los fondos liquidados en moneda Fiat.

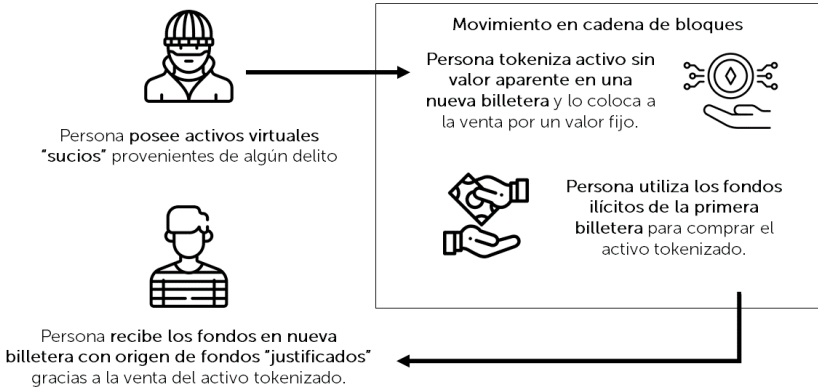
Nombre de la Tipología:	Encubrimiento mediante Finanzas descentralizadas
Descripción:	Uso de protocolos descentralizados de finanzas (DeFi) para dispersar y disfrazar fondos ilícitos mediante múltiples <i>swaps</i> ⁸ , inversión en pools de liquidez ⁹ o uso de préstamos flash ¹⁰ . Estos mecanismos permiten 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:	<i>Swaps</i> complejos en intercambios centralizados sin actividad económica legítima; uso de <i>tokens</i> de baja liquidez; transacciones en contratos nuevos o poco auditados.
Fuente:	FATF, Europol.
Diagrama ilustrativo:	Diagrama ilustrativo del encubrimiento mediante finanzas descentralizadas: Persona posee activos virtuales "sucios" provenientes de algún delito (representado por un icono de una persona con un casco). - Los activos se envían a un Intercambio descentralizado, donde se utilizan productos de Swaps, Pools de liquidez, yield farming y fast loans para dispersar y disfrazar los fondos ilícitos. - Los activos se envían a un Intercambio centralizado, donde se hace que se complique la trazabilidad para el mismo dado el flujo complejo generado anteriormente. - Finalmente, la persona recibe los fondos liquidados en moneda Fiat (representado por un icono de una persona con un sombrero).

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 blockchain.

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

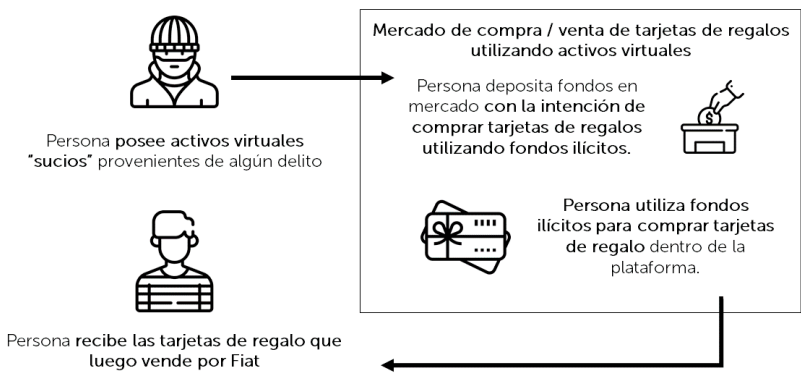
Nombre de la Tipología:	Uso de NFTs y mercados tokenizados
Descripción:	Compra-venta artificial de NFTs ¹² a precios inflados o ficticios para justificar transferencias de valor ilícitas. Los criminales también tokenizan activos ficticios y realizan ventas coordinadas para dar apariencia de legitimidad, haciendo posteriormente <i>cash-out</i> en intercambios.
Sector vulnerado:	Mercados virtuales de NFT, plataformas de subastas, servicios de custodia.
Señales de alerta:	Ventas rápidas entre direcciones vinculadas; patrones de <i>wash-trading</i> ¹³ ; discrepancia entre precios y mercado; retiros inmediatos tras ventas.
Fuente:	FATF, Europol.
Diagrama ilustrativo:	 Movimiento en cadena de bloques Persona posee activos virtuales "sucios" provenientes de algún delito Persona tokeniza activo sin valor aparente en una nueva billetera y lo coloca a la venta por un valor fijo. Persona utiliza los fondos ilícitos de la primera billetera para comprar el activo tokenizado. Persona recibe los fondos en nueva billetera con origen de fondos "justificados" gracias a la venta del activo tokenizado.

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, <i>phishing</i>). Posteriormente utilizan redes de mulas financieras y conversiones a fiat ¹⁴ a través de negociaciones <i>Over The Counter</i> (OTC) o intercambios lo que dispersa los fondos y complica la trazabilidad.
Sector vulnerado:	PSAV, plataformas de pago, redes sociales/ <i>marketplaces</i> .
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:	El diagrama ilustra el flujo de dinero en redes de mulas y estafas en línea. Se muestra a una persona con un casco y una máscara (representando un estafador) que posee activos virtuales 'sucios' provenientes de algún delito. Esta persona envía los fondos a un intercambio centralizado u OTC. En este intercambio, las mulas financieras crean cuentas con sus documentos en intercambios centralizados u OTC. Las mulas reciben parte de los activos virtuales ilícitos y los liquidan por moneda Fiat. Finalmente, la persona recibe los fondos en moneda Fiat provenientes de las mulas financieras.

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 retirados en cuentas bancarias no relacionadas; compras recurrentes de tarjetas prepago; fraccionamiento de valores.
Fuente:	FATF, Europol, AUSTAC.
Diagrama ilustrativo:	 Diagrama ilustrativo del uso de instrumentos prepagados: - Persona posee activos virtuales "sucios" provenientes de algún delito. - Mercado de compra / venta de tarjetas de regalos utilizando activos virtuales. - Persona deposita fondos en mercado con la intención de comprar tarjetas de regalos utilizando fondos ilícitos. - Persona utiliza fondos ilícitos para comprar tarjetas de regalo dentro de la plataforma. - Persona recibe las tarjetas de regalo que luego vende por Fiat.

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](https://europol.europa.eu)).

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](https://fincen.gov)).



**COMPILACIÓN DE TIPOLOGÍAS
RELACIONADAS AL USO DE
ACTIVOS VIRTUALES**

OCTUBRE 2025
