GALINDO
CONSULTORES LEGALES Y PERITOS JUDICIALES
BENLLOCH

GUÍA PROFESIONAL / INVESTIGACIÓN FORENSE

INVESTIGACIÓN FINANCIERA Y RUTA DEL DINERO EN CIBERESTAFAS

Metodología operativa y pericial para localizar, reconstruir, asegurar y recuperar activos



CIBERFRAUDE · CUENTAS MULA · PSP Y FINTECH · CRIPTOACTIVOS
SOCIEDADES PANTALLA · OSINT FINANCIERO · COOPERACIÓN INTERNACIONAL

Juan Carlos Galindo

Director de Galindo-Benlloch

EDICIÓN VISUAL · 16 DE OCTUBRE DE 2026

Delitos tecnológicos · blanqueo de capitales · investigación patrimonial

Documento técnico para uso profesional y formativo; adaptado al caso y al marco legal aplicable.

Resumen ejecutivo

La investigación financiera eficaz no comienza cuando ya se ha identificado al autor: comienza al mismo tiempo que la investigación del hecho. En ciberestafas, el tiempo entre la transferencia de la víctima y la dispersión de los fondos suele ser crítico. Por ello, la metodología de esta guía parte de una premisa: reconstruir la ruta del dinero en paralelo con la reconstrucción técnica y criminal del fraude.

El objetivo operativo es transformar movimientos aparentemente fragmentados —transferencias, tarjetas, cuentas de pago, fintech, exchanges, wallets, retiradas en efectivo, sociedades y testaferros— en una secuencia probatoria comprensible, verificable y jurídicamente útil. La investigación debe identificar no solo el destino inmediato del dinero, sino también las capas posteriores de dispersión, conversión y ocultación, los puntos de control institucional y los activos finales susceptibles de inmovilización, decomiso o restitución.

> **ACTUALIZACIÓN · OCTUBRE DE 2026**
>
> Actualizada al 16 de octubre de 2026: Real Decreto-ley 25/2026, Real Decreto 813/2026, verificación del beneficiario, MiCA, prueba electrónica y recuperación de activos. Se identifican expresamente las disposiciones ya vigentes y las pendientes de aplicación. [S11–S18]

> **PRINCIPIO RECTOR**
>
> Seguir el dinero es una investigación autónoma y simultánea: identifica beneficio criminal, intermediarios, nodos de control y patrimonio. MONEYVAL subraya que las investigaciones financieras deben realizarse simultáneamente con las investigaciones criminales para rastrear el beneficio material.

Mapa metodológico en diez fases

01. Preservación inmediata de evidencias y delimitación temporal del fraude.
02. Reconstrucción del pago inicial y de los identificadores financieros y tecnológicos.
03. Identificación de cuentas receptoras, titulares, autorizados, beneficiarios reales y dispositivos asociados.
04. Expansión del grafo: transferencias sucesivas, PSP, fintech, tarjetas, efectivo y criptoactivos.
05. Clasificación funcional de intervinientes: víctima, mula, facilitador, controlador, blanqueador profesional y beneficiario.
06. Investigación patrimonial paralela y localización de activos.
07. Medidas urgentes de bloqueo, inmovilización, embargo o aseguramiento cuando procedan.
08. Cooperación nacional e internacional, formal e informal, según el dato y la finalidad probatoria.
09. Construcción de una matriz probatoria reproducible: fuente, fecha, identificador, inferencia y nivel de certeza.
10. Recuperación, decomiso y restitución: diseñar desde el inicio una salida para el dinero localizado.

Cómo usar esta guía

Dirigida a peritos, investigadores, equipos de compliance, abogados, fiscales, policías y formadores. Cada técnica requiere habilitación legal y respeto a las reglas de obtención de prueba.

CONTENIDOS

Índice de la guía

16 capítulos de referencia y 19 anexos operativos: procedimientos, plantillas, casos y control de calidad.

CAPÍTULOS

01 Principios de investigación financiera

02 Marco jurídico y estándares de referencia

03 Modelo operativo: de la ciberestafa al activo recuperable

04 Preservación, fuentes y cadena de trazabilidad

05 Investigación bancaria, cuentas mula y beneficiarios

06 PSP, fintech, tarjetas y pagos instantáneos

07 Criptoactivos y análisis blockchain

08 Sociedades pantalla, testaferros y titularidad real

09 OSINT financiero y enriquecimiento de inteligencia

10 Investigación patrimonial y localización de activos

11 Cooperación nacional e internacional

12 Medidas cautelares, decomiso, recuperación y restitución

13 Metodología pericial y estándares de evidencia

14 Matrices, plantillas y checklists

15 Casos tipo y errores frecuentes

16 Bibliografía y fuentes oficiales

ANEXOS

I Modelo de conclusión pericial financiera

II Vocabulario operativo

III Ficha de control de calidad del informe

IV Playbook de actuación en las primeras 72 horas

V Investigación de blanqueadores profesionales, hawala y redes de compensación

VI Guía avanzada de análisis de cuentas mula

VII Requerimientos de información: modelos de contenido

VIII Analítica cuantitativa de flujos

IX Criptoactivos: playbook de investigación por escenarios

X Sociedades, facturación y blanqueo basado en comercio

XI Calidad, contradicción y defensa de la pericial

XII Programa formativo de 90 minutos basado en la guía

XIII Caso práctico integral

XIV Glosario ampliado de evidencias y campos

XV Principios finales de la metodología

XVI Indicadores de investigación por instrumento financiero

XVII Diccionario de datos para investigación de grandes volúmenes

XVIII Modelo de informe de situación y recuperación de activos

XIX Protocolo de revisión independiente

Abreviaturas y fuentes: en la bibliografía y en los Anexos II y XIV.

1. Principios de investigación financiera

1.1. Investigación paralela, no residual

La aproximación clásica que reserva la investigación patrimonial para el final del procedimiento pierde oportunidades. El dinero puede atravesar varias jurisdicciones, convertirse en criptoactivos, fragmentarse entre cuentas instrumentales o salir en efectivo antes de que exista una identificación completa de todos los responsables. La investigación financiera debe comenzar con el primer dato económico verificable y avanzar en paralelo a la atribución penal.

MONEYVAL identifica como elementos esenciales el acceso oportuno a información bancaria, registros mercantiles y de titularidad real, la disponibilidad de técnicas especiales de investigación y la capacidad de cooperación transfronteriza. La guía FATF de recuperación de activos de 2025 refuerza esta visión: localizar y asegurar activos con rapidez es parte central de una política efectiva de recuperación, no una consecuencia tardía.

1.2. Hipótesis, indicios y conclusiones

En una pericial o informe de investigación debe distinguirse entre hecho observado, dato obtenido de tercero, inferencia analítica e hipótesis pendiente de contraste. Un ingreso en una cuenta no acredita por sí mismo conocimiento del origen ilícito; del mismo modo, ser titular formal no identifica necesariamente al controlador efectivo. La fuerza de la atribución surge de la convergencia: patrones de movimientos, comunicaciones, dispositivos, geolocalización legítimamente obtenida, KYC, accesos, IP, beneficiarios posteriores, retiradas y relaciones societarias.

> **REGLA DE REDACCIÓN PROBATORIA**
>
> No escribir «X blanqueó el dinero» cuando la evidencia demuestra únicamente que una cuenta a su nombre recibió y transfirió fondos. Separar siempre: hecho comprobado → inferencia → elementos que faltan para confirmar o descartar la hipótesis.

1.3. Cinco objetivos simultáneos

- Atribución financiera: quién recibe, controla, ordena, convierte, retira o beneficia.
- Trazabilidad: por dónde pasa el valor, con qué velocidad, instrumentos y jurisdicciones.
- Contexto: por qué esos movimientos son o no coherentes con actividad económica legítima.
- Aseguramiento: qué activos pueden inmovilizarse antes de su desaparición.
- Restitución: cómo documentar el nexo entre pérdida de la víctima y activo recuperado.

2. Marco jurídico y estándares de referencia

2.1. España

La Ley 10/2010 constituye el eje preventivo español en PBC/FT, con actualización del texto consolidado publicada el 30 de septiembre de 2026 a raíz del Real Decreto-ley 25/2026, vigente desde el 1 de octubre. El Real Decreto 304/2014 sigue siendo el desarrollo reglamentario; su reforma por el Real Decreto 813/2026 tiene entrada en vigor general prevista el 28 de octubre. El análisis penal del blanqueo requiere acudir al Código Penal y las diligencias coercitivas a las normas procesales correspondientes. [S6, S7, S11, S15, S18]

En la práctica investigadora, la normativa preventiva es relevante porque determina qué información deben recabar y conservar determinadas entidades, cómo deben identificar al cliente y al titular real, qué operaciones deben

examinarse especialmente y qué documentación puede existir en un expediente KYC/AML. Sin embargo, el acceso del investigador externo a esa información exige siempre base jurídica o canal procesal adecuado.

2.2. Unión Europea 2024-2027

El paquete europeo de PBC/FT modifica el marco institucional y material. El Reglamento (UE) 2024/1624 será directamente aplicable con carácter general desde el 10 de julio de 2027; la Directiva (UE) 2024/1640 establece mecanismos que han de adoptar los Estados miembros; y el Reglamento (UE) 2024/1620 crea la autoridad europea AMLA. En materia de transferencias y criptoactivos, el Reglamento (UE) 2023/1113 y las directrices de la EBA sobre la travel rule siguen siendo referencias esenciales. Las fechas de aplicación deben diferenciarse del momento de publicación. [S5, S8, S9]

2.3. Estándares internacionales

- FATF/GAFI: Recomendaciones y guías de investigación financiera, cooperación y recuperación de activos.



Recreación conceptual generada con IA: conexiones financieras transfronterizas. No representa una investigación real.

- Egmont Group: cooperación entre unidades de inteligencia financiera.
- INTERPOL y UNODC: cooperación policial, análisis y asistencia internacional.
- StAR (Banco Mundial/UNODC): manuales prácticos de rastreo y recuperación de activos.
- MONEYVAL: evaluación de efectividad y principios para investigaciones financieras sistemáticas.

2.4. Real Decreto-ley 25/2026: modificaciones ya vigentes

El Real Decreto-ley 25/2026, de 29 de septiembre (BOE de 30 de septiembre), introdujo mediante su disposición final primera cambios en la Ley 10/2010, en vigor desde el 1 de octubre de 2026. Actualiza las definiciones de criptoactivo, proveedor de servicios de criptoactivos y dirección autoalojada; modifica la identificación de sujetos obligados del artículo 2.1.z), las relaciones de corresponsalía del artículo 13 y el régimen de determinadas infracciones vinculadas al Reglamento (UE) 2023/1113. Estos cambios son relevantes para identificar proveedores, entidades intervinientes y obligaciones de trazabilidad. [S18]

2.5. Real Decreto 813/2026: reforma reglamentaria pendiente de vigencia general

El Real Decreto 813/2026, de 7 de octubre, publicado en el BOE de 8 de octubre, modifica el Reglamento aprobado por el Real Decreto 304/2014. Su entrada en vigor general está fijada para el 28 de octubre de 2026; a la fecha de esta edición no deben presentarse sus nuevas reglas como ya exigibles. La reforma incorpora parcialmente la Directiva (UE) 2024/1640. [S11]

Entre las novedades de interés investigativo figuran la identificación formal, también en operaciones realizadas en cajeros de criptoactivos; la adaptación al DNI digital; las garantías de identificación no presencial; las reglas de diligencia debida ante indicios; la documentación del análisis de riesgos; y políticas en materia de sanciones y contramedidas financieras. Estas obligaciones permiten entender qué registros pueden obrar en poder de los sujetos obligados, pero no facultan por sí solas al investigador privado para obtener información protegida. [S11]

El real decreto prevé plazos específicos: seis meses desde su entrada en vigor para determinadas adaptaciones en el sector del juego; nueve meses para comunicar el nombramiento de representante ante el SEPBLAC en los supuestos de la disposición transitoria segunda; y dieciocho meses desde la publicación para la aplicabilidad de las modificaciones de los artículos 6.1.a) y 28 sobre identificación electrónica y su conservación. [S11]

3. Modelo operativo: de la ciberestafa al activo recuperable

3.1. La cadena de valor criminal

Una ciberestafa puede analizarse como una cadena de valor: captación o engaño → instrucción de pago → recepción → dispersión → estratificación → integración o extracción. Cada fase genera rastros distintos. El investigador debe construir un modelo temporal que una el evento técnico con el evento financiero: correo, mensajería, llamada, web falsa, autenticación, orden de transferencia, abono, nueva transferencia, retirada, compra de criptoactivos o adquisición de bienes.



FIGURA 02 · La cadena del fraude: del evento técnico a la transformación patrimonial.

3.2. Línea temporal maestra

Fecha/hora	Evento	Importe	Identificador	Fuente	Valor probatorio
T0	Engaño / instrucción	—	mensaje, URL, llamada	evidencia digital	contexto
T1	Orden de pago	€	IBAN / referencia	banco víctima	origen
T2	Abono receptor	€	IBAN / cuenta pago	entidad receptora	nodo 1
T3	Dispersión	€	destinos sucesivos	extractos / PSP	nodos 2+
T4	Conversión / retiro	€ / cripto	wallet / ATM / tarjeta	CASP / banco	transformación
T5	Activo final	valor	vehículo / inmueble / wallet	registro / custodia	recuperación

3.3. Grafo de flujo

Cuando existen más de dos saltos, una tabla lineal deja de ser suficiente. Conviene representar cada cuenta, wallet, tarjeta, sociedad o persona como un nodo y cada transferencia como una arista. El grafo debe conservar metadatos mínimos: importe, fecha y hora, moneda, concepto, referencia bancaria, entidad, país, dirección blockchain, hash de transacción y fuente documental.

> **OBJETIVO ANALÍTICO**
> El grafo no prueba por sí mismo una relación criminal. Sirve para localizar concentradores, nodos de paso, puntos de conversión, ciclos, fan-in/fan-out y activos finales que después deben contrastarse con evidencia independiente.

4. Preservación, fuentes y cadena de trazabilidad

4.1. Prioridad de preservación

- Justificantes originales de transferencia y extractos con referencia completa.
- Cabeceras completas de correo y archivos originales .eml/.msg cuando existan.
- Capturas acompañadas, cuando sea posible, de exportaciones o evidencias nativas.
- Conversaciones de mensajería con fecha y hora, identificadores de cuenta y archivos adjuntos.
- URL completas, dominios, certificados, resoluciones DNS históricas obtenidas de fuentes legítimas.
- IBAN, BIC/SWIFT, identificadores de pago, identificadores de comercio (merchant ID), referencias de tarjeta y PSP.
- Direcciones de criptoactivos y hashes completos de transacción; nunca trabajar solo con capturas.
- Documentación KYC o de acceso únicamente mediante canal legalmente habilitado.

4.2. Integridad y reproducibilidad

Toda evidencia digital usada en una pericial debe poder ser identificada y, cuando proceda, verificada mediante hash, metadatos y registro de adquisición. En fuentes web u OSINT debe conservarse la URL, la fecha y hora de consulta, el contenido relevante y el método de preservación. La reproducibilidad no significa que una página siga disponible meses después; significa que el perito puede explicar qué vio, cuándo, cómo lo obtuvo y qué controles aplicó.



FIGURA 03 · Trazabilidad de fuentes y construcción responsable de conclusiones.

4.3. Matriz de fuentes

Fuente	Dato típico	Riesgo	Control recomendado
Banco/PSP	titularidad, movimientos, KYC, accesos	dato incompleto o periodo insuficiente	requerimiento preciso + rango temporal
CASP/exchange	KYC, depósitos, retiros, wallets, IP	jurisdicción / custodia	identificar entidad legal y canal de cooperación
Blockchain	transacciones públicas	atribución errónea de wallet	separar trazabilidad de identidad
Registro mercantil	administradores, cuentas, actos	titular formal ≠ controlador	cruzar con titularidad real y flujos
OSINT	dominios, perfiles, anuncios, relaciones	fuente volátil o falsa	preservar y corroborar
Dispositivo	logs, apps, credenciales, sesiones	alteración / contexto	adquisición forense y cadena de custodia

5. Investigación bancaria, cuentas mula y beneficiarios

5.1. Qué es una cuenta mula desde el punto de vista investigativo

La expresión «cuenta mula» describe una función dentro del flujo y no debe sustituir al análisis individual de conocimiento, control y participación. Puede existir captación consciente, captación mediante engaño, cesión negligente de credenciales, control por tercero o suplantación. La investigación debe determinar quién abrió la cuenta, quién la controlaba durante el periodo relevante, quién ordenó los movimientos y quién obtuvo beneficio.



FIGURA 04 · Seis preguntas para distinguir titularidad, control y grado de participación.

5.2. Señales de interés

- Cuenta de reciente apertura con ingreso extraordinario y dispersión casi inmediata.
- Entrada seguida de múltiples transferencias de menor importe o envíos a varios países.
- Cambio súbito de comportamiento respecto del histórico del cliente.
- Accesos desde dispositivos, IP o ubicaciones incompatibles con el patrón ordinario, cuando esos datos sean legalmente accesibles.
- Transferencias a exchanges, plataformas de pago o adquirentes seguidas de retirada o conversión.

- Retiradas en efectivo próximas temporalmente al abono.
- Uso coordinado de varias cuentas con conceptos, importes o horarios similares.
- Coincidencias de teléfono, correo, dispositivo, dirección o beneficiario entre múltiples cuentas.

5.3. Datos a solicitar o preservar

Bloque	Información de interés	Finalidad
Identidad/KYC	documento, dirección, teléfono, correo, fecha alta, canal alta, titular real	atribución y contexto
Cuenta	IBAN/identificador, autorizados, vinculadas, fechas, estado	mapa de relaciones
Movimientos	extracto completo, ordenante/beneficiario, referencia, canal, concepto	trazabilidad
Acceso	logs disponibles, dispositivo, IP, autenticación, cambios de credenciales	control efectivo
Tarjetas	PAN tokenizado/identificador, tarjetas virtuales, wallets móviles, ATM/merchant	extracción o gasto
Alertas AML	solo mediante canal legal procedente y respetando restricciones	contexto institucional

5.4. Fan-out, fan-in y velocidad

Tres métricas simples mejoran mucho la lectura del flujo: velocidad de salida después del abono, número de destinos y porcentaje del importe original que permanece. Una cuenta que recibe 50.000 euros y distribuye el 98 % en 25 minutos a seis destinos presenta un patrón analíticamente distinto de una cuenta comercial que conserva saldo y opera con contrapartes históricas. Estas métricas son descriptivas; su interpretación debe incorporar contexto.

6. PSP, fintech, tarjetas y pagos instantáneos

6.1. No limitarse al IBAN

Las arquitecturas modernas de pago introducen capas: bancos patrocinadores, entidades de dinero electrónico, PSP, procesadores, adquirentes, wallets móviles y cuentas virtuales. El identificador visible para la víctima puede no coincidir con el identificador interno que permite seguir la operación. Deben conservarse todas las referencias técnicas disponibles.



FIGURA 05 · Modelo ilustrativo de capas e identificadores de pago.

6.2. Pagos instantáneos

La instantaneidad reduce el margen de reacción. La investigación debe registrar con precisión hora y zona horaria y activar cuanto antes los canales bancarios, policiales y judiciales disponibles. El objetivo inicial no es demostrar toda la estructura, sino impedir que el activo deje de ser localizable.

6.3. Tarjetas y comercios

- Identificar si el movimiento es compra, retirada, wallet, transferencia card-to-card o financiación.
- Solicitar merchant/acquirer, fecha, hora, localización, referencia y datos de autenticación disponibles.
- Distinguir tarjeta física, virtual y tokenizada en wallet móvil.
- Relacionar reembolsos, chargebacks y devoluciones con la ruta principal.

6.4. Verificación del beneficiario y pagos inmediatos en euros

En la zona del euro, desde el 9 de octubre de 2025 se exige, para los proveedores comprendidos en el calendario aplicable, la posibilidad de enviar transferencias inmediatas en euros y un servicio de verificación del beneficiario (Verification of Payee, VoP). Este compara el identificador de cuenta con el nombre facilitado y devuelve un resultado de coincidencia, aproximación o discrepancia antes de cursar el pago. No elimina el riesgo de fraude ni sustituye la diligencia del ordenante. Las entidades de pago y de dinero electrónico cuentan con hitos específicos de adaptación, que deben verificarse por tipo de proveedor. [S12]

En fraudes BEC o de sustitución de IBAN, debe preservarse, cuando se disponga lícitamente de ello, la información relativa al resultado de la verificación mostrada al pagador, las advertencias y la decisión final. Esos datos ayudan a contextualizar cómo se autorizó la operación, pero no prueban por sí solos quién cometió el engaño.

7. Criptoactivos y análisis blockchain

7.1. Trazabilidad no equivale a identidad

Las blockchains públicas pueden permitir seguir transacciones entre direcciones, pero una dirección no identifica por sí sola a una persona. La atribución requiere fuentes adicionales: datos de un CASP, dispositivos, comunicaciones, documentación KYC, incautaciones, confesiones, pagos correlacionados u otra evidencia.



FIGURA 06 · Los puntos de cruce entre dinero fiat, CASP y redes blockchain.

7.2. Flujo mínimo de análisis

01. Identificar blockchain, activo, dirección y hash sin errores de transcripción.
02. Verificar la transacción en más de una fuente cuando sea razonable.
03. Registrar timestamp, importe, fees, inputs/outputs o equivalente.
04. Construir la secuencia de saltos y marcar servicios custodiales conocidos solo con base contrastable.
05. Detectar entrada o salida de CASP donde pueda existir KYC.
06. Correlacionar fechas e importes con transferencias fiat, mensajes y eventos técnicos.
07. Documentar el método de clustering o atribución y sus limitaciones.

7.3. Travel Rule y puntos de identificación

Las directrices de la EBA relativas al Reglamento (UE) 2023/1113 obligan a PSP, PSP intermediarios, CASP e intermediarios a gestionar la información que acompaña transferencias de fondos y determinados criptoactivos. Para el investigador, esto aumenta la relevancia de identificar correctamente la entidad custodial que intervino y el tramo en el que se produce la conversión entre sistema financiero tradicional y criptoactivos.

7.4. Riesgos de sobreinterpretación

- Etiquetas de proveedores de analytics no siempre equivalen a prueba de identidad.
- Clustering heurístico debe describirse como técnica probabilística cuando corresponda.
- Mixers, bridges, swaps y cross-chain aumentan complejidad, pero no autorizan inferencias sin base.
- La ausencia de KYC en un tramo no impide buscar otros puntos de contacto con entidades reguladas.

7.5. MiCA y la identificación correcta del proveedor custodial

El Reglamento (UE) 2023/1114 (MiCA) proporciona un marco europeo para emisores y proveedores de servicios de criptoactivos. Sus reglas se aplican de forma escalonada, en gran parte desde el 30 de diciembre de 2024, con determinados períodos transitorios. Al formular una diligencia, conviene identificar la persona jurídica, la actividad efectivamente prestada, su jurisdicción y la situación de autorización o régimen transitorio, sin deducir la atribución de una dirección blockchain de la mera apariencia comercial de la plataforma. [S16]

8. Sociedades pantalla, testaferros y titularidad real

8.1. Formalidad frente a control

La investigación societaria debe diferenciar socio, administrador, apoderado, titular real y controlador de facto. Las estructuras pantalla suelen aprovechar la distancia entre la titularidad formal y el control operativo. El análisis financiero debe cruzar quién firma, quién accede a banca electrónica, quién aporta fondos, quién recibe beneficios, quién decide pagos y quién controla los activos.



FIGURA 07 · Comparación entre titularidad, control y beneficio económico.

8.2. Indicadores societarios

- Sociedad sin actividad aparente pero con elevado tránsito de fondos.
- Objeto social incongruente con contrapartes o volumen.
- Cambios frecuentes de administradores, domicilio o participaciones.
- Administradores de numerosas sociedades sin perfil económico coherente.
- Pagos circulares, préstamos socio-sociedad no documentados o facturación sin sustancia.
- Direcciones, teléfonos, dominios o asesores compartidos entre sociedades aparentemente independientes.

8.3. Beneficiario real

La titularidad real es un eje de PBC/FT y un dato de enorme valor investigativo, pero debe verificarse con evidencia dinámica. Una declaración registral o KYC es un punto de partida; el control efectivo puede revelarse por instrucciones de pago, credenciales, poderes, dispositivos, contratos privados, distribución de dividendos o uso del patrimonio.

9. OSINT financiero y enriquecimiento de inteligencia

9.1. Finalidad

OSINT no sustituye la obtención formal de datos protegidos. Su valor reside en generar y priorizar hipótesis: localizar sociedades, dominios, teléfonos, perfiles comerciales, direcciones, anuncios, litigios, sanciones públicas, conexiones corporativas y huellas digitales que permitan formular requerimientos más precisos.

9.2. Protocolo de preservación

01. Registrar consulta y objetivo.
02. Conservar URL exacta, fecha y hora y contenido relevante.
03. Distinguir fuente primaria, secundaria y agregador.
04. Capturar identificadores persistentes cuando existan.
05. Evitar asumir que dos perfiles corresponden a la misma persona solo por similitud nominal.

06. Corroborar cualquier dato decisivo con una fuente independiente o formal.

9.3. Matriz de confianza

Nivel	Ejemplo	Uso recomendado
A	registro oficial / documento auténtico	base factual
B	fuente institucional o entidad regulada	alta confianza, verificar contexto
C	fuente comercial reputada	orientar y corroborar
D	red social / foro / agregador	hipótesis, no conclusión
E	dato anónimo o no verificable	no usar salvo pista operativa

10. Investigación patrimonial y localización de activos

10.1. Cambiar la pregunta

La pregunta no es solo «¿dónde está el dinero transferido?», sino «¿qué valor controlan los intervinientes y qué nexo puede acreditarse entre ese patrimonio y la actividad investigada?». El activo final puede no ser el mismo dinero: puede haberse convertido en vehículo, inmueble, participaciones, saldo en plataforma, stablecoins, bienes de lujo o créditos frente a terceros.



Recreación conceptual generada con IA: análisis patrimonial y revisión documental; datos ficticios.

10.2. Inventario patrimonial

- Cuentas, depósitos, valores y productos financieros.
- Criptoactivos custodiales y autocustodia cuando existan indicios.
- Inmuebles, derechos reales y rentas.
- Vehículos, embarcaciones y bienes registrables.
- Participaciones y derechos económicos societarios.
- Créditos, préstamos, facturas y derechos de cobro.
- Bienes de alto valor y activos mantenidos mediante terceros.

10.3. Patrimonio incongruente

La desproporción patrimonial puede ser un indicador, pero requiere metodología. Deben compararse fuentes de ingresos acreditadas, patrimonio inicial, financiación, cargas, transmisiones y gastos. La ausencia de explicación en una fuente abierta no equivale a origen ilícito. El informe debe evitar convertir una laguna informativa en una conclusión.

11. Cooperación nacional e internacional

11.1. La dimensión transfronteriza es la regla

FATF, Egmont Group, INTERPOL y UNODC publicaron en 2025 un manual específico para acelerar la cooperación en detección, investigación y persecución del blanqueo. La elección del canal depende de la finalidad: inteligencia, preservación urgente, identificación, prueba admisible, bloqueo o ejecución de una resolución.



FIGURA 08 · Canales principales y distinto valor operativo o probatorio.

11.2. Formal e informal

Canal	Ventaja	Límite	Uso
Cooperación informal	velocidad	puede no producir prueba directamente	orientación, preservación, localización
UIF/Egmont	inteligencia financiera	restricciones de difusión/uso	vínculos financieros
Policial	rapidez operativa	depende de competencias	identificación y coordinación
Asistencia judicial	valor probatorio / medidas coercitivas	más formal y lenta	documentos, registros, bloqueo
Redes de recuperación	especialización patrimonial	según jurisdicción	localizar y asegurar activos

11.3. Peticiones útiles

Una solicitud internacional deficiente pide «toda la información». Una buena solicitud delimita sujeto, identificador, periodo, transacción, finalidad y medida concreta. Debe explicar la relación entre el dato solicitado y la investigación, identificar correctamente la entidad o jurisdicción y anticipar urgencia, conservación y formato.

11.4. Prueba electrónica transfronteriza: nuevo instrumento europeo

El Reglamento (UE) 2023/1543 relativo a órdenes europeas de producción y conservación de pruebas electrónicas es aplicable desde el 18 de agosto de 2026. Su utilización corresponde a las autoridades competentes en el marco de procedimientos penales y bajo los requisitos establecidos por la norma; no atribuye a los peritos privados facultades directas para exigir la entrega de registros de proveedores. Puede resultar relevante para preservar o producir datos de cuentas, comunicaciones y servicios cuando el objeto de la investigación y el proveedor se hallen dentro de su ámbito. [S14]

12. Medidas cautelares, decomiso, recuperación y restitución

12.1. Pensar en recuperación desde el minuto uno

La guía FATF de 2025 sitúa la recuperación de activos como prioridad operativa. La localización sin aseguramiento puede ser inútil si el activo se desplaza. Por ello, cada hallazgo patrimonial debe activar una pregunta: ¿qué medida legal existe para preservar este activo, quién puede solicitarla y qué información mínima necesita la autoridad competente?



FIGURA 09 · Secuencia para localizar, preservar y solicitar la restitución.

12.2. Mapa de decisión

01. Activo identificado con suficiente precisión.
02. Determinación de control y jurisdicción.
03. Evaluación del riesgo de dispersión o pérdida de valor.
04. Selección del instrumento de preservación o aseguramiento legalmente disponible.
05. Coordinación con autoridad competente y entidad custodial.
06. Documentación del nexo con el hecho investigado.
07. Gestión y conservación del valor durante el procedimiento.
08. Decisión final de decomiso, retorno o restitución conforme al marco aplicable.

12.3. Víctima y recuperación

En investigaciones de fraude, recuperar activos y compensar víctimas no debe considerarse un objetivo secundario. FATF destaca expresamente la compensación a víctimas dentro de su guía moderna de recuperación de activos. El

informe financiero debe conservar la trazabilidad entre pérdida individual, flujos agregados y activo asegurado para facilitar decisiones posteriores de restitución.

12.4. Directiva (UE) 2024/1260: recuperación y decomiso de activos

La Directiva (UE) 2024/1260 armoniza aspectos de localización, embargo y decomiso de activos en la Unión Europea. El plazo general para que los Estados miembros pongan en vigor las disposiciones necesarias concluye el 23 de noviembre de 2026, posterior a la fecha de esta edición. Por ello, debe consultarse la legislación de transposición efectivamente vigente en cada jurisdicción antes de invocarla como norma interna aplicable. Para la metodología pericial, subraya el valor de la identificación temprana, la gestión de activos y la coordinación entre autoridades. [S13]

13. Metodología pericial y estándares de evidencia

13.1. Estructura recomendada del informe

01. Objeto y alcance.
02. Documentación examinada.
03. Limitaciones y exclusiones.
04. Metodología y herramientas.
05. Cronología de hechos verificables.
06. Análisis de flujos financieros.
07. Análisis de intervinientes y control.
08. Análisis patrimonial.
09. Correlación con evidencia digital o societaria.
10. Conclusiones numeradas y graduadas por soporte.
11. Anexos de datos, hashes, tablas y gráficos reproducibles.

13.2. Cuatro categorías de afirmación

Categoría	Definición	Verbo recomendado	Ejemplo
Hecho	dato directamente documentado	consta / se observa	«Consta un abono de 12.500 €»
Cálculo	resultado reproducible	resulta / asciende	«El 92 % salió en 37 minutos»
Inferencia	deducción apoyada en varios hechos	es compatible / sugiere	«El patrón es compatible con cuenta de tránsito»
Hipótesis	explicación pendiente	debe contrastarse	«Debe contrastarse control por tercero»



FIGURA 10 · Cuatro grados de afirmación para redactar conclusiones periciales.

13.3. Reproducibilidad

Un tercero cualificado debe poder reconstruir los cálculos a partir de los anexos. Para ello conviene normalizar fechas y zonas horarias, conservar importes en moneda original y equivalente cuando se use conversión, registrar reglas de matching, explicar tratamiento de duplicados y documentar cualquier filtrado. En blockchain deben conservarse hashes y direcciones completos.

13.4. Visualización probatoria

- Una figura = una pregunta probatoria.
- No saturar el grafo con nodos irrelevantes.
- Mostrar claramente origen, destino, importe y secuencia temporal.
- Distinguir evidencia directa de nodos inferidos o etiquetados por terceros.
- Anexar tabla fuente detrás de toda visualización resumida.

14. Matrices, plantillas y checklists

14.1. Ficha de transacción

ID interno	_____
Fecha/hora y zona	_____
Importe / moneda	_____
Ordenante	_____
Beneficiario	_____
IBAN / cuenta / wallet	_____
Entidad / país	_____
Referencia / hash	_____
Canal	_____

Fuente documental	_____
Evento anterior relacionado	_____
Evento posterior relacionado	_____
Observación analítica	_____
Nivel de certeza	_____

14.2. Matriz de intervinientes

ID	Persona/entidad	Rol observado	Control	Evidencias	Pendiente

14.3. Checklist primeras 24 horas

- Obtener justificantes completos y referencias de todas las operaciones.
- Notificar inmediatamente a entidad emisora/receptora por canales de fraude disponibles.
- Preservar correos, mensajes, números, URLs y archivos originales.
- Identificar todos los IBAN, PSP, merchants, exchanges y wallets visibles.
- Crear línea temporal con zona horaria.
- Separar importe total perdido, recuperado, bloqueado y pendiente.
- Escalar a denuncia/autoridad competente y aportar identificadores estructurados.
- Solicitar preservación de datos cuando exista cauce legal aplicable.
- No alertar innecesariamente a posibles intervinientes si puede comprometer medidas.
- Actualizar el grafo cada vez que aparezca un nuevo destino.

14.4. Checklist requerimiento a entidad financiera

- Identificador exacto de cuenta o pago.
- Rango temporal razonado.
- Titulares, autorizados y apoderados relevantes.
- Documentación de alta/KYC y datos de contacto, si legalmente proceden.
- Extracto con contrapartes y referencias completas.
- Identificadores de operaciones instantáneas y devoluciones.
- Tarjetas, cuentas virtuales o productos vinculados relevantes.
- Información técnica de acceso cuando sea pertinente y autorizada.

- Conservación de evidencias antes de su borrado conforme a plazos internos.
- Formato estructurado cuando exista gran volumen de movimientos.

14.5. Checklist CASP/exchange

- Identidad jurídica exacta del prestador y jurisdicción.
- UID de usuario, correo, teléfono y KYC pertinente.
- Direcciones de depósito y retirada.
- Hashes de transacción y activos/redes utilizados.
- Historial de conversiones internas.
- Cuentas bancarias utilizadas para entradas/salidas fiat.
- Dispositivos/IP/logs si proceden legalmente.
- Direcciones externas destinatarias.
- Travel Rule data cuando corresponda y pueda obtenerse legalmente.

15. Casos tipo y errores frecuentes

15.1. BEC / fraude del proveedor

Caso tipo: la víctima recibe una instrucción de cambio de IBAN aparentemente legítima y transfiere fondos. El análisis debe unir autenticidad del mensaje, cronología del cambio, cuenta receptora, dispersión y beneficiarios. Error frecuente: concentrarse exclusivamente en quién comprometió el correo y no activar la investigación financiera hasta días después.

15.2. Inversión fraudulenta con cripto

Caso tipo: transferencia a cuenta de pago o compra de criptoactivos seguida de envíos a direcciones externas. Deben diferenciarse los movimientos realizados por la propia víctima bajo engaño de los realizados por terceros con control de su cuenta. El punto crítico suele ser identificar los CASP custodiales en los que existe información de usuario.

15.3. Cuenta mula reclutada

Caso tipo: una persona recibe fondos y los reenvía a cambio de comisión. La cuestión pericial no debe resolverse mediante etiquetas, sino analizando captación, comunicaciones, cuantía de la comisión, tiempo de reacción, control de credenciales, historial de la cuenta y destino posterior.

15.4. Sociedades y facturación simulada

Caso tipo: fondos criminales se integran en sociedades mediante facturas, préstamos o pagos aparentes. El análisis debe comparar sustancia económica, documentación contractual, capacidad real de prestación, flujos bancarios, fiscalidad, relaciones entre partes y destino final del dinero.

15.5. Errores que debilitan una pericial

- Confundir titularidad formal con autoría.
- Usar capturas sin conservar el dato subyacente.
- No documentar husos horarios.
- Asignar identidad a wallets únicamente por una etiqueta de terceros.
- Omitir movimientos que contradicen la hipótesis inicial.

- Construir conclusiones penales desde indicadores preventivos sin análisis adicional.
- No explicar limitaciones de los datos recibidos.
- Presentar cifras agregadas sin anexo reproducible.
- No distinguir recuperación potencial de recuperación efectiva.

16. Bibliografía y fuentes oficiales

Selección priorizada para mantener y ampliar esta metodología. Se recomienda comprobar siempre la versión vigente en la fecha del encargo.

S1. FATF/GAFI, Asset Recovery Guidance and Best Practices (4 noviembre 2025). · Consultar fuente oficial

S2. FATF, Egmont Group, INTERPOL y UNODC, International Co-operation on Money Laundering Detection, Investigation, and Prosecution Handbook (5 septiembre 2025). · Consultar fuente oficial

S3. MONEYVAL, Financial Investigations. · Consultar fuente oficial

S4. StAR (World Bank/UNODC), Asset Recovery Handbook: A Guide for Practitioners, Second Edition (2020). · Consultar fuente oficial

S5. EBA, Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113. · Consultar fuente oficial

S6. BOE, Ley 10/2010, de prevención del blanqueo de capitales y de la financiación del terrorismo, texto consolidado. · Consultar fuente oficial

S7. BOE, Real Decreto 304/2014, Reglamento de la Ley 10/2010, texto consolidado. · Consultar fuente oficial

S8. EUR-Lex, Reglamento (UE) 2024/1624 (AMLR). · Consultar fuente oficial

S9. EUR-Lex, Directiva (UE) 2024/1640. · Consultar fuente oficial

S10. FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – FATF Recommendations. · Consultar fuente oficial

S11. BOE, Real Decreto 813/2026, de 7 de octubre, por el que se modifican normas reglamentarias financieras; art. 5, disposiciones transitorias y final cuarta · Consultar fuente oficial

S12. Banco Central Europeo, Instant Payments Regulation; calendario y servicio de verificación del beneficiario · Consultar fuente oficial

S13. Directiva (UE) 2024/1260 sobre recuperación y decomiso de activos; art. 33, plazo de transposición · Consultar fuente oficial

S14. Reglamento (UE) 2023/1543 sobre órdenes europeas de producción y conservación de pruebas electrónicas · Consultar fuente oficial

S15. BOE, Ley 10/2010, texto consolidado; actualización publicada el 30 de septiembre de 2026 · Consultar fuente oficial

S16. Reglamento (UE) 2023/1114 relativo a los mercados de criptoactivos (MiCA) · Consultar fuente oficial

S17. Reglamento (UE) 2024/886 relativo a las transferencias inmediatas en euros y modificaciones conexas · Consultar fuente oficial

S18. BOE, Real Decreto-ley 25/2026, de 29 de septiembre, disposición final primera sobre la Ley 10/2010 · Consultar fuente oficial

Notas de actualización

Edición revisada a 16 de octubre de 2026. Se incorporan el Real Decreto-ley 25/2026 (vigente desde el 1 de octubre), el Real Decreto 813/2026 (vigencia general el 28 de octubre), el régimen de transferencias inmediatas, MiCA, las órdenes europeas de prueba electrónica y la Directiva de recuperación y decomiso (transposición hasta el 23 de noviembre). Las futuras reformas y los plazos transitorios se distinguen del derecho vigente. Criterio de mantenimiento: revisar anualmente y ante cada cambio normativo, jurisprudencial o de cooperación aplicable. [S11–S18]

ANEXOS / HERRAMIENTAS DE TRABAJO

ANEXO I. Modelo de conclusión pericial financiera

A modo de plantilla, una conclusión debe responder de forma separada a: (i) qué movimientos están acreditados; (ii) qué relaciones temporales y cuantitativas se observan; (iii) qué personas o entidades aparecen vinculadas documentalmente; (iv) qué inferencias son compatibles con esos datos; (v) qué extremos no pueden determinarse con la información disponible; y (vi) qué diligencias permitirían confirmar o descartar las hipótesis restantes.

Ejemplo metodológico: «De la documentación bancaria examinada consta que la cuenta A recibió 24.750 euros el día D a las 10:14 y que, en los 42 minutos siguientes, 23.900 euros fueron transferidos a las cuentas B, C y D. Este patrón acredita una dispersión rápida del 96,6 % del importe recibido. La documentación examinada no permite, por sí sola, determinar quién operó materialmente la cuenta A ni el conocimiento de su titular respecto del origen de los fondos; para ello serían relevantes, entre otros elementos, los registros de acceso, la documentación KYC, las comunicaciones y la identificación de los beneficiarios posteriores.»



FIGURA 12 · Datos didácticos del anexo: 24.750 €, 23.900 € y 42 minutos.

ANEXO II. Vocabulario operativo

Término	Definición de trabajo
Beneficiario real	Persona física que en último término posee o controla una entidad o relación, conforme al marco aplicable.
CASP	Crypto-Asset Service Provider; proveedor de servicios de criptoactivos.
Fan-in	Concentración de múltiples entradas en un mismo nodo.
Fan-out	Dispersión desde un nodo hacia múltiples destinos.
KYC	Know Your Customer; información de identificación y conocimiento del cliente.
OSINT	Inteligencia obtenida de fuentes abiertas.
PSP	Payment Service Provider; proveedor de servicios de pago.
Travel Rule	Obligaciones de información que acompañan determinadas transferencias de fondos y criptoactivos.

Término	Definición de trabajo
Wallet custodial	Dirección o saldo gestionado por un proveedor que controla las claves o la cuenta.
Wallet autocustodiada	Dirección cuyas claves son controladas directamente por el usuario, sin custodio central.

ANEXO III. Ficha de control de calidad del informe

- ¿Todas las cifras relevantes pueden recalcularse desde un anexo?
- ¿Todas las fechas indican zona horaria cuando puede existir ambigüedad?
- ¿Se han separado hechos, cálculos, inferencias e hipótesis?
- ¿Las conclusiones negativas explican también las limitaciones documentales?
- ¿Cada atribución personal tiene más soporte que la mera titularidad de una cuenta?
- ¿Las visualizaciones tienen respaldo en datos tabulares?
- ¿Se ha preservado el identificador completo de cada transacción, cuenta o wallet?
- ¿Se han considerado explicaciones alternativas razonables?
- ¿El informe identifica diligencias adicionales de alto valor?
- ¿Se explica de manera comprensible qué parte del dinero está localizada, bloqueada, recuperada o no localizada?

ANEXO IV. Playbook de actuación en las primeras 72 horas

En ciberestafas con salida de fondos, la primera ventana temporal tiene una lógica propia. Durante esas horas el investigador no dispone todavía de una imagen completa, pero sí de identificadores suficientes para preservar evidencias, activar canales de fraude y formular peticiones que eviten la pérdida definitiva de información o activos. El objetivo no es cerrar hipótesis prematuramente; es mantener abiertas las posibilidades de identificación, bloqueo y recuperación.



FIGURA 11 · Ventanas 0–6, 6–24 y 24–72 horas según el protocolo del anexo.

Fase 0–6 horas: preservar y fijar el punto de partida

- Confirmar exactamente qué ordenó la víctima, desde qué cuenta, a qué identificador y a qué hora.
- Obtener justificante bancario completo, no solo captura de pantalla. Conservar referencia end-to-end, concepto, ordenante, beneficiario, entidad y BIC cuando figuren.
- Preservar la evidencia del engaño en formato nativo cuando sea posible: correo .eml/.msg, exportación de chat, URL completa, archivos recibidos y grabaciones disponibles lícitamente.
- Separar operaciones autorizadas bajo engaño de operaciones no autorizadas. Esta distinción condiciona tanto el análisis técnico como la estrategia de reclamación.
- Contactar con el área de fraude de la entidad emisora para activar recall, solicitud de retención o comunicación interbancaria disponible.
- Preparar una ficha única de incidente con identificadores normalizados para que todas las actuaciones posteriores usen los mismos datos.

Fase 6–24 horas: construir el primer mapa financiero

Una vez fijado el pago inicial, debe elaborarse un mapa mínimo: cuenta de origen, cuenta o identificador receptor, entidad receptora, país, importe, hora, referencia y cualquier dato sobre el siguiente destino. Si la entidad de la víctima informa de que los fondos ya han salido, ese hecho debe documentarse y convertirse en una nueva pregunta de investigación: a qué destino, en qué cuantía y mediante qué instrumento.

- Denuncia estructurada con todos los identificadores financieros y digitales.
- Solicitud de preservación o requerimiento urgente por los canales legalmente procedentes.
- Identificación de si el receptor es banco, entidad de pago, EMI, fintech, merchant, exchange o cuenta virtual.
- Búsqueda de coincidencias entre teléfono, correo, dominio, IBAN, nombre comercial y otras denuncias o fuentes legítimas.
- Creación de una línea temporal unificada, expresando horas en la zona de referencia y conservando la zona original.

Fase 24–72 horas: expandir, priorizar y asegurar

En esta fase la investigación debe priorizar nodos con capacidad de identificación o de inmovilización. Un salto a un exchange custodial puede ofrecer más posibilidades de atribución que cinco saltos entre direcciones autocustodiadas; una transferencia a una cuenta empresarial puede abrir un vector societario; una retirada en cajero puede requerir preservación de imágenes antes de que expiren.

01. Actualizar el grafo con cada nuevo nodo.
02. Clasificar los nodos por valor operativo: identificación, bloqueo, evidencia o patrimonio.
03. Detectar destinos que aparezcan repetidos en más de una víctima o incidente.
04. Promover medidas de aseguramiento cuando exista base suficiente y riesgo de dispersión.
05. Iniciar cooperación internacional en cuanto la jurisdicción extranjera sea relevante, sin esperar a reconstruir toda la cadena.
06. Emitir una primera nota de situación que diferencie dinero localizado, posiblemente localizado, bloqueado, recuperado y no localizado.

> **MÉTRICA DE ÉXITO INICIAL**
>
> Durante las primeras 72 horas el éxito no se mide solo por recuperar dinero. También por preservar datos que desaparecerían, identificar nuevos destinos, fijar titulares o entidades custodiales y evitar que la investigación llegue tarde.

ANEXO V. Investigación de blanqueadores profesionales, hawala y redes de compensación

Las redes de blanqueo profesional pueden prestar servicios a múltiples grupos delictivos sin participar en el delito precedente. Su valor consiste en recibir, transformar, compensar, transferir o reintegrar valor, aprovechando estructuras comerciales, cuentas, efectivo, criptoactivos, comercio internacional o sistemas informales de transferencia. La investigación debe buscar la infraestructura compartida y no limitarse a la operación individual.

Indicadores de infraestructura profesional

- Múltiples cuentas o sociedades que reciben fondos de delitos no relacionados entre sí.
- Rotación de cuentas receptoras manteniendo teléfonos, dispositivos, apoderados, dominios o beneficiarios posteriores comunes.
- Compensaciones entre países en las que no existe transferencia bancaria directa equivalente al pago económico subyacente.
- Uso sistemático de comercios intensivos en efectivo, importación/exportación, joyería, compraventa, remesas o criptoactivos para balancear posiciones.
- Pagos cruzados entre terceros sin relación comercial aparente pero con importes compensatorios.
- Comisiones implícitas, descuentos o diferencias recurrentes entre importe entregado e importe recibido por el beneficiario final.

Hawala y sistemas similares

En un sistema de transferencia informal de valor, el dinero puede no cruzar físicamente la frontera. Un operador recibe fondos en una jurisdicción y otro operador entrega el equivalente en otra; la deuda entre ambos se liquida posteriormente mediante compensación, comercio, efectivo, activos o transferencias distintas. Por ello, seguir únicamente una transferencia bancaria concreta puede no revelar la transferencia económica real.

El análisis debe buscar libros, mensajería, códigos, listas de clientes, cuentas de compensación y relaciones estables entre operadores. También resulta útil comparar entradas y salidas por periodos y detectar si dos nodos presentan saldos recíprocos que se regularizan con operaciones comerciales o cripto.

Preguntas analíticas

- ¿El nodo presta servicio a múltiples remitentes no relacionados?
- ¿Existen contrapartes recurrentes en otros países sin una explicación comercial clara?
- ¿El volumen de pagos es coherente con la actividad declarada?
- ¿Se observan saldos que se compensan por periodos en lugar de operación por operación?
- ¿Hay uso paralelo de efectivo, bienes, facturas, stablecoins o remesadoras?
- ¿Puede diferenciarse el dinero de clientes del beneficio o comisión del operador?

La investigación de estas redes exige especial cautela terminológica. Un sistema informal puede tener usos legítimos o culturalmente asentados; la relevancia penal depende del conocimiento, finalidad, origen y contexto de los fondos, no de la mera existencia de un mecanismo alternativo de transferencia.

ANEXO VI. Guía avanzada de análisis de cuentas mula

Modelos de captación

No todas las cuentas mula responden al mismo perfil. Distinguir el modelo de captación ayuda a orientar las diligencias y evita imputaciones automáticas. Entre los escenarios más habituales están el reclutamiento consciente por comisión, la falsa oferta de empleo, el romance scam, el supuesto intermediario de pagos, la cesión de cuenta a un conocido, la venta de credenciales y la apropiación de una cuenta legítima.

Modelo	Indicadores	Dato clave	Hipótesis alternativa
Comisión consciente	porcentaje, instrucciones, repetición	mensajes y beneficio	puede alegarse desconocimiento del origen
Falso empleo	contrato informal, tareas de pagos	anuncio/reclutador	víctima secundaria
Romance/ingeniería social	relación previa, presión emocional	chat completo	engaño sobre finalidad
Venta/cesión de cuenta	cambio de dispositivo/credenciales	logs y contraprestación	control material de tercero
Account takeover	actividad anómala y cambio de acceso	autenticación/IP/dispositivo	titular ajeno a operaciones

Ejes de atribución

01. Apertura: quién creó la relación y con qué documentación.
02. Control: quién tenía credenciales, dispositivo y capacidad de ordenar pagos.
03. Conocimiento: qué información recibió sobre el origen o finalidad.
04. Beneficio: qué comisión, pago o ventaja obtuvo.
05. Repetición: si el patrón aparece una sola vez o de forma continuada.
06. Coordinación: relación con otras mulas, reclutadores o beneficiarios.
07. Conducta posterior: reclamación, denuncia, borrado, sustitución de dispositivo, retirada o huida.

Matriz de atribución recomendada

Para cada persona, puntuar cualitativamente —sin convertirlo en una escala penal automática— la fuerza de la evidencia sobre titularidad, control, conocimiento, beneficio y coordinación. El objetivo es visualizar qué elemento está probado y cuál sigue siendo una hipótesis. Una persona puede tener titularidad alta y control bajo, por ejemplo en un takeover; otra puede no ser titular y, sin embargo, controlar plenamente la cuenta.

> **PRECAUCIÓN**
>
> El término «mula» es una categoría operativa. En un informe pericial conviene describir primero la conducta observable y reservar cualquier calificación jurídica a quien corresponda.

ANEXO VII. Requerimientos de información: modelos de contenido

Los siguientes modelos no sustituyen un oficio judicial, policial o requerimiento legal. Sirven para estructurar la información que debería contener una solicitud para evitar respuestas incompletas, ambigüedades o pérdidas de tiempo.

Modelo A. Entidad bancaria o PSP

- Identificación del procedimiento o incidente y autoridad solicitante.
- Cuenta/IBAN/identificador de pago exacto y periodo relevante.
- Titular, cotitulares, autorizados, apoderados y fecha de alta/baja.
- Documentación de identificación y datos de contacto conservados.
- Extracto íntegro del periodo con ordenantes, beneficiarios y referencias.
- Detalle técnico de las operaciones objeto: canal, fecha y hora, referencia interna y externa.
- Cuentas y tarjetas asociadas relevantes, incluidas virtuales.
- Datos de acceso y autenticación conservados, si son pertinentes y legalmente solicitables.
- Destino de transferencias salientes y entidad receptora.
- Preservación de registros, CCTV o datos de ATM cuando el tiempo de retención sea limitado.

Modelo B. CASP/exchange custodial

- Identificador de usuario o dirección de depósito vinculada.
- KYC y cambios posteriores de identidad o contacto.
- Historial de depósitos, retiros, swaps y conversiones internas.
- Direcciones blockchain completas y hashes.
- Cuentas bancarias, tarjetas o PSP usados para entradas y salidas fiat.
- IP, dispositivo y sesiones relevantes cuando proceda.
- Beneficiarios o whitelisted addresses.
- Travel Rule information disponible para las transferencias afectadas.
- Congelación o preservación urgente cuando exista base legal.

Modelo C. Plataforma o proveedor tecnológico

- Identificador de cuenta, correo, teléfono, username o URL.
- Fecha de creación, recuperación y cambios de credenciales.
- Sesiones y direcciones IP relevantes dentro de un rango razonable.
- Contenido o metadatos concretos cuya conservación sea legalmente procedente.
- Método de pago y referencias de facturación cuando sean relevantes.
- Historial de dispositivos o autenticación disponible.

La precisión es decisiva: solicitudes excesivamente amplias pueden retrasar la cooperación o ser desproporcionadas. La petición debe explicar el nexo entre identificador, periodo y hecho investigado.

ANEXO VIII. Analítica cuantitativa de flujos

Una investigación financiera puede ganar objetividad incorporando métricas simples. No sustituyen la valoración jurídica, pero permiten comparar cuentas, priorizar nodos y explicar patrones al tribunal de forma reproducible.

Métricas básicas

Métrica	Cálculo	Interpretación
Velocidad de dispersión	tiempo entre abono y primera/última salida	urgencia y función de tránsito
% dispersado	salidas vinculadas / entrada × 100	retención frente a tránsito
Fan-out	número de destinos únicos	fragmentación
Fan-in	número de orígenes únicos	concentración
Recurrencia	número de incidentes/víctimas relacionados	infraestructura compartida
Profundidad	número de saltos hasta punto de identificación	complejidad de rastreo
Concentración	% que termina en los 3 mayores destinos	priorización de nodos

Análisis temporal

Los horarios revelan rutinas. Debe observarse si las operaciones se agrupan tras ingresos de víctimas, si se ejecutan en franjas repetidas, si existe actividad nocturna, si las retiradas se producen inmediatamente después de los abonos o si varias cuentas operan de forma sincronizada. La correlación temporal gana valor cuando se cruza con comunicaciones, accesos o presencia física obtenida por vías legales.

Análisis de red

En grafos grandes conviene calcular grado de entrada/salida, centralidad, comunidades y caminos más frecuentes, pero cualquier métrica debe explicarse en lenguaje accesible. Un nodo central puede ser un exchange legítimo, un banco corresponsal o un agregador técnico, por lo que la centralidad no implica culpabilidad. Sirve para priorizar dónde obtener información.

ANEXO IX. Criptoactivos: playbook de investigación por escenarios



Recreación conceptual generada con IA: entorno de trabajo de un investigador financiero; datos ficticios.

Escenario 1. Víctima compra cripto y envía a dirección indicada

Debe reconstruirse la compra fiat, identificar el CASP utilizado por la víctima, fijar la dirección de retirada y el hash, y seguir el activo hasta el primer punto de custodia o conversión identificable. Es importante distinguir claramente que la transacción fue técnicamente autorizada por la víctima pero inducida por engaño.

Escenario 2. Fondos bancarios llegan a exchange

El objetivo prioritario es identificar la cuenta de cliente del exchange que recibió el fiat o el cripto. Si existe un CASP regulado, los datos KYC, métodos de pago, direcciones de retirada y accesos pueden romper el anonimato aparente. La rapidez es especialmente importante si el saldo sigue bajo custodia.

Escenario 3. Bridges, swaps y cadenas múltiples

Cada cambio de red debe documentarse como un evento específico. Conservar el activo de origen, activo de destino, protocolo, hash en cada cadena y equivalencia temporal. No debe asumirse continuidad de identidad solo porque los importes sean parecidos; la correlación debe justificarse mediante estructura de la operación, tiempos, contratos y herramientas de análisis.

Escenario 4. Mixer o servicio de privacidad

La presencia de un mixer altera la calidad de la trazabilidad directa. El informe debe explicar exactamente qué puede y qué no puede concluirse, evitar presentar estimaciones probabilísticas como identidad cierta y buscar puntos posteriores de custodia, conversiones fiat o evidencia externa.

Escenario 5. Stablecoins

Las stablecoins son frecuentes por su estabilidad relativa y facilidad de transferencia. Debe identificarse red concreta —por ejemplo, el mismo ticker puede existir en distintas cadenas— y considerar si el emisor o los intermediarios disponen de mecanismos de congelación sujetos al marco legal y jurisdicción aplicables.

ANEXO X. Sociedades, facturación y blanqueo basado en comercio

Cuando el dinero se mezcla con actividad mercantil, la investigación debe comparar el flujo financiero con la realidad económica. Una factura, contrato o albarán prueba que existe un documento; no necesariamente que la operación se realizó en los términos declarados.

Pruebas de sustancia económica

- Capacidad del proveedor para prestar el servicio o suministrar el bien.
- Personal, instalaciones, licencias, compras y costes coherentes.
- Correspondencia entre fechas de factura, entrega, pago y contabilidad.
- Precios comparables y márgenes razonables.
- Evidencia logística: transporte, aduanas, almacén, recepción.
- Comunicación comercial previa y posterior.
- Destino del dinero después del cobro.
- Existencia de devoluciones, préstamos o pagos cruzados que neutralicen la operación.

Trade-based money laundering

El blanqueo basado en comercio puede utilizar sobre/subfacturación, múltiples facturas, descripción falsa de mercancías, envíos ficticios o estructuras triangulares. El análisis financiero debe coordinarse con documentación aduanera, logística y contable. Las discrepancias de valor son indicios que exigen explicación, no conclusiones automáticas.

ANEXO XI. Calidad, contradicción y defensa de la pericial

Prueba de resistencia

Antes de cerrar el informe conviene formular la mejor explicación alternativa para cada conclusión relevante. Si el patrón atribuido a una cuenta mula también puede explicarse por una apropiación de cuenta, ¿qué evidencia distingue ambos escenarios? Si una sociedad parece pantalla, ¿qué actividad real podría justificar sus movimientos? Si una cartera (wallet) aparece etiquetada por un proveedor, ¿qué fuente independiente confirma la atribución?

Preguntas previsibles en ratificación

- ¿De dónde procede exactamente este dato?
- ¿Puede reproducirse el cálculo?
- ¿Qué información no tuvo disponible?
- ¿Qué explicación alternativa consideró?
- ¿Por qué considera que dos operaciones están relacionadas?
- ¿Su herramienta de blockchain atribuye identidad o solo relación transaccional?
- ¿La titularidad de la cuenta implica necesariamente control?
- ¿Qué parte de su conclusión es técnica y qué parte sería jurídica?
- ¿Qué cambiaría su conclusión si apareciera nueva documentación?

Redacción robusta

Una pericial sólida no pretende eliminar la incertidumbre donde los datos no lo permiten. La explicita. Las expresiones «no puede determinarse», «no consta en la documentación examinada» o «la evidencia disponible es compatible con» son técnicamente más fuertes que una afirmación categórica no sustentada. La credibilidad pericial aumenta cuando el experto identifica límites y contradicciones.

ANEXO XII. Programa formativo de 90 minutos basado en la guía

Este esquema permite convertir la guía en una sesión de formación profesional orientada a ciberfraude y ruta del dinero.

Tiempo	Bloque
0–10 min	La ciberestafa como delito híbrido: engaño, tecnología y dinero.
10–20 min	Investigación financiera paralela y ventana crítica de 72 horas.
20–35 min	Cuentas mula, PSP, fintech y pagos instantáneos.
35–50 min	Criptoactivos: trazabilidad, CASP, travel rule y límites.

Tiempo	Bloque
50–60 min	Sociedades pantalla, titularidad real y blanqueo profesional.
60–70 min	Cooperación internacional y recuperación de activos.
70–80 min	Cómo construir una pericial financiera reproducible.
80–90 min	Caso práctico: reconstrucción de un flujo y decisiones de aseguramiento.

ANEXO XIII. Caso práctico integral

Supuesto: una empresa recibe un correo que aparenta proceder de un proveedor habitual. Se comunica un cambio de cuenta para una factura de 86.400 euros. La transferencia se ejecuta a las 09:42. A las 12:10 el proveedor real niega el cambio. La entidad emisora informa a las 13:05 de que el saldo ya no está disponible en la cuenta receptora.



FIGURA 13 · Cronología del supuesto didáctico de 86.400 €, sin atribución personal.

Datos iniciales

- Correo de cambio de IBAN recibido desde dominio visualmente similar al proveedor.
- IBAN receptor en entidad de otro Estado de la UE.
- Factura auténtica reutilizada con datos bancarios modificados.
- Transferencia de 86.400 euros.
- Dos números de teléfono usados para presionar al departamento administrativo.

Hipótesis de trabajo

Hipótesis A: compromiso del correo del proveedor. Hipótesis B: suplantación sin acceso a la cuenta real. Hipótesis C: información de la factura obtenida por un tercero distinto. En paralelo, la cuenta receptora puede ser controlada por el autor, por una mula consciente, por una mula engañada o por un tercero que obtuvo sus credenciales.

Actuaciones financieras

01. Fijar transferencia original y solicitar recall/retención.
02. Identificar entidad receptora y activar cooperación urgente.
03. Obtener titularidad, KYC, movimientos y destinos de salida por el canal legal pertinente.
04. Si el dinero se divide, representar cada salida como nodo separado.
05. Priorizar los destinos custodiales y aquellos con riesgo de retirada inmediata.
06. Cruzar titulares y contactos con los números utilizados en la ingeniería social.
07. Abrir investigación patrimonial sobre beneficiarios y controladores identificados.
08. Mantener una tabla de recuperación: localizado, bloqueado, devuelto y pendiente.

Conclusión provisional correcta

«La documentación disponible permite acreditar que 86.400 euros fueron transferidos por la víctima a la cuenta A tras una instrucción fraudulenta. La entidad emisora comunicó que los fondos habían salido de A antes de las 13:05. Con los datos actuales no puede determinarse quién controló materialmente A ni el destino final del importe. La prioridad investigativa es identificar los movimientos de salida, sus beneficiarios y los registros de control de la cuenta durante la ventana 09:42–13:05.»

Este tipo de conclusión evita confundir una constatación bancaria con una atribución penal y, al mismo tiempo, señala de forma concreta qué diligencias tienen mayor rendimiento.

ANEXO XIV. Glosario ampliado de evidencias y campos

Campo	Uso investigativo
IBAN	Identificador internacional de cuenta bancaria; no identifica por sí solo a la persona que la controla.
BIC/SWIFT	Identificador de entidad en el sistema financiero; útil para enrutar y precisar peticiones.
End-to-end reference	Referencia que puede acompañar la transferencia y facilitar correlación entre entidades.
Merchant ID	Identificador del comercio dentro de la cadena de adquirencia.
Acquirer	Entidad o proveedor que procesa cobros de un comercio.
Issuer	Entidad emisora de la tarjeta o instrumento.
MCC	Código de categoría del comercio.
Device fingerprint	Conjunto de atributos técnicos usados para reconocer un dispositivo o sesión; debe interpretarse con cautela.
IP	Dirección de red; puede corresponder a VPN, CGNAT, proxy o infraestructura compartida.
TxID / hash	Identificador de una transacción blockchain.
Address	Dirección blockchain; no es identidad civil.
Bridge	Protocolo que mueve o representa valor entre redes.
Swap	Conversión entre activos, centralizada o descentralizada.
Off-ramp	Punto de conversión de cripto a dinero fiat u otro activo utilizable.
On-ramp	Punto de entrada desde fiat a cripto.
Clustering	Agrupación heurística de direcciones posiblemente controladas por una misma entidad.
KYT	Know Your Transaction; análisis de riesgo y contexto de transacciones.
Recall	Petición de devolución o recuperación de una transferencia, sujeta a reglas y disponibilidad.

Campo	Uso investigativo
Beneficial owner	Titular real o persona física que en último término posee/controla según marco aplicable.
Asset tracing	Proceso de localizar y reconstruir movimientos y transformaciones de activos.

ANEXO XV. Principios finales de la metodología

01. Investigar el dinero desde el primer momento, no al final.
02. Preservar antes de interpretar.
03. Identificar el instrumento exacto: cuenta, tarjeta, PSP, merchant, CASP o wallet.
04. Separar titularidad de control material.
05. Separar trazabilidad de atribución personal.
06. Tratar la velocidad como variable investigativa.
07. Buscar puntos de custodia y conversión donde exista capacidad de identificación o bloqueo.
08. Construir grafos, pero respaldarlos siempre con tablas y fuentes.
09. Usar OSINT para orientar, no para sustituir la prueba formal.
10. Documentar la incertidumbre y las hipótesis alternativas.
11. Pensar en patrimonio y recuperación desde el inicio.
12. Diseñar cada conclusión para que pueda ser reproducida y defendida.

> **CIERRE**
>
> La ruta del dinero es el punto de unión entre la ciberestafa y su dimensión económica. Reconstruirla con rapidez, método y disciplina probatoria permite identificar intervinientes, comprender la infraestructura delictiva y aumentar las posibilidades de asegurar y restituir activos.

ANEXO XVI. Indicadores de investigación por instrumento financiero

Los indicadores siguientes no son pruebas de blanqueo ni de fraude por sí mismos. Funcionan como señales para priorizar revisión, formular hipótesis y decidir qué documentación adicional es necesaria. La interpretación debe considerar perfil del cliente, actividad declarada, histórico, cuantía, jurisdicción, relación entre las partes y explicación económica.

Transferencias bancarias

- Abono extraordinario seguido de salida total o casi total en minutos u horas.
- Fraccionamiento posterior hacia múltiples cuentas o países sin lógica comercial aparente.
- Conceptos genéricos o repetidos utilizados por múltiples ordenantes no relacionados.
- Entrada y salida con importes casi idénticos, dejando una pequeña diferencia compatible con comisión.
- Uso de varias cuentas del mismo titular para encadenar movimientos.
- Transferencias circulares que retornan total o parcialmente a nodos vinculados.

Pagos con tarjeta y adquirencia

- Compras de alto importe en comercios incompatibles con el perfil y seguidas de reembolsos a otro instrumento.
- Uso intensivo de tarjetas virtuales o wallets móviles tras recepción de fondos.
- Concentración en merchants de alto riesgo o intermediarios que dificultan identificar el destinatario económico.
- Discrepancia entre comercio visible para el usuario y entidad que procesa o recibe realmente el pago.
- Retiradas en ATM poco después de abonos procedentes de víctimas.

PSP, EMI y fintech

- Cuenta de pago reciente utilizada como nodo puente entre banco y exchange.
- Identificadores virtuales múltiples asociados a una misma persona o dispositivo.
- Transferencias instantáneas encadenadas entre proveedores distintos.
- Cambio frecuente de teléfono, correo o dispositivo alrededor de las operaciones investigadas.
- Uso de productos de fácil alta remota combinado con retirada o conversión inmediata.

Criptoactivos

- Entrada desde múltiples víctimas seguida de consolidación en una cartera (wallet).
- Conversión rápida a stablecoin y traslado a otra red.
- Paso por CASP y retirada inmediata a dirección externa.
- Uso de múltiples direcciones de depósito vinculadas a un mismo UID custodial.
- Secuencias repetidas de swaps/bridges sin finalidad económica aparente distinta de fragmentar trazabilidad.

Efectivo

- Retiradas repetidas inmediatamente después de recibir transferencias.
- Importes próximos a límites operativos o patrones de estructuración.
- Retiradas en lugares geográficamente alejados del domicilio o actividad habitual, cuando ese dato tenga relevancia.
- Uso de varias tarjetas/cuentas en cajeros próximos temporalmente.
- Ingresos en efectivo no coherentes con ventas, actividad o documentación.

Indicadores de contexto que aumentan el valor analítico

- Coincidencia de teléfono, dispositivo, correo o dirección entre varias cuentas receptoras.
- Misma contraparte final para fondos procedentes de víctimas diferentes.
- Repetición del patrón en fines de semana o franjas horarias concretas.
- Relación entre movimientos financieros y comunicaciones operativas del fraude.
- Uso de sociedades sin sustancia aparente como receptores o emisores intermedios.
- Compra de activos o bienes poco después de la recepción de fondos.

> **USO CORRECTO DE INDICADORES**
>
> Un indicador abre una pregunta; no la responde. La conclusión debe apoyarse en documentación, contexto y convergencia de evidencias.

ANEXO XVII. Diccionario de datos para investigación de grandes volúmenes

Cuando se reciben miles de movimientos, la calidad del análisis depende de normalizar los datos antes de buscar patrones. El objetivo de este diccionario es que extractos de bancos, PSP, CASP y registros internos puedan integrarse sin perder el dato original.

Campo	Contenido	Tipo	Regla
case_id	Identificador del asunto	texto	estable y no reutilizable
transaction_id	ID interno de transacción	texto	preservar original
source_system	banco/PSP/CASP/blockchain	texto	nombre entidad y sistema
event_time_original	fecha y hora original	datetime/texto	sin modificar
timezone	zona horaria	texto	UTC offset o zona conocida
event_time_utc	fecha y hora normalizada	datetime	derivada, no sustituye original
amount_original	importe original	decimal	sin redondeo
currency_original	moneda/activo	texto	ISO o ticker/red
amount_eur	equivalente EUR	decimal	indicar fuente/tipo de cambio
originator_name	ordenante	texto	tal como consta
originator_id	cuenta/wallet origen	texto	completo
beneficiary_name	beneficiario	texto	tal como consta
beneficiary_id	cuenta/wallet destino	texto	completo
institution_origin	entidad origen	texto	
institution_destination	entidad destino	texto	
reference	concepto/referencia	texto	no limpiar original
channel	web/app/ATM/API/etc.	texto	si consta
device_id	dispositivo/fingerprint	texto	si es legalmente disponible
ip_address	IP	texto	preservar versión IPv4/IPv6
tx_hash	hash blockchain	texto	completo
network	red blockchain	texto	imprescindible
evidence_source	documento/archivo	texto	trazabilidad
evidence_hash	hash de evidencia	texto	cuando proceda
analyst_note	nota analítica	texto	separada del dato bruto
confidence	grado de soporte	texto	hecho/cálculo/inferencia/hipótesis

Reglas de normalización

01. Conservar siempre una copia inalterada del fichero recibido.
02. No sustituir el valor original por el normalizado; añadir columnas derivadas.
03. No truncar IBAN, direcciones blockchain ni hashes en la base de trabajo.
04. Registrar explícitamente conversiones de moneda y su fuente.

05. Evitar inferir zona horaria cuando no consta; marcarla como desconocida.
06. Resolver duplicados mediante identificador y reglas documentadas, no por eliminación manual opaca.
07. Separar nombres de personas de identificadores de cuenta para evitar falsos matches.
08. Mantener una tabla de entidades y alias con fuente de cada equivalencia.
09. Registrar cada transformación de datos en un log de procesamiento.

Calidad de los datos

Los errores más graves suelen aparecer antes del análisis: fechas importadas como texto, comas decimales interpretadas como miles, truncamiento de ceros, hashes abreviados, mezcla de zonas horarias o nombres normalizados que fusionan personas distintas. La revisión de calidad debe ejecutarse antes de construir grafos o estadísticas.

ANEXO XVIII. Modelo de informe de situación y recuperación de activos

Un informe de situación periódico permite que dirección letrada, investigación y cliente comprendan qué se sabe, qué dinero sigue en riesgo y qué diligencias están abiertas. No sustituye la pericial final; es un documento de gestión y toma de decisiones.

1. Identificación del incidente

- Fecha de detección y fecha de los hechos.
- Víctima(s) y cuantía total denunciada.
- Tipología: BEC, inversión, phishing, smishing, fraude de soporte, romance, cripto, etc.
- Jurisdicciones y entidades financieras inicialmente implicadas.

2. Estado económico

Concepto	Importe
Pérdida bruta	€ _____
Devuelto espontáneamente	€ _____
Bloqueado/inmovilizado	€ _____
Recuperado efectivamente	€ _____
Localizado pero no asegurado	€ _____
No localizado	€ _____

3. Ruta conocida

Describir cada salto con identificador, entidad, importe, hora y fuente. Si existen rutas alternativas, separarlas. No usar frases como «el dinero acabó en…» cuando solo se ha probado un tramo intermedio.

4. Nodos prioritarios

- Nodos con saldo potencialmente disponible.
- Nodos custodiales con KYC.
- Nodos repetidos en varios incidentes.

- Nodos societarios o patrimoniales.
- Nodos que requieren cooperación internacional urgente.

5. Actuaciones realizadas

- Comunicaciones a entidades.
- Denuncia y ampliaciones.
- Requerimientos u oficios conocidos.
- Preservaciones de datos.
- Cooperación internacional iniciada.
- Medidas cautelares solicitadas/adoptadas.

6. Riesgos

- Caducidad de logs o CCTV.
- Retirada o conversión de activos.
- Disolución/traspaso societario.
- Movimiento transfronterizo.
- Identificadores incompletos que impiden continuar la trazabilidad.

7. Próximas diligencias recomendadas

Ordenarlas por rendimiento y urgencia. Para cada una indicar qué pregunta resolvería, qué autoridad o entidad debe ejecutarla y qué impacto tendría sobre identificación o recuperación.

ANEXO XIX. Protocolo de revisión independiente

En asuntos de elevada cuantía o complejidad es recomendable una revisión independiente antes de emitir conclusiones. El revisor no necesita rehacer toda la investigación, pero sí comprobar los puntos donde un error produciría una conclusión distinta.



FIGURA 14 · Lista gráfica de pruebas antes de finalizar la revisión independiente.

- Reconciliar importe inicial con total de destinos rastreados.
- Recalcular porcentajes y tiempos de dispersión.
- Verificar aleatoriamente hashes, IBAN y referencias contra la fuente primaria.
- Comprobar que los grafos no omiten nodos contradictorios.
- Revisar atribuciones personales y su soporte independiente.
- Revisar clasificación de hecho/inferencia/hipótesis.
- Confirmar que se han declarado las limitaciones documentales.
- Comprobar consistencia entre conclusiones, tablas y anexos.

Criterio de cierre del encargo

Una investigación puede cerrarse aunque no se conozca el destino final de todo el dinero, siempre que el informe defina con precisión el límite alcanzado. El cierre debe indicar el último nodo acreditado de cada ruta, las diligencias pendientes o inviables, los activos efectivamente recuperados y las hipótesis que no pudieron verificarse.

CRÉDITOS · EDICIÓN PROFESIONAL 2026

Nota sobre la elaboración de esta guía

Esta guía ha sido redactada por Juan Carlos Galindo con herramientas de IA. Empleada como apoyo en la redacción, organización, revisión documental, actualización de referencias y maquetación profesional.

La autoría y la validación de su contenido, la valoración técnica y jurídica y la adaptación a cada caso concreto corresponden a Juan Carlos Galindo y, cuando proceda, a los profesionales competentes. La guía no sustituye las autorizaciones judiciales ni las obligaciones legales aplicables.

Juan Carlos Galindo
Director de Galindo-Benlloch
Valencia · 16 de octubre de 2026