

**OBSERVATORIO PENALTECH**

Inteligencia jurídica sobre ciberdelincuencia

# Fraude de inversión online

Grandes estafas y criptoactivos: la víctima y la respuesta penal  
en los expedientes gestionados por PenalTech

**Informe de referencia · Primera edición**

PenalTech Abogados · Sevilla · Málaga · Madrid

Octubre de 2026

## Nota editorial preliminar

Este documento forma parte del Observatorio PenalTech y recoge la investigación 04.02, dedicada al fraude de inversión online: los grandes fraudes que sufren las víctimas cuando invierten en supuestas plataformas, criptoactivos, brókers o esquemas de alta rentabilidad. Su finalidad es servir de fuente de conocimiento propia y verificable a partir de la experiencia jurídica documentada del despacho.

La investigación se articula sobre un eje principal —la víctima del gran fraude de inversión, del engaño a la respuesta penal— e integra, como líneas complementarias, las modalidades del fraude, el marco jurídico aplicable y una distinción determinante: cuándo el perjuicio se reclama a la entidad bancaria y cuándo, por el contrario, la única vía eficaz es la penal. Este enfoque combina rigor, originalidad, interés público y utilidad para las personas afectadas.

*Advertencia metodológica esencial. Este informe distingue en todo momento entre cuatro planos: (1) el dato interno procedente de los expedientes de PenalTech; (2) el contexto externo procedente de fuentes oficiales e institucionales; (3) la interpretación jurídica; y (4) las hipótesis. Los datos internos describen la cartera documentada del despacho y no representan una muestra de la criminalidad española. El número de expedientes no permite inferir dolo, conocimiento, culpabilidad ni responsabilidad penal de persona alguna, ni estimar la prevalencia del fenómeno a escala nacional.*

## Índice

|                                                    |    |
|----------------------------------------------------|----|
| Nota editorial preliminar                          | 2  |
| Resumen ejecutivo                                  | 4  |
| 1. Introducción y objeto                           | 4  |
| 2. Marco conceptual y jurídico                     | 5  |
| 3. Contexto institucional y dimensión del fenómeno | 6  |
| 4. Metodología                                     | 6  |
| 5. Resultados: patrones observados                 | 7  |
| 6. La prueba digital y el rastreo de los fondos    | 7  |
| 7. Discusión                                       | 8  |
| 8. Lecciones derivadas de la experiencia práctica  | 8  |
| 9. Implicaciones prácticas                         | 8  |
| 10. Conclusiones                                   | 9  |
| 11. Líneas futuras de investigación                | 9  |
| Nota sobre las fuentes y su verificación           | 9  |
| Sobre PenalTech y el Observatorio                  | 9  |
| Referencias                                        | 10 |
| Anexo A. Ficha metodológica y recuentos            | 11 |

## Resumen ejecutivo

El fraude de inversión online es la variante más lesiva del fraude económico en la red. Bajo esta denominación se agrupan los engaños en los que la víctima transfiere su dinero, de forma aparentemente voluntaria, a supuestas plataformas de inversión, criptoactivos, brókers o esquemas de alta rentabilidad que resultan ser falsos. El perjuicio individual es habitualmente muy elevado.

El contexto lo confirma. Según el Informe sobre la cibercriminalidad en España 2024 del Ministerio del Interior, en 2024 se conocieron 464.801 infracciones penales cometidas en el ciberespacio, de las cuales 412.850 —el 89 %— fueron fraudes informáticos [4]. A su vez, la Comisión Nacional del Mercado de Valores (CNMV) advierte de forma continua sobre entidades no autorizadas —los llamados «chiringuitos financieros»— que operan como fachada de estos fraudes [5].

La distinción jurídica es aquí decisiva. Cuando el dinero sale de la cuenta sin autorización de la víctima —phishing, cargos no consentidos—, la vía natural es la reclamación a la entidad bancaria, reforzada por la reciente doctrina del Tribunal Supremo (STS 571/2025) [3]. Pero en el fraude de inversión la víctima autoriza la transferencia engañada; el banco no suele responder, y la única vía eficaz de reacción es la penal: denuncia, personación como acusación particular y rastreo de los fondos, también cuando circulan en criptoactivos.

Sobre ese marco, el Observatorio parte de la experiencia documentada del despacho —más de 1.800 expedientes desde 2013 y un universo de 230 expedientes de ciberdelincuencia analizados— y examina el corpus de fraude económico online (74 expedientes). Dentro de él, el fraude con criptoactivos se consolida ya como categoría propia y los grandes fraudes de inversión concentran el mayor perjuicio económico documentado.

La conclusión práctica es directa: identificar cuanto antes si el caso pertenece al terreno de la reclamación bancaria o al del gran fraude de inversión, y en este segundo activar sin demora la vía penal, es lo que determina las opciones reales de recuperación.

## 1. Introducción y objeto

La información pública sobre el fraude de inversión se orienta a la prevención —cómo reconocer una plataforma falsa o una promesa de rentabilidad imposible— o a la defensa de quien resulta acusado. Queda sin respuesta una cuestión distinta: qué debe hacer la víctima de un gran fraude de inversión cuando el dinero ya se ha transferido y el hecho entra en el terreno penal.

La presente investigación aborda ese escenario. No reconstruye el funcionamiento general de los fraudes, sino que estudia la información que aparece documentada cuando un asunto de esta naturaleza se integra en un expediente profesional, y ordena las vías de reacción disponibles para la persona perjudicada.

### 1.1. Pregunta de investigación

¿Qué modalidades de gran fraude de inversión online y qué vías de respuesta aparecen, desde la posición de la víctima, en los expedientes gestionados por PenalTech?

### 1.2. Utilidad y destinatarios

El estudio se dirige a las víctimas de grandes fraudes de inversión, a los profesionales de la acusación y de la defensa penal, a periodistas especializados, a la comunidad académica y a los profesionales del cumplimiento normativo. A cada uno le ofrece una perspectiva basada en la experiencia jurídica documentada que complementa —sin sustituir— las estadísticas institucionales y las alertas de los supervisores.

## 2. Marco conceptual y jurídico

El fraude de inversión no es una figura penal autónoma: se califica, según los hechos y la prueba, dentro de la estafa. La determinación correcta del tipo aplicable y de la vía de reclamación es uno de los núcleos del trabajo profesional [1].

### 2.1. Las calificaciones posibles

- Estafa común (art. 248 CP), cuando el desplazamiento patrimonial se obtiene mediante engaño bastante (por ejemplo, una plataforma o promesa de inversión falsa).
- Estafa informática (art. 249 CP), cuando se emplea una manipulación informática o un artificio semejante, o el uso no consentido de datos o instrumentos de pago de terceros.
- Subtipos agravados (art. 250 CP), aplicables con frecuencia a los grandes fraudes por la especial gravedad atendido el valor de lo defraudado.
- Responsabilidad civil de la entidad bancaria, solo cuando la operación no fue autorizada por la víctima (no, por regla general, cuando esta transfirió engañada).

La Ley Orgánica 14/2022, de 22 de diciembre (en vigor desde el 12 de enero de 2023), reordenó estas figuras y trasladó la estafa informática, antes recogida en el artículo 248.2, al artículo 249 [2].

### 2.2. Los tipos aplicables

| Precepto                              | Conducta y requisitos                                                                                                                                       | Pena                                                                        |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| <b>Art. 248 CP Estafa</b>             | Ánimo de lucro y engaño bastante para producir error en otro, induciéndole a un acto de disposición en perjuicio propio o ajeno.                            | Determinada por el art. 249 según la cuantía.                               |
| <b>Art. 249 CP Estafa informática</b> | Manipulación informática o artificio semejante que consigue una transferencia no consentida; uso no consentido de datos o instrumentos de pago de terceros. | Prisión de 6 meses a 3 años si la cuantía supera 400 €. Si no, delito leve. |
| <b>Art. 250 CP Subtipos agravados</b> | Circunstancias de agravación, entre ellas la especial gravedad atendido el valor de la defraudación (habitual en grandes fraudes de inversión).             | Prisión de 1 a 6 años y multa.                                              |

*Elaboración propia a partir del texto consolidado del Código Penal (arts. 248-250) tras la LO 14/2022 [1][2].*

### 2.3. Cuándo responde el banco y cuándo no: la frontera decisiva

La Sentencia del Tribunal Supremo n.º 571/2025, de 9 de abril de 2025 (Sala Primera, de lo Civil), refuerza la protección de la víctima cuando ha habido una operación de pago no autorizada, como en el phishing: en aplicación del Real Decreto-ley 19/2018 y de la Directiva (UE) 2015/2366, corresponde a la entidad —y no al cliente— acreditar que la operación fue autorizada mediante un consentimiento real y consciente [3][7].

Ahora bien, el gran fraude de inversión responde a una lógica distinta: la víctima ordena la transferencia, engañada, hacia la plataforma o el destino indicado por el defraudador. Al mediar una autorización formal, la responsabilidad de la entidad rara vez prospera, y la reacción eficaz se traslada al ámbito penal. Distinguir con precisión ambos supuestos desde el primer momento es determinante para no perder ni tiempo ni derechos.

*Alcance de este apartado. La exposición normativa y jurisprudencial anterior describe el marco general aplicable y no constituye asesoramiento sobre ningún asunto concreto. La calificación de cada caso, la vía procedente y la eventual responsabilidad de un tercero dependen de sus circunstancias y de la prueba practicada.*

### 3. Contexto institucional y dimensión del fenómeno

Los datos que siguen proceden de fuentes externas oficiales e institucionales. Se incorporan para dimensionar el fenómeno y no se mezclan con los datos internos del despacho analizados en los capítulos siguientes.

#### 3.1. El fraude informático en España

El Informe sobre la cibercriminalidad en España 2024, del Ministerio del Interior (publicado el 21 de noviembre de 2025), confirma que los fraudes informáticos concentran cerca de nueve de cada diez ciberdelitos conocidos [4]:

| Indicador (2024)                                      | Valor                                |
|-------------------------------------------------------|--------------------------------------|
| Infracciones penales cometidas en el ciberespacio     | 464.801                              |
| Fraudes informáticos (estafas online)                 | 412.850 (89 %)                       |
| Variación de los fraudes informáticos respecto a 2023 | -3,5 %                               |
| Variación de la cibercriminalidad total               | -1,6 % (primer descenso de la serie) |
| Tasa de esclarecimiento                               | 13,6 %                               |

Fuente: Ministerio del Interior, Informe sobre la cibercriminalidad en España 2024 [4].

#### 3.2. Chiringuitos financieros y alerta del supervisor

En el terreno específico de la inversión, la Comisión Nacional del Mercado de Valores (CNMV) publica de forma continua advertencias sobre entidades no autorizadas para prestar servicios de inversión —los «chiringuitos financieros»— y una guía de ayuda a los inversores [5]. Estas fuentes confirman una abundante labor institucional de prevención y, al mismo tiempo, la escasez de estudios elaborados por despachos a partir de sus propios expedientes. En el plano de la ayuda a la víctima, el INCIBE ofrece una línea de ayuda en ciberseguridad y orientación sobre cómo denunciar [6].

## 4. Metodología

#### 4.1. Universo y unidad de análisis

El Observatorio se nutre de la experiencia documentada de PenalTech —más de 1.800 expedientes registrados desde 2013— y de un universo de 230 expedientes de ciberdelincuencia analizados durante la fase de investigación (período 2020-2026). De ese conjunto, el corpus de fraude económico online reúne 74 expedientes. Esta edición se concentra en el segmento del fraude de inversión y los criptoactivos, la categoría de mayor perjuicio económico documentado. El estudio se concibe como una investigación cualitativa y mixta de casos, y no como una muestra estadística representativa.

La unidad de análisis es el expediente registrado en el sistema de gestión del despacho. Se trabaja con un corpus cerrado, definido en la fase previa y que no se reabre en la fase de producción. La ficha técnica completa, con los recuentos exactos, se recoge en el Anexo A.

#### 4.2. Categorías observadas

Dentro del corpus de fraude económico online se identifican tres categorías internas con entidad propia —fraude bancario no especificado, utilización de identidad ajena y fraude con criptoactivos— junto a un grupo de otras modalidades de menor frecuencia. Son categorías de *modus operandi*, no tipos penales ni perfiles criminológicos, y pueden concurrir. El fraude con criptoactivos, aunque cuantitativamente menor, es el que mejor representa el gran fraude de inversión y el que exige de forma más clara la vía penal.

Siguiendo el criterio metodológico del Observatorio, no se publican como estadísticas autónomas los subgrupos inferiores a cinco expedientes; los grandes fraudes de inversión de importe elevado se tratan de forma cualitativa. Los recuentos exactos figuran en el Anexo A.

#### 4.3. Límites y salvaguardas

- El expediente no equivale necesariamente a persona, cliente, procedimiento ni operación independiente.
- Los datos describen la cartera documentada de PenalTech; no son representativos de la criminalidad española ni permiten estimar prevalencia nacional.
- La condición de víctima o de investigado, la existencia de una transferencia o de una inversión no permiten inferir dolo, conocimiento, culpabilidad ni responsabilidad penal.
- No se publican resultados procesales ni tasas de éxito ni promesas de recuperación.
- Anonimización: no se incorporan fechas exactas, cuantías singulares, entidades, juzgados, números de procedimiento ni secuencias fácticas que permitan reidentificar a una persona o a un asunto.

### 5. Resultados: patrones observados

Del análisis del corpus se obtienen tres constataciones principales, formuladas siempre en referencia a los expedientes analizados por PenalTech.

**Primera. El gran fraude de inversión concentra el mayor perjuicio.** Aunque numéricamente el fraude bancario es más frecuente, los expedientes de fraude de inversión —criptoactivos, brókers y plataformas de alta rentabilidad— presentan de forma característica los importes individuales más altos, y son los que con mayor claridad exigen la vía penal frente a la civil bancaria.

**Segunda. Los criptoactivos como vía consolidada.** El fraude con criptoactivos aparece ya como categoría propia dentro del corpus, habitualmente asociado a supuestas inversiones y con particularidades probatorias derivadas de la trazabilidad de la cadena y de la dimensión transfronteriza.

**Tercera. La utilización de identidad ajena como medio.** Con frecuencia el defraudador se sirve de datos o de la identidad de un tercero para articular el fraude o dificultar su rastreo. Se emplea como categoría de medio comisivo, sin prejuzgar la calificación de cada caso.

*Un rasgo transversal: banco frente a vía penal. En la experiencia del despacho, la primera bifurcación de cada asunto es determinar si hubo una operación no autorizada (terreno de la reclamación bancaria) o una transferencia consentida bajo engaño (terreno del gran fraude de inversión, propio de la vía penal). De esa calificación temprana depende toda la estrategia de recuperación.*

### 6. La prueba digital y el rastreo de los fondos

En el fraude de inversión, la evidencia digital —órdenes de transferencia, comunicaciones con la supuesta plataforma, movimientos hacia cuentas puente y, en su caso, direcciones de criptoactivos— constituye el principal soporte para reconstruir el recorrido del dinero. Los expedientes analizados reflejan esa centralidad probatoria.

Esa centralidad, sin embargo, no equivale a una capacidad explicativa absoluta. La trazabilidad técnica responde a qué operación se realizó y hacia dónde, pero el éxito de la recuperación depende también de la rapidez de la reacción, de la cooperación entre jurisdicciones y de la eventual identificación de los destinos finales, con frecuencia fuera de España.

De aquí deriva la aportación central con relevancia práctica para la víctima: la reconstrucción técnica es el punto de partida del análisis, no su conclusión. Documentar tempranamente la prueba, orientar el caso por la vía correcta y activar sin demora la investigación penal y el rastreo de activos son los factores que amplían las opciones de recuperación.

## 7. Discusión

La mayor parte de la información pública sobre el fraude de inversión tiene una finalidad preventiva o se centra en la defensa de quien resulta acusado. Este estudio adopta una perspectiva diferente: analiza qué ocurre cuando el fenómeno se convierte en un procedimiento penal, desplazando el foco hacia la posición de la víctima y hacia la elección de la vía adecuada.

El principal aprendizaje metodológico es que estos asuntos raramente se comprenden a partir de un único indicador y que la primera decisión —banco o vía penal— condiciona todo lo demás. La segunda aportación es demostrar que la experiencia jurídica sistematizada de un despacho puede convertirse en conocimiento reutilizable sin comprometer la confidencialidad de los asuntos.

## 8. Lecciones derivadas de la experiencia práctica

Las observaciones que siguen derivan de la experiencia profesional sistematizada durante la gestión de los expedientes analizados. No constituyen resultados estadísticos independientes y deben interpretarse como tales.

### 8.1. La rapidez de reacción condiciona la recuperación

En el fraude de inversión, cada hora cuenta: los fondos se dispersan con rapidez hacia cuentas puente o criptoactivos. La actuación inmediata amplía de forma significativa las opciones de bloqueo y recuperación.

### 8.2. Elegir la vía correcta desde el inicio

Confundir un gran fraude de inversión con una reclamación bancaria, o a la inversa, hace perder tiempo y derechos. La calificación temprana —operación no autorizada frente a transferencia consentida bajo engaño— orienta toda la estrategia.

### 8.3. La acusación particular como palanca

En estos asuntos, la personación como acusación particular permite impulsar la investigación, dirigir el rastreo de los fondos y reclamar la reparación, más allá de la actuación de oficio.

## 9. Implicaciones prácticas

### 9.1. Para las víctimas de grandes fraudes de inversión

La experiencia del despacho permite ordenar la reacción de la víctima en una secuencia sencilla:

- **Reaccionar de inmediato:** contactar con la entidad y con la plataforma de pago para intentar el bloqueo o la retrocesión, antes de que los fondos se dispersen.
- **Documentar la prueba:** conservar contratos, comunicaciones, justificantes de transferencia y direcciones o identificadores; no borrar nada.
- **Calificar la vía:** determinar si hubo operación no autorizada (reclamación al banco) o transferencia consentida bajo engaño (vía penal).
- **Denunciar:** ante la Policía Nacional o la Guardia Civil, con apoyo, en su caso, en la línea de ayuda del INCIBE, y verificar si el destino figura entre las advertencias de la CNMV.
- **Personarse en el proceso:** valorar la acusación particular para impulsar la investigación, el rastreo de activos y la reparación del perjuicio.

### 9.2. Para periodistas especializados

Frente al tratamiento habitual —centrado en campañas y cifras—, el estudio aporta un enfoque basado en expedientes reales que explica qué sucede cuando el gran fraude de inversión se convierte en procedimiento, siempre preservando la anonimización de las personas afectadas.

### 9.3. Para universidades e investigadores

La metodología demuestra que un despacho puede producir conocimiento aplicado cuando estructura adecuadamente la información generada por su actividad, diferenciando evidencia empírica, interpretación y conclusiones, y preservando la anonimización.

### 9.4. Para supervisores, entidades y cumplimiento

Sin analizar protocolos internos, el informe ilustra cómo determinadas modalidades de fraude de inversión aparecen documentadas cuando el asunto se integra en un procedimiento penal, lo que complementa la labor de alerta de los supervisores y los enfoques estrictamente preventivos.

## 10. Conclusiones

**Primera.** El fraude de inversión online es la variante más lesiva del fraude económico en la red y su víctima dispone de más recursos jurídicos de los que habitualmente conoce.

**Segunda.** La primera decisión —reclamación bancaria por operación no autorizada frente a vía penal por transferencia consentida bajo engaño— condiciona toda la estrategia de recuperación.

**Tercera.** Los criptoactivos se consolidan como vía propia del gran fraude de inversión, con particularidades probatorias y transfronterizas.

**Cuarta.** La reconstrucción técnica de la operación no equivale a su valoración jurídica: es el punto de partida del análisis, no su conclusión.

**Quinta.** La aportación del Observatorio no consiste en explicar el fenómeno en general, sino en ofrecer una fuente de conocimiento basada en la experiencia jurídica documentada, susceptible de actualización periódica.

## 11. Líneas futuras de investigación

El diseño del Observatorio responde a una lógica acumulativa. Cada nueva edición permitirá ampliar el universo analizado, comprobar la estabilidad de las categorías e incorporar nuevas variables cuando la evidencia lo justifique. Se identifican como líneas de continuidad la evolución del fraude de inversión y de los criptoactivos, el seguimiento de la doctrina sobre responsabilidad bancaria, el rastreo transfronterizo de activos y el desarrollo de indicadores longitudinales comparables entre ediciones.

## Nota sobre las fuentes y su verificación

Las fuentes externas citadas se han recopilado mediante investigación documental y se relacionan íntegramente en el apartado de referencias, con indicación de su localizador completo. La jurisprudencia y las cifras oficiales deben verificarse en el momento de cada uso, dado que las estadísticas y las advertencias se actualizan periódicamente. En esta versión, la Sentencia del Tribunal Supremo 571/2025 se ha contrastado en fuentes jurídicas independientes; las resoluciones de la Sala Segunda que puedan incorporarse en ediciones sucesivas se validarán individualmente en el Centro de Documentación Judicial (CENDOJ) antes de su publicación.

## Sobre PenalTech y el Observatorio

El Observatorio PenalTech es la línea de investigación de PenalTech, despacho de abogados fundado en 2020 y especializado en la intersección entre el Derecho Penal y la tecnología: ciberdelincuencia, delitos informáticos y prueba digital, con sedes en Madrid, Sevilla y Málaga. Dirigido por Fran Peláez, asume desde 2021 la asesoría jurídica penal de la Asociación Pro Guardia Civil (APROGC) y fue el primer despacho penalista andaluz acreditado por el Instituto Nacional de Ciberseguridad (2022). Su experiencia en la defensa y en la acusación en delitos económicos y tecnológicos constituye la base de este Observatorio.

Esa experiencia es la que el Observatorio transforma, mediante una metodología homogénea y respetuosa con la confidencialidad, en conocimiento estructurado y verificable de interés general. En materia de fraude de inversión, la principal conclusión de este informe tiene una consecuencia práctica directa para la víctima: elegir cuanto antes la vía correcta y activar la respuesta penal cuando procede es lo que abre las opciones reales de recuperación.

## Referencias

- [1] España. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (arts. 248-250), texto consolidado. BOE, núm. 281. Referencia BOE-A-1995-25444. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>
- [2] España. Ley Orgánica 14/2022, de 22 de diciembre, de transposición de directivas y reforma del Código Penal. BOE. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2022-21800>
- [3] España. Tribunal Supremo (Sala Primera, de lo Civil). Sentencia n.º 571/2025, de 9 de abril de 2025 (responsabilidad de la entidad bancaria en operaciones de pago no autorizadas). A verificar en CENDOJ en el momento de cada cita.
- [4] Ministerio del Interior. Informe sobre la cibercriminalidad en España 2024 (publicado el 21 de noviembre de 2025). Disponible en: <https://www.interior.gob.es/opencms/es/detalle/articulo/La-cibercriminalidad-se-redujo-un-16-por-ciento-en-2024-el-primer-descenso-de-la-serie-historica/>
- [5] Comisión Nacional del Mercado de Valores (CNMV). Advertencias sobre entidades no autorizadas («chiringuitos financieros») y Guía del inversor. Disponible en: <https://www.cnmv.es/portal/advertencias>
- [6] INCIBE (Instituto Nacional de Ciberseguridad). Cómo denunciar si has sido víctima de un fraude o delito. Línea de Ayuda en Ciberseguridad. Disponible en: <https://www.incibe.es/ciudadania/ayuda/denuncia>
- [7] Unión Europea y España. Directiva (UE) 2015/2366 sobre servicios de pago y Real Decreto-ley 19/2018, de servicios de pago (régimen de operaciones no autorizadas y carga de la prueba).

## Anexo A. Ficha metodológica y recuentos

Este anexo recoge los recuentos exactos del corpus de fraude económico online analizado, del que esta edición examina el segmento de inversión y criptoactivos. Los datos describen la cartera documentada de PenalTech y no constituyen una muestra representativa de la criminalidad española; las categorías se solapan y no permiten inferir dolo, conocimiento, culpabilidad ni prevalencia nacional.

### A.1. Ficha técnica del corpus

| Parámetro                                       | Valor                                                           |
|-------------------------------------------------|-----------------------------------------------------------------|
| Base documental del despacho                    | +1.800 expedientes (desde 2013)                                 |
| Universo de ciberdelincuencia analizado         | 230 expedientes (2020-2026)                                     |
| Corpus de fraude económico online               | 74 expedientes                                                  |
| Foco de esta edición                            | Fraude de inversión y criptoactivos                             |
| Concordancia entre revisores                    | 90 %                                                            |
| Umbral de publicación como estadística autónoma | ≥ 5 expedientes                                                 |
| Tipo de investigación                           | Estudio cualitativo / mixto de casos (basado en la experiencia) |

### A.2. Categorías internas observadas (recuentos)

| Categoría interna (modus operandi)                     | Expedientes | Sobre 74     |
|--------------------------------------------------------|-------------|--------------|
| Fraude bancario no especificado                        | 31          | 41,9 %       |
| Utilización de identidad ajena (como medio del fraude) | 20          | 27,0 %       |
| <b>Fraude con criptoactivos (foco de esta edición)</b> | <b>5</b>    | <b>6,8 %</b> |
| Otras modalidades (<5, cualitativas)                   | 18          | 24,3 %       |

Las categorías describen modus operandi, no calificaciones jurídicas; pueden concurrir y no se publican como estadísticas autónomas los subgrupos inferiores a cinco expedientes. Los grandes fraudes de inversión de importe elevado se tratan de forma cualitativa.

Observatorio PenalTech · Fraude de inversión online · Primera edición · Octubre de 2026.