Incautación y comiso de criptoactivos en Colombia

Seizure and forfeiture of crypto-assets in Colombia

Apreensão e confisco de criptoativos na Colômbia

Carlos Vicente Pérez Giraldo[1]

DOI: https://doi.org/10.47741/17943108.846

Cómo citar: Pérez-Giraldo, C. V. (2026). Incautación y comiso de criptoactivos en Colombia. *Revista Criminalidad, 68(1)*: 297-313. https://doi.org/10.47741/17943108.846

- **Fecha de recepción: 2025/12/22**
- **Fecha de aprobación: 2026/02/12**

Resumen Este artículo examina el régimen jurídico aplicable a la incautación y el comiso de criptoactivos en Colombia. Se define el marco conceptual y normativo de la materia, con especial referencia a la naturaleza jurídica y tecnológica de las criptomonedas y de los *tokens* no fungibles (NFT, por sus siglas en inglés: *non-fungible tokens*), así como a los actores institucionales y privados que pueden intervenir en estas actuaciones: la Fiscalía General de la Nación, los jueces de la República, los órganos de policía judicial y los proveedores de servicios de activos virtuales centralizados (PSAVC). Asimismo, se diferencia, desde una perspectiva técnico-operativa, el ecosistema en que pueden encontrarse los criptoactivos, distinguiendo entre regímenes de heterocustodia y de autocustodia. De la mano con los lineamientos trazados por la Fiscalía General de la Nación, se examinan y proponen técnicas idóneas para la ejecución de estas medidas. Por último, se enfatiza la necesidad de ejercer un control de legalidad sobre los procedimientos y de garantizar el respeto al debido proceso, al derecho de defensa del investigado, de las víctimas y de los terceros con interés legítimo en la actuación.

Palabras clave

Criptoactivos; criptomonedas; incautación; comiso; Ley 906 de 2004; PSAVC; cadena de custodia digital; autocustodia; heterocustodia

Open Access | Diamond Open Access | CC BY-NC-ND 4.0© por Policía Nacional de Colombia

1. Magíster en Ciencias Penales y Criminológicas. Universidad Externado de Colombia. Bogotá, D. C., Colombia.
vicente.perez@uexternado.edu.co

Abstract This article examines the legal framework governing the seizure and forfeiture of crypto-assets in Colombia. It defines the conceptual and regulatory framework of the subject, with particular reference to the legal and technological nature of cryptocurrencies and non-fungible tokens (NFTs), as well as the institutional and private actors that may be involved in these proceedings, including the Attorney General's Office (Fiscalía General de la Nación), judges, judicial police bodies and centralised providers of virtual asset services. Similarly, from a technical and operational perspective, the article distinguishes the ecosystems in which crypto-assets may be situated, differentiating between custody and self-custody regimes. In line with the guidelines established by the Attorney General's Office, the article examines and proposes appropriate techniques for the implementation of these measures. Finally, it emphasises the need to exercise legal oversight over the procedures and to ensure respect for due process and the right of defence of the person under investigation, the victims and third parties with a legitimate interest in the proceedings.

Keywords
Crypto-assets; cryptocurrencies; seizure; forfeiture; Law 906 of 2004; PSAVC; digital chain of custody; self-custody; third-party custodyi

Resumo Este artigo examina o regime jurídico aplicável à apreensão e ao perdimento de criptoativos na Colômbia. Define-se o referencial conceitual e normativo da matéria, com especial ênfase à natureza jurídica e tecnológica das criptomoedas e dos tokens não fungíveis (NFTs), bem como aos atores institucionais e privados que podem intervir nesses procedimentos, incluindo a Procuradoria-Geral da Nação (Fiscalía General de la Nación), os juízes, os órgãos de polícia judiciária e os fornecedores de serviços de ativos virtuais centralizados. Do mesmo modo, sob uma perspectiva técnico-operacional, distinguem-se os ecossistemas nos quais os criptoativos podem estar inseridos, diferenciando-se entre regimes de heterocustódia e de autocustódia. Em consonância com as diretrizes estabelecidas pela Procuradoria-Geral da Nação, o artigo examina e propõe técnicas adequadas para a execução dessas medidas. Por fim, enfatiza-se a necessidade de exercer controle de legalidade sobre os procedimentos e de garantir o respeito ao devido processo legal e ao direito de defesa do investigado, das vítimas e de terceiros com interesse legítimo na atuação.

Palavras-chave
Criptoativos; criptomoedas; apreensão; perdimento; Lei 906 de 2004; fornecedores de serviços de ativos virtuais centralizados; cadeia de custódia digital; autocustódia; custódia por terceiros

Introducción

Los criptoactivos constituyen una de las innovaciones tecnológicas y económicas de mayor impacto en los últimos tiempos, en tanto representan herramientas de libertad monetaria, descentralización financiera y resistencia a la censura (Ammous, 2018). No obstante, como ocurre con cualquier creación humana, también pueden ser empleados para fines ilícitos, tal como sucede con el dinero de curso legal que puede utilizarse en la comisión de delitos o derivar de conductas punibles. En consecuencia, es necesario evaluar los procedimientos penales para la incautación y el comiso de estos activos digitales, con un doble propósito: establecer mecanismos eficaces de prevención de la criminalidad y, a la vez, garantizar el debido proceso a los ciudadanos.

El presente artículo examina el régimen jurídico de la incautación y el comiso de criptoactivos en el procedimiento penal colombiano. En primer lugar, se indaga si los criptoactivos son objeto susceptible de tales medidas en el derecho colombiano; posteriormente, se analizan el procedimiento y las técnicas disponibles para hacerlas efectivas. El estudio distingue entre el aseguramiento de activos en entornos heterocustodiales (PSAVC/Exchanges) y la incautación en cadena (*on-chain*) respecto a las billeteras de autocustodia. Asimismo, articula las recientes regulaciones nacionales (Fiscalía General de la Nación, Unidad de Información y Análisis Financiero [UIAF], Sociedad de Activos Especiales [SAE]) con los estándares internacionales (Grupo de Acción Financiera Internacional [GAFI]/Grupo de Acción Financiera de Latinoamérica [GAFILAT]).

Se sostiene que la eficacia de las medidas de incautación depende, en gran medida, del entorno en que se desarrollen las operaciones y del tipo de criptoactivo involucrado. En los entornos de heterocustodia y tratándose de criptomonedas con emisor centralizado, cobran particular importancia las órdenes de incautación y las medidas cautelares que pueden solicitarse ante los jueces de control de garantías. En contraste, los entornos de autocustodia y los criptoactivos descentralizados representan un desafío mayor de eficacia, por cuanto requieren el acceso a los dispositivos y claves privadas que los resguardan. Por último, se subraya la importancia de la inferencia por motivos fundados entre los criptoactivos y la actividad delictiva como presupuesto de la incautación y el comiso, así como la necesidad de salvaguardar los derechos de terceros, en especial de las víctimas y de los prestadores de servicios.

Marco conceptual y normativo: criptoactivos, comiso e incautación

Criptoactivos, criptomonedas y NFT

Desde una perspectiva jurídica, los criptoactivos constituyen bienes, en tanto objetos de apropiación que integran el patrimonio y son susceptibles de valoración económica. Su rasgo esencial es la inmaterialidad e intangibilidad, dado que existen y se transfieren mediante tecnologías como la

cadena de bloques (*blockchain*). Entre ellos se encuentran, en primer lugar, las criptomonedas, entendidas como archivos de datos "cuyo objetivo primordial es cumplir las mismas funciones que el dinero tradicional (unidad de medida, reserva de valor y medio de pago)" (Andrade, 2023, p. 99). Asimismo, se incluyen los *tokens* no fungibles (NFT, por sus siglas en inglés), que se diferencian de los anteriores por ser únicos e irrepetibles, aunque igualmente alojados en la cadena de bloques y dotados de contenido patrimonial, lo que los hace susceptibles de transferencia o enajenación (*ibidem*).

En este estudio resulta fundamental distinguir el ecosistema en que los criptoactivos son custodiados y administrados. Una primera modalidad corresponde a la heterocustodia, en la cual el titular delega la gestión en un tercero o prestador de servicios de activos virtuales centralizado (PSAVC), como los denominados *exchanges* o brókeres. Estas plataformas actúan como intermediarias en el intercambio de criptomonedas y NFT, y concentran la administración de los activos, pues la posesión y custodia en la cadena de bloques permanece bajo el control del prestador de servicios, quien detenta la clave privada (Torres, 2019).

El segundo escenario es el de la autocustodia (*self-custody*), en el que los criptoactivos son asegurados y gestionados directamente por sus dueños mediante billeteras frías (hardware *wallets*), que mantienen las claves privadas fuera de la red, o billeteras de software. En este caso, cada persona administra sus claves privadas y, en consecuencia, no existe un tercero al cual acudir para solicitar, por ejemplo, la transferencia o el congelamiento de los fondos. Esta práctica ofrece mayor privacidad y autonomía, bajo la premisa extendida en el ámbito cripto de que la propiedad efectiva de los activos corresponde a quien controla las claves privadas (*Not your keys, not your coins*). Ello refuerza la seguridad frente a estafas y ataques informáticos (Gideon, 2025), pero plantea un reto adicional para lograr la incautación y el comiso por parte de las autoridades.

Por último, cabe diferenciar entre los criptoactivos emitidos por un agente centralizado; es decir, una persona o plataforma que crea y distribuye *tokens* con control sobre sus protocolos y sistemas de registro de saldos y transacciones (Arango-Arango et al., 2018). Tal es el caso de ciertas criptomonedas estables (*stablecoins*), entre las cuales destacan las que ofrecen paridad con el dólar estadounidense, como Tether (USDT), emitido por Tether Limited, con sede en Hong Kong, o USD Coin (USDC), emitido por la estadounidense Circle Internet Group, Inc.

El escenario opuesto lo representan los criptoactivos descentralizados, como bitcoin, que carecen de una autoridad emisora o ente central de control. Su protocolo está diseñado para que el registro de saldos y operaciones sea público y validado directamente por los participantes de la red (*ibidem*). En consecuencia, respecto de este tipo de activos no existe un emisor al cual acudir para su control, de modo que su aseguramiento dependerá exclusivamente del entorno de custodia en que se encuentren.

Comiso e incautación: generalidades

El comiso es una medida jurídica que extingue, en favor del Estado, el derecho de dominio sobre los "efectos provenientes del delito y de los instrumentos con que se ejecutó" (ASALE, 2025), salvo que se trate de bienes pertenecientes a un tercero de buena fe. La jurisprudencia colombiana ha sostenido que no constituye una pena, sino una consecuencia del fallo condenatorio, con carácter de medida de política criminal, orientada a fines preventivos y portadora de "un mensaje ético en el sentido de que el delito no es un medio legítimo para producir riqueza (…)" (CSJ, AP4073-2024, 24 jul. 2024, rad. 60055; AP5421-2019, 12 dic. 2019, rad. 56507).

Así fue consagrado en el artículo 100 del Código Penal colombiano, conforme al cual el comiso recae sobre los "instrumentos y efectos con los que se haya cometido la conducta punible o que provengan de su ejecución".

Por su parte, el artículo 82 del Código de Procedimiento Penal (Ley 906 de 2004) dispone que la medida de comiso recae: (a) "sobre los bienes y recursos del penalmente responsable que provengan o sean producto directo o indirecto del delito"; (b) sobre "aquellos utilizados o destinados a ser utilizados en los delitos dolosos como medio o instrumento para la ejecución del mismo"; y (c) sobre los bienes del penalmente responsable "cuyo valor corresponda o sea equivalente al de bienes producto directo o indirecto del delito". Todo lo anterior, "sin perjuicio de los derechos que tengan sobre ellos los sujetos pasivos o los terceros de buena fe".

La pregunta de si los criptoactivos pueden ser objeto de comiso se responde afirmativamente. En términos generales, pueden constituir efectos o bienes provenientes de delitos, o ser utilizados para la comisión de conductas dolosas. Más en concreto, el parágrafo del artículo 82 de la Ley 906 de 2004 establece que, para estos efectos, "se entenderán por bienes todos los que sean susceptibles de valoración económica o sobre los cuales pueda recaer derecho de dominio, corporales o incorporales, muebles o inmuebles (…)". En consecuencia, al ser objeto de derecho de propiedad y susceptibles de valoración económica, tanto las criptomonedas como los NFT constituyen bienes que, en la medida en que guarden relación con una conducta punible, pueden ser objeto de comiso.

En cuanto a la incautación, esta se configura como una medida cautelar de carácter material consistente en la toma de posesión de bienes muebles por parte de la autoridad competente. Tiene una relación de medio a fin con el comiso, de manera que no se limita a la mera aprehensión de los bienes, sino que constituye una "medida cautelar al servicio de una consecuencia jurídica definitiva como lo es el comiso" (CSJ, SP1136-2025, 30 abr. 2025, rad. 67446).

La jurisprudencia ha precisado que la incautación, en tanto medida cautelar, debe ser objeto de legalización en audiencia preliminar ante el juez de control de garantías, conforme al artículo 84 de la Ley 906 de 2004; mientras que el comiso, como medida definitiva, está supeditado a la definición de la acción penal y corresponde adoptarlo al juez de conocimiento (*ibidem*).

De igual forma, la Corte Suprema de Justicia ha distinguido entre la aprehensión de bienes con fines de incautación para efectos de comiso y la función constitucional de la Fiscalía General de la Nación de practicar actos de investigación orientados a la recolección de elementos materiales

probatorios, los cuales deben asegurarse bajo cadena de custodia (CSJ, SP2129-2022, 25 may. 2022, rad. 54153). Esta diferenciación resulta relevante: en el primer escenario, el levantamiento de la incautación debe solicitarse ante el juez de control de garantías; mientras que, respecto de los elementos materiales probatorios que poseen valor comercial pero no han sido objeto de medida cautelar, la ley dispone que deben ser examinados, registrados para efectos de preservación de la prueba y, posteriormente, devueltos a su propietario, poseedor o tenedor legítimo, siempre que no hayan sido utilizados para la comisión del delito y no se requiera promover acción de extinción de dominio (cf. arts. 88 y 266 C. de P. P.).

Estándares internacionales y de derecho extranjero

Los estándares internacionales contra el lavado de dinero y la financiación del terrorismo del Grupo de Acción Financiera Internacional (FATF, por sus siglas en inglés, 2021) constituyen uno de los referentes globales más influyentes en la materia. Este organismo no solo precisó las definiciones básicas de "activo virtual" y de prestador de servicios de activos virtuales centralizado (PSAVC), sino que extendió su alcance a fenómenos emergentes como las *stablecoins*, cuya paridad con monedas estatales ha facilitado su utilización en esquemas de blanqueo transfronterizo. Asimismo, reforzó la denominada *Travel Rule*, imponiendo a los intermediarios la obligación de transmitir información verificable tanto del ordenante como del beneficiario en cada transacción, e introdujo directrices específicas para enfrentar el creciente volumen de operaciones *peer-to-peer* (P2P) que prescinden de intermediarios regulados. Tales lineamientos buscan reducir los espacios de anonimato y consolidar estándares homogéneos de debida diligencia, indispensables para la cooperación internacional en investigaciones financieras.

Por su parte, el Consejo de Europa (2021) elaboró una guía operativa que trasciende la dimensión normativa para ofrecer procedimientos concretos de incautación de criptoactivos. El documento describe, con ejemplos prácticos y diagramas de flujo, la forma en que deben asegurarse los activos almacenados en software *wallets*, hardware *wallets* y extensiones de navegador, cada uno con riesgos y técnicas propias. Resalta, en particular, la importancia de verificar la autenticidad de los *tokens* y de los contratos inteligentes antes de ejecutar traslados, así como la necesidad de gestionar adecuadamente los *approvals* en redes basadas en Ethereum Virtual Machine (EVM), en las que terceros pueden detentar permisos de disposición sobre los fondos. Esta aproximación metodológica convierte la guía en un manual técnico útil para investigadores y jueces, al tiempo que permite alinear la práctica forense con los estándares de legalidad y de cadena de custodia exigidos por el derecho penal europeo.

La Europol, en su informe más reciente (2022), complementó este panorama al documentar patrones de abuso criminal asociados a los criptoactivos. Entre ellos, se destacan el uso de *mixers*, *tumblers* y protocolos de privacidad como Monero o Tornado Cash, así como la creciente utilización de *stablecoins* para pagos ilícitos de alto volumen. No obstante, también resaltó la utilidad investigativa derivada de la trazabilidad pública de las *blockchains* abiertas, como bitcoin y Ethereum, que

permiten reconstruir flujos financieros con un grado de transparencia inédito frente al dinero en efectivo. El informe subraya que, cuando estas herramientas se combinan con órdenes judiciales de cooperación internacional y técnicas de análisis de *big data*, se constituyen en un mecanismo útil para seguir el rastro del patrimonio ilícito.

En el contexto latinoamericano, la guía del Ministerio Público Fiscal de Argentina (UFECI, 2023) constituye un ejemplo de adaptación regional de las recomendaciones internacionales. Este instrumento consolidó una metodología integral para la identificación, preservación y traslado de criptoactivos; estandarizó formatos de actas y procedimientos para la manipulación segura de semillas BIP-39, e incluyó advertencias específicas sobre riesgos técnicos como la existencia de *sweeper scripts* –programas automatizados que barren de manera inmediata los saldos de una billetera cuando detectan actividad–, los cuales pueden frustrar el aseguramiento estatal si no se actúa con la debida celeridad.

Directrices institucionales

Cooperación interinstitucional e internacional

La Unidad de Información y Análisis Financiero (UIAF) fortaleció el marco de control de los criptoactivos con la expedición de la Resolución 314 de 2021, mediante la cual impuso obligaciones de reporte a los prestadores de servicios de activos virtuales centralizados (PSAVC) en Colombia. Esta resolución exige a los intermediarios implementar procedimientos de debida diligencia y reportar operaciones sospechosas relacionadas con criptoactivos, con el fin de proporcionar a las autoridades de investigación insumos tempranos para la inmovilización y trazabilidad de estos activos. La articulación entre las obligaciones administrativas de los PSAVC y las medidas cautelares penales evidencia la convergencia entre derecho administrativo y derecho penal, orientada a cerrar los espacios de anonimato y a fortalecer la cooperación interinstitucional en la persecución del patrimonio ilícito.

La obligación de reporte a cargo de los proveedores de servicios de activos virtuales refuerza la capacidad del Estado para preservar evidencia contable y digital, garantizando que las transacciones no se diluyan en el anonimato característico de las redes descentralizadas. La coordinación entre la UIAF y la Fiscalía General de la Nación resulta esencial para detectar vínculos entre criptoactivos y cuentas bancarias tradicionales, lo cual facilita rastrear el flujo del dinero híbrido. Asimismo, permite identificar contrapartes relevantes y jurisdicciones de riesgo en las que suelen operar esquemas de ocultamiento transnacional.

En el ámbito internacional, la asistencia jurídica mutua constituye un instrumento imprescindible para la incautación de criptoactivos custodiados en *exchanges* extranjeros. Mediante convenios y acuerdos especializados, las autoridades pueden solicitar la inmovilización de fondos y la entrega certificada de registros digitales. Para agilizar estos procesos, se recomienda el uso de

plantillas estandarizadas que incluyan especificaciones técnicas precisas, como la identificación de direcciones públicas, hashes de transacciones y formatos de exportación de información. Este nivel de detalle evita demoras y garantiza que la evidencia recolectada cumpla con los estándares probatorios exigidos.

Los estándares del GAFI, y en particular la *Travel Rule*, imponen a los PSAVC la obligación de transmitir datos verificables tanto del ordenante como del beneficiario en cada transacción. Esta exigencia facilita el seguimiento de operaciones transfronterizas y la cooperación entre jurisdicciones, incluso en escenarios en los que intervienen mezcladores, protocolos de privacidad o puentes de intercambio entre distintas cadenas de bloques.

Por último, el Manual de Policía Judicial y los lineamientos sobre cadena de custodia complementan y establecen pautas prácticas para la preservación y documentación de elementos materiales probatorios digitales. Entre estas técnicas se incluyen las capturas de pantalla, el registro de direcciones públicas y códigos de transacción, así como la utilización de bolsas de Faraday para prevenir la manipulación remota de dispositivos incautados. Estas herramientas reflejan que los actos de investigación relacionados con criptoactivos exigen la adaptación de las técnicas forenses tradicionales al escenario digital. En consecuencia, el aseguramiento no se limita a la aprehensión formal del activo, sino que requiere la implementación de procedimientos técnicos que garanticen la fiabilidad de la prueba y la posibilidad de su valoración en juicio.

"Guía para la adopción de medidas cautelares en relación con criptoactivos en el proceso penal y de extinción de dominio"

En marzo de 2025, la Fiscalía General de la Nación expidió la Resolución 0-0053 de 2025, mediante la cual adoptó como lineamiento la "Guía para la adopción de medidas cautelares en relación con criptoactivos en el proceso penal y de extinción de dominio" (FGN, 2025). Este documento regula el procedimiento para la adopción de las siguientes medidas sobre criptoactivos: (a) incautación con fines de comiso; (b) suspensión del poder dispositivo; (c) adopción de medidas orientadas al restablecimiento de derechos de la víctima; y (d) embargo y secuestro en el marco del proceso de extinción del derecho de dominio. Su alcance, no obstante, se limita a las criptomonedas, pues no aborda la incautación de *tokens* no fungibles (NFT, por sus siglas en inglés: *non-fungible tokens*).

La guía inicia con un glosario de definiciones básicas destinado a orientar la labor de los fiscales y funcionarios intervinientes. Entre los conceptos incluidos se destacan: *blockchain*, minería, criptoactivo, criptomoneda, *token*, Ethereum, ERC-20, ERC-721, *DeFi*, billetera, billetera fría, billetera de software, palabra o frase semilla, *hash* transaccional, *fee* o comisión, entre otros.

Dispone que el fiscal puede ordenar la incautación con fines de comiso, en los términos de los artículos 83 y siguientes de la Ley 906 de 2004. Para ello, debe seguir tres fases: (a) planeación, que comprende las actividades de alistamiento y logística previas al procedimiento; (b) medida cautelar, consistente en la ejecución de las medidas diseñadas, así como en la documentación

de cada actividad, con la correspondiente legalización ante el juez de control de garantías; y (c) administración, que implica la entrega de los activos virtuales a la entidad encargada de su custodia en nombre del Estado.

En la fase de planeación resulta esencial identificar el ecosistema en el que se encuentren los criptoactivos y la modalidad de custodia, pues de ello depende el acceso a la clave privada o la necesidad de obtener la frase semilla. En primer término, debe establecerse el origen o uso ilícito de los criptoactivos y su relación con los indiciados. Para este fin, es indispensable identificar el tipo de activo (por ejemplo, Tether-USDT, USDC, Bitcoin, ETH, entre otros), lo cual determina la cadena de bloques en que se encuentra y el protocolo aplicable. En segundo lugar, deben identificarse los dispositivos utilizados para realizar las transacciones (computadores, teléfonos inteligentes, tabletas, billeteras frías o de software). Y, por último, las aplicaciones empleadas para efectuar dichas transacciones, especificando si se trata de billeteras con custodia o sin custodia (FGN, 2025).

Esta última distinción reviste especial importancia, en la medida que determina si se trata de un entorno administrado por un PSAVC o de autocustodia (*on-chain*). Sin embargo, la nomenclatura adoptada por la guía no resulta enteramente precisa, pues identifica el entorno custodial únicamente con la administración centralizada. Como se ha señalado, todos los criptoactivos requieren de algún tipo de custodia; la diferencia fundamental radica en si esta es ejercida directamente por el titular (autocustodia) o por un tercero intermediario (heterocustodia).

Procedimiento según el tipo de control del activo

En los entornos de heterocustodia

Cuando los criptoactivos son administrados por proveedores de servicios de activos virtuales centralizados (PSAVC) –esto es, *exchanges* o brókeres–, la medida cautelar no se dirige directamente al investigado, sino a un tercero, quien se convierte en sujeto obligado a cooperar con las autoridades judiciales. En estos escenarios, el fundamento jurídico se encuentra tanto en las disposiciones procesales de la Ley 906 de 2004, que habilitan la incautación y la suspensión del poder dispositivo, como en la Resolución 314 de 2021 de la UIAF, que impone deberes de reporte y trazabilidad a los PSAVC.

En estos casos, la Fiscalía debe identificar el proveedor en el que opera el investigado, las cuentas utilizadas para la administración de fondos, las políticas internas del PSAVC y los canales de notificación judicial. Para tal fin, la policía judicial debe elaborar un informe que relacione las cuentas o billeteras vinculadas a la actividad delictiva, el tipo de criptoactivo, la red, el monto, el usuario del indiciado y sus datos de identificación ante el proveedor. Este estándar probatorio resulta necesario para satisfacer la exigencia de inferencia por motivos fundados.

Debe recordarse que los reglamentos internos de los PSAVC imponen políticas de conocimiento del cliente (KYC, *know your customer*), que obligan a los usuarios a registrarse con información personal autenticada (nombre, nacionalidad, documento de identificación, dirección de domicilio).

Este elemento es fundamental en los procedimientos de incautación con fines de comiso, puesto que permite acreditar la titularidad de los criptoactivos por parte del investigado. En este sentido, las transacciones realizadas desde una cuenta asociada a datos personales del investigado constituyen un indicio primario de propiedad. En contraste, cuando las operaciones se realizan a través de cuentas de terceros, corresponde al investigador establecer la inferencia entre el titular formal y el investigado, así como entre las transacciones y la conducta punible.

De acuerdo con la "Guía" de la Fiscalía, el fiscal debe determinar la procedencia del bloqueo de cuentas por parte del PSAVC, para evitar la pérdida de fondos; y "[s]i el PSAVC accede al congelamiento, esta acción equivale a una incautación con fines de comiso" (FGN, 2025, p. 41).

Esta disposición merece críticas en dos aspectos. Primero, el congelamiento de fondos o la suspensión de cuentas dentro de las plataformas de intercambio no equivale a la incautación, por dos razones: (a) la incautación implica la aprehensión material –en este contexto, técnica– del bien, mientras que el congelamiento únicamente supone su inmovilización sin transferencia de control; y (b) la incautación es una actividad procesal reglada en cabeza de autoridades judiciales, de manera que, conforme a la Ley 906 de 2004 (arts. 201 y ss.), resulta irregular atribuir a los PSAVC funciones de policía judicial que no les competen.

En este sentido, el congelamiento se asimila a una medida cautelar innominada, prevista en el literal c) del numeral 1 del artículo 590 del Código General del Proceso, aplicable por remisión al procedimiento penal (art. 1, *ibidem*). Esta disposición faculta al juez para adoptar "cualquier medida que encuentre razonable para la protección del derecho objeto de litigio, impedir su infracción o evitar las consecuencias derivadas de la misma, prevenir daños, hacer cesar los que se hubieren causado o asegurar la efectividad de la pretensión". En el proceso penal, tales medidas deben ser solicitadas ante el juez de control de garantías, en el marco del debido proceso y con participación de los intervinientes. Así, si la audiencia es previa a la imputación, será reservada (art. 212B, Ley 906 de 2004); en cambio, si ocurre tras la formulación de imputación, deberá contar con la presencia de la defensa, de las víctimas y del propio PSAVC.

La segunda crítica radica en la debilidad de la orden de incautación, en la medida que la "Guía" establece una simple solicitud al PSAVC, el cual, con base en sus políticas internas, podría rehusarse a ejecutarla. Conviene recordar que las normas de procedimiento penal son de orden público, y por tanto no son derogables ni subordinables a reglamentos privados.

De ahí que, si la Fiscalía dispone de elementos probatorios suficientes para sustentar la inferencia sobre la materialidad de la conducta y la intervención del investigado, no resulta necesario recurrir a una medida previa como el congelamiento de los fondos. Lo procedente es ordenar al PSAVC la transferencia de los fondos a las billeteras oficiales administradas por la Fiscalía General de la Nación, de manera que se produzca la aprehensión técnica de los criptoactivos por parte de los órganos con funciones de policía judicial, con posterior control de legalidad ante el juez de garantías dentro del plazo de 36 horas. En este sentido, el congelamiento responde a protocolos internos de seguridad de los intermediarios, y no a una medida procesal autónoma prevista en la ley.

Ahora bien, puede ocurrir que el PSAVC se encuentre ubicado fuera de la jurisdicción nacional. En tal caso, el fiscal deberá consultar a la Dirección de Asuntos Internacionales de la Fiscalía para

verificar la existencia de convenios de cooperación o, en su defecto, gestionar la asistencia judicial mutua mediante carta rogatoria. De igual forma, debe determinar si la solicitud puede tramitarse en idioma español o si requiere traducción oficial de la orden y de los informes respectivos.

Por último, el fiscal, como director de la investigación, debe asegurarse de que el entorno en el que se recibirán los criptoactivos esté técnicamente habilitado para gestionar las transacciones. Ello incluye verificar que las billeteras institucionales dispongan del saldo suficiente para cubrir las comisiones de la red, y que sean compatibles con la criptomoneda objeto de la medida. Una omisión en este aspecto podría ocasionar la pérdida de los fondos, con responsabilidad para el fiscal y los funcionarios ejecutores. En consecuencia, resulta indispensable la documentación rigurosa de todo el procedimiento, máxime cuando las operaciones realizadas en la cadena de bloques son de verificación pública.

En los entornos de autocustodia

En los casos de autocustodia, la diligencia de incautación adquiere una complejidad particular, puesto que la clave privada o la frase semilla de recuperación resulta imprescindible para habilitar el acceso y disposición de los fondos. En consecuencia, el aseguramiento requiere la aprehensión física de dispositivos como las billeteras frías o ubicar las billeteras de software y, además, obtener las frases semilla o las contraseñas mnemotécnicas.

La "Guía" de la Fiscalía interpreta que, en estos escenarios, los criptoactivos se encuentran "en el lugar de los hechos" (FGN, 2025, p. 42). Sin embargo, conviene precisar que los criptoactivos en sí mismos no se hallan en dicho lugar, sino en la *blockchain*; lo que se encuentra físicamente en el sitio son los dispositivos mediante los cuales se gestionan, o la información correspondiente a las claves privadas y frases semilla necesarias para ejercer su control.

Para la ejecución de estos procedimientos, la "Guía" establece que deben otorgarse facultades a la policía judicial para practicar allanamientos y registros, tanto de los lugares donde se presuma la existencia de dispositivos de custodia (como billeteras frías) como de soportes físicos o digitales que contengan claves privadas o frases semilla. En esta labor, se contempla la búsqueda de archivos digitales, libretas, notas manuscritas o recordatorios, aunque en la práctica de la autocustodia se recomienda que los usuarios conserven la información fuera de línea y en soportes resistentes a accidentes (como placas metálicas capaces de resistir incendios o inundaciones).

Asimismo, se establece la viabilidad de que la persona investigada colabore facilitando la información o localización de las claves privadas. No obstante, esta posibilidad es absolutamente voluntaria del sujeto, puesto que, en el ordenamiento jurídico colombiano, por mandato del artículo 33 constitucional, se garantiza el principio *nemo tenetur*, en virtud del cual se puede guardar silencio para no declarar contra sí mismo.

Al respecto, es paradigmático el caso de la caña de pescar en Irlanda (*fishing rod case*), en el que las autoridades incautaron múltiples billeteras que contienen aproximadamente 6000 bitcoins provenientes del tráfico de drogas, pero hasta la fecha no se han podido desbloquear los fondos, ya que las claves privadas estaban escritas en una hoja de papel que no fue encontrada por los

investigadores. Esto evidencia que, en entornos de autocustodia y tratándose de criptomonedas descentralizadas, aunque se incauten las billeteras, los fondos permanecen inaccesibles si no se obtienen las claves privadas.

Sin perjuicio de lo anterior, una vez bajo control estatal los dispositivos y las claves, resulta indispensable ejecutar de inmediato la transferencia de la totalidad de los activos hacia direcciones institucionales. Para reforzar la seguridad, la "Guía" recomienda el almacenamiento en frío (*cold wallets*), con el fin de neutralizar intentos de sustracción remota o automatizada, aunque también autoriza el uso de billeteras de software. No obstante, también reconoce que no siempre resulta razonable transferir saldos inferiores a las comisiones de red, en cuyo caso la decisión debe documentarse debidamente.

Por último, la "Guía" enfatiza la necesidad de protocolos de cadena de custodia digital, que aseguren la integridad probatoria. La finalidad no es únicamente el aseguramiento del activo, sino también la documentación estandarizada de cada operación técnica, incluyendo direcciones públicas, códigos *hash* y transacciones (TxID) asociadas a cada billetera. Este procedimiento busca prevenir cuestionamientos posteriores sobre manipulación, pérdida o sustracción, y permite al juez de control de garantías verificar la trazabilidad de la medida. La exigencia de documentación digital equipara la incautación de criptoactivos a la de evidencias físicas, trasladando al entorno virtual los principios de inmutabilidad y verificabilidad que gobiernan la cadena de custodia tradicional.

En todo caso, la "Guía" presenta algunas limitaciones que conviene advertir. No ofrece un tratamiento diferenciado para las billeteras multifirma, cuya incautación resulta especialmente compleja, pues exige la concurrencia de varios firmantes y no basta con la aprehensión de un único dispositivo o semilla. Tampoco contempla de manera suficiente las particularidades de las billeteras determinísticas jerárquicas (HD *wallets*), en las que una sola semilla puede generar un número indefinido de direcciones, lo que plantea riesgos de incautaciones incompletas. Igualmente, omite referencias a amenazas técnicas como los *sweeper scripts*, que pueden barrer saldos de manera inmediata al detectar actividad en la billetera, comprometiendo la eficacia de la medida si no se adoptan precauciones previas. A ello se suma la ausencia de lineamientos sobre la necesidad de reforzar la seguridad mediante transacciones parcialmente firmadas en frío (PSBT, por sus siglas en inglés) o de estandarizar la verificación pública de operaciones en exploradores de bloques, prácticas que fortalecen la transparencia y la trazabilidad en juicio. Por tanto, aunque la guía constituye un avance importante, en una futura oportunidad sería conveniente actualizar los lineamientos para lograr un mayor acoplamiento entre las técnicas de investigación judicial y las sofisticaciones de la tecnología *blockchain*, a fin de garantizar que la incautación y el comiso de criptoactivos no se frustren en la práctica.

Medidas complementarias para el entorno *DeFi*

En los escenarios en que los criptoactivos presentan características técnicas adicionales, son necesarias las medidas complementarias específicas. Así, tratándose de *stablecoins* cuyos emisores cuentan con la facultad de incluir direcciones en listas negras, resulta procedente solicitar directamente al emisor la inmovilización de los fondos. Tal es el caso de Tether (USDT), cuyo emisor, Tether

Limited, ha ejercido esta potestad en múltiples ocasiones para bloquear direcciones asociadas a ilícitos financieros o a sanciones internacionales. Por ejemplo, en el 2023, Tether y el *Exchange* OKX colaboraron con el Departamento de Justicia de Estados Unidos para congelar aproximadamente 225 millones de USDT vinculados a una red de tráfico de personas en Asia. Esta acción garantiza que los activos no puedan ser transferidos por el investigado, aun cuando conserve las claves privadas.

En el ámbito de las finanzas descentralizadas (DeFi), cuando existan contratos inteligentes, la prioridad consiste en cerrar las posiciones abiertas y transferir los activos a billeteras bajo control estatal, con el fin de reducir el riesgo de liquidaciones automáticas o de pérdidas derivadas de la volatilidad del mercado. Un ejemplo de ello lo constituye el protocolo MakerDAO, en el cual las garantías depositadas pueden ser liquidadas automáticamente si el valor del colateral desciende por debajo del umbral exigido, lo que generaría la pérdida inmediata de fondos vinculados a la investigación (Damsker, 2024).

En los casos que involucran *tokens* envueltos (*wrapped tokens*) o transferencias mediante puentes (*bridges*), se requiere coordinación con las autoridades de la cadena de destino para evitar la pérdida de valor por traslados no controlados o por cambios de red. Ejemplos como el ataque al Wormhole Bridge en el 2022 –que ocasionó la sustracción de más de 300 millones de dólares en ETH envuelto (wETH)– ilustran los riesgos inherentes a este tipo de operaciones cuando no existe un control adecuado de la infraestructura.

Estas experiencias evidencian que la incautación de criptoactivos no puede concebirse como una operación meramente formal, sino como un proceso dinámico que integra facultades procesales tradicionales con conocimiento técnico especializado. Solo de esta manera es posible garantizar la eficacia de la medida cautelar, así como la protección del debido proceso y de los derechos de terceros con interés legítimo en la actuación

Control de legalidad y debido proceso

Es necesario insistir en que el debido proceso y el respeto de las garantías fundamentales constituyen el pilar de toda investigación penal. Ello implica que las autoridades de policía judicial deben practicar las diligencias de incautación con fines de comiso, en estricto cumplimiento de los protocolos técnicos previstos para la aprehensión y administración de criptoactivos. Asimismo, corresponde al fiscal acudir ante el juez de control de garantías dentro de las 36 horas siguientes a la incautación, a fin de que se examinen los procedimientos y resultados de la actuación.

Para este fin, resulta imprescindible que los actos de investigación previos a la incautación se hubieran realizado en cumplimiento de los mandatos legales; es decir, por orden del fiscal, dirigida al órgano de policía judicial, dentro del plazo previsto, con la correspondiente elaboración de actas y la producción de informes. El objetivo principal de tales exigencias es acreditar, de manera suficiente, el estándar de motivos fundados que permita inferir que los bienes son producto directo o indirecto de un delito doloso; que han sido o estén destinados a ser utilizados como instrumento de un delito doloso, o que constituyen el objeto material de la infracción.

Si bien los lineamientos de la Fiscalía General de la Nación han sido diseñados para que estas actuaciones se adelanten en la etapa de indagación, conviene subrayar que es igualmente viable ordenar la incautación de criptoactivos con fines de comiso con posterioridad a la formulación de imputación; esto es, cuando la persona ya ha sido vinculada al proceso penal. En tal circunstancia, la actuación no reviste carácter reservado, puesto que dicha restricción solo procede durante la indagación (art. 212B, C. de P. P.). En consecuencia, y en garantía del derecho de defensa, resulta imprescindible convocar a la audiencia de legalización posterior al imputado y a su defensor, así como a los terceros con interés en la actuación (víctimas y PSAVC).

En el examen de legalidad del estándar de inferencia, el juez debe descartar que los criptoactivos correspondan a bienes pertenecientes al sujeto pasivo del delito, a las víctimas o a terceros de buena fe, casos en los que no procede el comiso, sino la devolución a estas personas.

Cuando el juez de control de garantías no avala los resultados de la incautación, los criptoactivos deben devolverse a su legítimo propietario, sea el investigado, las víctimas o los terceros con interés legítimo. Aquí surge un problema adicional: la variación del valor de los criptoactivos, dada su alta volatilidad. Es posible que en pocas horas el precio de mercado aumente o disminuya considerablemente. En caso de aumento, no se genera perjuicio; pero si se presenta una disminución, pueden originarse controversias jurídicas por responsabilidad extracontractual del Estado (Henao, 1998).

Por último, debe reiterarse que la decisión sobre el comiso es de carácter definitivo y corresponde al juez de conocimiento en la sentencia condenatoria (CSJ, AP4073-2024, 24 jul. 2024, rad. 60055; AP5421-2019, 12 dic. 2019, rad. 56507). Sin embargo, una lectura sistemática del Código de Procedimiento Penal permite concluir que esta decisión también puede adoptarse en la preclusión decretada por el juez de conocimiento, o en la concesión del principio de oportunidad por el juez de control de garantías; por cuanto se trata de providencias con efectos equivalentes a la sentencia, que ponen fin al proceso y hacen tránsito a cosa juzgada. En este sentido, el artículo 90 del Código de Procedimiento Penal establece que "[s]i en la sentencia o decisión con efectos equivalentes" se omite pronunciamiento definitivo sobre el comiso, la defensa, el fiscal o el Ministerio Público podrán solicitar la adición de la decisión.

Conclusiones

El marco jurídico colombiano demuestra que no es necesario promover reformas legislativas inmediatas para enfrentar los desafíos de la incautación y el comiso de criptoactivos. El derecho vigente –en particular, la Ley 906 de 2004, en armonía con el Código Penal y la jurisprudencia– ofrece un andamiaje suficiente para ordenar medidas cautelares sobre bienes de cualquier índole, siempre que se acredite con motivos fundados la relación entre dichos activos y una conducta punible.

Por tanto, el desafío no radica en el plano legislativo, sino en la adaptación práctica de las autoridades a las exigencias técnicas que plantean los criptoactivos. La "Guía" expedida por la Fiscalía General de la Nación en el 2025 constituye un avance destacable, en tanto traduce la complejidad

tecnológica de la *blockchain* al lenguaje operativo de la investigación penal. Sin embargo, sus protocolos requieren fortalecimiento, en especial para asegurar la aprehensión técnica de los activos en entornos de heterocustodia y para anticipar escenarios complejos de autocustodia, multifirmas, billeteras jerárquicas o contratos inteligentes.

La eficacia del régimen colombiano se sostiene sobre cuatro pilares que dialogan con los estándares internacionales más avanzados: (a) la viabilidad de realizar la incautación con fines de comiso de criptoactivos, tanto en entornos de heterocustodia como de autocustodia, motivados por el estándar de inferencia y los criterios de necesidad, idoneidad y proporcionalidad; (b) un control judicial de legalidad temprano dentro de las treinta y seis horas siguientes a la incautación, que asegura la razonabilidad de la medida; (c) la implementación de protocolos de custodia digital, incluyendo almacenamiento en frío; y (d) la cooperación efectiva con los proveedores de servicios de activos virtuales, tanto nacionales como extranjeros, en línea con la *Travel Rule* y con las exigencias de reporte trazadas por el FATF/GAFILAT.

La experiencia colombiana se inscribe en una tendencia global de convergencia entre el derecho penal, el derecho administrativo y las técnicas forenses digitales. Estas prácticas no solo cumplen una función instrumental en la prevención de la criminalidad financiera, sino que también operan como garantías para el ejercicio de las libertades ciudadanas. Por tanto, reconocen que los criptoactivos tienen un espacio legítimo de existencia dentro del ordenamiento jurídico, sometido al debido proceso, lo cual implica que el derecho penal contemporáneo regula los bienes digitales sin sacrificar los principios que sostienen el Estado constitucional de derecho.

Conflicto de interés

No se presentó conflicto de interés en el desarrollo de la presente investigación académica. Declaro que no mantengo ninguna relación financiera, profesional o personal que pudiera influir en el diseño del estudio, así como en la interpretación y publicación de los resultados obtenidos. Asimismo, manifiesto el cumplimiento de las normas éticas y de integridad científica, de conformidad con las directrices establecidas por la comunidad académica y por la presente revista.

Referencias

Normativa colombiana

Congreso de la República de Colombia. (2000). Ley 599 de 2000 (Código Penal), artículo 100. *Diario Oficial*, 44097 de julio 24 de 2000.

Congreso de la República de Colombia. (2004). Ley 906 de 2004 (Código de Procedimiento Penal), artículos 83, 84, 88. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14787

Fiscalía General de la Nación. (2025). Resolución 0-0053 de 2025. *Guía para la adopción de medidas cautelares en relación con criptoactivos en el proceso penal y de extinción de dominio*. https://www.fiscalia.gov.co/colombia/wp-content/uploads/0-0053.pdf

Fiscalía General de la Nación. (2018). *Manual de Sistema de Cadena de Custodia*. https://www.fiscalia.gov.co/colombia/wp-content/uploads/MANUAL-DEL-SISTEMA-DE-CADENA-DE-CUSTODIA.pdf

Fiscalía General de la Nación. (s. f.). *Manual Único de Policía Judicial*. https://www.fiscalia.gov.co/colombia/wp-content/uploads/Manual-de-Policia-Judicial-Actualizado.pdf

Unidad de Información y Análisis Financiero (UIAF). (2021). Resolución 314 de 2021. *Obligaciones de reporte para proveedores de servicios de activos virtuales* (PSAV/VASP). https://www.uiaf.gov.co/sites/default/files/2024-10/Resoluci%C3%B3n_314_de_2021_AV.pdf

Jurisprudencia colombiana

Corte Suprema de Justicia, Sala de Casación Penal. (2019, 12 de diciembre). Auto AP5421-2019, rad. 56507.

Corte Suprema de Justicia, Sala de Casación Penal. (2022, 25 de mayo). Sentencia SP2129-2022, rad. 54153.

Corte Suprema de Justicia, Sala de Casación Penal. (2024, 24 de julio). Auto AP4073-2024, rad. 60055.

Corte Suprema de Justicia, Sala de Casación Penal. (2025, 30 de abril). Sentencia SP1136-2025, rad. 67446.

Organismos internacionales y derecho extranjero

Consejo de Europa. (2021). *Guide on seizing cryptocurrencies*. Cybercrime Programme Office of the Council of Europe.

Europol. (2022). *Cryptocurrencies: Tracing the evolution of criminal finances*. https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

Financial Action Task Force (FATF). (2021). *Updated guidance for a risk-based approach to virtual assets and VASPs*. https://www.fsb.org/2021/10/updated-guidance-for-a-risk-based-approach-to-virtual-assets-and-virtual-asset-service-providers/

Ministerio Público Fiscal de Argentina, UFECI. (2023). *Guía práctica para la identificación, trazabilidad e incautación de criptoactivos*. https://www.mpf.gob.ar/ufeci/files/2023/05/Informe_Criptoactivos.pdf

Doctrina

Ammous, S. (2018). *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Wiley.

Andrade Castro, J. A. (2023). Criptoactivos, metaverso y derecho penal. *Revista de la Academia Colombiana de Jurisprudencia*, julio-diciembre, 95-126.

Arango-Arango, C. A., Barrera-Rego, M. M., Bernal-Ramírez, J. F., & Boada-Ortiz, A. (2018). *Criptoactivos*. Banco de la República.

Asociación de Academias de la Lengua Española (ASALE). (2025). *Diccionario panhispánico del español jurídico*. Versión en línea. https://dpej.rae.es/

Damsker, A. (2024). *Understanding DeFi*. O'Reilly.

Gideon, D. (2025). *Crypto security made simple: 10 essential steps to safeguard your digital assets, defend against hacks and scams*. Publicación independiente (edición Kindle).

Henao, J. C. (1998). *El daño: análisis comparativo de la responsabilidad extracontractual del Estado en Derecho colombiano y francés*. Universidad Externado de Colombia.

Torres, J. M. (2019). *Criptomonedas: qué son, cómo utilizarlas y por qué van a cambiar el mundo*. Editorial Planeta Colombiana.