MINISTERIO DE SEGURIDAD DE LA NACIÓN

Protocolo General de Actuación para la identificación, preservación y secuestro de potenciales elementos de prueba vinculados con criptoactivos

- ENERO DE 2025 -

IF-2025-04547034-APN-DCYAC#MSG

Índice

CAPÍTULO I - REGLAS GENERALES

1.1 **Objeto:** El presente PROTOCOLO GENERAL DE ACTUACIÓN (en adelante “PGA”) tiene por objeto establecer las pautas y procedimientos al que deberán atenerse los miembros de las fuerzas policiales y de seguridad federales al momento de la identificación de la presencia potencial de criptoactivos en el lugar del allanamiento y su posterior secuestro. El presente PGA se genera en cumplimiento de los objetivos establecidos en la Resolución Nro 19/2025 del Ministerio de Seguridad de la Nación en el marco del “Programa de fortalecimiento en ciberseguridad e investigación del ciberdelito” (ForCIC).

1.2 **Alcance y Aplicación:** El presente PGA es de aplicación obligatoria en todo el país para todo el personal de POLICÍA FEDERAL ARGENTINA, GENDARMERÍA NACIONAL ARGENTINA, POLICÍA DE SEGURIDAD AEROPORTUARIA, PREFECTURA NAVAL ARGENTINA y el SERVICIO PENITENCIARIO FEDERAL, debiéndose tener en cuenta que su accionar debe ajustarse en un todo a la Constitución Nacional, las leyes penales, las pautas procesales y los protocolos vigentes.

1.3 **Complementariedad:** Los procedimientos que el presente PGA pretende describir serán de aplicación complementaria a las disposiciones emanadas de la autoridad judicial a cargo de la investigación. Particularmente, se deberán tener en cuenta las pautas establecidas por el “Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital”, Resolución Nro 232/2023 del Ministerio de Seguridad de la Nación. Como también la “Guía práctica para la identificación, trazabilidad e incautación de criptoactivos”, documento elaborado por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), Resolución Nro 33/23 de la Procuración General de la Nación.

CAPÍTULO II - CONTEXTO DE LOS CRIPTOACTIVOS

2.1 Los criptoactivos han adquirido gran relevancia en la actualidad, transformando la manera en que interactuamos con el dinero y los activos financieros, revolucionando así la economía global y abriendo nuevas posibilidades en diversos campos. A medida que la tecnología Blockchain y los criptoactivos continúan ganando popularidad y son utilizadas en diversos aspectos de la vida moderna, también se han convertido en una herramienta atractiva para actividades delictivas como el lavado de dinero, el fraude y la financiación del terrorismo. La naturaleza de los criptoactivos, tales como su carácter intangible, alta volatilidad, liquidación rápida y posibilidad de un expedito cruce de fronteras en las transacciones, plantean un desafío único para la investigación y el enjuiciamiento. Al momento de un allanamiento o tareas de prevención policial cotidianas es clave la identificación de indicios que sugieran la presencia de criptoactivos en la escena. Su detección temprana asociada a actividades delictivas brinda una oportunidad crucial para actuar con rapidez y asegurar dichos activos de manera apropiada.

2.2 La importancia de identificar pruebas relacionadas con criptoactivos radica en que, a diferencia de los bienes físicos tradicionales, como efectivo o propiedades, los criptoactivos pueden transferirse de manera rápida y sencilla desde ubicaciones remotas. Si un grupo de delincuentes sospecha que sus criptoactivos han sido descubiertos, pueden intentar moverlos a otras billeteras o llevar a cabo transacciones complejas para dificultar su rastreo. Estas medidas evasivas frente a la acción judicial pueden llevarse a cabo desde cualquier dispositivo. En otras palabras, durante un procedimiento de allanamiento en un lugar donde haya indicios de utilización ilegal de criptoactivos, es fundamental actuar de manera inmediata en la identificación, el inventario y el posterior secuestro de los criptoactivos. Existe una alta probabilidad de que, si no se actúa con celeridad, estos elementos probatorios sean difíciles de vincular con la investigación en curso.

2.3 Por ello, la rápida transferencia hacia una billetera controlada por las

autoridades permitirá tener el control sobre los activos incautados y evitar posibles movimientos de los delincuentes para dispersar los fondos y dificultar su recuperación. Una vez asegurados los criptoactivos, se puede proceder con la investigación y el análisis forense adecuado para establecer su origen y vinculación con actividades criminales, lo que resulta crucial para presentar pruebas sólidas en un proceso judicial. La colaboración entre fuerzas de seguridad, expertos forenses y la autoridad judicial es esencial para llevar a cabo con éxito el protocolo de secuestro de criptoactivos y salvaguardar la integridad de la investigación y el debido proceso.

CAPÍTULO III - CONCEPTOS Y GLOSARIO.

Las definiciones detalladas a continuación son aplicables en el marco del presente documento:

3.1 **Cadena de Bloques (Blockchain)**[1]: Libro de contabilidad digital distribuido compuesto por transacciones firmadas criptográficamente que se agrupan en bloques. Cada bloque se vincula criptográficamente con el anterior después de su validación y tras someterse a una decisión consensuada. A medida que se añaden nuevos bloques, los más antiguos se vuelven más difíciles de modificar (creando una resistencia a la manipulación). Los nuevos bloques se replican en las copias del libro mayor dentro de la red, y cualquier conflicto se resuelve automáticamente utilizando las reglas establecidas (NISTIR 8202).

3.2 **Activos Virtuales (AV)**[2]: Representación digital de valor que se puede comercializar o transferir digitalmente y utilizar para pagos o inversiones. En ningún caso se entenderá como activo virtual la moneda de curso legal en territorio nacional y las monedas emitidas por otros países o

[1] Apartado 2.3 Blockchain del Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital, disponible en https://www.mpf.gob.ar/ufeci/files/2023/05/Informe_Criptoactivos.pdf

[2] Artículo 2, Inciso a) de la Resolución Nro 94/2024 de la Unidad de Información Financiera, disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/305109/20240325).

jurisdicciones (moneda fiduciaria GAFI 2021). Este género de archivos digitales, se desarrollan sobre plataformas basadas en el uso de técnicas criptográficas y bases de datos sostenida por un sistema de cadena de bloques. Pueden representar diferentes especies de criptoactivos.

3.3 **Criptoactivos**: Es una especie de AV; y su distinción o clasificación está dada por las diferentes formas de implementación que son proporcionadas por la plataforma en donde funcionan. Este concepto es aceptado por la costumbre del ecosistema digital; y es utilizada para diferenciar los tipos de AV. Vale aclarar que el dinamismo propio del ecosistema criptográfico y el volumen de proyectos apoyados por diferentes plataformas dificultan realizar un catálogo final.

3.4 **Dirección:** Es el identificador único desde donde se pueden recibir o bien desde donde se pueden enviar criptoactivos. Es el destino u origen digital que se localiza en el libro mayor público de la cadena de bloques, el cual permite consultar el historial de transacciones asociadas a esa dirección. Básicamente, consiste en un código alfanumérico que se genera como resultado de la aplicación de operaciones estandarizadas sobre una clave pública, la que se obtiene, a su vez, por medio de otra serie de cálculos preestablecidos y ejecutados sobre una clave privada, la que es generada por el usuario o por la plataforma utilizada por aquél a los fines de operar en la red. Dependiendo de la tecnología que se utilice se podrán observar diferentes tipos de direcciones.

3.5 **ID de Transacción:** También conocido como hash de la transacción, se trata de un identificador único de cada transacción. Se denomina transacción a la acción de transferencias de criptoactivos. En una sola transacción pueden existir movimientos de fondos desde una o varias direcciones de origen y a una o más direcciones de destino. El ID de las transacciones poseen el mismo formato en la mayoría de las plataformas: un valor hexadecimal de 64 caracteres (ello debido a que el identificador es el resultado de la aplicación de la función Hash SHA-256 a la transacción).

3.6 **Potencial Elemento de Prueba (PEP)**[3]: Se consideran potenciales elementos de prueba (PEP) aquellos dispositivos susceptibles de contener información (representación física), los cuales almacenan potencial evidencia digital (representación lógica).

3.7 **Potencial Elemento de Prueba de Criptoactivos (PEP de Criptoactivos)**: Cualquier PEP que esté asociado potencialmente a la presencia de criptoactivos. Los mismos pueden ser tanto físicos o digitales.

3.8 **Potencial Elemento de Prueba digital (PEP digital)**[4]: Cualquier dato (registro o archivo) que puede ser generado, transmitido o almacenado por equipos de tecnología informática y que está constituido por campos magnéticos y pulsos electrónicos, los cuales pueden ser recolectados y analizados con herramientas o técnicas especiales.

3.9 **Primer interventor:** Es el responsable de la exploración, localización, valoración, identificación y recolección de PEPs que pudieran contener evidencia digital y se encuentren asociados al hecho investigado, siendo los mismos de interés para el análisis pericial en el laboratorio de la especialidad, procurando la relevancia, suficiencia, validez legal y confiabilidad durante el proceso de identificación, recolección y adquisición de los mismos. Conforme lo expuesto, aquellos funcionarios que sean designados como primeros intervinientes, deberán tratar a los criptoactivos como parte de PEPs o PEPs digitales, vinculados a la causa judicial.

3.10 **Proveedores de servicios de Activos Virtuales (PSAV)**[5]**:** Cualquier persona humana o jurídica que, como negocio, realiza una (1) o más de las siguientes actividades u operaciones para o en nombre de otra persona humana o jurídica: i. intercambio entre activos virtuales y

[3] Apartado 2.21 Potencial Elemento de Prueba (PEP) del Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital, disponible en https://www.argentina.gob.ar/normativa/nacional/resolución-232-2023-382307

[4] 2.22 Potencial Elemento de Prueba digital (PEP digital) del Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital, disponible en https://www.argentina.gob.ar/normativa/nacional/resolución-232-2023-382307

[5] Artículo 2, Inciso r) de la Resolución Nro 94/2024 de la Unidad de Información Financiera, disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/305109/20240325).

monedas de curso legal (monedas fiduciarias); ii. intercambio entre una (1) o más formas de activos virtuales; iii. transferencia de activos virtuales; iv. custodia y/o administración de activos virtuales o instrumentos que permitan el control sobre los mismos; y v. participación y provisión de servicios financieros relacionados con la oferta de un emisor o venta de un activo virtual. Entre los proveedores de servicio más conocidos se destacan las denominadas “Exchanges”.

3.11 **Personal Especialista:** Personal idóneo con conocimientos especializados en criptoactivos, perteneciente a las fuerzas policiales y de seguridad y que cuentan con las capacidades para recomendar y tomar acciones relativas al tratamiento de criptoactivos.

3.12 **Rig de Minería:** Conjunto de elementos de hardware instalados y configurados para el minado de criptoactivos.

3.13 **Triage**[6]: Proceso de selección de dispositivos o filtrado de información ordenado por la autoridad judicial, quien aporta los criterios de evaluación sobre los dispositivos electrónicos en el lugar del hecho, susceptibles a ser secuestrados para llevar a cabo un posterior análisis forense. Este proceso puede traer aparejada la alteración de datos informáticos por lo que resulta necesario tomar recaudos y precauciones, analizar los riesgos inherentes a esta clase de intervenciones e informar a la autoridad judicial sobre los mismos, así como documentar adecuadamente las tareas realizadas. El proceso del Triage servirá para sustentar la decisión judicial de secuestro o no de los elementos, realización de imágenes o copias forenses, detenciones, entre otras posibles medidas procesales. El proceso de Triage deberá ser liderado por Personal Especialista.

3.14 **Secuestro:**[7] medida procesal por la cual se procede a la recolección de lo que se hallare en virtud de un allanamiento o de una requisa personal dejando constancia de ello en el acta respectiva y dando cuenta inmediata del procedimiento realizado al juez o fiscal intervinientes. Los elementos

[6] Apartado 2.26 “Triage” del Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital, disponible en https://www.argentina.gob.ar/normativa/nacional/resolución-232-2023-382307 2.26.

[7] Apartado 2.25 “Secuestro” del Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital, disponible en https://www.argentina.gob.ar/normativa/nacional/resolución-232-2023-382307 2.26.

de prueba serán recolectados según las reglas aplicables al tipo de objeto, garantizando la cadena de custodia.

3.15 **Wallet/billetera virtual:** Dispositivo electrónico, servicio de banca electrónica o aplicación móvil que permite el intercambio de AV por bienes y/o servicios. Para cada criptoactivo, existen numerosos formatos de billeteras que pueden funcionar en diferentes tipos de dispositivos –computadoras de escritorio, teléfonos móviles y tabletas– y/o sistemas operativos –Linux, Windows, MacOs, Android, iOS–. Nos encontramos también con programas que resguardan toda la información localmente, es decir, en el dispositivo en el cual se utilizan, y otras plataformas en las que los usuarios deben crearse una cuenta, con un nombre de usuario y una contraseña, y la información en cuestión es almacenada en los servidores de la empresa que brinda el servicio.

3.16 **Billetera Institucional:** Todo aquel software, aplicación o servicio que posibilita la interacción con una dirección en el sistema blockchain permitiendo la realización de operaciones de transferencias o recepción de AV controlados por una institución pública, ya sean fuerzas de seguridad, autoridades del Poder Judicial o del Ministerio Publico Fiscal.

3.17 **Frase Semilla**[8]: Es un mecanismo utilizado por muchas aplicaciones de monedero de AV para generar claves privadas a partir de una única clave nemotécnica “semilla”, que toma la forma de un código conformado por una secuencia de entre 12 y 24 palabras en distintos idiomas (inglés, japonés, coreano, español, chino, francés e italiano), que funcionan como un respaldo (back up) para el monedero, permitiendo que en caso de pérdida de control sobre el mismo (por ejemplo, debido al robo, pérdida o desperfecto técnico del dispositivo en el que se encuentra almacenada), sea posible recrearlo introduciendo en la aplicación correspondiente las palabras en el orden provisto originalmente. Funciona como una copia de seguridad que permite generar claves privadas idénticas por medio de

[8] Apartado 52 Las “palabras semilla” o “frase semilla” (“Seed words” o “Seed phrase”) de la Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales del GAFI, disponible en https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Gui%CC%81a-sobre-aspectos-relevantes-y-pasos-apropiados-para-la-investigacio%CC%81n-identificacio%CC%81n-incautacio%CC%81n-y-decomiso-de-AV.pdf

otra billetera, posibilitando al acceso a todos aquellos activos depositados en las direcciones gestionadas por esta para generar claves privadas idénticas en otra billetera.

CAPÍTULO IV - SECUESTRO DE CRIPTOACTIVOS

4.1 En el caso de un allanamiento u orden de presentación, previamente a llevar a cabo el procedimiento, se recomienda coordinar con la autoridad judicial las reglas de intervención en el caso de la existencia de indicios de criptoactivos. Dicha coordinación debería anticipar posibles formas de proceder ante las circunstancias presentadas, tales como posibles triage, identificación de posibles aplicaciones de billeteras virtuales, presencia de frases semilla en formato físico o digital, claves de accesos, billeteras de depósito donde deberán ser enviados los criptoactivos incautados, capacidades del personal interviniente, vías de comunicación, etc.

4.2 En caso de que el primer interventor verifique la presencia de **PEPs** que pudiesen contener potenciales criptoactivos, procurará en el acta prevista labrada con las formalidades legales vigentes, que conste una fijación narrativa, precisa y detallada que suministre una noción clara del lugar donde fueron hallados los medios tecnológicos informáticos o evidencia física, de toda la incidencia que hubiere acontecido durante el procedimiento policial. Se procurará que la fijación narrativa se complemente con fotografías, filmaciones, planos del lugar y del sitio de ubicación de cada efecto. Para mayor detalle consultar el “Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital”

4.3 En caso de considerarlo pertinente, el primer interventor podrá realizar la consulta remota con el área especializada de la fuerza a la que pertenece, a los efectos de preservar la información que los PEPs pudieran contener. No se debe interactuar innecesariamente ni buscar información en los mismos, excepto cuando se prevea adquirir datos volátiles o se efectúen operaciones urgentes de triage bajo el liderazgo del personal especialista, debiéndose en todos los casos documentar el proceso realizado.

a. Allanamiento con información previa sobre posible presencia de criptoactivos.

4.4 En este escenario planteado, al momento de proceder al allanamiento u orden de presentación, la investigación previa tiene conocimiento de la potencial existencia de criptoactivos en el sitio a allanar.

4.5 Previamente a llevar a cabo el procedimiento, se sugiere que las acciones sean articuladas de manera efectiva entre las autoridades judiciales y los oficiales que vayan a diligenciar la medida, incluyendo los primeros intervinientes y personal especializado, a fin de poder realizar de manera eficiente las primeras actividades en el lugar. Por ende, se sugiere, que la autoridad judicial evalúe la posibilidad de ejecutar las siguientes acciones:

a) En caso de contar con direcciones propias creadas con anterioridad, informarlas para realizar la transacción total de los activos a secuestrar.

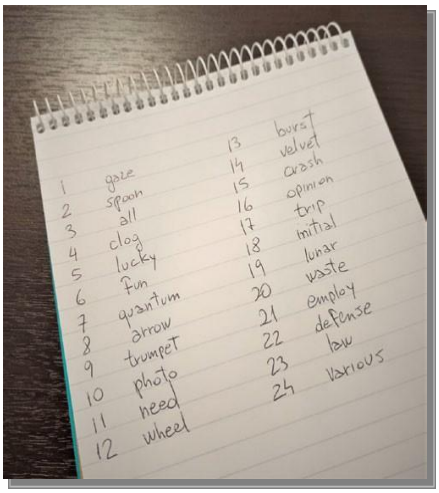
b) De presentarse la oportunidad de ingresar a una billetera en el lugar del hecho, inventariar todos los tipos de criptoactivos que hubiera en dicha billetera detallando su respectivo valor acorde al día y hora que se lleve a cabo la medida, en virtud de la volatilidad de los mismos, como así también, en la medida de lo posible, se realice un pormenorizado detalle que permita preservar el historial de transacciones y sus correspondientes identificadores.

c) Secuestrar y transferir los AV que se hallen en cuentas y billeteras virtuales identificadas o que se encuentren asociados a frases semilla o claves privadas. Cuando se transfieran los AV a la dirección generada, se dejará constancia que la/las transferencias implican el pago de una tasa, y teniendo en cuenta el rápido resguardo de los AV, se optará por la opción más rápida, dejando constancia del saldo que se acreditará en la dirección bajo control de una institución pública, (fuerzas de seguridad, autoridades del Poder Judicial o del Ministerio Publico Fiscal).

d) Evaluar si es viable realizar el congelamiento de cuentas de Exchange/Plataformas de Pago detectadas durante el allanamiento.

4.6 Al momento del allanamiento el Primer Interviniente deberá prestar atención a la presencia de PEPs asociados a criptoactivos. Se detallan a continuación posibles indicios, pudiendo existir otros adicionales condicionado a los avances tecnológicos en la materia y las costumbres del caso:

a) Frases semillas escritas en papel.

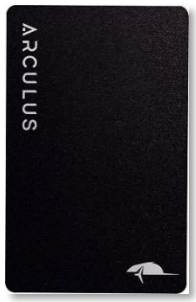


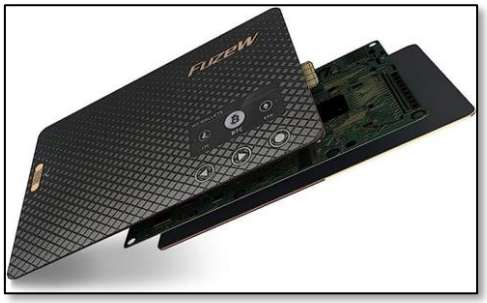
b) Frases semillas en otros formatos.

c) Billeteras frías con formato pendrive.



d) Billeteras frías en formato tarjeta con tecnología NFC.





e) Billeteras fría formato papel.

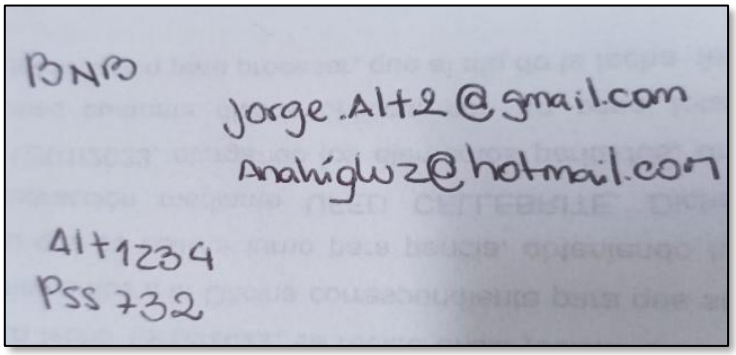
f) Código QR.

g) Credenciales de acceso o inicios de sesión documentadas, tales como:

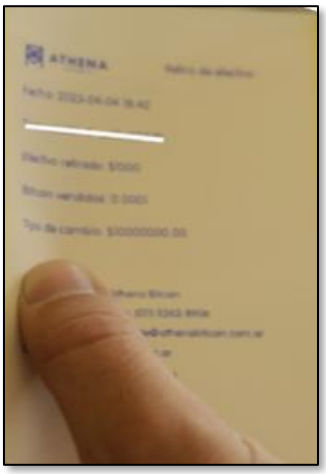
1) Posibles direcciones de email con o sin contraseñas

2) Posibles nombres de usuario con o sin contraseñas

3) Tarjetas SIM o número de abonado (que podrían ser utilizados como segundo factor de autenticación al momento del inicio de sesión).



h) Ticket y o comprobantes de cajeros automáticos de criptoactivos.



i) Anotaciones en las que figuren direcciones de envió o recepción de AV con las características más comunes, entre las que se encuentran las siguientes:

	BITCOIN	ETHEREUM	RIPPLE	LITECOIN	DASH	MONERO	ZCASH	TRON	BNB Smart Chain
Abreviatura	BTC	ETH	XRP	LTC	DASH	XMR	ZEC	TRX	BSC
Dirección comienza con:	1 3 bc1q bc1p	0x	r, x	L	X	4, 8	t1 t3 z1 z3	T	0X
Cantidad de caracteres de la Dirección	26 - 90	42	25 - 35	26 - 35	34	95	35 -96	34	42
Blockchains que soportan USDT	-	ETH_USDT	-	-	-	-	-	TRX_USDT	BSC_USDT

j) Anotación en las que figure “ID de transacciones” (más comunes).

1) En la blockchain de Bitcoin: Por ejemplo, c6e0749f0d986b905e4be2d3d4518425497023eda6b665505621b5de0be025c2

2) En la blockchain de Ethereum: Por ejemplo, 0x80451481bb8007924e82d72d06fb2055972592fe5b47d8b56f993b45facfd515

3) En la blockchain de Tron: Por ejemplo, 00611ff9ebbc9c9930a86baf06219af950d2855238cb8a79386c2a417b36ffd8

4.7 Ante la detección de indicios, el primer interviniente y el personal especializado realizarán un inventario de los mismos, detallando cuando sea posible:

a) Tipo de dispositivo tecnológico detectado.

b) Tipo de billetera encontrada.

c) Tipos de criptoactivo.

d) Direcciones de las billeteras.

e) Billetera papel.

f) Indicar circunstancia de hallazgo.

4.8 Del mismo modo, ante la detección de indicios el primer interventor comunicará a la autoridad judicial el detalle de los PEPs de criptoactivos detectados y consultará sobre las medidas a tomar. Sin embargo, si de la investigación ya se hubieran desprendido indicios respecto al uso de criptoactivos, resultaría conveniente que la orden de registro incluya tanto el desbloqueo compulsivo de dispositivos como así también el secuestro de los criptoactivos que sean identificados. Ello, teniendo presente que el tiempo en formular la consulta podría resultar perjudicial para realizar la incautación de estos activos, pues podrían transferirse de manera remota desde cualquier otro dispositivo que tuviera acceso a las claves privadas.

4.9 Si la autoridad judicial decidiera el secuestro de los PEPs de Criptoactivos, el Primer Interviniente procederá al secuestro de los elementos identificados en cumplimiento con lo establecido en el protocolo vigente.

4.10 Si el primer interviniente encontrara “frases semilla” deberá proceder de acuerdo al apartado “b. Tratamiento de PEPs con frases semilla” de este documento.

4.11 Si la autoridad judicial ordenara la realización de un “Triage” a los equipos detectados a fin buscar posibles PEPs de criptoactivos, se deberá proceder de acuerdo al apartado “c. Triage de equipos y dispositivos móviles[9]”.

[9] Ver Anexo I - Flujogramas “TRIAGE DE EQUIPOS”

4.12 Toda presencia de PEPs de criptoactivos, deberá quedar documentada en el acta prevista labrada con las formalidades legales vigentes, con una fijación narrativa, precisa y detallada que suministre una noción clara del lugar donde fueron hallados los indicios de criptoactivos. El acta se complementará con fotografías, filmaciones, croquis del lugar y del sitio de ubicación de cada efecto, todo ello a fin de asegurar que el procedimiento pueda ser reconstruido, en caso de ser solicitado por la autoridad judicial.

b. Tratamiento de PEPs con "Frases Semilla"[10]

4.13 En el caso de que el primer interventor identifique la presencia de "frases semilla" en el allanamiento, se deberá tomar particular cuidado para preservar la confidencialidad de las mismas a fin de que no puedan ser utilizadas por terceros para recrear la billetera, incluyendo esto también a los testigos y otros presentes en la escena del allanamiento.

4.14 El hallazgo de las "frases semillas" será comunicado a la autoridad judicial con la mayor celeridad posible, con el fin de evitar dilataciones innecesarias en la recreación, inspección y posible incautación de los activos gestionados por esta. Dicha actividad podría llevarse a cabo in situ por el primer interventor o bien de forma remota por la autoridad judicial interviniente. Para la transmisión de las "frases semilla", se sugiere el empleo de video llamadas, evitando la comunicación escrita o mediante fotografías enviadas por cualquier medio electrónico, remarcando la importancia de que dicha información no debe ser accesible por terceros debido a la facilidad de recreación de la billetera y la posible pérdida de los criptoactivos.

4.15 Una vez comunicadas las frases semillas, el primer interventor procederá al secuestro del PEP con "frase semilla" e inclusión del mismo en la cadena de custodia, manteniendo las mismas precauciones de confidencialidad mencionadas anteriormente.

4.16 Todo el proceso deberá ser documentado en el acta prevista y labrada

[10] Ver Anexo I - Flujograma "TRATAMIENTO PEPs CON FRASE SEMILLA".

con las formalidades legales vigentes, con una fijación narrativa, precisa y detallada que suministre una noción clara del lugar donde fueron hallados los PEPs de criptoactivos.

c. Triage de equipos y dispositivos móviles

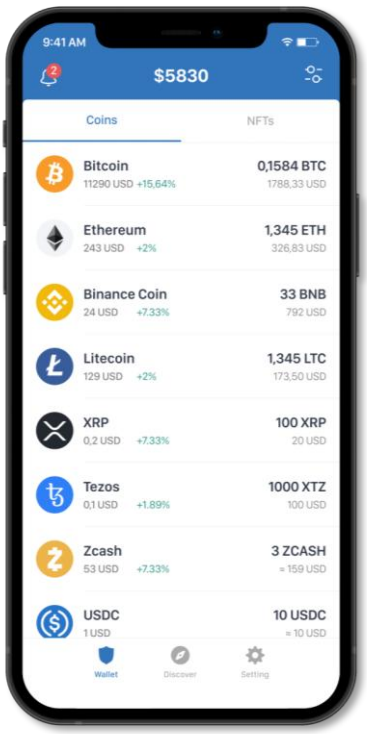
4.17 En el caso de que la autoridad judicial solicite un triage de dispositivos a fin de identificar posibles PEPs de criptoactivos, el mismo será liderado por personal especialista y consistirá en un examen manual (sin herramientas forenses) usando las funciones propias del dispositivo con las limitaciones del caso. Dichas interacciones quedarán registradas en el dispositivo por lo cual deberán quedar correctamente documentadas. Cabe destacar que, en caso de aquellos equipos y/o dispositivos móviles con contraseña o clave de acceso, resultará de vital importancia contar con la autorización judicial correspondiente para realizar el desbloqueo compulsivo de los mismos.

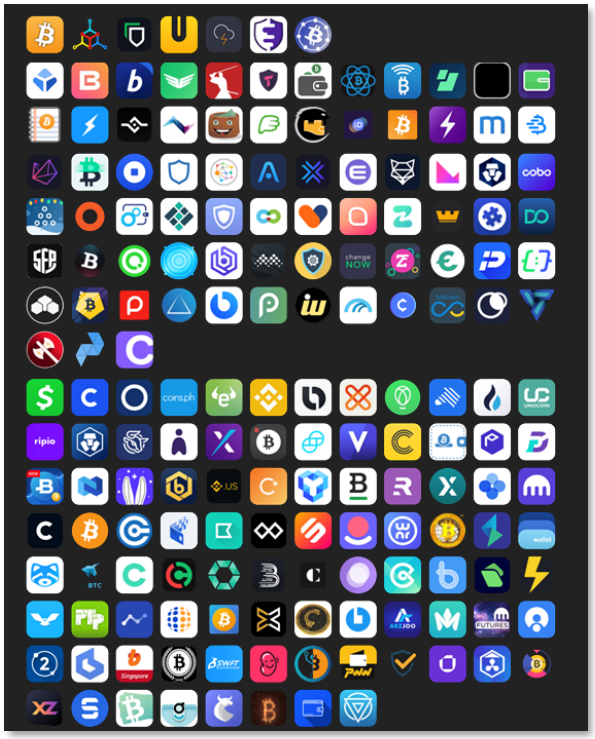
4.18 De detectarse posibles PEPs de criptoactivos tales como:

a) Aplicaciones de billeteras y/o plataformas que admitan la gestión de criptoactivos.

b) Software de billeteras y/o plataformas que admitan la gestión de criptoactivos.

Se deberá solicitar a la autoridad judicial la autorización para el ingreso a las mismas y tomar su control para gestionar aquellos AV que se encontrarán vinculados con estas.





4.19 Autorizado este último punto y, en el caso de poder acceder al control de la billetera, se procederá al inventario de los criptoactivos presentes (tipos y cantidades y valor actual) comunicando esto a la autoridad judicial para la autorización del secuestro de los mismos

4.20 En aquellos casos en que no se autorice el ingreso a la billetera o no se pueda acceder al control de la misma, el personal interviniente podrá recomendar a la autoridad judicial el congelamiento de las cuentas de Exchange / Plataforma de Pago detectadas.

d. Transferencia de criptoactivos

4.21 Comunicado el inventario de los criptoactivos detectados y, de autorizarse su secuestro, los mismos serán transferidos a las direcciones de depósito gestionados por la billetera bajo control del primer interventor o bien de la autoridad judicial interviniente.

4.22 El personal especialista procederá a la transferencia de los criptoactivos a la dirección bajo control del primer interventor o bien de la autoridad judicial interviniente, informando el monto final transferido y el costo de la comisión de la transferencia, teniendo como prioridad la mayor celeridad posible en el tiempo de la transferencia.

4.23 En conocimiento de este procedimiento, el primer interventor o la autoridad judicial deberá confirmar la recepción de los criptoactivos transferidos a la billetera bajo su control.

4.24 Las acciones mencionadas anteriormente deben ser plasmadas en el acta del procedimiento en cuestión. Asimismo, se deberá incluir el listado de los ID de transacción de cada operación efectuada y registrar mediante vistas fotográficas y fílmicas, desde el inicio hasta su finalización, cada uno de los detalles inventariados y movimientos realizados en las plataformas digitales de criptoactivos. Estas tareas deben ser realizadas en presencia de los testigos del procedimiento.

e. Allanamiento sin información previa sobre posible presencia de criptoactivos

4.25 En este escenario, al momento de proceder al allanamiento y/o orden de presentación, no se cuenta con conocimiento previo de la potencial existencia de criptoactivos en el sitio a allanar y dicha información se hace presente al momento del procedimiento. Se detallan a continuación los pasos a llevarse adelante:

4.26 Al momento del allanamiento el Primer Interviniente deberá prestar atención a la presencia de PEPs asociados a criptoactivos. En el punto 4.6 se indican algunos posibles indicios, pudiendo existir otros adicionales condicionado a los avances tecnológicos en la materia y las costumbres del caso.

4.27 Ante la detección de indicios, el primer interviniente y el personal especializado realizarán un inventario de los mismos, detallando cuando sea posible:

a) Tipo de dispositivo tecnológico detectado

b) Tipo de billetera encontrada

c) Tipos de criptoactivo

d) Direcciones de las billeteras

e) Billetera papel.

4.28 El primer interventor comunicará a la autoridad judicial el detalle de los PEPs de criptoactivos detectados y consultará sobre las medidas a tomar.

4.29 Si la autoridad judicial decidiera el secuestro de los PEPs de Criptoactivos, el Primer Interviniente procederá al secuestro de los elementos identificados, en cumplimiento con lo establecido en el protocolo vigente. En caso de considerarlo pertinente, el primer interventor podrá realizar la consulta remota con el área especializada de la fuerza a la que pertenece, a los efectos de preservar la información que los PEPs de criptoactivos pudieran contener.

4.30 Toda presencia de PEPs de criptoactivos, deberá quedar documentada en el acta prevista y labrada con las formalidades legales vigentes, con una fijación narrativa, precisa y detallada que suministre una noción clara del lugar donde fueron hallados los indicios de criptoactivos. El acta se complementará con fotografías, filmaciones, planos del lugar y del sitio de ubicación de cada efecto, todo ello a fin de asegurar que el procedimiento pueda ser reconstruido, en caso de ser solicitado por la autoridad judicial.

CAPITULO V – TRATAMIENTO DE RIGS DE MINERIA

5.1 Al momento del allanamiento el Primer Interviniente deberá prestar atención a la presencia de equipos asociados a la minería de criptoactivos (Rigs de minería). Se detallan a continuación posibles tipos de equipos, pudiendo existir otros adicionales condicionado a los avances tecnológicos en la materia:

a) Equipos mineros con placas de video (GPU):

b) Equipos mineros con hardware dedicado (ASIC):

5.2 Si al momento del allanamiento, el primer interviniente encontrara Rigs de Minería, procederá teniendo en cuenta las siguientes consideraciones:

a. RIGs de minería encendidos

5.3 Informar a la autoridad judicial sobre la presencia de Rigs de minería encendidos, sugiriendo se autorice a exigir a él/los propietarios las direcciones se de depósito donde se reciben las ganancias producidas por el Rig, con el objeto de conocer el flujo de los criptoactivos.

5.4 Si la autoridad judicial lo autorizara, el personal especialista procederá al triage del Rig a fin de obtener de acuerdo a lo solicitado:

a) Adquisición de la memoria volátil.

b) Relevamiento de la IP a la cual envía el resultado de las pruebas de trabajo realizas por el rig de minería.

c) Direcciones de depósito.

d) Pool de minería utilizado.

b. RIGs de minería apagados

5.5 Si al momento del allanamiento, el primer interviniente identificara Rigs de minería apagados, este procederá a informar tal circunstancia a la autoridad judicial y, si la misma lo autorizara, procederá al secuestro de la unidad tal como si fuera una computadora de escritorio de acuerdo al

protocolo de evidencia digital[11].

CAPÍTULO VI - RECOMENDACIONES PARA LA CREACIÓN DE BILLETERAS

6.1 A continuación, se enumeran una serie de recomendaciones generales para la creación y gestión de billeteras de criptoactivos por:

a) **Billeteras de Criptoactivos:** Se recomienda optar por billeteras de criptoactivos confiables y bien establecidas que ofrezcan opciones de seguridad robustas. Las billeteras hardware (dispositivos físicos) y las billeteras de software con medidas de seguridad sólidas son recomendables para almacenar criptoactivos de manera segura. Se recomienda en particular usar doble factor de autenticación para el ingreso a las billeteras como así también la posibilidad de la **opción "multisig"**[12] para asegurar movimientos controlados de los criptoactivos. En este punto, es recomendable además optar por una billetera institucional teniendo en consideración la compatibilidad con diferentes cadenas de bloques y AV que eventualmente sean objeto de decomiso, sumada al tipo de custodia empleada sobre los mismos y la disminución en los importes correspondientes a las comisiones transaccionales.

b) **Procedimientos de Generación de Claves:** Se recomienda que las claves privadas y "frases semilla" se generen en un entorno seguro, aislado de internet y posibles amenazas cibernéticas. Esto minimiza el riesgo de exposición no autorizada. No se recomienda su almacenamiento en dispositivos informáticos, optando por su transcripción manual.

[11] Apartado Equipo informático de escritorio, del Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital, disponible en https://www.argentina.gob.ar/normativa/nacional/resolución-232-2023-382307

[12] Multisig: significa firma múltiple, es un tipo específico de firmas digitales que hace posible que dos o más usuarios firmen documentos digitales como un grupo. Por lo tanto, se produce una firma múltiple mediante la combinación de varias firmas únicas, para realizar una transferencia de fondos o perfeccionar contratos inteligentes, entre otras operaciones.

c) **Almacenamiento Seguro:** Se sugiere que las claves privadas y las frases de recuperación se almacenen en ubicaciones físicas seguras, como cajas de seguridad. El acceso a estas ubicaciones debe ser restringido y documentado adecuadamente.

d) **Borrado de aplicaciones / billeteras:** En el caso de que, una vez realizada la incautación de criptoactivos, no se desee conservar la billetera de depósito en el equipo donde fue creada, se recomienda eliminar la billetera y cualquier archivo relacionado con la aplicación, ya sea de forma manual o mediante el uso de un programa de desinstalación o borrado seguro. Esta actividad se realiza con el objetivo de prevenir que, en caso de una posible reinstalación de la aplicación, la billetera se vincule automáticamente a la misma cuenta, utilizando la misma frase semilla.

CAPÍTULO VII - COOPERACIÓN PUBLICO PRIVADA.

7.1 Teniendo en cuenta que la tecnología Blockchain evolucionada cada día más rápida, es indispensable generar una relación de trabajo colaborativo entre el sector privado (Proveedores de Servicios de Criptoactivos), la autoridad judicial y los agentes de las fuerzas de seguridad en su rol de auxiliares de justicia. No solamente la capacitación reciproca es necesaria sino también, debido a las diferentes clases de criptoactivos, en necesario contar con la información con la que cuenta los Proveedores de Servicios de Criptoactivos, en caso de una medida urgente que los mismo puedan congelar los depósitos de criptoactivos de un investigado en sede penal, con el solo hecho de asegurar la prueba digital correspondiente.

CAPITULO VIII - DENUNCIAS DE ROBO DE CRIPTOACTIVOS

8.1 Se presenta a continuación una guía de preguntas para el primer interviniente en la recepción de una denuncia asociada al robo de criptoactivos.

a) ¿Qué tipo de billetera/servicio fue afectado?

b) ¿En qué fecha fue habilitada la billetera involucrada?

c) ¿Qué criptoactivos había en la billetera? (BTC, ETH, BNB, USDT, etcétera). Enumere todos los tipos y cantidades.

d) ¿Qué criptoactivos fueron robados de la billetera? Enumere todos los tipos y cantidades

e) ¿Cuál fue la última acción realizada por el denunciante en la cuenta? De ser posible, adjunte una captura de pantalla

f) ¿Cuál fue la primera acción realizada por delincuente en la cuenta y cuáles fueron sus posteriores acciones?

g) De ser posible, incluir los siguientes detalles, adjuntando capturas de pantalla:

    1) Hash de transacciones

    2) Direcciones de envío

    3) Direcciones de recepción

h) ¿Se registró la dirección IP del delincuente al iniciar sesión en su billetera? (ciertos servicios registran las direcciones IP desde las que se realizó la conexión e informan al cliente cuando se realizó una conexión desde una nueva dirección). En caso afirmativo, especifique la dirección IP.

i) ¿Además la billetera, fueron comprometidas otras cuentas de la propiedad del denunciante durante el mismo período de tiempo? (Facebook, correo electrónico, etc.).

j) ¿Es o fue usuario de alguna plataforma relacionada con criptoactivos?

k) En el caso de haber sido estafado (inversión, piramidal, trading, etc.), ¿Con quién interactuó?

    1) Datos completos, nombre, teléfono, medio por el cual se comunicó.

    2) Sitios web que utilizaba para acceder a ver rendimientos o realizar

pagos

3) Dirección de depósito a donde recibía ganancia y pagos de ingreso

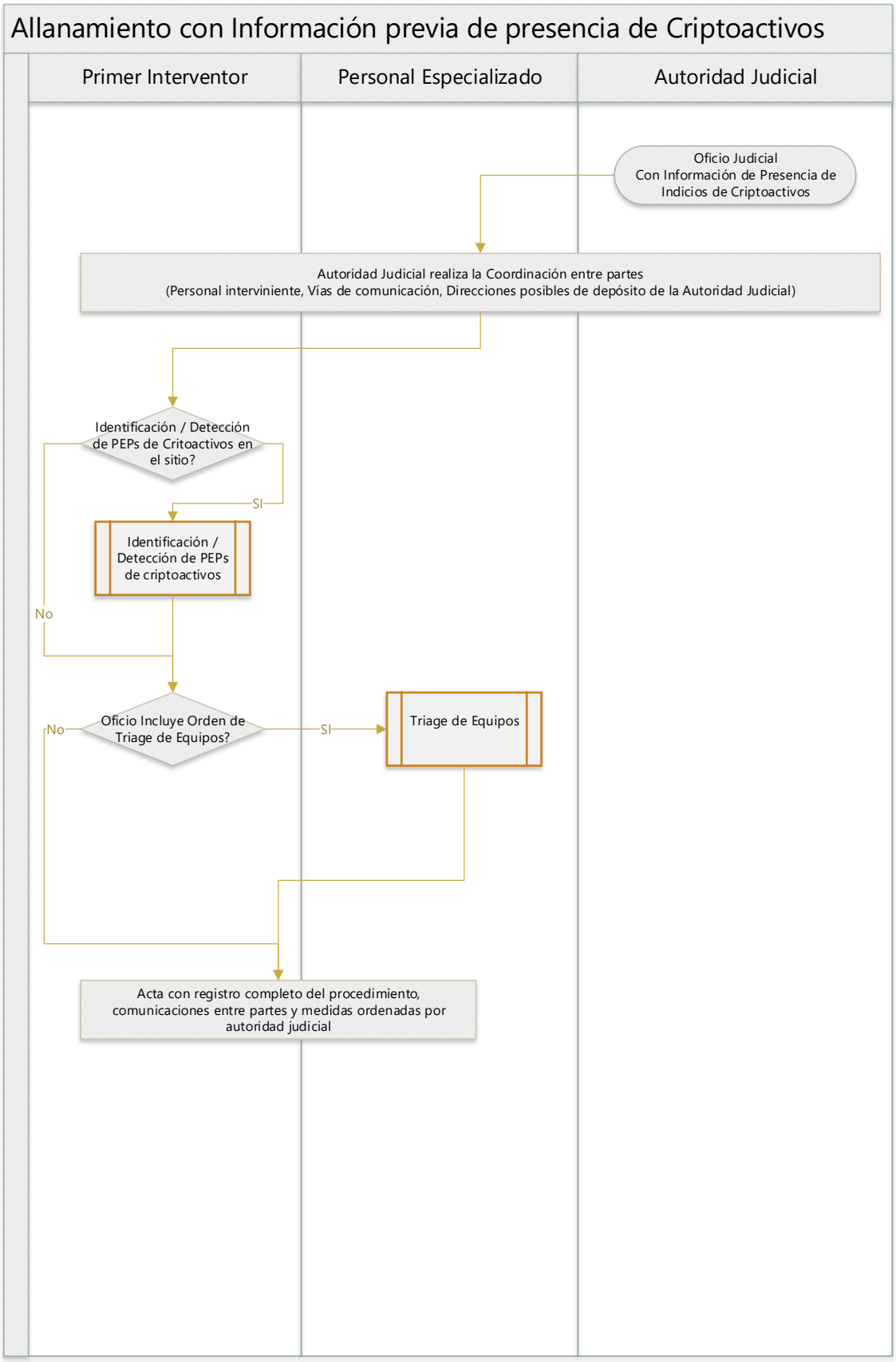
4) Monto de inversión

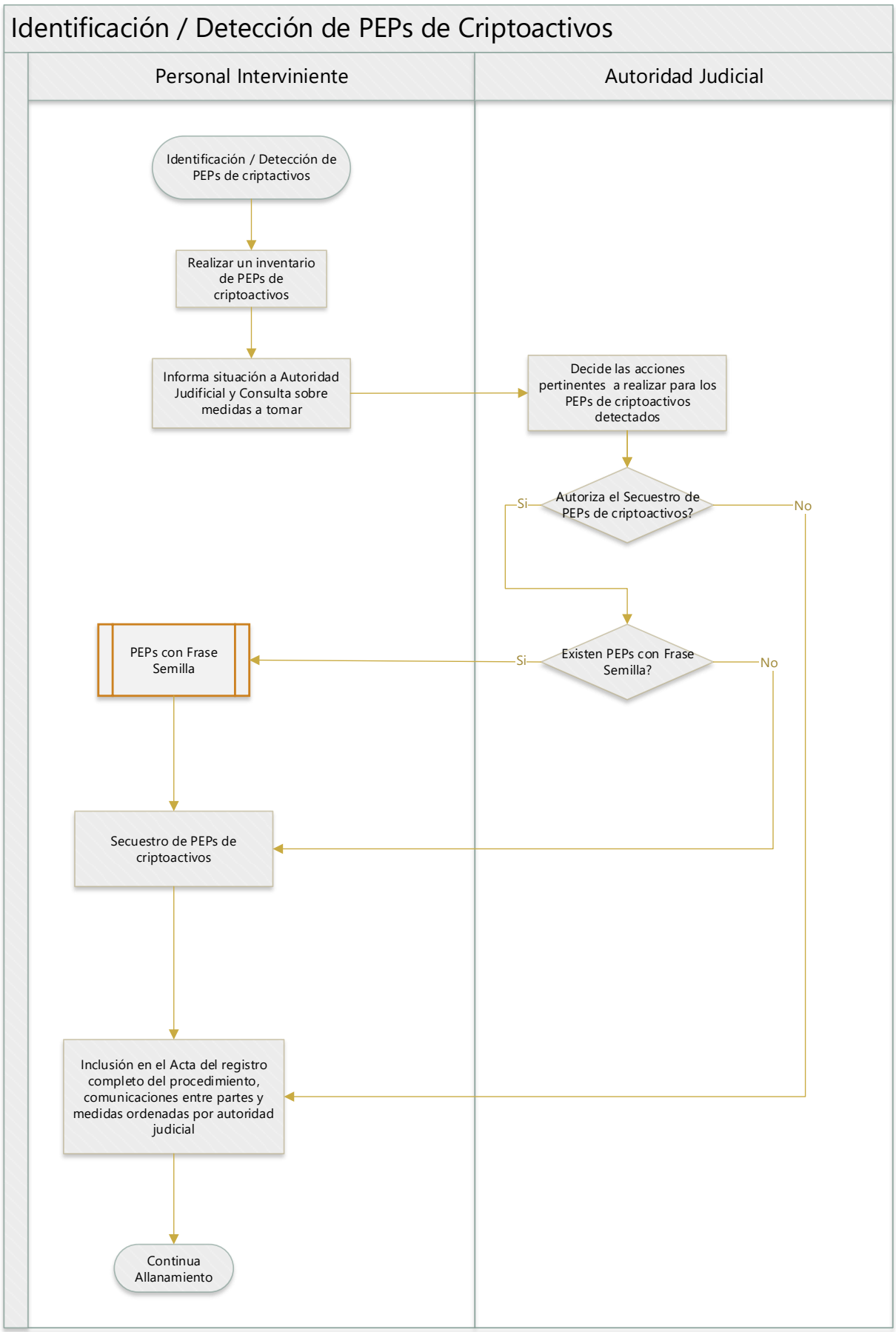
5) Detalles de transacciones históricas (HASH)

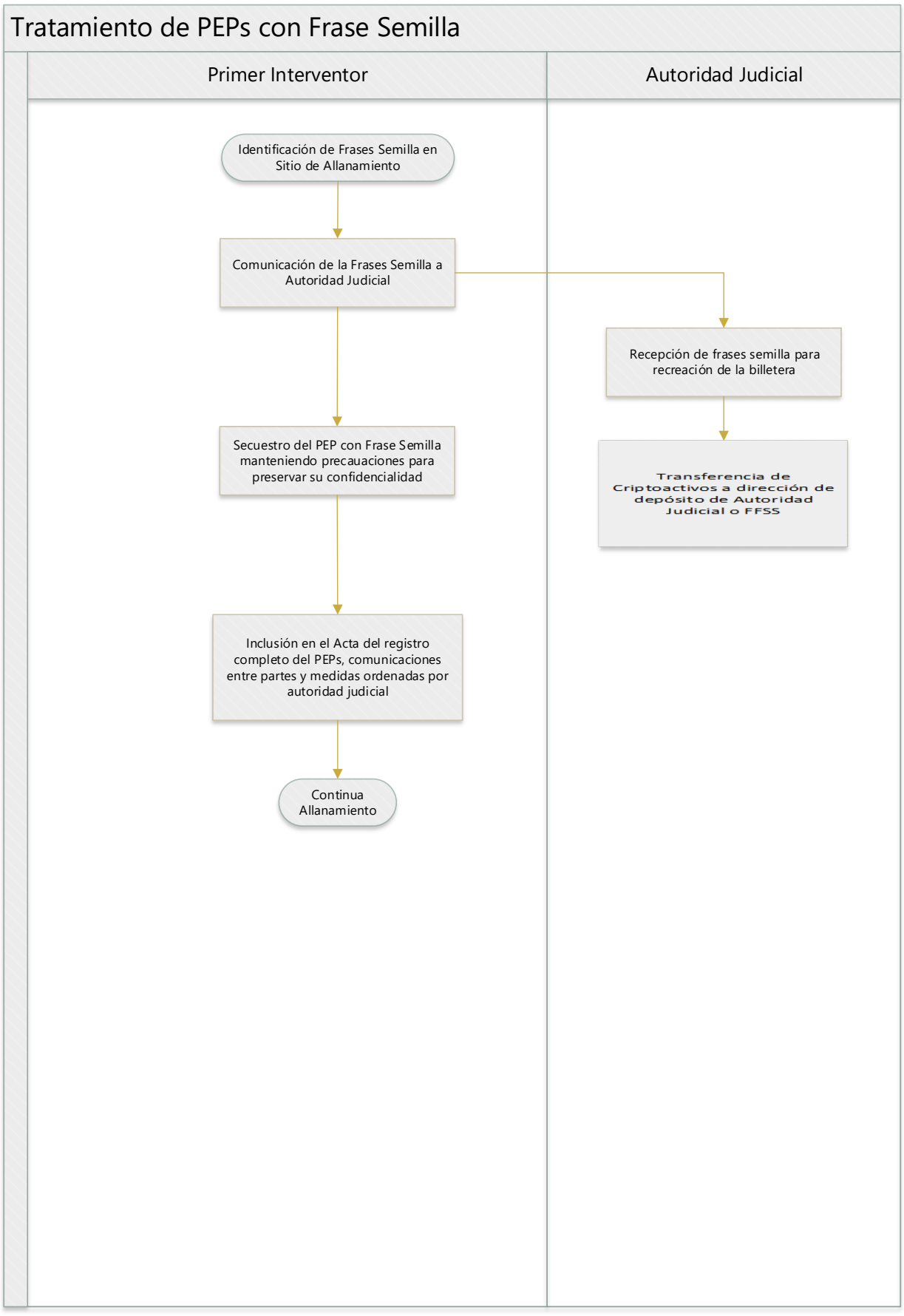
l) En caso de haber sufrido un phishing, sextorsión, ransomware, entre otros por medio de la recepción de un correo electrónico.

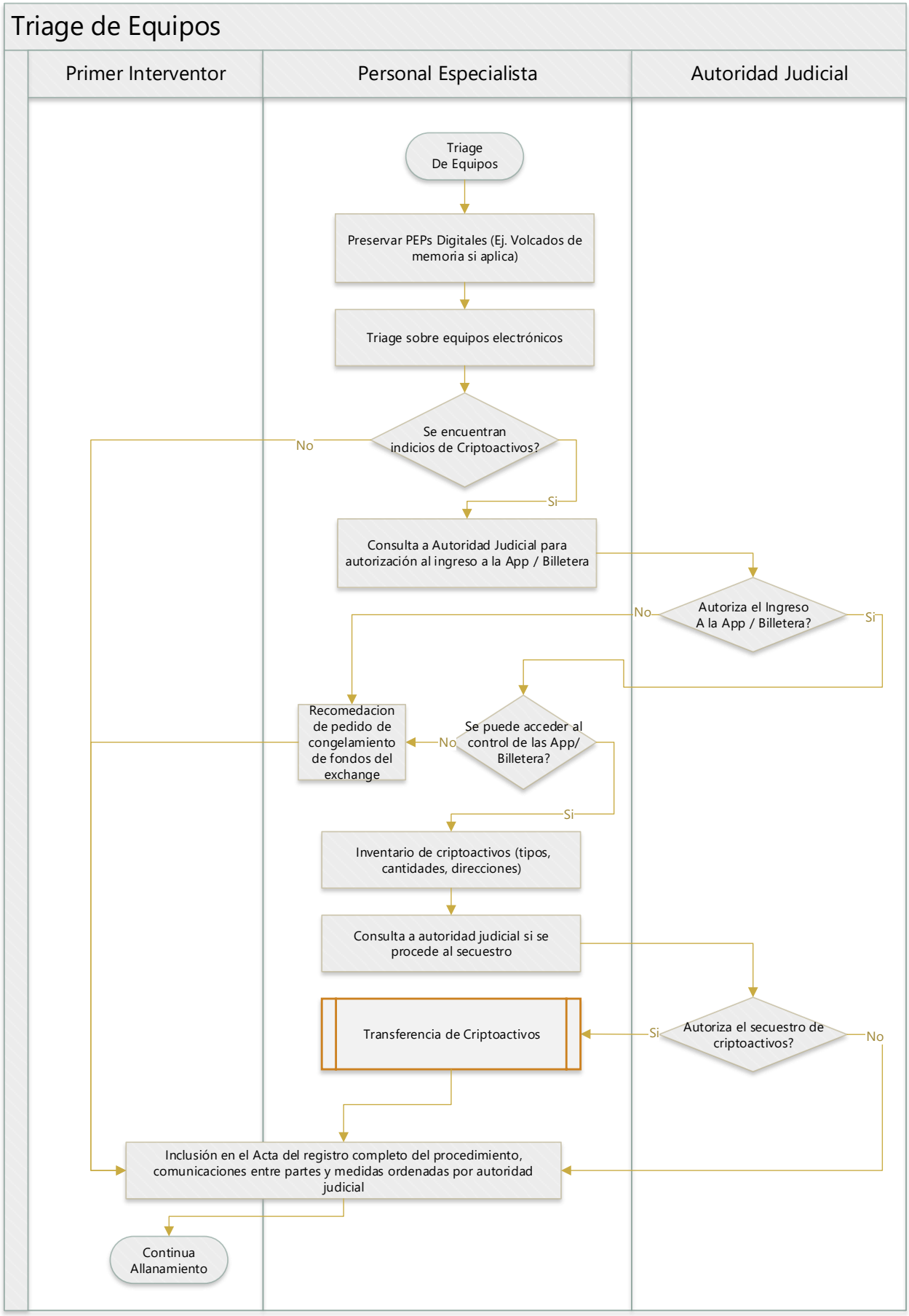
m) Solicitar el apoyo del personal especializado para la correcta preservación y presentación de la evidencia tales como: encabezado del email, archivos adjuntos, direcciones de depósito de criptoactivos para el pago, etc.

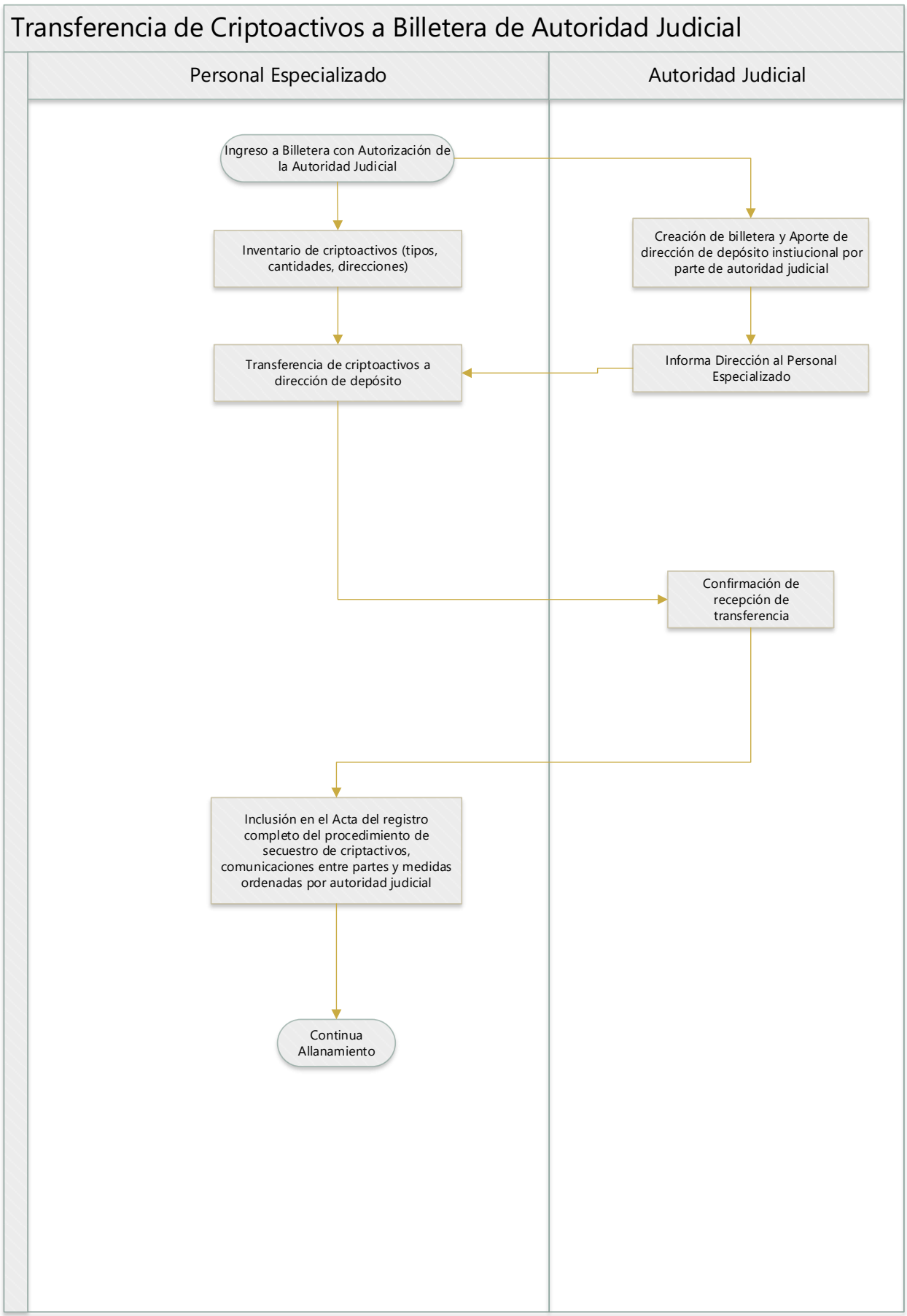
ANEXO I – DIAGRAMAS DE FLUJO

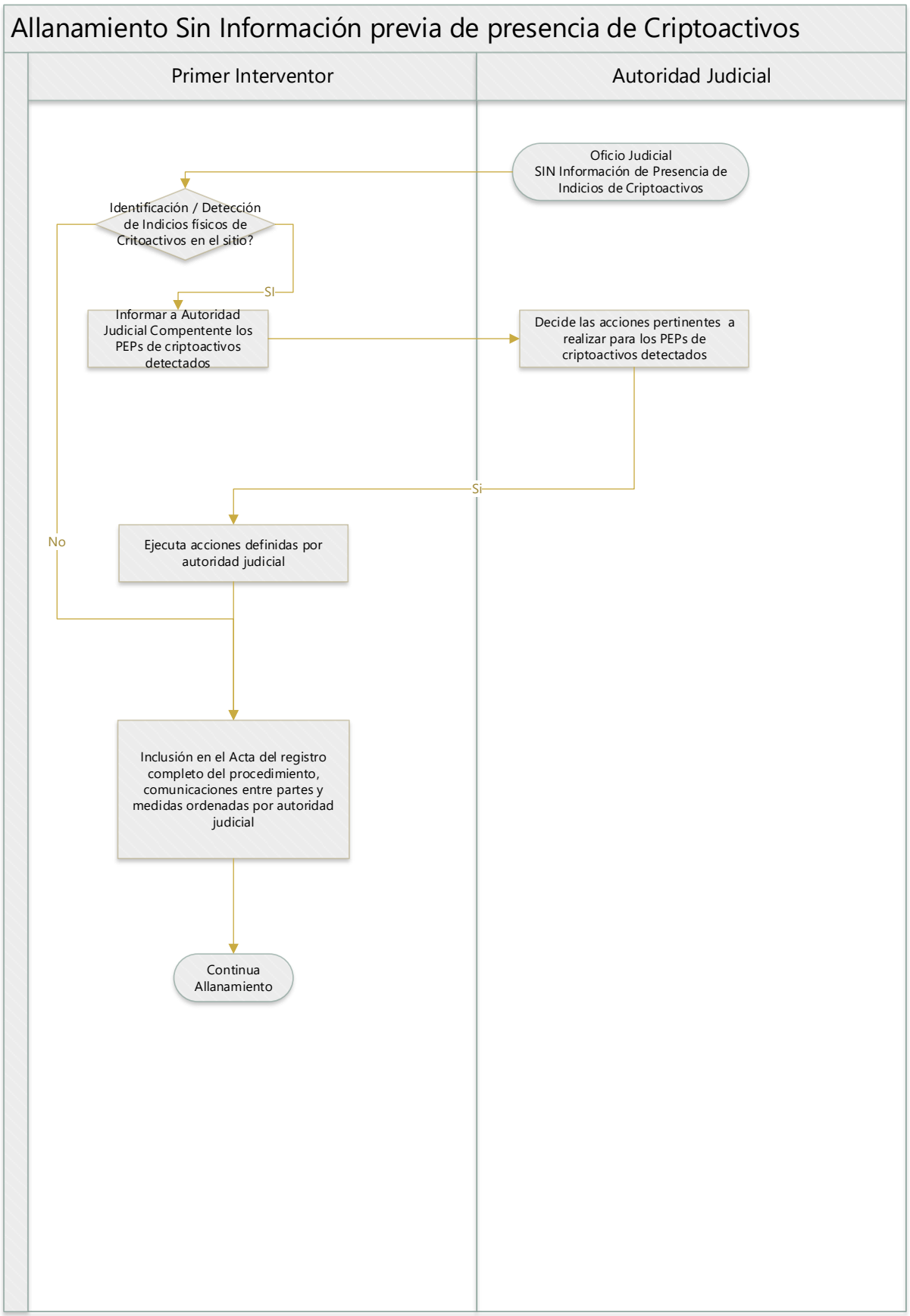



Identificación / Detección de PEPs de Criptoactivos
Personal Interviniente
Autoridad Judicial
Identificación / Detección de PEPs de criptactivos
Realizar un inventario de PEPs de criptoactivos
Informa situación a Autoridad Judificial y Consulta sobre medidas a tomar
Decide las acciones pertinentes a realizar para los PEPs de criptoactivos detectados
Autoriza el Secuestro de PEPs de criptoactivos?
Si
No
Existen PEPs con Frase Semilla?
Si
No
PEPs con Frase Semilla
Secuestro de PEPs de criptoactivos
Inclusión en el Acta del registro completo del procedimiento, comunicaciones entre partes y medidas ordenadas por autoridad judicial
Continua Allanamiento

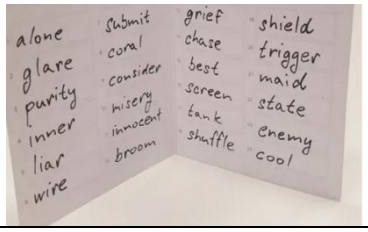

Tratamiento de PEPs con Frase Semilla
Primer Interventor
Autoridad Judicial
Identificación de Frases Semilla en Sitio de Allanamiento
Comunicación de la Frases Semilla a Autoridad Judicial
Secuestro del PEP con Frase Semilla manteniendo precauaciones para preservar su confidencialidad
Inclusión en el Acta del registro completo del PEPs, comunicaciones entre partes y medidas ordenadas por autoridad judicial
Continua Allanamiento
Recepción de frases semilla para recreación de la billetera
Transferencia de Criptoactivos a dirección de depósito de Autoridad Judicial o FFSS

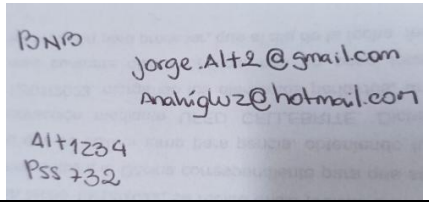

Triage de Equipos
Primer Interventor
Personal Especialista
Autoridad Judicial
Triage
De Equipos
Preservar PEPs Digitales (Ej. Volcados de memoria si aplica)
Triage sobre equipos electrónicos
Se encuentran indicios de Criptoactivos?
No
Si
Consulta a Autoridad Judicial para autorización al ingreso a la App / Billetera
Autoriza el Ingreso A la App / Billetera?
No
Si
Recomedacion de pedido de congelamiento de fondos del exchange
Se puede acceder al control de las App/ Billetera?
No
Si
Inventario de criptoactivos (tipos, cantidades, direcciones)
Consulta a autoridad judicial si se procede al secuestro
Transferencia de Criptoactivos
Autoriza el secuestro de criptoactivos?
Si
No
Inclusión en el Acta del registro completo del procedimiento, comunicaciones entre partes y medidas ordenadas por autoridad judicial
Continua Allanamiento


Transferencia de Criptoactivos a Billetera de Autoridad Judicial
Personal Especializado
Autoridad Judicial
Ingreso a Billetera con Autorización de la Autoridad Judicial
Inventario de criptoactivos (tipos, cantidades, direcciones)
Creación de billetera y Aporte de dirección de depósito instiucional por parte de autoridad judicial
Transferencia de criptoactivos a dirección de depósito
Informa Dirección al Personal Especializado
Confirmación de recepción de transferencia
Inclusión en el Acta del registro completo del procedimiento de secuestro de criptactivos, comunicaciones entre partes y medidas ordenadas por autoridad judicial
Continua Allanamiento


Allanamiento Sin Información previa de presencia de Criptoactivos
Primer Interventor
Autoridad Judicial
Oficio Judicial
SIN Información de Presencia de
Indicios de Criptoactivos
Identificación / Detección
de Indicios físicos de
Critoactivos en el sitio?
SI
Informar a Autoridad
Judicial Compentente los
PEPs de criptoactivos
detectados
Decide las acciones pertinentes a
realizar para los PEPs de
criptoactivos detectados
Si
No
Ejecuta acciones definidas por
autoridad judicial
Inclusión en el Acta del registro
completo del procedimiento,
comunicaciones entre partes y
medidas ordenadas por autoridad
judicial
Continua
Allanamiento

ANEXO II – GUIA RÁPIDA DE ACTUACION PARA PEPs de CRIPTOACTIVOS

	ACCIONES		
Tipos de PEPs de criptoactivos FISICOS	**Primer Interventor**	**Autoridad Judicial**	**Foto**
Frases Semilla	Informar las palabras a Autoridad Judicial. Si es autorizado, proceder al secuestro físico de las mismas para evitar su filtración.	Si lo considera, recrear billetera para el secuestro de criptoactivos Si lo considera, autorizar al secuestro físico	
Billeteras Papel	Informar su presencia a Autoridad Judicial, y si es autorizado, proceder a su secuestro físico	Si lo considera, autorizar al secuestro físico	 
Billeteras en Código QR	Informar su presencia a Autoridad Judicial, y si es autorizado, proceder a su secuestro físico	Si lo considera, autorizar al secuestro físico	
Billeteras Frías en Formato Pendrive	Informar su presencia a Autoridad Judicial, y si es autorizado, proceder a su secuestro físico	Si lo considera, autorizar al secuestro físico	

Rigs de Minería	Informar su presencia a Autoridad Judicial. Si el equipo está encendido sugerir la ejecución del triage mediante personal especializado. Posteriormente, Si es autorizado, proceder a su secuestro físico de acuerdo al Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital	Si lo considera, autorizar el triage por personal especializado. Si lo considera autorizar al secuestro físico	
Direcciones de Email, Nombres, Posibles Contraseñas	Informar su presencia a Autoridad Judicial, y si es autorizado, proceder a su secuestro físico	Si lo considera, autorizar al secuestro físico	
Celulares y/o Tarjetas SIM (Potencialmente usados para Segundo Factor de Autenticación)	Informar su presencia a Autoridad Judicial, y si es autorizado, proceder a su secuestro físico de acuerdo al Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital	Si lo considera, autorizar al secuestro físico	

	ACCIONES		
Indicios de PEPs de Criptoactivos en Triage de Equipos Móviles / Equipos Informáticos	**Personal Especialista**	**Autoridad Judicial**	**Foto**
Aplicaciones / Software de Billeteras	Con orden de triage, informa su presencia a Autoridad Judicial. En el caso de identificar billeteras asociadas a Exchanges/Plataformas de Pagos, recomendar a la autoridad judicial el congelamiento de las cuentas Si es autorizado, intentar ingresar a billetera e inventariar su tipo, identificar criptoactivos presentes, direcciones y saldos Si es autorizado y es posible el control de la billetera, transferir criptoactivos a billetera informada por autoridad judicial	Si lo considera, autorizar al ingreso a billeteras Si lo considera, solicitar el congelamiento de cuentas en Exchange / Plataformas de Pago Si lo considera, autorizar la transferencia de criptoactivos a billetera de la autoridad judicial	

BIBLIOGRAFIA DE CONSULTA

- “Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital” – Resolución 232/2023 del Ministerio de Seguridad de la Nación Argentina.

  (https://www.boletinoficial.gob.ar/detalleAviso/primera/284720/20230419)

- “Protocolo de Actuación para la Investigación Científica en el Lugar del Hecho” – Resolución 528/2021 del Ministerio de Seguridad de la Nación Argentina.

  (https://www.boletinoficial.gob.ar/detalleAviso/primera/253486/20211126)

- “Guía práctica para la identificación, trazabilidad e incautación de criptoactivos”, Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) -2023.

  (http://www.mpf.gob.ar/ufeci/files/2023/05/Informe_Criptoactivos.pdf)

- “Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales” – GAFILAT, diciembre 2021.

  (https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/guias-17/4225-gui-a-sobre-aspectos-relevantes-y-pasos-apropiados-para-la-investigacio-n-identificacio-n-incautacio-n-y-decomiso-de-av/file)

MIEMBROS DEL EQUIPO DE TRABAJO

MINISTERIO DE SEGURIDAD DE LA NACION ARGENTINA

Ing Santiago González Bellengeri, Director de Ciberdelito y Asuntos Cibernéticos
Lic. Antonio Javier MAZA, Coordinador de la Dirección de Ciberdelito y Asuntos Cibernéticos

POLICÍA FEDERAL ARGENTINA
Principal Luis Eduardo CEJAS, Departamento Técnico del Cibercrimen
Cabo Primero Walter TRULLET, Departamento Técnico del Cibercrimen

GENDARMERIA NACIONAL ARGENTINA
Alférez Matías Esequiel CARBALLO, Subdirección de Investigación de Delitos Tecnológicos
Cabo Primero Fabricio Ezequiel REVOLERO OVIEDO, Subdirección de Investigación de Delitos Tecnológicos

POLICÍA DE SEGURIDAD AEROPORTUARIA
Subinspector Jorge Martín GIAYETTO, Departamento de Inteligencia Criminal Aeroportuaria
Oficial Mayor Guadalupe VIVAS, Unidad Operacional Control del Narcotráfico y Delitos Complejos Central

PREFECTURA NAVAL ARGENTINA
Subprefecto Cristian David Alberto CASTELLO, División Apoyo Técnico Profesional
Cabo Primero Alfredo Sebastián LOPEZ BAGUE, División Investigaciones de Ciberdelitos

CONSULTORES DEL MINISTERIO PUBLICO FISCAL DE LA NACION

Dra. Romina DEL BUONO, Directora General DATIP
Dr. Eric DEUTERIS, Sub Director General DATIP
Dr. Javier VILLAR, Secretario DATIP
Ing. Nicolás SANGUINETI, Subsecretario Administrativo DATIP
Dr. Horacio AZZOLIN, Fiscal General UFECI
Dr. Christian MANSILLA, Auxiliar Fiscal UFECI
Dr. Matías GRONDONA, Secretario Adjunto UFECI
Dra. Carolina AYALA, Secretaria Adjunta UFECI
Dr. Esteban SKALANY, Secretario Adjunto UFECI

República Argentina - Poder Ejecutivo Nacional
AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA

Hoja Adicional de Firmas
Anexo

Número: IF-2025-04547034-APN-DCYAC#MSG

CIUDAD DE BUENOS AIRES
Martes 14 de Enero de 2025

Referencia: ANEXO - PGA Identificación, preservación y secuestro de PEP vinculados con criptoactivos

---

El documento fue importado por el sistema GEDO con un total de 36 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.01.14 12:07:09 -03:00

Santiago Gonzalez Bellengeri
Director
Dirección de Ciberdelito y Asuntos Cibernéticos
Ministerio de Seguridad

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
Date: 2025.01.14 12:07:10 -03:00