ICD
INSTITUTO COSTARRICENSE SOBRE DROGAS

GOBIERNO DE COSTA RICA

2023
IV EDICIÓN

UNIDAD DE INTELIGENCIA FINANCIERA

TIPOLOGÍAS

RIESGOS DE LAVADO DE DINERO Y FINANCIAMIENTO AL TERRORISMO
APARTADO ESPECIAL SOBRE LOS ACTIVOS VIRTUALES (AVS)

WWW.ICD.GO.CR

Advertencia de uso

Contenido

Introducción

El presente documento ha sido elaborado por la Unidad de Inteligencia Financiera del Instituto Costarricense sobre Drogas con base aportes de información, alertas, reportes de operaciones sospechosas y tratamiento de casos de investigación, cuyos insumos se generan de fuentes como el sector financiero, actividades y profesiones no financieras, y casos de investigación aportados por los operadores de justicia, policías, órganos de supervisión y colegios profesionales.

Los delitos de legitimación de capitales y el financiamiento al terrorismo afectan severamente a un país y ponen en riesgo la integridad del sistema financiero nacional. La identificación de tipologías y alertas resultan una actividad necesaria para implementar un sistema de prevención eficaz e idóneo en la lucha contra estos delitos.

En esta IV edición del Compilado de Tipologías se consolidan descripciones puntuales y resumidas planteadas a modo de lectura rápida, dando a conocer las principales alertas de riesgo que podrían constituir operaciones de lavado de dinero y financiamiento al terrorismo como ejemplos de riesgos y posibles manifestaciones criminales en el medio con el fin de comprender y evaluar en el campo de acción de cada parte y que ello complemente las labores de la investigación, la debida diligencia del cliente y fundamente políticas y procedimientos de mejora continua.

Corrupción y soborno

1. Caso de corrupción y soborno transnacional

Descripción general

Se alerta de la recepción en Costa Rica por parte de colaboradores de una persona extranjera que ocupaba un cargo político de alto nivel de ese país.

Se trata de una persona expuesta políticamente (PEP) quien, al parecer, recibió varios millones de dólares como soborno por la adjudicación de una concesión y construcción de infraestructura en su país de origen.

Los consorcios constructores de uno de los países involucrados, realizaron diversos pagos ilícitos de manera escalonada durante un tiempo de varios años de manera consecutiva, con recursos no contabilizados que se encontraban en empresas offshore que seguían órdenes del concesionario adjudicado.

Los fondos fueron trasladados a Costa Rica luego de un "puenteo" entre países de Europa y paraísos fiscales para difuminar el rastro y evadir el control de las autoridades. Para lograr los objetivos de opacidad en cuanto al origen del dinero se configuró con la participación de varias personas de confianza (testaferros) y familiares cercanos de dueño del capital, quienes crearon empresas ficticias en Costa Rica y abrieron cuentas bancarias a nombre de las personas jurídicas, cuyas acciones fueron endosadas a favor del PEP.

Inmediatamente después de la creación de las supuestas empresas, se configura la recepción de las dádivas de manera secuencial por varios millones de dólares producto de los sobornos.

Una vez que el dinero ingresa a las cuentas se realizaron pagos al país origen por la compra de inmuebles y también se generaron traslados a cuentas bancarias a nombre los titulares en las supuestas empresas. Además, con la finalidad de ocultar otra parte de los fondos, los involucrados promovieron la obtención de créditos bancarios millonarios de manera rápida con facilidades y colaboraciones internas para simular compromisos bancarios pendientes que le justificarían la remisión de los fondos ilícitos a su país de origen.

Como resultados del proceso se decomisaron varios millones de dólares.

Señales de alerta:

- Participación de personas políticas de alto nivel (PEP).
- Pago de sobornos por adjudicación de concesiones.
- Movilización de los fondos por diferentes jurisdicciones con la finalidad de ocultar el rastro.
- Sumas millonarias sin justificación del origen de los fondos.
- Creación de personas jurídicas de fachada.
- Recepción de transferencias internacionales y operaciones emergentes inusuales.
- Puenteo de dinero entre cuentas y remisión de fondos al exterior.

Juego en línea y apuestas

2. Juegos en línea y apuestas deportivas

Descripción general

Esta tipología fue detectada a través de alertas espontáneas e información de inteligencia recibidas por cooperación internacional de UIF a UIF procedente de países catalogados como de alto riesgo ubicados en el sur de Europa y el norte de África realizando operaciones de remisión de dinero a través de cuentas bancarias de empresas involucradas con juegos remotos y apuestas deportivas en el país de origen.

Las supuestas empresas en el exterior se vinculan con actividades de piratería y dumping de fichas a través de artimañas del juego.

Las empresas vinculadas no lograron respaldar el origen de sus fondos, acreditados a través de transferencias internacionales que fueron catalogadas como injustificadas.

Señales de alerta

- Estructuración de montos bajos en cuenta remota de la compañía radicada en Costa Rica.
- Uso de cuentas relacionadas a una misma persona física involucrada en actividades ilegítimas.
- Depósito de fondos a través de tarjeras de crédito.
- Utilización de fraude de tarjetas y artimañas en la modalidad de juegos de azar para apuestas deportivas.
- Aprovechamiento de las debilidades de los sistemas de control interno bancarios.
- Multiplicidad de depósitos bajo una estructuración, sin respaldo del origen de fondos.

Cajitas de Seguridad

3. Uso de cajitas de seguridad

Descripción general

Un sujeto obligado (APNFD) almacenó dinero en efectivo en cajitas de seguridad en una entidad financiera sin tener justificación ni requisitos sobre el origen del dinero.

La suma del dinero en efectivo supera los USD$ 300.000,00 para justificar su origen hace referencia a la suscripción de un contrato de administrador de fondos de terceros con una sociedad extranjera de una jurisdicción de riesgo la cual está relacionada a una actividad comercial conocida en el país, pero no es congruente ni razonable con el comportamiento sobre el almacenamiento de dinero en divisa extranjera en efectivo.

El dinero sospechoso se justifica en la actividad comercial de ventas de la compañía acumulado en varios períodos lo que tampoco resulta consistente ni proporcionado a una actividad empresarial, además que financieramente las empresas requieren de capital de trabajo para continuar produciendo.

Señales de alerta

- Justificación de acumulación de dinero en efectivo en dólares durante casi 4 años, incluyendo período de pandemia, cuando las empresas comerciales se vieron fuertemente afectas por las medidas sanitarias mundiales.

- Uso de dinero en efectivo provenientes de las supuestas ventas de productos y bebidas.

- Origen del capital de jurisdicción de riesgo y actividad que no justifica el movimiento de dinero en efectivo.

- Uso irregular de cajas de seguridad por no contar con justificación adecuada sobre el origen del dinero.

- Contratos de servicios firmados entre empresas poco conocidas.

Transferencias Internacionales

3 casos representativos

4. Redes de testaferros recibiendo transferencias internacionales

Descripción general

Se han identificado redes de testaferros recibiendo transferencias internacionales. Varias investigaciones realizadas determinaron la acreditación de dineros a través de transferencias internacionales provenientes desde Estados Unidos con ordenantes en condiciones que se identifican denominadores comunes tales como: a) no existe un vínculo aparente entre el ordenante y beneficiario, b) dichas transacciones se encontraban fuera del perfil financiero normal de los beneficiarios.

Se identifican en este tipo de modalidades a personas registradas como amas de casa o estudiantes quienes poseen un perfil transaccional bajo y la actividad podría ser considerada también de bajo riesgo.

Al momento de ser acreditado el dinero en las cuentas bancarias de los titulares, de inmediato es retirado en efectivo, lo cual no permite darle una trazabilidad al destino; sin embargo, las investigaciones reflejan que los fondos son entregados a una sola persona en común, que funge como acopiador o receptor del dinero en efectivo.

Señales de alerta

- Ordenantes en Estados Unidos envían sumas cercanas a las USD$1.000.00 a varias personas que conforman redes sin relación aparente.
- Los propietarios de las cuentas bancarias prestan el nombre y la cuenta para recibir dinero de terceros que posiblemente son organizaciones criminales y de esta forma se permite el ingreso del dinero ilícitos
- Los beneficiarios en Costa Rica poseen características similares en cuanto a lugar de residencia, actividad económica de bajo riesgo, montos bajos de las transferencias que generalmente no sobrepasan el monto de ingresos declarado.
- El dinero es retirado en efectivo minutos después de recibir la transferencia por lo que se infiere que se trata de un puenteo de dinero de origen ilícito.

- No se logra establecer vínculo familiar o de negocios legítimos entre el ordenante y el beneficiario lo que aumenta exponencialmente la sospecha.
- Utilización de productos bancarios de alto riesgo (transferencias internacionales)
- Cuenta bancaria abierta recientemente con el fin de recibir la transferencia del exterior cuya actividad declarada no coincide con el ingreso de fondos a través de este producto.
- Actividad declarada de bajo riesgo y movilización de bajas cuantías de dinero para evitar alertas de control en las entidades financieras, pero que al analizar el movimiento de redes similares, las cuantías de dinero suman miles o cientos de miles de dólares de manera estructurada.

Las transferencias Internacionales son uno de los servicios con mayor incidencia en los Reportes de Operaciones Sospechosas y las investigaciones seguidas donde las personas no pueden demostrar el origen lícito del dinero y muchas veces están recibiendo dinero proveniente de un delito.

5. Envío de fondos a sociedades extranjeras sin justificación a través de portales bancarios regionales.

Descripción general

Personas de nacionalidad costarricense miembros del mismo grupo familiar reclutan personas y utilizan cuentas propias para el envío de transferencias internacionales por altas sumas de dólares a cuentas de sociedades extranjeras dedicadas aparentemente a la comercialización de mercadería (vestido y calzado).

Estas personas en primera instancia realizan los depósitos en efectivo en sus cuentas personales en bancos, los cuales poseen presencia en la región y a través de depósitos centroamericanos y/o transferencias regionales el dinero es trasladado a las sociedades extranjeras, las cuales poseen cuentas en los mismos bancos en Centroamérica.

Las personas reclutadas para la apertura de las cuentas en Costa Rica y transferir los fondos poseen perfiles de actividades económicas dentro de una descripción de no calificadas y poseen nacionalidades de países con alto grado de migración.

Señales de alerta

- Apertura de cuentas en bancos con presencial en la región de Centroamérica.
- Miembros de un mismo grupo familiar que abren cuentas masivamente.
- Depósitos en efectivo a través de transacciones estructuradas en un mismo día en una misma sede bancaria.
- Ninguno de los miembros del núcleo familiar posee el perfil transaccional para justificar el manejo del dinero en las cuentas bancarias.
- Envío de fondos a sociedades extranjeras a través del portal regional o depósitos centroamericanos.
- Personas con actividades económicas no calificadas y con altos índices de endeudamiento.

6. Extorsión y supuesto error administrativo en transferencia internacional enviada

Descripción general

Recepción de transferencias internacionales por altas sumas de dinero en cuentas de extranjeros, quienes al momento de realizarle la debida diligencia y solicitarle la documentación que justifique la recepción de los fondos recibidos, no tienen la capacidad de presentar el origen y razonabilidad de los mismos.

Paralelamente al proceso de justificación de fondos, la entidad bancaria es contactada por diversos medios por parte de los ordenantes de las transferencias, quienes manifiestan estar siendo extorsionados por el "beneficiario" del dinero y los mismos, solicitan la devolución de los fondos alegando un error administrativo y operativo en el traslado internacional del dinero, asumiendo sin problema el costo de las comisiones que se puedan generar por los procesos del trámite.

De igual manera, el banco emisor de la transferencia también se suma, por instrucción del ordenante, a requerir la devolución de los fondos transferidos lo que confirma una estructuración perpetrada por delincuentes.

Señales de alerta:

- Recepción de dinero por sumas conglomeradas superior a los $500,000.00, por medio de transferencia internacional que supera el perfil de ingresos declarado.
- Documentación insuficiente para respaldar el origen de los fondos.
- El ordenante de la transferencia internacional aduce un error operativo de envío de fondos y una presunta extorsión del beneficiario de estos.
- Reclamo tardío por parte del ordenante al banco del reclamo de los fondos recibidos por un presunto error operativo.
- Se sospecha la vinculación de los capitales recibidos con fraudes con créditos financieros.

Certificaciones de CPA

7. Certificaciones de Contadores Públicos Autorizados (CPA).

Descripción general

Personas físicas que se encuentran relacionadas con alertas de Inteligencia confidenciales por la movilización de flujos financieros de dudosa procedencia.

Las personas declararon dedicarse a la venta informal de ropa, calzado y otras actividades sobre las cuales no hay certeza y tienen elementos de informalidad.

Respaldan sus ingresos a través de la búsqueda de certificaciones emitidas por contadores públicos autorizados a raíz de que se trata de una actividad informal o inexistente la cual podría no estar amparada al orden socioeconómico como lícita y legítima.

El tipo de certificación resulta coincidente con las sospechas de opacidad por lo que se sospecha que se trate de una tipología de red donde participan los profesionales intermediando y haciendo un uso irregular de la fe pública que ostentan.

Los estudios toman como base estados de cuenta carecen de fuentes fidedignas de prueba, no contemplan declaraciones del IVA, declaraciones del impuesto sobre la renta, contratos, ni registro ante la Administración Tributaria.

Señales de alerta

- Personas físicas menores de 25 años, costarricenses, dedicadas a la supuesta venta informal de ropa y calzado movilizando grades sumas de dinero en poco tiempo a través del Sistema Financiero Nacional.
- Utilización de certificaciones de ingresos emitidas por CPA, que no detallan las fuentes de información ni los procedimientos utilizados para la confección de éstas.

- Certificaciones recurrentes emitidas por un mismo CPA elaboradas únicamente con base en Estados de Cuenta Bancarios sin detallar la actividad lícita y legítima.
- Depósitos en efectivo estructurados que no parecen obedecer a una actividad comercial congruente con la descripción.
- Personas con domicilio en zonas catalogadas de alto riesgo geográfico.
- Sospechas de vínculos relacionados al tráfico de drogas en las zonas de domicilio.

Activos Virtuales

3 casos representativos

8. Compra y venta de activos virtuales y relación con fraudes informáticos.

Descripción general

Se considera el uso de redes de testaferros involucrados en la movilización de fondos asociados a la compra y venta de Activos Virtuales (AVs).

Se trata de personas físicas con edades entre los 20 y 35 años edad del área metropolitana que declaran ante la entidad financiera actividades económicas como asesoría financiera, diseño de sitios web, asesoría en mercadeo y venta de productos por catálogo.

Estas personas prestan sus cuentas bancarias para recibir fondos por parte de terceros mediante diversos canales y servicios electrónicos (SINPE, SINPE Móvil, Ameritransfer, entre otros). Posteriormente, en cortos períodos, retiran los fondos en efectivo de manera estructurada o bien los acreditan a nombre de terceros a través de los canales electrónicos anteriormente mencionados.

Señales de alerta

- Clientes se vinculan a la entidad declarando un ingreso inferior a los US$5.000,00 mensuales evitando el suministro de la evidencia de ingresos.
- Clientes recién vinculados reciben en cortos períodos de tiempo (de dos a tres meses) sumas acumuladas que rondan entre los US$200.000,00 y US$300.000,00 de terceros no relacionados con sus actividades comerciales.
- Estructuración en alto volumen de retiros en efectivo por montos menores a los US$10.000,00 evitando los controles como la generación del ROE.
- Transferencias electrónicas realizadas desde y hacia personas vinculadas a reportes de operaciones sospechosas por utilizar las mismas tipologías.

9. Organización Criminal dedicada a estafas en criptomonedas y adquisición de bienes usando sociedades fachada

Descripción general

Persona física que se dedica a la supuesta inversión en criptomonedas realiza acciones como receptora de fondos de naturaleza dudosa en sus cuentas recibiendo transferencias de múltiples ordenantes que coinciden en temporalidad de día y mes (eventos programados o estructurados), posteriormente con el mismo modus operandi, egresa los dineros a múltiples beneficiarios, aplicando un "puenteo".

Una segunda persona física (relacionada por medio de una sociedad anónima con la primera persona), se dedicada a realizar préstamos informales, recibe en sus cuentas transferencias internacionales desde una institución financiera donde realiza las operaciones de cambio de activos virtuales a moneda de curso legal.

Personas físicas y jurídicas, nacionales y extranjeros mantienen relaciones comerciales con las personas primera y segunda, movilizando fondos en sus cuentas para la adquisición de bienes de alto valor, utilizando diferentes sociedades de fachada en las cuales realizan mezcla de fondos de dudosa procedencia con el cual han adquirido los bienes en cuestión, especialmente vehículos y propiedades en zonas turísticas, desconociéndose la fuente de ingresos que respalda el alto nivel socioeconómico que ostentan.

La organización se vale del uso de profesionales intermediarios en la rama de contabilidad para emitir certificaciones de ingresos aprovechándose de la potestad de ser fedatario público para justificar a través de supuestos estudios contables los flujos de dinero que moviliza.

Los fondos movilizados alcanzan la suma de $2 000 000.00, provenientes de Europa y otras latitudes.

Señales de alerta:

- Actividad comercial relacionada a inversiones en criptomonedas (actividad de alto riesgo).
- Uso de profesionales intermediarios que certifican ingresos valiéndose de la facultad de fe pública para introducir el dinero en entidades financieras.

- Alertas negativas por facilitar cuentas bancarias para recibir dineros producto de transferencias electrónicas fraudulentas.
- Relaciones comerciales con personas vinculadas con alertas relacionadas a delitos de lavado de activos.
- Negocio emergente que refleja una movilización de capital relevante cuyo origen es desconocido.
- Ingresos y egresos de fondos en efectivo de manera estructurada.
- Utilización de sociedades fachada o de papel para movilizar y mezclar los fondos de naturaleza dudosa.
- Estilo de vida de las personas que componen la organización criminal difiere de sus perfiles económicos y actividad declarada ante el Sistema Financiero.

10. Pago de secuestro extorsivo con criptomonedas

Descripción general

Sujeto empresario extranjero (país X) reportado como desaparecido de manera misteriosa, cuando viajaba en el camino. El sujeto era propietario de un negocio ubicado en la capital.

Ante esa situación, las autoridades recibieron una denuncia de un familiar del ofendido, por lo que la Fiscalía Adjunta contra el Narcotráfico y Delitos Conexos, en colaboración con la Policía Judicial, llevaron a cabo una serie de diligencias importantes para determinar lo ocurrido.

En las primeras horas posteriores al secuestro los captores realizaron comunicaciones por medio de WhatsApp, donde solicitaban el pago de sumas de varios millones de dólares equivalentes en bitcoins que serían transferidos a tres diferentes direcciones de bitcoin.

Familiares realizaron el pago equivalente a una primera parte en cada una a una de las direcciones de depósito suministradas por la banda. Tanto la Unidad Investigadora de Secuestros como la Sección Especializada Contra el Cibercrimen, trabajaron en avanzar la investigación, logrando obtener sospechosos relacionados al secuestro extorsivo; siendo que una parte de éstos abandonó el país, con destino final Europa.

De esa manera, el Ministerio Público descubrió el plan delictivo de un grupo familiar. El resultado final fue el asesinato de la víctima a pesar de haber recibido parte del dinero por una suma muy relevante y se da la huida del país, sin embargo, se logró la sentencia por los hechos.

El rastreo telefónico permitió determinar quién era el líder de la organización criminal, así como identificar a las otras personas que participaron en el acto delictivo incluyendo la colaboración de otros oficiales, que facilitaron el secuestro de la víctima.

El grupo tenía roles muy específicos, algunos se encargaron del manejo de la información de las criptomonedas, otras del sitio del cautiverio y otros ejecutaron actos materiales como vigilancias, seguimientos y contactos. El grupo realizó acciones de inteligencia relevantes para identificar a quién contactar, una vez que los criminales lograron obtener el beneficio económico y, tras el asesinato de la víctima, huyeron en ruta a países del sur y Caribe y luego hacia Europa ubicándose en lugares de alta plusvalía para vivir y luego buscaban protección por asuntos de extradición.

Se logra la identificación de varias direcciones de bitcoin donde llegaron parte de los fondos que se transfirieron inicialmente y por medio de diferentes consultas a distintos

exchanges o intercambiadores se logró obtener la información de los dueños de dichas direcciones de bitcoin, generada por la política que tienen estas empresas sobre el conocimiento del cliente (KYC).

Desde las primeras horas posteriores a la denuncia del secuestro, cuando se realizaron los rastreos por parte de la policía judicial, lograron tener conocimiento e identificar a algunos de los participantes, lo que también resultó en la generación de alertas migratorias internacionales, que permitieron seguir el rastro de los imputados en los países por los cuales circularon.

Tras varias coordinaciones, se ejecutaron diligencias de allanamiento, las cuales permitieron detener tanto a los imputados que se encontraban en ese país europeo como los que se mantenían en territorio nacional.

Finalmente se logró realizar una operación conjunta entre Costa Rica y el país de Europa, resultando en el arresto de varios miembros de la banda. A quienes se les enjuició con resultado de 50 años de cárcel.

Principales delitos relacionados a criptoactivos

De acuerdo con la información suministrada por Sección Especializada contra el Cibercrimen del Organismo de Investigación Judicial, en el 2023 se ha identificado un aumento del 80% de casos relacionados a criptomonedas, en comparación con años anteriores, los cuales involucra distintos tipos de delitos que se vienen investigando en los cuales figura el tema de los criptoactivos, tales como:

- Estafas
- Legitimación de Capitales
- Secuestros Extorsivos
- Homicidio
- Extorsiones
- Administración Fraudulenta
- Violación de Comunicaciones Electrónicas.

Uso de cuentas de menores de edad

11. Uso de cuentas de menores de edad

Descripción general

Uso de cuentas aperturadas a menores de edad por parte de personas que aducen ser comerciantes que operan en la informalidad incluyendo la venta de lotería ilegal mediante operaciones a través de los servicios de la plataforma SINPE Móvil.

Tutores o encargados de los menores de edad con bajo perfil de la zona metropolitana se presentan a la entidad financiera para abrir cuentas infantiles con el objetivo de utilizarlas para sus negocios que en varios casos ingresan dinero de procedencia dudosa.

Al momento de ser contactados para justificar sus operaciones financieras no suministran el soporte documental suficiente que evidencie la legalidad de este y de sus operaciones.

Señales de alerta

- Uso inadecuado de una cuenta infantil para operaciones comerciales relacionadas con la comercialización y pago de premios de lotería ilegal.
- Cliente no facilita el soporte documental que evidencie el origen de los fondos movilizados por medio de su cuenta ni existe evidencia de ingresos que justifique su perfil transaccional.
- Algunas personas al encontrarse en situaciones similares han contactado Contadores Públicos Autorizados para tratar de justificar los ingresos.
- Alto volumen de transferencias electrónicas por medio de la plataforma SINPE Móvil que en un periodo menor a un año superan las 10 000 transacciones por un monto promedio de US$5,00 por transacción.
- Comportamiento transaccional no acorde con el perfil del cliente (menor de edad).

Organizaciones religiosas

12. Líderes de organizaciones religiosas y sin fines de lucro

Descripción general

Líder de una organización religiosa registrada como una organización sin fines de lucro, reciben múltiples depósitos en efectivo en oficinas bancarias de zonas rurales, indicando que los depósitos corresponden a donaciones, ofrendas y/o diezmos para su líder quien es miembro de una congregación religiosa.

Entre los depositantes se encuentran personas asociadas con actividades delictivas.

Existe una clara sospecha que este tipo de organización cuenta con el apoyo y asesoramiento de empleados bancarios quienes los orientan en las justificaciones que deben indicar a la hora de realizar los depósitos, con la finalidad de evadir los controles normativos establecidos en las entidades financieras lo que hace sospechas que reciben un beneficio económico por la asesoría.

Los depósitos son realizados en efectivo de manera estructurada en la cuenta personal del líder religioso.

Señales de alerta

- Depósitos en efectivo utilizados de forma estructurada cercanos a la cifra de los $10,000 con intenciones de evadir controles al umbral establecido de los ROE.
- Sospecha de origen de los fondos ligados a actividades de narcomenudeo.
- Personas con domicilio en zonas catalogadas de alto riesgo geográfico.
- Sospechas de operativa con vínculos relacionados al tráfico de drogas.
- Comportamiento transaccional no acorde con el perfil del cliente / líder religioso.


Presta cuentas
Presta nombres

13. Presta cuentas / presta nombres

Descripción general

Esta tipología hace referencia a clientes habituales de las instituciones financieras que solicitan abrir cuentas nuevas, en moneda colones y en dólares.

Posterior a la apertura de las cuentas, el cliente habitual solicita e incorpora como autorizados a extranjeros sin aportar documentos ya que se trata de un registrado indirecto.

De manera emergente, el sistema de monitorio alerta de movimientos acumulados en las cuentas que sobrepasan el perfil transaccional del titular de la cuenta, quien presenta documentos de su actividad económica, como presunto documento de respaldo de los ingresos movilizados en la cuenta.

Sin embargo, al analizar las operaciones detalladamente, se determina que las personas que movilizaron el dinero son los autorizados extranjeros y no el dueño directo de la cuenta, haciendo incurrir en un error a la entidad financiera para la movilización de dinero de origen desconocido hacia un beneficiario final diferente al registrado.

Sobre este tipo de modalidades se exige implementar acciones de control para aplicar la verificación de la actuación en nombre de un tercero, por ello las instancias de cumplimiento deben estar atentas a identificar este tipo de operaciones.

Señales de alerta

- Dueño de la cuenta es cliente habitual pero incluye terceros autorizados son relación aparente.
- Cambia de modalidad aperturando nuevas cuentas bancarias pese a ser ya cliente de la institución
- Solicitud de cuentas bancarias en colones y dólares para aplicar la misma modalidad.
- Inclusión de autorizado para movilización de fondos de nacionalidad extranjera.
- Altos volúmenes de dinero sin justificación sobre el origen de los fondos.
- Sospechas generales sobre el origen del dinero que pueda estar vinculado a narcotráfico.

14. Presta cuentas

Descripción general

Se ha identificado un incremento desmedido de personas presta-cuentas, y los casos de investigación han revelado que los dineros, en muchos casos, se destinan a personas relacionadas con delitos.

Se trata de una situación en la cual una persona “A” le solicita a través de artimañas a una persona “B” que le preste la cuenta bancaria para recibir fondos a cambio de una comisión por el préstamo y esto a su vez es el mismo hecho relacionado con facilitar el nombre para realizar una transacción bancaria de un tercero.

Estas situaciones comprometen a terceras personas en condición de necesidad o vulnerabilidad para ser involucradas en actividades delictivas con la ayuda que les dan a terceros para consumar el ocultamiento de capitales ilegítimos.

Señales de alerta:

- Perfiles transaccionales muy limitados de los clientes y que luego incrementan de manera emergente.
- Aumenta la actividad transaccional repentina y evidentemente fuera del parámetro normal y posteriormente se detiene.
- Investigaciones revelan aumento del uso de personas en esta modalidad.
- Recepción de transferencias internas secuenciales sin una razón aparente.
- Recepción de transferencias internacionales sin justificación.
- Desconocimiento del origen de los fondos.
- No existe justificación del origen de los fondos.

Ingreso de efectivo mediante cajero multifuncional

15. Ingreso de efectivo mediante cajero multifuncional para compra de bienes.

Descripción general

Detección de depósitos en efectivo a través de cajeros multifuncionales en cuentas personales y menores de edad.

En el momento que el sistema ya no le permite depositar más, el dinero es acreditado a cuentas de familiares que posteriormente le trasladan mediante transferencias en la plataforma virtual. Al utilizar diversas cuentas para ingresos de efectivo en pequeñas cantidades es muy difícil su detección, sin embargo, al final se acumulan grandes cantidades de dinero (lo que se conoce como acopiador).

Al solicitar respaldo documental del origen de fondos presenta facturas por ventas de ganado. Estudios realizados determinan que existe una secuencia de facturas las cuales son confeccionadas el mismo día en que se solicitaron. Las facturas tienen minutos de diferencia, descripción del mismo producto y la misma cantidad con diferentes montos y sin información del supuesto cliente comprador.

Todo el dinero acumulado fue utilizado para comprar bienes muebles e inmuebles. Incluso se evidencian remisiones al exterior para la compra de bienes que no se identifican en el Registro Nacional.

Señales de alerta

- Depósitos en secuencia utilizando cajeros multifuncionales.
- Acumulación de grandes cifras de dinero para compra de bienes muebles e inmuebles.
- Uso de cuentas personales, cuentas de menor y cuentas de familiares relacionados para la movilización del dinero.
- Envío de transferencias internacionales por supuestas compras de bienes que nunca se identificaron sus registros.
- Fondos sospechosos sin justificación satisfactoria.
- Respaldos inadecuados y uso de facturación evidentemente ficticia.

Inversiones Fraudulentas

16. Inversiones fraudulentas

Descripción general

Se recibe alerta confidencial por cooperación internacional que pone en conocimiento un esquema de estafas e inversiones fraudulentas por altas cifras en dólares, cuyo capital es desviado a cuentas de bancos ubicados en Costa Rica, a favor de empresas también costarricenses dedicadas al comercio.

Las transferencias fueron enviadas bajo pretextos fraudulentos y entregadas a favor de personas jurídicas cuya actividad económica no es la intermediación financiera ni bursátil por lo que se identifican como empresas fachada.

La propuesta consistía en la apertura de cuentas para invertir en una empresa comercializadora de metales preciosos, con la finalidad de obtener supuestas ganancias lucrativas las cuales se otorgaron en un primer momento para funcionar como enganche; sin embargo el estafador continúa insistiendo en el aporte adicional de altas sumas de dinero pero esta vez hacia cuentas extranjeras, utilizando una serie de artimañas para tratar de generar confianza a sus potenciales víctimas. Las cuales en su mayoría son adultos mayores jubilados con ingresos altos por pensiones o rentas del gobierno.

Señales de alerta:

- Transferencias internacionales por altas sumas de dinero sin relación entre el ordenante y el beneficiario.
- Uso de sociedades mercantiles para la recepción del dinero como empresas fachada.
- Depósitos estructurados para evadir los controles de umbrales.
- Cuentas bancarias recién aperturadas que muestran movimientos emergentes y relevantes.
- Actividad declarada incongruente con los movimientos financieros.

Compra de vehículos mediante el uso de efectivo

17. Compra de vehículo de lujo en efectivo

Descripción general

Se recibe alerta por medio de Reporte de Operación en Efectivo (ROE) de una agencia de vehículos, por concepto de compra de vehículo de alta gama, realizado por una persona relativamente joven la cual reporta actividades económicas como: ventas y comercio de productos.

El pago del valor de los vehículos se realiza a través de movimientos por medio de la plataforma SINPE, también trasferencias y pagos en efectivo estructurados. El valor de mercado del vehículo supera los $90.000,00.

Después de realizado el último pago del bien transcurre más de un mes desde la cancelación total del valor del automotor lo que denota desinterés del propietario por retirarlo de la agencia. No se tramitan los procedimientos de registro.

Estas alertas previas permitieron que, entre las autoridades competentes, se gestionara el decomiso inmediato del bien. El bien fue catalogado como bien de interés económico por su valor y debido a sus características y fue entregado en custodia a la oficina administradora de bienes incautados.

Señales de alerta:

- Depósitos estructurados en efectivo en cortos períodos de tiempo, en cuentas bancarias de agencias de vehículos bajo una modalidad para deshacerse rápidamente del dinero.
- Compradores de los vehículos con actividades económicas poco claras.
- Compra de vehículos de alta gama con pagos recurrentes en efectivo.
- Transferencias estructuradas.
- Uso de sociedades mercantiles para la tenencia de bienes de alto valor económico.
- Incertidumbre acerca del origen del efectivo para realizar operaciones de cambio de divisa.

18. Simulación en la compra de bienes de lujo pagando en efectivo

Descripción general

Persona física “A” que se acerca a una agencia de vehículos de lujo para la compra de un auto de alta gama, realizando depósitos en efectivo para su reservación, los pagos del costo del automotor son realizados directamente en la venta de autos en moneda dólares, de manera sistemática, estructurada y por montos cerrados.

La persona “A” es identificada como un asalariado de una entidad del sector público e indica que la compra del vehículo la va a realizar a través de un fondo de una asociación, por lo que solicita que se le haga la devolución del dinero que entregó a la agencia de vehículos a través de una transferencia electrónica, sin que la compra inicial se logre concretar. Esto es una dinámica de devolución de dinero utilizado como ardid para legitimar.

Posteriormente la persona “A” alega desinterés en continuar con el trámite de compra del vehículo aduciendo retrasos en la entrega y facilidades en otros lugares.

Señales de alerta

- Depósitos estructurados y sistemáticos en efectivo en una agencia de vehículos.
- Depósitos en moneda dólares.
- Uso de la tipología de devolución del dinero
- Personas asalariadas del Sector Público.
- Solicitud de devolución del dinero a través de transferencia electrónica.


Ataque Cibernético

19. Ataque cibernético

Descripción general

Se recibieron alertas de cooperación internacional desde Europa y en Asia, informando que la Policía de esos países, ha estado investigando un caso de obstrucción de negocios al dañar una computadora operadora de los servicios y un posible caso de financiamiento del terrorismo.

Lo anterior ya que los sitios web de agencias gubernamentales, compañías ferroviarias y otras compañías claves fueron atacadas cibernéticamente (ataques distribuidos de denegación de servicio (ataque DDoS[1])) por piratas informáticos desconocidos; sin embargo, un grupo de piratas informáticos, se atribuyeron el mérito de los ataques mediante una publicación de un mensaje en Internet.

A través de la investigación, se descubrió que estos grupos solicitan fondos en criptomonedas a través de Internet como parte de un pago extorsivo. Se logró rastrear las cuentas de billetera utilizadas como cuentas receptoras de los fondos y se llegó a las cuentas de un Proveedor de Servicios de Activos Virtuales (PSAV), aparentemente radicado en Costa Rica.

Producto de la investigación realizada en Costa Rica, se determinó que el P.S.A.V que recibió los fondos fue constituido y domiciliado en Costa Rica; sin embargo se identificó que la sociedad se encuentra en un estado disuelta.

No fue posible obtener la información del titular de la cuenta que poseía en el Exchange identificado ni de confiscar la información del titular de la cuenta.

Señales de alerta:

- Transacciones realizadas desde direcciones IP consideradas no confiables.
- Cambios frecuentes en la información del cliente, como correo electrónico y dirección IP.

[1] Un ataque DDoS, o ataque distribuido de denegación de servicio, es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente. Puede generarse con ejemplos como cientos de solicitudes de transporte compartido falsas las cuales hacen que se envíen conductores al lugar de servicio y genera colapsos viales y obstrucciones.

- Presentación de documentación falsa a la hora de crear direcciones para criptomonedas.
- Los recursos cambian y se envían a países considerados de riesgo o de baja regulación a los activos virtuales.
- Movimientos atípicos en flujos de dinero.
- Transacciones internacionales sin justificación.
- Transacciones no acordes al perfil financiero del cliente.
- Uso abusivo de personas jurídicas bajo la modalidad de empresas fachada.

Vendedores de golosinas

20. Vendedor de golosinas o confites

Descripción general

Se recibió información confidencial por parte de una entidad bancaria sobre un sujeto "A" quien es costarricense y declaró que sus ingresos eran producto de su actividad económica como comerciante, sin especificar mayor detalle.

El caso llama la atención dado que el sujeto "A" presentó un desvío transaccional en sus cuentas bancarias relevante al identificarse la remisión de aproximadamente de una cifra superior a los USD $ 300.000 a países vecinos.

En virtud de lo anterior, los funcionarios bancarios realizaron una debida diligencia reforzada con el objetivo de ampliar la información sobre la actividad bancaria declarada por el sujeto "A", quien declaró en ese momento que compraba artículos para fiestas, principalmente golosinas (confites) para vender, sin especificar la vía de ingreso de las mercancías ni suministrar documentación formal de las supuestas compras e importaciones realizadas, lo que sugiere el ingreso de mercancías de contrabando y su distribución a lo interior del país en establecimientos comerciales.

Señales de alerta

- Actividad económica no especificada.
- Altos movimientos de dinero sin justificación.
- Desvío transaccional relevante por medio de transferencias internacionales.
- Ausencia de documentación que respalde el origen del dinero.
- No específica la vía de ingreso de las mercancías.
- No parece contar con documentación formal.
- Se sospecha que sus actividades se relacionen a las actividades informales y posible contrabando de mercancías con movimientos financieros relevantes.

Comercio de contenedores y repuestos

21. Comercio de contenedores y repuestos

Descripción general

Se recibió información de inteligencia y confidencial en la cual se menciona una supuesta actividad de comercio de contenedores y repuestos y por esta razón justifican el envío y recepción de transferencias desde y hacia el exterior sin razón aparente.

Esta persona indica que sus ingresos son producto de la venta de dispositivos para almacenamiento de mercancía que trae del exterior para venderlos en el país y producto de esta actividad económica realiza transferencias internacionales a empresas que en la Web se encuentran identificadas con actividades de manufactura de este tipo de dispositivos; además, recibe gran cantidad de fondos que hacen referencia al pago de estos artículos.

Sin embargo, al revisar el historial de las importaciones no hay registros al menos durante 3 años; lo que hace sospechar sobre la actividad real.

Señales de alerta

- Recepción de transferencias internacionales sin justificación aparente.
- Desvío transaccional relevante por medio de transferencias internacionales.
- Ausencia de documentación que respalde el origen del dinero.
- No específica la vía de ingreso de las mercancías.
- No parece contar con documentación formal.
- Se sospecha de una posible evasión fiscal u otras actividades delictivas.

Remesas remitidas a personas sospechosas

22. Remesas remitidas a personas sospechosas.

Descripción general

Se presenta el giro de recursos entre personas que no tienen relación entre sí y cuyo origen de los fondos es desconocido. Las operaciones se presentan entre personas de catalogadas como de alto riesgo, las cuales frecuentemente se encuentran incluidas en las listas de alerta internacional.

Este tipo de comportamientos son considerados como tipologías utilizadas por organizaciones criminales, relacionadas con redes de tráfico de personas. En este caso, se identifican personas principalmente de origen africano o de oriente medio que ingresan a América a través de Brasil o Venezuela, y son extorsionadas en su intento por llegar desde Sudamérica y continuar hasta los Estados Unidos o Canadá.

Ante esa situación, se detectan envíos de dinero por medio de remesas sobre las cuales se sospecha que podrían estar relacionados con pagos parciales para garantizar la continuidad de la actividad ilegal, para el financiamiento de la red de tráfico o simplemente para ocultar el posible origen ilícito de las sumas recibidas.

Además, con regularidad las personas que aparecen como remitentes o beneficiarios son mencionadas en noticias internacionales con redes de tráfico de migrantes.

Señales de Alerta

- El beneficiario del dinero aparece relacionado con posibles delitos cometidos en el extranjero, presenta antecedentes criminales o su reputación es cuestionada en noticias publicadas por la prensa internacional.

- La nacionalidad de la persona beneficiaria de los recursos no se encuentra entre las nacionalidades que frecuentemente ingresan al país; por el contrario, suele formar parte de zonas geográficas en donde proliferan redes terroristas, de tráfico de personas, de tráfico de armas o de narcotráfico.

- En el país no existen registros formales de actividad económica remunerada de la persona que recibe el dinero.

- Se desconoce el origen de los fondos recibidos por el beneficiario, al no existir parentesco o relación evidente (laboral, profesional o cualquier otra similar) con la persona remitente de los giros.

- El dinero es recibido por personas que no tiene domicilio formal o que registra centros de hospedaje (hotel) como lugar de habitación, pudiendo abandonar rápidamente el lugar o cambiarlo constantemente.

- Se aprovechan las facilidades que brinda el servicio de remesas, el cual suele ser menos exhaustivo al aplicar la debida diligencia del cliente.

Actividad ficticia de cría y venta de ganado

23. Actividad ficticia de cría y venta de ganado

Descripción general

Se recibió información confidencial de un sujeto "C" dedicado a los Servicios Agrícolas, a través de una empresa en la cual figura como representante legal, la actividad económica refiere a la venta de ganado y el ingreso mensual declarado es de varios millones de dólares.

La empresa comercial es de recién constitución y para demostrar el ingreso en sus cuentas bancarias presenta como evidencia un flujo de caja proyectado (supuestos ingresos por recibir por las ventas del ganado)

El sujeto "C" aportó estados financieros en los cual registra aportes de capital por una cifra mayor a los ¢150 millones de colones y ventas a mayo de este mismo año por más de ¢100 millones de su empresa de reciente constitución.

Las declaraciones de renta reflejan haber tenido ingresos por venta de bienes y servicios por la suma de ¢0, lo que resulta incongruente con los movimientos reales de dinero.

En un arqueo posterior se revela que ha movilizado en las cuentas más de $1.5 millones en un año. No se logró ubicar información real con la posible participación de la empresa en subastas ganaderas tampoco se encuentra inscrita como patrono y pese a encontrarse inscrita ante la Administración Tributaria, sus declaraciones de renta parecen no reflejar ingresos por ventas sumado al hecho que la sociedad no aparece inscrita ante la Caja Costarricense del Seguro Social.

Señales de alerta

- Altos movimientos de dinero sin justificación aparente.
- Recepción de transferencias electrónicas y movimientos a través de Sinpe por aparente venta de ganado que no se logró comprobar.
- Ausencia de documentación que respalde el origen del dinero.
- Los flujos financieros se consideran relevantes con una incongruencia sobre su origen y reciente constitución de la empresa.
- No se ubicó en la información tributaria congruente con la posible participación de la empresa en subastas ganaderas.
- No se encuentra inscrita como patrono en la Caja del Seguro Social.

Fraude notarial y registral

24. Fraude notarial y registral

Descripción general

Esta tipología fue detectada a través de los mecanismos de fiscalización que ejecuta la Dirección Nacional de Notariado sobre la labor de supervisión y control de los notarios públicos, así como de la actividad de investigación policial y de las autoridades judiciales.

Se identificaron modalidades delictivas que como eje común, instrumentalizan al servicio notarial por sus efectos legales y registrales, con el fin de obtener beneficios patrimoniales líquidos para el financiamiento de estructuras criminales, así como para legitimar capitales de origen ilícito.

Esquema 1: En cuanto a los modos de operar se ha identificado una primera modalidad, en la que el notario es instrumentalizado en tanto no colabora conscientemente con la actividad criminal. No obstante, las estructuras criminales se aprovechan de las debilidades en la detección de falsificaciones por parte del notario, ya sea sobre documentos de identificación que facilitan la actuación por medio de suplantador, o bien, sobre documentos falsos que supuestamente facultan al frenteador, quien participa con documentos de identidad reales, para emitir actos o contratos a nombre de un tercero sin su conocimiento o consentimiento (titular real de los bienes y víctima del ilícito).

Esquema 2: El otro esquema, involucra una participación directa del profesional, donde el notario es sujeto activo al participar de forma consciente del ilícito, y en este caso emite diversos actos notariales sin cumplir ninguna de las formalidades mínimas (como la emisión de testimonios sin matriz), que posteriormente se presentan ante las autoridades registrales así como las entidades financieras para materializar un enriquecimiento ilícito o bien la legitimación de un capital de origen ilícito.

Las organizaciones reclutan personas usualmente de escasos recursos como suplantadores y como frenteadores, como primera línea utilizada para articular estas actividades criminales, y se consideran miembros descartables en tanto no dejan mayor trazabilidad que permita vincular la estructura de crimen organizado.

Señales de alerta

- Urgencia por concretar la negociación y recibir el dinero en efectivo.
- Estructuración de precios “ganga” sobre bienes cuyo monto resulta muy por debajo del valor de mercado.
- Ofrecimiento de descuentos para convencer al comprador de mantener la transacción.

- Al haber fondos bancarizados, solicitan la emisión de cheques a nombre de una tercera persona.
- Propiedades que se encontraban pasivas registralmente durante un período amplio y posteriormente registran múltiples movimientos de cambio de propietarios recientes.
- Propiedades de personas extranjeras que no habitan o visitan regularmente el país ni vigilan sus bienes.
- Propiedades de personas adultos mayores en zonas rurales o alejadas de alta plusvalía.
- Inexistencia de expediente notarial donde constan publicaciones, ni avisos en diario oficial advirtiendo de una sucesión.
- Presencia de terceros a la hora de firmar la escritura.
- El supuesto dueño de la propiedad no habla español por lo que interviene un tercero en todo momento.
- Uso de poderes especiales para la venta de bienes sin demostrar que cuenta con una escritura pública firmada por el propietario registral legítimo.
- Uso de cuentas relacionadas a terceras personas que no son parte del acto o contrato.
- Uso de pagos en efectivo sin respaldo del origen de fondos.
- Utilización de documentos de identidad falsos o alterados.
- Aprovechamiento de las debilidades de los notarios para la detección de identidades falsas.
- Aprovechamiento de las debilidades de los notarios para la confirmación inmediata de ingresos y salidas del país de extranjeros.

Apartado especial sobre los Activos Virtuales (AVs) Repaso de conceptos

Apartado especial sobre los Activos Virtuales / repaso de conceptos

Extracto sobre los principales conceptos de la Guía del GAFI sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales (diciembre/2021)

Aportes de revisión sobre la implementación práctica de las autoridades: Unidad de Inteligencia Financiera UIF del ICD y La Sección Especializada contra el Cibercrimen del Organismo de Investigación Judicial.

USO DE PROGRAMAS ESPÍA

El uso de programas requiere analizar al investigado sobre el uso de las redes para identificar las vulnerabilidades para infiltrarlas, el "exploit" para tomar el control de sus sistemas; y tercero, monitorear la información capturada de ese blanco de investigación.

RECONOCIMIENTO

Se aplica con la herramienta intrusiva en la aplicación o el sistema operativo utilizando técnicas de OSINT (Inteligencia de fuentes abiertas) para analizar datos, relacionarlos y transformarlos en información útil. Este reconocimiento incluye la identificación de defensas como firewall o antivirus para penetrar el equipo.

INTRUSIÓN

Se realiza la instalación del programa espía en el equipo del investigado lo cual se debe hacer de forma remota el cual puede ser un spyware registrador de tecleado, vigilancia de audio o video. Para esto se pueden utilizar técnicas de engaño para propiciar que abran un archivo o presionar algún ícono para la activación del programa espía.

AVs CENTRALIZADOS

Establecer la diferencia si estamos frente a los AV centralizados o descentralizados.

Funciona con dependencia de una autoridad central que pueda ser alcanzada de una orden judicial o mandato para congelarlos o inmovilizarlos facilitando la incautación o decomiso

AVs DESCENTRALIZADOS

En el caso de las criptomonedas, no existe una autoridad como un Banco Central o instancia similar que pueda aplicar el congelamiento o inmovilización de los fondos acatando la orden judicial.

TRANSACCIONES IRREVERSIBLES

Las transacciones con “monedas” descentralizadas tienen la característica de ser irreversibles en el Blockchain.

CLAVE PRIVADA

Quien tenga la clave privada es quien puede disponer de los fondos asociados a la dirección de AVs. Las claves privadas pueden estar almacenadas en diferentes lugares y formatos, por ende, también pueden ser accedidos por diferentes personas. Esto hace difícil la aplicación de una medida cautelar. Aún en las condiciones que la AOP obtenga la clave privada, otra tercera persona que también la tenga puede hacer una transferencia de estos.

MONEDERO CONTROLADO

Al incautar los AVs no solo se debe secuestrar la computadora o el dispositivo en el que se encuentra alojado el monedero de las criptomonedas la mejor y más segura forma de actuación es cuando se transfieren a un monedero controlado por las AOP de manera inmediata.

PROTOCOLOS INTERNOS

- ❑ Definir los autorizados para llevar a cabo los procesos de incautación y transacciones.
- ❑ Tipos de formatos y notificaciones internas y externas para el tratamiento de los casos.
- ❑ Procedimientos de recolección y preservación de la evidencia electrónica.
- ❑ Protocolos relacionados a la cadena de custodia.

PREPARACIÓN PREVIA

Conocer con qué clase de criptomoneda y monederos operan. El interfaz de los monederos para que las personas puedan recibir y transferir criptomonedas son las aplicaciones que tienen las claves privadas creadas por el propietario usuario.

Determinad si los AVs se encuentran alojados en un monedero en custodia y que los tenga un proveedor de servicios de Avs y si este proveedor se encuentra regulado en materia antilavado para hacer efectiva la orden judicial.

Si no están alojados en monederos en custodia, el proceso de incautación es más complejo ya que los fondos no están en manos de un tercero sino del mismo propietario.

FRASE SEMILLA

Si los AVs no se encuentran alojados en monederos en custodia, la incautación solamente se puede realizar averiguando la clave privada o frase semilla para poder transferirlos a un monedero controlado por el Estado. Las claves pueden estar almacenadas en computadoras, dispositivos portátiles como USB, o incluso impresas en papel. Si se utiliza el monedero, la información de la clave estaría identificada entre 12, 18 o 24 palabras en distintos idiomas que conforman la frase semilla.

INVESTIGACIÓN PATRIMONIAL

TIPOS DE MONEDEROS: Existen diferentes tipos de monederos cuyas claves no están en custodia. Los tipos de monederos pueden ser físicos cuyas claves se almacenan en dispositivos como llaves USB, monederos virtuales o software y móviles. Para los teléfonos inteligentes, existen monederos online para sistemas como IOS o Android y los del tipo multi firma, que requieren de la autorización de por lo menos 2 personas para confirmar una transacción.

FORMATO DE DIRECCIÓN

Se deben identificar los diferentes formatos de direcciones de AVs de cada criptomoneda. Para reconocer el tipo de criptomoneda se debe identificar los rasgos de una dirección de AVs tales como: los números, distribución y caracteres.

Para identificar un formato desconocido, se utilizan herramientas en internet con el fin de saber el tipo de AV.

Ejemplos de criptomonedas y abreviaturas	La Dirección inicia con:
Arbitrum (ARB)	0x
Avalanche (AVAX)	0x
Bitcoin (BTC)	1, 3, bc1 (bech32), bc1p o lnbc
Bitcoin (BTC), (Lightning Network)	lnbc
Bitcoin Cash (BCH)	bitcoincash:q o bitcoincash:p
Bitcoin Cash (BCH)	1 o 3
Cardano (ADA)	4, A o D
Cosmos (ATOM)	cosmos
Dash (DASH)	X
Dogecoin (DOGE)	D
Energy Web Token (EWT)	0x
Ethereum (ETH), (incluye ERC-20)	0x
Ethereum Classic (ETC)	0x

BUENAS PRÁCTICAS

- Anticipación: Utilizar mecanismos y protocolos de patrones de conducta, monitoreo y vigilancia para identificar el momento en el que los dispositivos del investigado se encuentran en uso.
- Considerar que pueden encontrarse cuentas que requieran autenticación de doble factor
- Procurar el acceso de las huellas digitales u otros datos biométricos para acceder a dispositivos. Esto al tenerlo en custodia u obteniendo una autorización.

AUTORIZACIÓN JUDICIAL

Anticipación:

Obtener la autorización judicial al momento del registro, para secuestrar todos los dispositivos de almacenamiento que puedan encontrarse en el domicilio.

[Discos duros, CDR, DVDR, memory sticks, USB]

Estos pueden ser monederos físicos o contener información importante en formato digital, como las “palabras semilla”.

MOMENTO OPORTUNO PARA INCAUTAR AVs

El momento oportuno para hacer efectiva la incautación de criptomonedas es cuando el monedero que tiene las claves privadas se encuentra abierto o se localiza la contraseña o la frase semilla para abrirlo.

También se deben aislar a las personas para impedir que se conecten a Internet o puedan contactarse con el exterior para realizar alguna operación de salida de valor o que la persona destruya u oculte la información de acceso al monedero.

EVIDENCIA RELEVANTE

Durante el registro de un domicilio (habitacional, oficinas, automotores o embarcaciones) los investigadores deben buscar evidencia del tipo de frase semilla para permitir la incautación o decomiso de Avs.

Ejemplo:

1. Computadoras u otros dispositivos con información electrónica (teléfonos móviles, tabletas, medios USB, discos rígidos extraíbles)
2. Monederos de AV, ya sea virtuales o físicos como hardware o de papel.
3. Información que permita acceso a los monederos o la transferencia de Avs: pines, monederos en línea, contraseñas, direcciones de AV,
4. Información de claves privadas o “frases semilla” para concretar la incautación de monedas virtuales.

MONEDERO ALMACENADO EN DISPOSITIVO FÍSICO

Busque notas escritas a mano, cuadernos, apuntes, agendas, notas adhesivas que puedan utilizarse para anotar contraseñas o pines.

MONEDEROS DE PAPEL

Pueden ser documentos en papel u otro material en que pueda imprimirse información. En ellos se indica la dirección AV y las claves pública y privada. Se utiliza también texto plano o plaintext y códigos QR para utilizar con el teléfono inteligente.

TRANSFERENCIA A UN MONEDERO BAJO CONTROL ESTATAL

Se introducen en un monedero hardware como el Ledger- las 12 18 o 24 palabras y al finalizar la última, se obtiene una copia exacta del monedero original.

NÚMERO DE USUARIO DE RETORNO

Número de usuario de retorno: es el número con el que algunos mezcladores de AVs identifican aquellas personas que utilizan sus servicios más de una vez, para evitar que los fondos ilícitos en AVs se paguen dos veces al mismo cliente.

Sirve para identificar al mezclador específico que procesó los AVs del investigado y permite rastrear mediante técnicas de "Chain analysis".

EJECUCIÓN

Obtenga las claves privadas, palabras semilla o monederos de la persona que está siendo investigada.

La medida debe ser aplicada por personal especializado y además debe efectuarse rápidamente para garantizar el éxito de la incautación.

El mejor momento para realizar la incautación de AVs en un monedero suele ser cuando se encuentra desbloqueado y en uso.

De lo contrario probablemente requiera del ingreso de una contraseña, ya que su contenido se va a encontrar protegido mediante encriptación.

MONEDERO BLOQUEADO

Al encontrar un monedero bloqueado y no cuenta con la contraseña de acceso se debe secuestrar el dispositivo ya que se considera que contiene evidencia.

Se aplican los protocolos relacionados a la evidencia digital y actuar de la manera más rápida posible.

En la investigación, deben activarse las medidas urgentes y pertinentes para obtener las contraseñas y aplicar la incautación de los AVs.

BIENES POR UN VALOR EQUIVALENTE

Si no es posible acceder al monedero o se encuentre vacío, el blockchain suple la información sobre el monto de los fondos quedando registradas las transacciones con Avs.

Con la dirección de la persona investigada, se puede consultar el Blockchain para conocer el monto de las transacciones realizadas y con ello se pueden aplicar mecanismos de incautación de bienes de valor equivalente en aquellos países que dispongan de este tipo de regulación.

MÚLTIPLES DIRECCIONES

Se pueden encontrar escenarios en los cuales el monedero de criptomonedas puede alojar múltiples direcciones y también diferentes criptomonedas que pueden ser objeto de incautación.

TRASLADO DE LOS ACTIVOS VIRTUALES

Los archivos digitales que contienen monederos virtuales se deben exportar con ayuda de una herramienta informática.

Se debe hacer una imagen digital del monedero completo y copias o imágenes de las claves privadas o palabras semilla encontradas en papel, documentos y archivos,

Se deben trasladar a la computadora de la agencia de investigación que cuente con sistemas y software para incautar.

Paso final: se transfieren los AVs desde la dirección del investigado a la billetera de la Autoridad Competente la cual debe estar sincronizada con la respectiva Blockchain.

Las direcciones de monederos de custodia Estatal deben estar en formato QR para evitar errores de digitación. En caso contrario se deben realizar 2 o 3 revisiones por protocolo.

Al ser transacciones irrevocables, en caso de que, por error se remitan a una dirección equivocada, no se pueden recuperar.

En la medida de lo posible debe evitarse que el Estado no utilice direcciones controladas, en monederos de papel y que sean multi-firmas.

Una vez concretada la incautación, se realicen verificaciones periódicas de los saldos.

ACCIONES POST-INCAUTACIÓN

Deben observarse todas las consideraciones posteriores por parte de las autoridades competentes especialmente la decisión de su liquidación para convertir a moneda fiduciaria, condiciones de fluctuación de valor.

Decisiones:

- ❑ Retener los Avs hasta que exista una resolución final de decomiso.
- ❑ Convertir en moneda fiduciaria (posibilidad de pérdida de valor).
- ❑ Convenir con el titular lo que se vaya a disponer para librar responsabilidades.

LA VENTA

1. De forma directa.
2. A través de subasta pública.
3. Convenio o contrato con un operador privado especializado en el intercambio.

EXPERIENCIA EN COSTA RICA

La Sección Especializada Contra el Cibercrimen, del Organismo de Investigación Judicial, ha venido trabajando casos relacionados con criptomonedas desde el año 2015. Durante estos 8 años las investigaciones de este tipo han abarcado delitos tales como secuestros extorsivos, homicidios, legitimación de capitales, estafas y otros.

El aumento en este tipo de denuncias ha sido constante, el cual para el 2023 se refleja en un aumento del 500% en casos nuevos. Esta situación también ha permitido ir especializando agentes, gracias al apoyo internacional, donde se cuenta con Especialistas y Fiscales capacitados y certificados.

Dicha experiencia ha permito al país individualizar y capturar grupos criminales, aunado a realizar la incautación de criptoactivos, los cuales se custodian en billeteras del Estado. Adicionalmente se ha colaborado con Policías extranjeras, donde también recientemente se realizó una incautación.

RETOS PARA EL PAÍS

- ❑ Avanzar en las discusiones de los proyectos de ley actuales relacionados al tema de los AVs.
- ❑ Establecer una regulación adecuada para los criptoactivos.
- ❑ Considerar la prevención del lavado de dinero y el financiamiento al terrorismo.
- ❑ Capacitación y especialización de más personas que intervengan en el proceso de investigación y la prevención.
- ❑ Invertir en herramientas y equipo especializado para poder desarrollar las labores técnicas adecuadamente.
- ❑ Sensibilizar a la población en general para conocer e informarse del tema.

OTROS DESAFÍOS IDENTIFICADOS

1. Las Autoridades del Orden Público (AOP) deben contar con las herramientas informáticas necesarias.
2. Repensar sus estructuras organizativas y operacionales, volteando a la especialización en el uso de tecnologías.
3. El uso de spyware para los fines investigativos y falta de regulación sobre su uso.
4. Diseñar programas informáticos y contratar desarrollo especializado.
5. Trabas y requisitos en regulaciones así como las garantías que no aplican al crimen organizado.
6. Cuando las AOP se limitan para actuar bajo criterios de selección y deben limitarse a blancos investigativos específicos.
7. Fuga de recurso humano y que sea reclutado por inescrupulosos y delincuentes.
8. Generar nuevas técnicas y mecanismos de cadena de custodia.
9. Apelación sobre la afectación de derechos individuales o relacionados a la privacidad e intimidad de las personas.
10. El conocimiento por parte de los abogados defensores sobre las medidas de investigación aplicadas.
11. Posibles cuestionamientos relacionados con la certificación de los programas utilizados.
12. Definición de procedimientos relacionados a la desinstalación de los programas.
13. Políticas o protocolos que regulen la incautación.
14. Tratamiento a los AVs Incautados.
15. Toma de decisiones relativas a la post-incautación y posibilidades de venta de los AVs.

Agradecimiento especial

Oficialía de Cumplimiento del Banco BAC.	Por su aporte de tipologías identificadas en los procesos monitoreo y prevención.
Oficialía de Cumplimiento del Banco de Costa Rica.	Por su aporte de tipologías identificadas en los procesos monitoreo y prevención.
Sección Especializada contra el Ciber Crimen del Organismo de Investigación Judicial.	Por su aporte en casos de investigaciones realizadas con relación a los Activos Virtuales.
Fiscalía Adjunta Especializada en Delincuencia Organizada, Ministerio Público.	Por su aporte en casos de investigaciones realizadas con relación a los Activos Virtuales.
Dirección Nacional de Notariado del Ministerio de justicia.	Por su aporte en casos de alerta e investigaciones relacionadas con fraudes registrales y otros delitos.
Marianela Herrera Mora, Johanna Chinchilla Aguzzi, Franklin Morales Hidalgo, Olger Bogantes Calvo, Alonso Arce Zárate, Ricardo Meza Cambronero, Alex Cascante Arce, Jorge Madrigal Guillén.	Por su aporte en análisis y procesamiento de información así como la elaboración de tipologías.

Elaborado por:
Unidad de Inteligencia Financiera

Coordinación, dirección y edición
Unidad de Inteligencia Financiera

ICD

Instituto Costarricense sobre Drogas

Unidad de Inteligencia Financiera

GOBIERNO

DE COSTA RICA