EVALUACIÓN SECTORIAL DE RIESGOS DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO DE LOS ACTIVOS VIRTUALES Y LOS PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES DE LOS PAÍSES DEL GAFILAT

Julio/2025

El presente documento fue elaborado por el Grupo de Acción Financiera de Latinoamérica (GAFILAT), en el marco del "Programa para el Fortalecimiento de los Sistemas ALA/CFT de los países del GAFILAT para la Quinta Ronda de las Evaluaciones Mutuas" financiado mediante cooperación técnica otorgada por el Banco Centroamericano de Integración Económica (BCIE).

CONTENIDO

LISTA DE SIGLAS Y ABREVIATURAS 4

I. RESUMEN EJECUTIVO 5

a. Metodología 5

b. Contexto y panorama regional 6

c. Las principales amenazas 7

d. Las principales vulnerabilidades 8

e. Los principales riesgos 9

f. Recomendaciones para la mitigación los riesgos 9

II. INTRODUCCIÓN 11

III. METODOLOGÍA 13

a. Objetivos de la ESR 13

b. Alcance 13

c. Métodos y técnicas de investigación 13

d. Fuentes e información utilizada 14

e. Etapas de implementación 19

f. Metodología para la evaluación de los riesgos 19

IV. CONTEXTO Y PANORAMA REGIONAL 22

a. Implementación normativa 23

b. Proveedores de Servicios de Activos Virtuales en la región del GAFILAT 24

c. Relación entre el sector financiero tradicional y los PSAV 30

V. PRINCIPALES AMENAZAS 32

a. Uso ilícito de activos virtuales a nivel regional 33

b. Principales amenazas de los AV y PSAV 37

c. Análisis de las amenazas de los AV y PSAV 38

VI. PRINCIPALES VULNERABILIDADES 41

a. Desconocimiento y falta de capacitación 41

b. Marco jurídico insuficiente 43

c. Capacidades técnicas en relación con los activos virtuales 50

d. Infraestructura tecnológica y herramientas insuficientes 52

e. Licenciamiento o registro y supervisión efectiva a los PSAV 54

f. Características intrínsecas de los AV 58

g. Análisis de las vulnerabilidades 59

VII. PRINCIPALES RIESGOS 65

VIII. RECOMENDACIONES PARA MITIGAR LOS RIESGOS IDENTIFICADOS 68

a. Construcción de un conocimiento más sólido y contextualizado 68

b. Acercamiento de los reguladores, supervisores y/o autoridades competentes al sector de PSAV 69

c. Evaluación sectorial de riesgos 70

d. Integración de los hallazgos de la evaluación sectorial de riesgos al marco jurídico 70

e. Establecimiento del control prudencial 71

f. Promover la relación entre el sector financiero tradicional y los PSAV 72

g. Actualización y mejora continua de los mitigadores de riesgo del sector 72

IX. CONCLUSIONES 73

FUENTES Y REFERENCIAS 78

Anexo 1: Patrones de actividades inusuales o sospechosas identificadas por los sujetos financieros tradicionales 82

Anexo 2: Señales de alerta identificados por las UIF 84

Anexo 3: Medidas de ciberseguridad implementadas por los países 88

Anexo 4. Medidas de mitigación implementadas por los PSAV e instituciones financieras 89

a. Medidas de mitigación implementadas por los PSAV 89

b. Medidas de mitigación implementadas por las instituciones financieras 90

Anexo 5. Entornos regulatorios experimentales: Colombia y Honduras 92

LISTA DE SIGLAS Y ABREVIATURAS

ALA	Antilavado de activos
AOP	Autoridades de orden público
APNFD	Actividades y profesiones no financieras designadas
AV	Activos virtuales
CFT	Contra el financiamiento del terrorismo
DAPPS	Aplicaciones descentralizadas por sus siglas en inglés
DDC	Debida diligencia del cliente
DDI	Debida diligencia intensificada
DeFi	Finanzas Descentralizadas
DEX	Intercambio descentralizado por sus siglas en inglés
DLT	Tecnología de registro distribuido por sus siglas en inglés
EBR	Enfoque basado en riesgos
ENR	Evaluación nacional de riesgos
ESR	Evaluación sectorial de riesgos
FT	Financiamiento del terrorismo
GAFI	Grupo de Acción Financiera
GAFILAT	Grupo de Acción Financiera de Latinoamérica
KYC	Política de conocimiento del cliente por las siglas en inglés "*Know Your Customer*"
LA	Lavado de activos
NFT	Tokens no fungibles por sus siglas en inglés
PSAV	Proveedores de servicios de activos virtuales
ROS	Reporte de operaciones sospechosas
SFC	Superintendencia Financiera de Colombia
UIF	Unidad(es) de inteligencia financiera

I. RESUMEN EJECUTIVO

1. En el marco del «Programa para el fortalecimiento de los sistemas ALA/CFT de los países del GAFILAT para la quinta ronda de Evaluaciones Mutuas» suscrito entre el GAFILAT y el BCIE, se resolvió desarrollar una Evaluación Sectorial de Riesgos asociados al LA/FT provenientes de las actividades con Activos Virtuales (en adelante AV) y de los Proveedores de Servicios de Activos Virtuales (en adelante PSAV) de alcance regional (en adelante, la ESR). Este proyecto surge en respuesta a la necesidad de adaptarse a los avances tecnológicos y comprender los riesgos específicos relacionados con los AV y los PSAV, sobre todo en vista de la quinta ronda de evaluaciones mutuas.

2. Este informe analiza la creciente adopción de AV y la operación de los PSAV en la región del GAFILAT, destaca los desafíos regulatorios, las principales amenazas y vulnerabilidades identificadas, y las estrategias propuestas para mitigar los riesgos asociados. Con base en las encuestas, análisis de evaluaciones de riesgos y experiencias regionales, el documento ofrece una visión integral de la dinámica y complejidad del ecosistema de activos virtuales en América Latina.

3. Esta ESR busca evaluar los riesgos regionales asociados al LA/FT provenientes de las actividades con AV y de los PSAV. Para ello, se buscó:

A. Analizar las, amenazas y vulnerabilidades en materia de LA/FT relacionados a los AV y PSAV; y,
B. Evaluar los riesgos de LA/FT a los que se encuentran expuestos los AV y PSAV a nivel regional.

4. La ESR incluyó información de los 18 países miembros del GAFILAT. El análisis y las recomendaciones específicas de la situación de cada país, se ejecutó con base en la información que se tuvo a disposición. Este enfoque permitió una comprensión integral de la región y, al mismo tiempo, brindó una apreciación detallada de las dinámicas nacionales.

a. Metodología

5. La metodología utilizada realizó un abordaje mixto que combinó elementos cualitativos y cuantitativos con un enfoque exploratorio holístico que permitió utilizar la información existente de cada país. La recopilación de datos se realizó mediante una variedad de técnicas, incluyendo mesas redondas para obtener un amplio espectro de opiniones, análisis detallado de documentos, estudios de caso, y encuestas para recoger datos cuantitativos.

6. En particular, la metodología utilizada para evaluar los riesgos del sector AV y PSAV se basó en la Guía para una Evaluación Nacional de Riesgos de Lavado de Dinero[1] del GAFI (actualizada en

[1] GAFI. Guía para la Evaluación Nacional del Riesgo del Lavado de Activos (2024). https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Spanish-Money-Laundering-National-Risk-Assessment-Guidance.pdf.coredownload.inline.pdf

2024) y en la Guía para el Análisis de Riesgos de FT (2019)[2],las cuales contemplan como principales variables la amenaza y la vulnerabilidad.

7. Respecto a la información documental consultada para elaborar esta ESR, en primer lugar, se revisaron diversos documentos publicados por el GAFILAT.[3] Igualmente, se solicitaron insumos a las autoridades relevantes y al sector privado. Se incluyeron aportes de las autoridades de orden público, reguladores y supervisores financieros, UIF y las autoridades de regulación tecnológica. En cuanto al sector privado, se contó con la participación del sector financiero tradicional, y de los propios PSAV, así como de algunas empresas de análisis de blockchain. La inclusión y análisis de información tanto de las autoridades regulatorias como del sector privado fue clave para evaluar efectivamente los riesgos asociados al LA/FT en el sector de los AV.

8. Se circularon encuestas a los 18 países miembros del GAFILAT, dirigidas a distintas agencias, entre ellas, las autoridades de orden público (AOP), UIF, supervisores financieros, reguladores tecnológicos, reguladores y supervisores del sector FINTECH y; además, también se consultó a los PSAV y el sector financiero en la mayoría de los países. Se realizaron dos mesas regionales de trabajo que sirvieron para identificar información, validar hallazgos y priorizar riesgos.

b. Contexto y panorama regional

9. La adopción de criptomonedas en América Latina muestra una diversidad de casos de uso que varían según las condiciones económicas de cada país. Mientras que, en algunos países, las criptomonedas se utilizan como una herramienta para mitigar la inflación y facilitar las remesas, en otros mercados, han evolucionado hacia un vehículo de inversión especulativa. Estas tendencias indican que, impulsada por factores económicos locales y una creciente confianza en el mercado, la adopción de criptomonedas en Latinoamérica continúa en ascenso. A medida que las tecnologías cripto sigan desarrollándose y las economías latinoamericanas enfrenten nuevos desafíos, es probable que se generen nuevos casos de uso adaptados a las necesidades específicas de la región. Las perspectivas futuras para la industria de activos virtuales en América Latina muestran una tendencia de crecimiento, lo que anticipa una mayor integración de los activos virtuales (criptomonedas en particular) en el sistema financiero tradicional y un incremento en la adopción y diversificación de inversiones en la región.

---

[2] GAFI 2019. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf.coredownload.pdf

[3] Informes de Evaluaciones Mutuas de la 4° Ronda del GAFILAT; Informes de avances y recalificación del cumplimiento técnico de los países del GAFILAT; Informes y actualizaciones de Amenazas Regionales del GAFILAT; Informes de Tipologías del GAFILAT; Guía sobre ESR del GAFILAT, septiembre 2020; Análisis sobre el impacto de la implementación de la R15 - Nuevas Tecnologías, GAFILAT 2020; Informe del GAFI sobre Activos Virtuales -Señales de Alerta, GAFI 2020; Guía actualizada para un EBR de AV y PSAV, GAFI 2021; Guía sobre Aspectos Relevantes y pasos apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales, GAFILAT 2021; Actualización Específica sobre la Implementación de los Estándares del GAFI sobre Activos Virtuales y Proveedores de Servicios de Activos Virtuales, GAFI 2022; Guía para la Regulación ALA/CFT de AV/PSAV en la Región del GAFILAT, agosto 2023.

10. Debido al incremento del uso de los AV y sus riesgos para los flujos financieros ilícitos a nivel global, el GAFI, mediante la Recomendación 15, requiere una serie de obligaciones para los países y los PSAV buscando evitar el uso indebido de los AV. Dentro de estas medidas se pueden mencionar algunas como el entendimiento de los riesgos de LA/FT, el otorgamiento de licencias, la supervisión enfocada en el riesgo de los PSAV, así como la implementación de las medidas preventivas ALA/CFT por parte de los PSAV.

11. En este sentido, los países del GAFILAT están implementando esta recomendación y particularmente, en relación con el otorgamiento de licencias o registros a los PSAV, algunos países como Colombia, El Salvador, México y Nicaragua han informado sobre las medidas que están implementando. Cuba ha establecido el marco jurídico, sin embargo, no ha informado sobre la emisión de licencias o registros al momento de realización de la encuesta. La disponibilidad de información sobre el número de PSAV operando en la región es limitada. Seis países, Argentina, Chile, Colombia, El Salvador, Paraguay y Perú aportaron información. Sin embargo, aún es necesario contar con información precisa y actualizada sobre los PSAV que efectivamente operan regionalmente.

c. Las principales amenazas

12. Para identificar las amenazas relacionadas con los activos virtuales y PSAV, se consultó a los PSAV, las UIF, AOP, autoridades reguladoras de PSAV y financieras, así como a los sujetos obligados tradicionales. Al inventariar las respuestas fue posible agruparlas en:

A. Amenazas relacionadas con la explotación de las características inherentes de los activos virtuales para la comisión de diferentes tipos de delitos.

- Ciberataques y disrupciones para retener fondos y exigir pagos en AV para liberar datos o restaurar sistemas.[4]
- Uso ilícito de *mixers (o tumblers)* y comercio ilícito a través de la *Dark Web*.
- Fraude y estafas de inversión.

B. Amenazas en que los activos virtuales se utilizan para facilitar el lavado de recursos y activos de otros delitos:

- Tráfico de estupefacientes y psicotrópicos: Uso de AV para financiar o legitimar recursos provenientes del narcotráfico.
- Trata de personas.
- Defraudación tributaria: Contribuyentes aceptan pagos en AV para evadir impuestos, dificultando la identificación del origen territorial de la renta.
- Corrupción: Fondos estatales vinculados al enriquecimiento ilícito podrían ser convertidos a AV.

[4] Por ejemplo, los ataques de fuerza bruta, malware, suplantación de identidad y phishing, extorsión y secuestro de información datos o equipos (ransomware).

- Financiamiento del terrorismo.

13. Es de notar que el financiamiento al terrorismo no se identifica como una de las principales amenazas de la región. Sin embargo, con el fin de analizar el nivel de riesgo para financiamiento al terrorismo, es importante considerar este aspecto desde el análisis de las amenazas.

d. Las principales vulnerabilidades

14. Las principales vulnerabilidades fueron señaladas por los encuestados y en las mesas de trabajo con el sector público y privado, para lo cual se analizaron las respuestas recibidas agrupándolas por tema. Estas vulnerabilidades se agruparon en las siguientes categorías:

A. **Desconocimiento y falta de capacitación.** Esta vulnerabilidad comprende:
   - Falta de comprensión del sector por parte de:
     - Autoridades gubernamentales.
     - Sector financiero tradicional.
     - Proveedores de Servicios de Activos Virtuales (PSAV).
     - Población en general.
   - Los PSAV carecen de conciencia sobre la importancia del cumplimiento regulatorio.

B. **Marco jurídico insuficiente.** Esta vulnerabilidad comprende:
   - Falta de regulación integral en materia de ALA/CFT y operación de PSAV.
   - Disparidad normativa y ausencia de unificación de criterios a nivel regional.
   - Carencia de facultades de las autoridades de orden público.
   - Falta de licenciamiento, registro y supervisión de PSAV.
   - Marco sancionatorio insuficiente o inadecuado.
   - Necesidad de normativa prudencial para PSAV.

C. **Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV.** Esta vulnerabilidad comprende:
   - Limitaciones en la comprensión del sector y aplicación de la ley a delitos relacionados con AV.
   - Falta de trabajo articulado entre las fuerzas del orden.
   - Carencia de personal especializado en la materia (policías, jueces, fiscales) y recursos adecuados.

D. **Infraestructura tecnológica y herramientas insuficientes.** Esta vulnerabilidad comprende:
   - Recursos limitados para adquirir herramientas tecnológicas avanzadas.
   - Infraestructura inadecuada para supervisión e investigación.
   - Necesidad de herramientas de análisis de blockchain y otras tecnologías relevantes.

E. **Falta de supervisión a PSAV.** Esta vulnerabilidad comprende:
   - Los PSAV operan sin supervisión efectiva en materia de ALA/CFT.

- Los supervisores carecen de comprensión y experiencia para supervisar el sector de manera efectiva.
- Ausencia de reportes por parte de los sujetos obligados.

F. Características intrínsecas de los AV. Esta vulnerabilidad comprende:

- Anonimato y pseudonimato.
- Intercambio Peer-to-Peer (P2P).
- Alcance global y velocidad de las transacciones.
- Ecosistemas descentralizados (smart contracts y DApps).
- Menor costo de las operaciones.

15. De conformidad a la metodología utilizada, los cálculos del impacto de las distintas vulnerabilidades cuando se materializan las amenazas indican que, cuando la actividad criminal se aprovecha de las características inherentes de los AV para la comisión de diferentes tipos de delitos, como el fraude y estafas, los ataques cibernéticos y el uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web, se presenta una mayor magnitud de vulnerabilidad.

e. Los principales riesgos

16. Se muestra un nivel de riesgo muy alto utilizando AV y PSAV para el LA del producto que deriva de los delitos de fraude y estafas, los ataques cibernéticos, y el tráfico de drogas. El lavado de activos producto de la trata de personas tiene un nivel alto de riesgo. Por su parte, el uso de los AV para LA mediante esquemas de defraudación tributaria, la corrupción y el uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web, tiene un nivel de riesgo medio.

17. Finalmente, el FT refleja un riesgo medio para la región. Es de notar que, aunque en general la amenaza es baja, el nivel considerable de vulnerabilidad, que en el momento de la elaboración de este estudio presenta el sector de los AV y PSAV, permite concluir que el riesgo de FT para este sector es medio.

f. Recomendaciones para la mitigación los riesgos

- Construcción de un conocimiento más sólido y contextualizado del sector.
- Acercamiento de los reguladores, supervisores y/o autoridades competentes al sector de PSAV.
- Evaluación sectorial de riesgos.
- Integración de los hallazgos de la evaluación sectorial de riesgos al marco jurídico.
- Establecimiento del control prudencial.
- Promover la relación entre el sector financiero tradicional y los PSAV.
- Actualización y mejora continua de los mitigadores de riesgo del sector.
- Fortalecer las medidas de mitigación implementadas por los PSAV.
- Fortalecer las medidas de mitigación implementadas por las instituciones financieras.

18. Se concluye motivando a que los países del GAFILAT implementen estrategias de mejora continua en supervisión, capacitación e innovación tecnológica, asegurando que las autoridades estén preparadas para enfrentar los desafíos presentes y futuros del ecosistema de activos virtuales en la región.

II. INTRODUCCIÓN

1. El Grupo de Acción Financiera de Latinoamérica (GAFILAT) es una organización intergubernamental que incluye a 18 países miembros en América[5] y se dedica a combatir el lavado de activos (LA), el financiamiento del terrorismo (FT) y la proliferación de armas de destrucción masiva (FP). En el marco de su trabajo colaborativo con organismos observadores, entre otros, el GAFILAT desarrolla y ofrece a sus miembros productos y acciones de asistencia técnica que promueven y posibilitan la implementación efectiva de las Recomendaciones del GAFI.

2. En la actualidad, debido al crecimiento acelerado e impacto de los desarrollos tecnológicos, los países enfrentan desafíos regulatorios y de supervisión para prevenir y combatir el LA/FT asociados a los activos virtuales (AV) y proveedores de servicios de activos virtuales (PSAV).

3. En ese sentido, dentro del «Programa para el fortalecimiento de los sistemas ALA/CFT de los países del GAFILAT para la quinta ronda de Evaluaciones Mutuas» (en adelante el Programa), suscrito en el marco de cooperación entre el GAFILAT y el Banco Centroamericano de Integración Económica (BCIE), se ha resuelto desarrollar una Evaluación Sectorial de Riesgos asociados al LA/FT proveniente de las actividades con Activos Virtuales y de los Proveedores de Servicios de Activos Virtuales de alcance regional (en adelante, la ESR). Este proyecto surge en respuesta a la necesidad de adaptarse a los avances tecnológicos y comprender los riesgos específicos relacionados con los AV y los PSAV, sobre todo en vista de la quinta ronda de evaluaciones mutuas.

4. El objetivo principal consiste en la realización de la ESR asociados al LA/FT proveniente de las actividades con AV y de los PSAV de alcance regional, a fin de que los países miembros del GAFILAT cuenten con una herramienta para identificar los riesgos de abuso de los AV y PSAV en la región.

5. Este informe analiza la creciente adopción de AV y la operación de los PSAV en la región del GAFILAT, destacando los desafíos regulatorios, las principales amenazas y vulnerabilidades identificadas, y las estrategias propuestas para mitigar los riesgos asociados. Con base en las encuestas, análisis de evaluaciones de riesgos y experiencias regionales, el documento ofrece una visión integral de la dinámica y complejidad del ecosistema de AV en América Latina.

6. Este documento se extiende a los 18 países miembros del GAFILAT, considerando las especificidades y contextos de cada uno. Originalmente, se proponía que el estudio abarcara desde 2018 (año en que se introdujo la definición de AV y PSAV en los estándares del GAFI (FATF, 2012-2023). Sin embargo, no en todos los casos hubo información disponible.

7. Este documento describe la metodología utilizada donde se realizó un abordaje mixto que combinó elementos cualitativos y cuantitativos con un enfoque exploratorio, a fin de establecer

[5] Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana y Uruguay.

una base sólida para ejercicios futuros en la materia. La recopilación de datos se realizó mediante una variedad de técnicas, incluyendo mesas redondas para obtener un amplio espectro de opiniones, análisis detallado de documentos, estudios de caso, y encuestas para recoger datos cuantitativos.

8. En particular, la metodología utilizada para evaluar los riesgos del sector AV y PSAV se basó en la Guía para una Evaluación Nacional de Riesgos de Lavado de Dinero[6] del GAFI (actualizada en 2024) y la Guía para el Análisis de Riesgos de FT (2019)[7], las cuales contemplan como principales variables la amenaza y la vulnerabilidad a través de la medición del impacto y probabilidad de ocurrencia.

9. Este documento hace una contextualización del mercado de criptomonedas de la región donde se resalta que, en algunos países, las criptomonedas se utilizan como una herramienta para mitigar la inflación y facilitar las remesas. En otros mercados, han evolucionado hacia un vehículo de inversión especulativa. Es de notar que a medida que las tecnologías cripto sigan desarrollándose y las economías latinoamericanas enfrenten nuevos desafíos, es probable que se generen nuevos casos de uso adaptados a las necesidades específicas de la región. Por ello, las perspectivas futuras para la industria de AV en América Latina muestran una tendencia de crecimiento, lo que anticipa una mayor integración de los activos virtuales (criptomonedas en particular) en el sistema financiero tradicional y un incremento en la adopción y diversificación de inversiones en la región.

10. Luego, el documento expone el proceso para la identificación y análisis de las principales amenazas regionales que afectan a los AV y a los PSAV, así como una priorización y definición de la magnitud de las vulnerabilidades. Con ello se concluye el nivel de riesgo que enfrenta la región en materia de LA y de FT.

11. A manera de recomendaciones, el documento presenta medidas que se están implementando por algunos sectores o autoridades, como buenas prácticas. Así también, se incorporan sugerencias que las autoridades de cada país pueden adoptar para mitigar los riesgos que los AV y PSAV pueden presentar en cada uno de los países.

12. Finalmente, se resalta que los AV y PSAV son una realidad en la región. Su actividad no debe considerarse como negativa, por el contrario, con una buena regulación y supervisión, el sector de las criptomonedas puede apoyar el desarrollo económico de los países y contribuir con el crecimiento de otros mercados menos tradicionales que utilizan la tecnología en su favor.

[6] GAFI. Guía para la Evaluación Nacional del Riesgo del Lavado de Activos (2024). https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Spanish-Money-Laundering-National-Risk-Assessment-Guidance.pdf.coredownload.inline.pdf

[7] GAFI 2019. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf.coredownload.pdf

III. METODOLOGÍA

13. A continuación, se detalla la metodología utilizada en la ESR. Se explica también el alcance geográfico y temporal del análisis, y las particularidades regionales que influyeron en los resultados del análisis. Se detalla la información recolectada para completar el estudio. Adicionalmente, se identifican y describen las limitaciones y desafíos que surgieron durante la ejecución de la ESR, así como las estrategias para abordarlos.

a. Objetivos de la ESR

14. Con la realización de la ESR asociados al LA/FT proveniente de las actividades con AV y de los PSAV de alcance regional, se busca como objetivo principal que los países miembros del GAFILAT cuenten con una herramienta para identificar los riesgos de abuso de los AV y PSAV en la región.

15. Como objetivos específicos, se presentan los siguientes:

a) Analizar las amenazas y vulnerabilidades en materia de LA/FT relacionados a los AV y PSAV.

b) Evaluar los riesgos de LA/FT a los que se encuentran expuestos los AV y PSAV a nivel regional.

b. Alcance

16. El análisis abarca a los 18 países miembros del GAFILAT, considerando las especificidades y contextos de cada uno. Inicialmente, se propuso que el estudio abarcara desde 2018 (año en que se introdujo la definición de AV y PSAV en los estándares del GAFI (FATF, 2012-2023). Sin embargo, en algunos casos, la información disponible fue limitada.

17. La ESR incluyó información de los 18 países miembros de GAFILAT, siempre que la información estuvo disponible se adaptó el análisis y las recomendaciones a la situación específica de cada país. Este enfoque permitió una comprensión integral de la región y, al mismo tiempo, brindó una apreciación detallada de las dinámicas nacionales.

c. Métodos y técnicas de investigación

18. La propuesta metodológica se basó en un abordaje mixto que combinó elementos cualitativos y cuantitativos con un enfoque exploratorio, a fin de establecer una base sólida para ejercicios futuros en la materia. La recopilación de datos se realizó mediante una variedad de técnicas, incluyendo mesas redondas para obtener un amplio espectro de opiniones, análisis detallado de documentos, estudios de caso, y encuestas para recoger datos cuantitativos.

19. Las encuestas fueron circuladas entre los 18 países miembros del GAFILAT y estuvieron dirigidas a distintas agencias, entre ellas, las AOP, UIF, supervisores financieros, reguladores tecnológicos, reguladores y supervisores del sector FINTECH y; además, también se consultó a los PSAV y al sector financiero en la mayoría de los países.

d. Fuentes e información utilizada

20. En esta sección se identifican y detallan los elementos para llevar a cabo esta evaluación sectorial. Un aspecto fundamental fue contar con datos precisos, actualizados y relevantes para desarrollar las conclusiones y recomendaciones. Por lo tanto, durante todo el proceso se hizo énfasis en la adquisición y el acceso a conjuntos de datos exhaustivos, que abarcaran información detallada sobre AV y PSAV en cada país miembro del GAFILAT. Esto incluyó, pero no se limitó a, datos regulatorios, transaccionales, de mercado, así como informes y estudios relevantes.

21. Respecto a la información documental utilizada para elaborar esta ESR, en primer lugar, se consultaron diversos documentos publicados por el GAFILAT.[8] Se solicitaron insumos a las autoridades relevantes y al sector privado. Se incluyó a las autoridades de orden público, reguladores y supervisores financieros, UIF y las autoridades de regulación tecnológica. En cuanto al sector privado, se contó con la participación del sector financiero tradicional, y de los propios PSAV, así como de las empresas de análisis de blockchain. La recopilación y análisis de información tanto de las autoridades regulatorias como del sector privado fueron claves para evaluar efectivamente los riesgos asociados al LA/FT en el sector de los AV.

Encuestas

22. La mayor cantidad de la información se solicitó mediante una encuesta, para lo cual se diseñó un formulario electrónico a fin de facilitar la recolección de datos. En respuesta a las encuestas, los países proporcionaron información de distintas agencias, entre ellas, las AOP, UIF, supervisores financieros e integrantes del sector financiero de los países, que registraron alta participación mientras que se registró un menor número de respuestas de reguladores tecnológicos, reguladores y supervisores del sector FINTECH. Igualmente, se recibieron respuestas de los PSAV y el sector financiero tradicional de la mayoría de los países.

- Sector público

23. Debido a la necesidad de contar con insumos de las diversas agencias involucradas en los sistemas ALA/CFT, se incluyó a los supervisores financieros, UIF, AOP, y reguladores tecnológicos.

[8] Informes de Evaluaciones Mutuas de la 4° Ronda del GAFILAT; Informes de avances y recalificación del cumplimiento técnico de los países del GAFILAT; Informes y actualizaciones de Amenazas Regionales del GAFILAT; Informes de Tipologías del GAFILAT; Guía sobre ESR del GAFILAT, septiembre 2020; Análisis sobre el impacto de la implementación de la R15 - Nuevas Tecnologías, GAFILAT 2020; Informe del GAFI sobre Activos Virtuales -Señales de Alerta, GAFI 2020; Guía actualizada para un EBR de AV y PSAV, GAFI 2021; Guía sobre Aspectos Relevantes y pasos apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales, GAFILAT 2021; Actualización Específica sobre la Implementación de los Estándares del GAFI sobre Activos Virtuales y Proveedores de Servicios de Activos Virtuales, GAFI 2022; Guía para la Regulación ALA/CFT de AV/PSAV en la Región del GAFILAT, agosto 2023.

Es importante considerar que, en múltiples casos, más de una agencia de la misma naturaleza aportó insumos. Por ejemplo, en el caso de los supervisores financieros, o las autoridades de orden público, múltiples instituciones o unidades tienen mandatos especializados. En contraste, en los casos de las unidades de inteligencia financiera o los reguladores tecnológicos sólo hay una agencia del tipo por país. Por tanto, participaron las siguientes autoridades:

- Supervisores financieros: 20 supervisores del sector financiero tradicional participaron en la encuesta. (Ver gráfico 1)
- Autoridades de orden público: La encuesta fue respondida por 62 autoridades de orden público de los países miembros del GAFILAT. (Ver gráfico 2)

Gráfico 1 Participación de supervisores financieros que respondieron a la encuesta por país

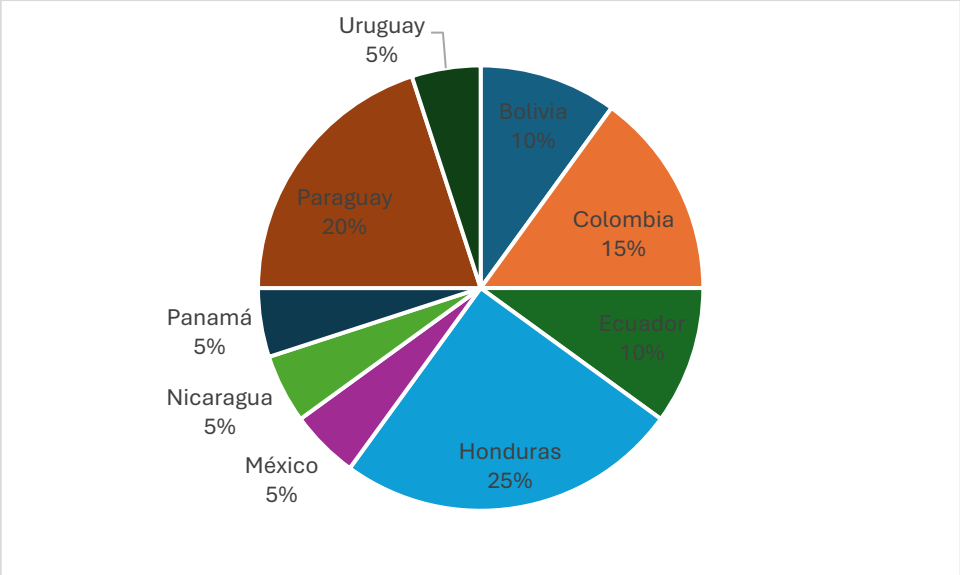
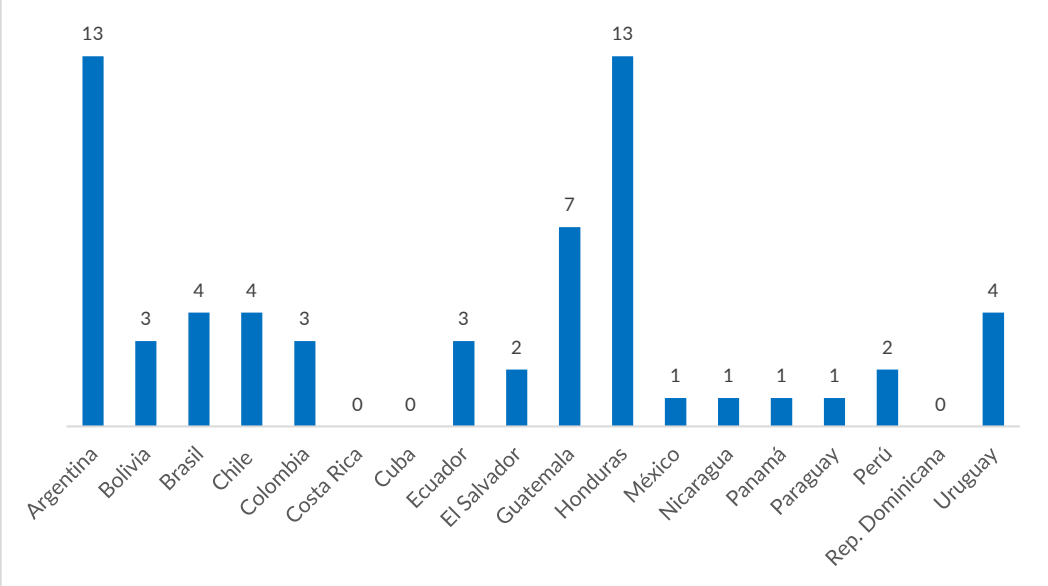


Gráfico 2 Número de autoridades de orden público que respondieron a la encuesta



- Sector privado

24. Integrar información del sector privado es fundamental en un ejercicio de esta naturaleza. Por un lado, la información proporcionada por los PSAV permite comprender qué y cómo están prestando servicios en la región, conocer su forma de operación y las acciones de entendimiento y mitigación de riesgos, así como su actitud ante la regulación. Por otro lado, contar con insumos del sector financiero tradicional facilita identificar las interacciones que tienen con el sector de PSAV, sus actitudes ante este nuevo sector, así como las medidas que han tomado para comprender y mitigar riesgos específicos. Por tanto, participaron las siguientes entidades:

- Proveedores de servicios de activos virtuales: Se recibieron 63 respuestas de 10 países miembros de GAFILAT. (Ver gráfico 3).
- Sector financiero tradicional: 225 entidades financieras respondieron a la encuesta. (Ver gráfico 4).

Gráfico 3 Participación de PSAV que respondieron a la encuesta por país

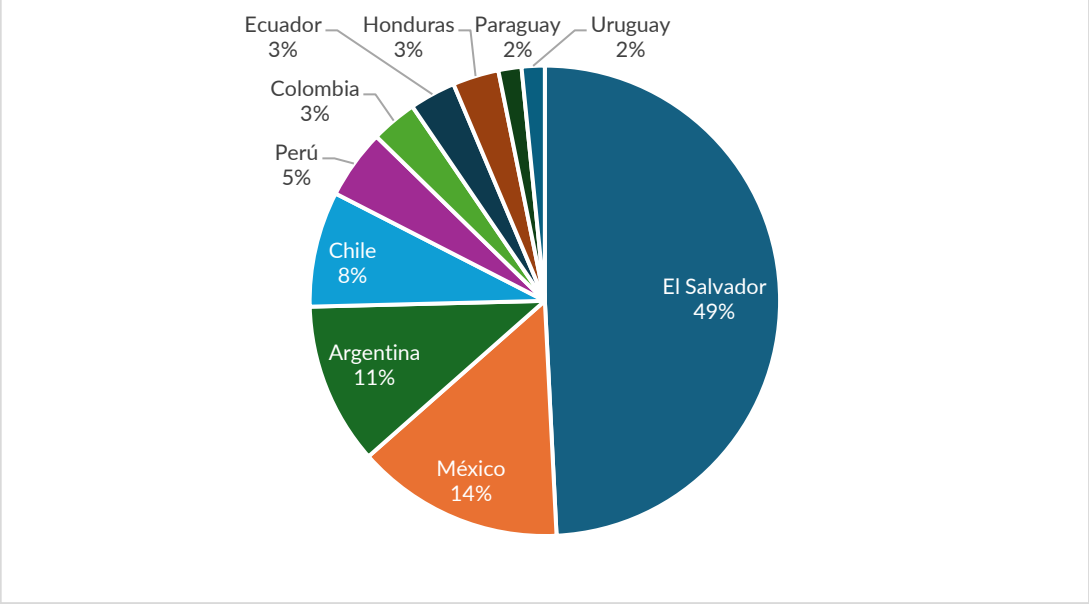
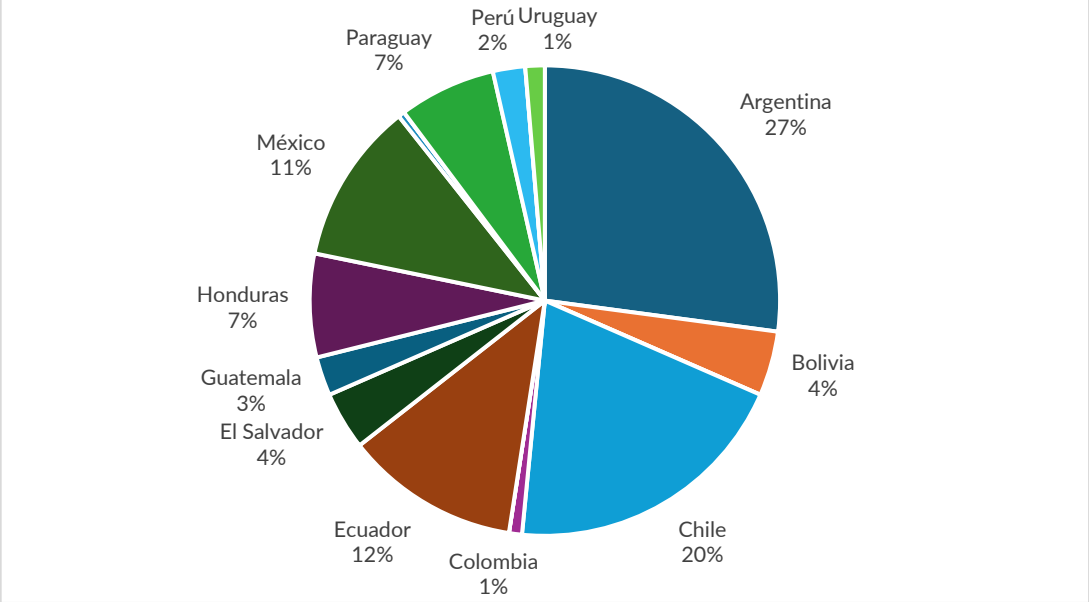


Gráfico 4 Participación de sujetos financieros tradicionales que respondieron a la encuesta por país



Mesas presenciales para la obtención de información

- Mesa regional de trabajo en Lima, Perú – abril 2024

25. Del 16 al 18 de abril de 2024 se llevó a cabo una mesa de trabajo en la ciudad de Lima, Perú, con el propósito de identificar y analizar los riesgos específicos relacionados con los AV/PSAV en los países miembros del GAFILAT. El objetivo de esta mesa de trabajo fue el de facilitar el intercambio de experiencias y mejores prácticas en regulación y supervisión, diseñar estrategias efectivas para abordar los riesgos identificados y promover la alineación con las Recomendaciones del GAFI. Todos los países miembros del GAFILAT participaron, 17 países participaron de forma presencial mientras que 1 país participó de forma remota.

26. Como resultado de la mesa de trabajo, las discusiones y el acercamiento a los países, se identificaron nuevos insumos para completar la evaluación de riesgos. Las presentaciones enfocadas en las experiencias de los países aportaron información y ejemplos concretos. La interacción entre los participantes enriqueció la perspectiva y refinó el enfoque de esta evaluación.

- Mesa regional de trabajo en Antigua, Guatemala – noviembre de 2024

27. El 5 de noviembre de 2024 se llevó a cabo una segunda mesa regional de trabajo en la ciudad de Antigua, Guatemala, con el propósito de presentar los principales hallazgos, calificar las amenazas y asignar prioridades de atención a las vulnerabilidades. Los 18 países miembros del

GAFILAT participaron de forma presencial y brindaron su percepción de los distintos componentes del riesgo.

Sesiones de consulta con el sector privado y validación

- Resultados de la I Sesión conjunta sobre activos virtuales y proveedores de servicios de activos virtuales (AV/PSAV) – Panamá, 2023

28. Bajo la coordinación conjunta de los grupos de trabajo sobre análisis de riesgos (GTAR) y de apoyo operativo (GTAO) se llevó a cabo junto al sector privado, una sesión de debate especial sobre AV/PSAV. Esta actividad acercó a las autoridades nacionales con entidades representativas de la industria de AV y PSAV; en el marco de este encuentro los países lograron extraer importantes conclusiones y aprendizaje. Aunado a ello, se sentaron las bases para un acercamiento fundamental con el sector privado que permitirá en el futuro seguir desarrollando actividades para el fortalecimiento de la coordinación nacional e internacional en la prevención y combate al LA/FT/FP.

29. Dentro de los retos presentados y el panorama de la regulación en la región, los ponentes coincidieron en que la regulación del sector es importante y para ello, es necesario identificar los riesgos en cada país. También destacaron la relevancia de la capacitación tanto del sector privado, como del sector público y de los usuarios, con el fin de lograr resultados efectivos, realistas y de acuerdo con el estándar internacional, y al riesgo y contexto de cada país.

- II Sesión conjunta sobre Activos Virtuales y Proveedores de Servicios de Activos Virtuales - Asunción, Paraguay, 2024

30. Esta sesión tuvo como objetivo intercambiar las perspectivas entre el sector privado y el sector público para dar a conocer cuáles son las experiencias que se tienen a nivel de la prevención, incluyendo los análisis de riesgos y, por otro lado, su relación con la investigación y recuperación de AV. Esta fue una iniciativa conjunta entre el Grupo de Trabajo de Análisis de Riesgo (GTAR) y el Grupo de Trabajo de Apoyo Operativo (GTAO), en la cual participaron representantes de todos los países del GAFILAT, así como de otros países observadores. El diálogo se realizó con representantes de PSAV y del sector financiero tradicional.

31. Las principales conclusiones del evento incluyen la importancia de los procesos de análisis de riesgos, incluyendo este ejercicio regional, así como los sectoriales y empresariales. Segundo, se resaltó la importancia de la coordinación entre el sector público y privado para evitar el uso indebido de los activos virtuales. Se insistió en que los AV no son negativos per se, solo que la falta de conocimiento, y los casos recientes en los que han sido mal utilizados generan una percepción negativa. Sin embargo, con las medidas apropiadas y con la implementación adecuada de las recomendaciones del GAFI se puede mitigar su uso indebido.

32. Finalmente, se instó a los asistentes a no perder de vista la vinculación directa que tiene el nivel de riesgo de los AV con la investigación y persecución del delito de LA/FT. El riesgo permite entender cómo y dónde direccionar los esfuerzos para detectar el LA/FT a través de los AV.

e. Etapas de implementación

33. La ESR se desarrolló en cinco etapas:

1) Análisis de documentación.
   a. Recopilación de informes de evaluaciones mutuas y otras guías relevantes.
   b. Análisis detallado de la documentación recopilada.
   c. Síntesis de la información clave para incorporar en la ESR.
2) Diseño y diseminación de encuestas.
   a. Diseño y desarrollo de herramientas de encuesta.
   b. Diseminación de las encuestas para recopilación de la información.
3) Realización de mesas de trabajo y entrevistas.
   a. Organización y coordinación de mesas regionales de trabajo.
   b. Análisis y síntesis de la información recogida en estas sesiones.
4) Elaboración de la evaluación sectorial de riesgos.
   a. Revisión de informes y documentos relevantes.
   b. Análisis de datos estadísticos y tendencias regionales.
   c. Identificación de amenazas y vulnerabilidades en el sector AV y PSAV.
   d. Redacción del informe de ESR, incluyendo conclusiones y recomendaciones.
5) Consulta con el sector privado y validación de los resultados de los miembros del GAFILAT previa aprobación.

f. Metodología para la evaluación de los riesgos

34. La metodología utilizada para evaluar los riesgos del sector AV y PSAV se basó en la Guía para una Evaluación Nacional de Riesgos de Lavado de Dinero[9] del GAFI (actualizada en 2024) y la Guía para el Análisis de Riesgos de FT (2019)[10]. La cual contempla como principales variables la amenaza y la vulnerabilidad.

i. Calculando la amenaza

35. El GAFI define la amenaza como *"en general, es una persona, grupo o actividad con el potencial de causar daño al estado, la sociedad o la economía. En el contexto del lavado de dinero, esto se refiere a individuos, grupos o entidades delictivas y a sus facilitadores que tratan de ocultar los orígenes ilícitos*

[9] GAFI. Guía para la Evaluación Nacional del Riesgo del Lavado de Activos (2024). https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Spanish-Money-Laundering-National-Risk-Assessment-Guidance.pdf.coredownload.inline.pdf

[10] GAFI 2019. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Terrorist-Financing-Risk-Assessment-Guidance.pdf.coredownload.pdf

de los fondos a través de actividades pasadas, presentes y futuras de lavado de dinero (y no a los delitos determinantes en sí mismos). La evaluación de amenazas suele servir como un punto de partida esencial para desarrollar una comprensión del riesgo de LA."[11]

36. Para definir la amenaza se consideraron las sub-variables de probabilidad e impacto. En este contexto, la probabilidad se refiere a la posibilidad de materialización de la amenaza y el impacto sería la magnitud del daño que podría causar si se llegara a concretar la amenaza. Este daño puede ser al sector, a la economía o a la sociedad.

37. Para analizar el ranking tanto de la probabilidad, así como del impacto, se consideró una escala del 1 al 8, donde 1 representa la mayor probabilidad o impacto y 8 la menor. Luego, para calificar estas variables se aplicaron las siguientes fórmulas:

- Calificación de Probabilidad = 9 - Ranking de Probabilidad
- Calificación de Impacto = 9 - Ranking de Impacto

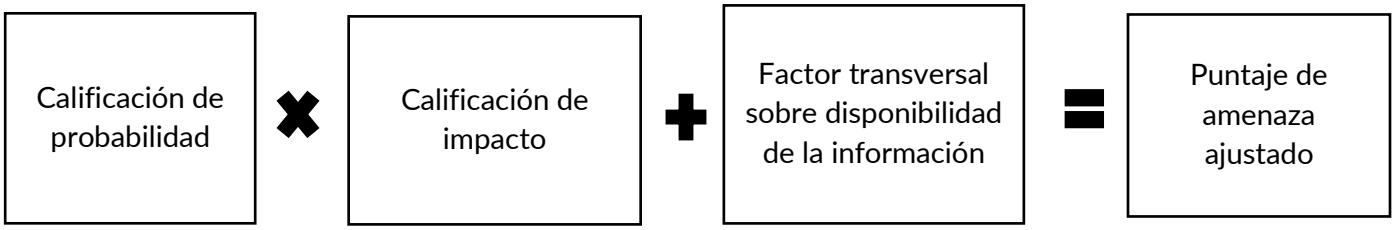
38. Finalmente, el puntaje de la amenaza se obtiene multiplicando las calificaciones de probabilidad e impacto:

Puntaje de la amenaza = Calificación de probabilidad × Calificación de impacto

39. Posteriormente, a fin de considerar la existencia de información regional específica sobre cómo se utilizan los AV y PSAV para el LA y delitos precedentes, se sumó un factor transversal que coadyuvó a reflejar la falta de información en la materia. En ese sentido, se utilizó una escala numérica del 1 a 3:

- 3: En la región existe poca o ninguna información disponible sobre esta amenaza y su vinculación con los AV y PSAV.
- 2: En la región existe cierta información, pero es incompleta o poco confiable.
- 1: En la región existe información suficiente y confiable sobre esta amenaza y su vinculación con los AV y PSAV.

40. En ese sentido, para obtener la ponderación final de la amenaza, se sumó el factor transversal sobre disponibilidad de la información en el cálculo inicial del puntaje de la amenaza, es decir:



[11] GAFI. Guía para la Evaluación Nacional del Riesgo del Lavado de Activos (2024). Pg. 10

41. Para la elaboración de la ESR, se consideró que ninguna amenaza puede ser considerada como de probabilidad de ocurrencia cero, sino hasta que exista más información y datos disponibles sobre cómo se usan indebidamente AV y se abusa de los PSAV en la región, ya sea para generar recursos ilícitos, o bien, para lavarlos.

ii. Calculando la vulnerabilidad

42. El GAFI explica que *"la vulnerabilidad puede ser explotada por la amenaza o puede apoyar o facilitar sus actividades. En el contexto de la evaluación de riesgos del LA, considerar las vulnerabilidades como algo distinto de la amenaza significa centrarse, por ejemplo, en las características inherentes de un sector en particular, un producto financiero o un tipo de servicio que los hacen atractivos y factibles para los fines del LA. [...] Las vulnerabilidades también pueden estar relacionadas con deficiencias en la ley, la regulación, la supervisión o la aplicación de la ley."*[12]

43. Para calcular las vulnerabilidades, los representantes regionales discutieron el orden de importancia de las vulnerabilidades identificadas y su prioridad de atención. Ahora bien, con el propósito de reflejar la magnitud de la vulnerabilidad se asignaron calificaciones numéricas inversas, siendo 5 la mayor prioridad y magnitud y 1 la menor.

44. Posteriormente, a fin de conocer el nivel de impacto de la amenaza una vez que ésta se aprovecha de las vulnerabilidades, se enlistaron las vulnerabilidades que podrían ser explotadas por cada amenaza.

45. Una vez vinculado el listado de vulnerabilidades con cada amenaza, para calcular el puntaje final de vulnerabilidad se sumaron las magnitudes que representa cada vulnerabilidad para determinada amenaza. Por ello es posible que varias vulnerabilidades se repitan en las distintas amenazas. Por ejemplo: Si se identificaron 3 vulnerabilidades con magnitud 1, 2 y 3, la vulnerabilidad tendría un puntaje de 6.

iii. Calculando el riesgo

46. Como se comentó anteriormente, el riesgo se define como una función de la amenaza y vulnerabilidades. En este sentido y con el propósito de determinar el nivel de riesgo en función de los puntajes obtenidos del análisis de las amenazas y las vulnerabilidades se utilizó la siguiente fórmula:

Puntaje de la amenaza	+	Puntaje de las vulnerabilidades (Sumatoria de las magnitudes)	=	Calificación de riesgo

[12] GAFI. Guía para la Evaluación Nacional del Riesgo del Lavado de Activos (2024). Pg. 11

47. Para determinar los niveles de exposición al riesgo de LA/FT de los AV y PSAV, se definieron las siguientes escalas conforme a las amenazas y vulnerabilidades identificadas.

Escala	Nivel de riesgo
40 a más	Muy alto
26 – 40	Alto
10 – 25	Medio
Menor de 10	Bajo

48. Considerando esta metodología, a continuación, se presenta el análisis principal del documento y sus conclusiones.

IV. CONTEXTO Y PANORAMA REGIONAL

49. De acuerdo con Chainalysis (2020, 2021, 2022, 2023 y 2024), América Latina ha emergido como una región de interés en el ámbito de los AV, motivada por una combinación de factores económicos y sociales que han fomentado su adopción. Entre 2020 y 2023, la región representó entre el 5% y el 9% de la actividad global en criptomonedas, y mostró patrones únicos de uso[13], impulsados principalmente por la falta de acceso a servicios bancarios tradicionales, la necesidad de remesas y la inestabilidad monetaria en varios países. Estos factores han convertido a las criptomonedas en una solución atractiva tanto para individuos como para empresas que buscan alternativas para almacenar valor y realizar transacciones comerciales transfronterizas de manera más eficiente. Así también, se considera que Latinoamérica es la segunda región con mayor crecimiento en el 2024, con una tasa de crecimiento interanual de aproximadamente el 42,5%. Gran parte de ese crecimiento se debe a los diversos y fuertes mercados de criptomonedas en Venezuela, Argentina y Brasil.

50. A lo anterior, se pueden sumar las observaciones de Bitso (s.f.a), señalando que en 2023 el panorama cripto en Latinoamérica muestra un crecimiento sostenido en la adopción de criptomonedas, a pesar de las turbulencias en la industria. Bitcoin y las stablecoins (USDC y USDT) son las más compradas en los mercados locales, con Bitcoin representando el 53% de las carteras promedio de los usuarios. La participación de las mujeres en el mercado cripto está aumentando con rapidez, especialmente en Colombia y Brasil, aunque la industria sigue dominada por hombres.

[13] Tales como: el uso de criptomonedas para remesas, cobertura contra la inflación monetaria, la alta adopción de *stablecoins* frente a otras regiones con fines prácticos (ahorro, pagos, comercio), uso comercial y empresarial, entre otros. (*Latin America: Venezuela and Argentina Stand Out as Examples of Crypto's Unique Utility* de octubre 2023; *Latin America's Key Crypto Adoption Drivers: Storing Value, Sending Remittances, and Seeking Alpha* de octubre 2022)

51. En el primer semestre de 2024, el panorama de las criptomonedas en América Latina se caracterizó por el fortalecimiento y la consolidación de Bitcoin dentro de los portafolios de inversión regionales, impulsado por eventos significativos como el halving de Bitcoin, su máximo histórico alcanzado en marzo de 2024, y la aprobación de fondos cotizados en bolsa (ETFs) tanto para Bitcoin como para Ether (Bitso, s.f.b). Paralelamente, se observó un crecimiento notable en las altcoins y memecoins, dentro de los que se destacan Solana y Pepe, respectivamente, lo que refleja una diversificación creciente en las carteras de los inversores. Más de un tercio de los usuarios de Bitso poseen tres o más criptomonedas, indicando una tendencia hacia la diversificación, influenciada por factores como un mayor apetito por el riesgo, la educación financiera y las condiciones socioeconómicas específicas de cada país.

52. En cuanto a la base de clientes, Bitso observó un crecimiento sostenido, con una predominancia de individuos en el rango de edad de 25 a 54 años, que corresponde a la población económicamente activa. Las preferencias de compra varían geográficamente, con México liderando en la adquisición de Bitcoin y Argentina en la preferencia por stablecoins. La actividad de trading está correlacionada con los ciclos de pago salarial, y muestra picos de actividad en días cercanos a la fecha de cobro y durante las primeras horas del día. Además, el ecosistema de Solana ha mostrado un crecimiento significativo, impulsado por su alta velocidad de transacción y bajas comisiones, lo que ha atraído un mayor capital especulativo.

53. Como se observa, la adopción de criptomonedas en América Latina muestra una diversidad de casos de uso que varían según las condiciones económicas de cada país. Mientras que, en algunos países, las criptomonedas se utilizan como una herramienta para mitigar la inflación y facilitar las remesas, en otros mercados, han evolucionado hacia un vehículo de inversión especulativa. Estas tendencias indican que, impulsada por factores económicos locales y una creciente confianza en el mercado, la adopción de criptomonedas en Latinoamérica continúa en ascenso. A medida que las tecnologías cripto sigan desarrollándose y las economías latinoamericanas enfrenten nuevos desafíos, es probable que se generen nuevos casos de uso adaptados a las necesidades específicas de la región. Las perspectivas futuras para la industria de activos virtuales en América Latina muestran una tendencia de crecimiento, lo que anticipa una mayor integración de los activos virtuales (criptomonedas en particular) en el sistema financiero tradicional y un incremento en la adopción y diversificación de inversiones en la región.

a. Implementación normativa

54. En 2023, se publicó la Guía para la Regulación ALA/CFT de Activos Virtuales y Proveedores de Servicios de Activos Virtuales en la Región del GAFILAT (2023) en la que se presentaba el estado de la regulación y normatividad de los países. En dicha guía se explicaban los diferentes enfoques adoptados por los países, a saber:

- Régimen regulatorio específico
- Integración en el régimen ALA/CFT
- Modificación o emisión de normativa ALA/CFT secundaria

- Establecimiento de obligaciones para sujetos obligados tradicionales
- Sin regulación

55. Desde la publicación de esa Guía, Bolivia, Honduras, Perú y Uruguay han modificado su legislación o emitida normatividad en relación con los AV. Para mayor detalle del panorama normativo actual se puede consultar el anexo de actualización de adopción normativa.

b. Proveedores de Servicios de Activos Virtuales en la región del GAFILAT

56. De acuerdo con el GAFI (2012-2023), los proveedores de servicios de activos virtuales se definen como *"cualquier persona física o jurídica que no esté cubierta en ningún otro lugar en virtud de las Recomendaciones y que, como negocio, realiza una o más de las siguientes actividades u operaciones para o en nombre de otra persona física o jurídica:*

i. intercambio entre activos virtuales y monedas fiat;
ii. intercambio entre una 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 activos virtuales; y,
v. participación y provisión de servicios financieros relacionados con la oferta de un emisor y / o venta de un activo virtual."

57. A fin de conocer el ecosistema de PSAV que operan en la región se solicitó información tanto a los países como a los propios PSAV. A continuación, se presentan los datos relevantes que permiten una mejor comprensión de dicho ecosistema.

i. Régimen de registro o licenciamiento

58. En relación con el otorgamiento de licencias o registro, Colombia, El Salvador, México y Nicaragua informaron sobre las medidas implementadas para el otorgamiento de licencias o registro a los PSAV. Por su parte, Argentina indicó que la regulación en materia de registración fue emitida en el año 2024 y que los PSAV deben registrarse ante la Comisión Nacional de Valores (CNV)[14] y la Unidad de Información Financiera (UIF). Por otro lado, Cuba ha establecido el marco jurídico, sin embargo, hasta el momento no ha informado el otorgamiento de licencias o registros al momento de realización de la encuesta.

Tabla 1 Requisitos para el otorgamiento de licencias o registro a PSAV

País	Requisitos
Colombia	• Constitución de la empresa como entidad vigilada por la SFC si los recursos otorgados como crédito provienen del público. • Adopción de un sistema de autocontrol y gestión del riesgo de LA/FT/FP.

[14] https://www.argentina.gob.ar/cnv/registro-de-proveedores-de-servicios-de-activos-virtuales

	• Reporte mensual de transacciones y de usuarios activos, inactivos y desvinculados.
Cuba	• Solicitud y documentación: Objeto social y estatutos, certificación de registro, estructura de gobierno, infraestructura y controles internos, políticas de divulgación de riesgos. • Sistema de Prevención: Procedimientos relacionados con el sistema de prevención y enfrentamiento al LA/FT. • Reportes: Emitir reportes de operaciones sospechosas y de transferencias de activos virtuales que superen ciertos umbrales.
El Salvador	• Preinscripción e inscripción en el registro, validación de requisitos regulatorios. • Documentación: Identificación de accionistas, servicios solicitados, organización y ejecutivos claves, situación financiera, gestión de riesgos, entre otros. • Supervisión: Monitoreo y visitas de supervisión post-licenciamiento.
México	• Previo al alta y registro de quienes operan con activos virtuales como sujetos obligados en materia de Actividades Vulnerables, deberán entregar de manera física al SAT (autoridad supervisora) la totalidad de la siguiente documentación: o Para personas morales, entre otros, se deben aportar el acta constitutiva y las modificaciones de sus estatus sociales; comprobante de domicilio; información de los socios o accionistas; nombre comercial y páginas electrónicas, y; los datos de identificación de su representante legal o apoderado. o En el caso de personas físicas, se requiere presentar su comprobante de domicilio; nombre comercial y páginas electrónicas, así como su identificación oficial, Clave Única de Registro de Población (CURP) y Registro Federal de Contribuyente (RFC).
Nicaragua	• Requisitos Generales: Constitución como persona jurídica, presentación de solicitud de licencia de operación. • Documentación requerida: Escritura de constitución, lista de accionistas, identificación del representante legal, certificados de antecedentes judiciales y policiales, registro ante la Unidad de Análisis Financiero, plan de negocio, contratos y acuerdos de negocios.

ii. PSAV registrados

59. La disponibilidad de información sobre el número de PSAV operando en la región es limitada, por lo que se solicitó información estadística sobre la actividad de los PSAV dentro de los países miembros del GAFILAT. Seis países, Argentina, Chile, Colombia, El Salvador, Paraguay y

Perú aportaron información. Sin embargo, aún no se cuenta con información precisa y actualizada sobre los PSAV que efectivamente operan regionalmente.

Tabla 2 Número de PSAV registrados en los países miembros del GAFILAT

	2018	2019	2020	2021	2022	2023
Argentina*	0	0	0	0	0	28
Chile	0	9	14	18	19	16
Colombia	0	0	0	7	88	63
El Salvador**	1	1	0	11	22	49
Paraguay***	0	0	2	4	29	11
Perú****	0	0	0	0	0	3
Total	1	1	16	40	158	170

Aclaraciones de la información proporcionada por los países:

** En el año 2024, mediante la RG N° 994/2024 la Comisión Nacional de Valores (CNV) creó el Registro de PSAV con el objetivo de identificar a las personas humanas y jurídicas que proveen en el país servicios relativos a Activos Virtuales (AV), conforme el alcance definido en el artículo 4° Bis de la Ley 25.246. A la fecha se cuenta con 28 PSAV -personas jurídicas- registrados en CNV, de los cuales solo 3 son entidades extrajeras y no se han registrado personas humanas.*

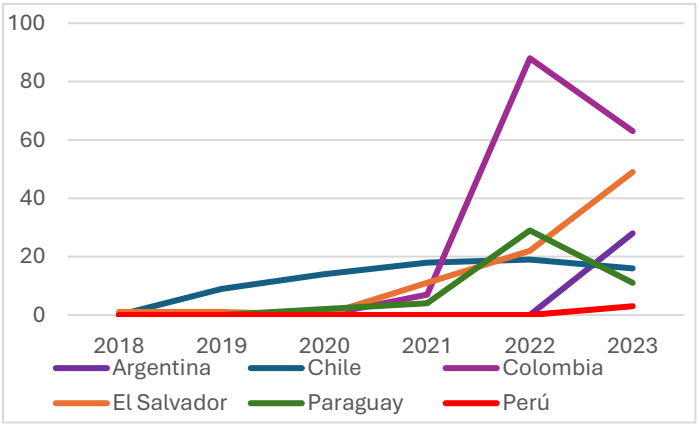
*** En 2018 y 2019, existían 2 sujetos obligados que se encontraban registrados en la UIF, previos a ser PSAV hasta 2021.*

**** En Paraguay, los PSAV han sido determinados como SO en el año 2020 mediante la Resolución SEPRELAD N° 08/20. Es importante señalar que, por Res. SEPRELAD N° 88/23, se ha dispuesto la informatización del registro de SO de la UIF, estableciendo un periodo de reinscripción para todos los SO que efectivamente desarrollen las actividades calificadas como obligadas, disponiendo que el registro de aquellos que no procedan a renovar su inscripción mediante el sistema indicado, serán dados de baja, por lo cual actualmente Paraguay cuenta con 11 PSAV debidamente catastrados.*

*****En Perú, los PSAV fueron incorporados como sujetos obligados a reportar a la UIF mediante Decreto Supremo N° 006-2023-JUS de julio de 2023. Posteriormente, mediante Resolución SBS N°2648-2024 de fecha 30 de julio de 2024, se emitió la Norma para la Prevención del LA/FT aplicable a los PSAV. En consecuencia, al mes de setiembre de 2024 se tienen registrados ante la UIF a 21 PSAV, de los cuales 13 cuentan con oficial de cumplimiento aprobado, y el resto se encuentra en trámite de aprobación.*

60. En el siguiente gráfico se puede ver el número de PSAV registrados en los países que respondieron, el cual muestra un crecimiento significativo a partir de 2020 con un notable pico en 2022, y una ligera estabilización en 2023.

Gráfico 5 Número de PSAV registrados por país que respondió a la pregunta (2019-2023)



iii. Servicios que prestan los PSAV

61. Con el fin de complementar la información y obtener un panorama más completo sobre la operación de los PSAV, se solicitó directamente a estos proveedores que aportaran información por medio de una encuesta. 63 PSAV de diez países miembros del GAFILAT respondieron la encuesta (Argentina, Chile, Colombia, Ecuador, El Salvador, Honduras, México, Paraguay, Perú y Uruguay).

62. Las respuestas de los PSAV muestran que la mayoría de los encuestados ofrecen más de un tipo de servicios cubierto por la definición del GAFI, además de otros servicios no incluidos en dicha definición. Dentro de los servicios que se ofrecen están:

- Intercambio entre activos virtuales y monedas fiat: Cambio de AV - fiat
- Intercambio entre una o más formas de activos virtuales: Cambio de AV - AV
- Transferencia de activos virtuales: Procesamiento de pagos cripto
- Custodia y/o administración de activos virtuales o instrumentos que permitan el control sobre activos virtuales
  - Custodia de activos virtuales
  - Monederos (wallet)
- Participación y provisión de servicios financieros relacionados con la oferta de un emisor y/o venta de un activo virtual
  - Inversión en activos virtuales
  - Negociación de derivados
  - Préstamos en activos virtuales
  - Financiamiento de tokens
  - Intercambio de tokens no fungibles
  - Mercados de tokens DeFi
  - Préstamos DeFi
  - Plataformas de juegos[15]

63. Conviene recordar que la definición de los PSAV según el GAFI abarca actividades que involucran la intermediación, custodia, intercambio y administración de AV, o servicios financieros relacionados con su emisión o venta. Sin embargo, se identificó que los PSAV ofrecen servicios auxiliares relacionados, aunque estos no se incluyen en la clasificación del GAFI. Entre los servicios auxiliares están: el análisis de blockchain, alojamiento físico o en la nube, el desarrollo de smart-contracts, auditoría y cumplimiento, autoridad de certificación, marketing y publicidad cripto, los exploradores de blockchain, emisión de stablecoins, las aplicaciones DApps; y minería o validación de AV.

15 En principio las plataformas de juego no entran en la definición del GAFI como PSAV a menos que estén involucradas directamente en la oferta o administración de activos virtuales, como el uso de criptomonedas o tokens en las transacciones o premios del juego. Si estas plataformas facilitan la transferencia, intercambio, o custodia de activos virtuales, por ejemplo, permitiendo el uso de criptomonedas para comprar bienes virtuales o tokens dentro de un ecosistema de juego, entonces podrían caer bajo la regulación de PSAV. Sin embargo, una plataforma de juego que simplemente ofrece entretenimiento sin manejar activos virtuales no entraría bajo la definición del GAFI.

Cuadro 1. PSAV en operación identificados por Argentina

En 2020, Argentina identificó 27 empresas activas que brindaban servicios de AV, "de las cuales 19 se encontraban registradas en el país y 8 en el extranjero. Los servicios ofrecidos eran los siguientes:

- Compraventa de AV contra pesos (exchange) y custodia de saldos en billeteras virtuales (wallet) son los servicios más frecuentes (20)
- Plataforma para la compraventa de AV entre usuarios (operaciones punto a punto/peer-to-peer (P2P) (6)
- En un caso se ofrece servicio de compraventa de AV a través de cajeros automáticos
- Una empresa que se dedica al minado de bitcoin
- Algunos servicios de pagos como el cobro en AV para comercios o el envío de remesas, entre otros (4)
- Realizar inversiones con AV, en general con stablecoins, que ofrecen una tasa fija anual en dólares (5)
- BTC es el AV más operado (26), seguido de ETH (19)
- USDT (10), DAI (9) y USDC (5) son las stablecoins más operadas
- Monedas aceptadas ARS y USD (limitado a pocos casos)"

Fuente: Comité de Coordinación para la Prevención y Lucha contra el Lavado de Activos, la Financiación del Terrorismo y la Proliferación de Armas de Destrucción Masiva, s.f., p. 110.

64. En las siguientes tablas se muestra la distribución de las respuestas recibidas respecto a los tipos de servicios prestados por los PSAV encuestados de la región. Más del 85% prestan más de un servicio, y sólo 8 PSAV ofrecen únicamente un tipo de servicio. Adicionalmente, 27 PSAV indicaron que también prestaban servicios auxiliares.

Tabla 3 Tipos de servicios ofrecidos por PSAV encuestados (no incluye PSAV que ofrecen un único servicio)

Servicio	N° de PSAV que lo ofrecen
Cambio de AV – fiat	43
Cambio de AV – AV	41
Custodia de activos virtuales	36
Monederos (wallet)	34
Procesamiento de pagos cripto	20
Inversión en activos virtuales	19
Negociación de derivados	8
Préstamos en activos virtuales	5
Financiamiento de tokens	4
Intercambio de tokens no fungibles (NFT)	4
Mercados de tokens DeFi	4
Aplicaciones descentralizadas (Dapps)	2
Minería/validación de AV	2

Servicio	N° de PSAV que lo ofrecen
Préstamos DeFi	1
Emisión de stablecoins	1
Plataformas de juegos	1

Tabla 4 PSAV encuestados que ofrecen un único tipo de servicio

Servicio	N° de PSAV que lo ofrecen
Procesamiento de pagos cripto	3
Inversión en activos virtuales	3
Cambio de AV - AV	1
Minería/validación de AV	1

Tabla 5 Servicios auxiliares prestados por PSAV

Servicio	N° de PSAV que lo ofrecen
Análisis de blockchain	23
Alojamiento físico/en la nube	6
Desarrollo de smart-contracts	6
Auditoría y cumplimiento	4
Autoridad de certificación	3
Marketing y publicidad cripto	3
Explorador de blockchain	3
Otros	3

iv. Tokens transados

65. Otro aspecto importante, para entender el funcionamiento de los PSAV es el de los tipos de tokens transados. Se consultó a los PSAV con cuáles tokens operaban, las respuestas muestran que Bitcoin sigue siendo la criptomoneda dominante. La alta adopción de stablecoins, particularmente Tether, indica una demanda significativa por almacenamiento de valor estable en el volátil mercado de criptomonedas. La fuerte presencia de Ethereum y Solana sugiere un creciente interés y utilización de plataformas que soportan contratos inteligentes y aplicaciones descentralizadas. Las monedas de privacidad y los tokens no fungibles (NFT por sus siglas en inglés) atienden necesidades de mercado específicas, como la privacidad y los coleccionables digitales, pero son menos adoptadas. Los tokens de seguridad no son ampliamente ofrecidos.

Tabla 6 Tokens con los que operan los PSAV de la región del GAFILAT

Token	N° de PSAV que lo operan
BTC	55
Stablecoins	40
Tether	34
ETH	33

Token	N° de PSAV que lo operan
SOL	19
LTC	18
XRP	17
ADA	17
BNB	17
BCH	16
Monero	7
Dash	6
Zcash	5
Utility tokens	10
Security tokens	6
NFT	6
Otros tokens de privacidad	3

66. Cabe resaltar el uso de monedas de privacidad diseñadas ex profeso para ofrecer un mayor nivel de anonimato y protección en las transacciones. Estas monedas implementan características criptográficas que ocultan detalles clave de las transacciones, como las direcciones de las partes involucradas, los montos transados y la estructura general de la transacción. Entre los ejemplos más conocidos con los que operan los PSAV encuestados están Monero (XMR), Zcash (ZEC) y Dash (en su modo privado).

c. Relación entre el sector financiero tradicional y los PSAV

67. Debido a que los PSAV dependen de los servicios bancarios tradicionales para funciones críticas como pagos, transferencias y custodia de fondos, es fundamental comprender la relación entre ambos sectores. Un buen entendimiento de esta interacción busca identificar cómo garantizar que los PSAV operen dentro del marco regulatorio sin restricciones que fomenten el uso de canales informales. Además, una relación sólida y transparente refuerza la confianza del público y los reguladores en la seguridad de los activos virtuales, y así promueve su adopción responsable.

68. El sector financiero tradicional cuenta con mayor experiencia y mecanismos ALA/CFT más robustos y maduros. Conocer cómo este sector interactúa con los PSAV es clave para mejorar la prevención del uso ilícito de los activos virtuales. Un marco normativo coherente que alinee los requisitos aplicables a ambos sectores es crítico para evitar brechas que puedan ser explotadas por delincuentes.

69. Si los PSAV no logran integrarse armoniosamente con el sector financiero, se corre el riesgo de que operen de forma clandestina, lo que aumentaría la probabilidad de actividades ilícitas no detectadas. Esta desconexión también podría afectar la estabilidad financiera regional, especialmente si los PSAV continúan creciendo sin estar bajo un adecuado control.

70. En la encuesta circulada entre los sujetos obligados tradicionales, se le hicieron múltiples preguntas a fin de conocer su percepción y actitud hacia los PSAV; y, en general, hacia los usuarios de activos virtuales. De las respuestas recibidas se observa que 189 (84%) encuestados no han tenido interacción comercial o financiera con PSAV, mientras que 36 (16%) sí han tenido algún tipo de interacción con PSAV en el período de 2018 a 2023, según se muestra a continuación.

Gráfico 6 Instituciones financieras tradicionales con interacciones comerciales con PSAV 2018 -2023

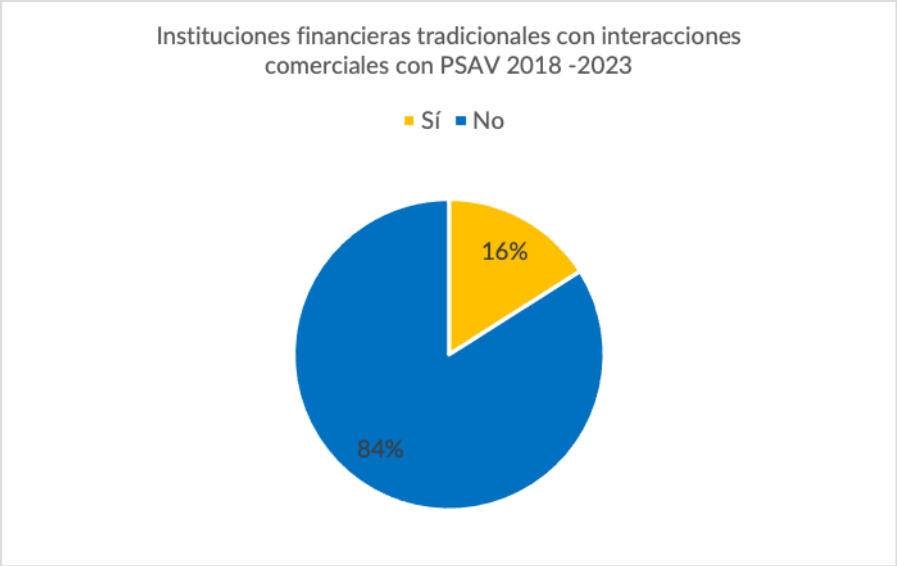
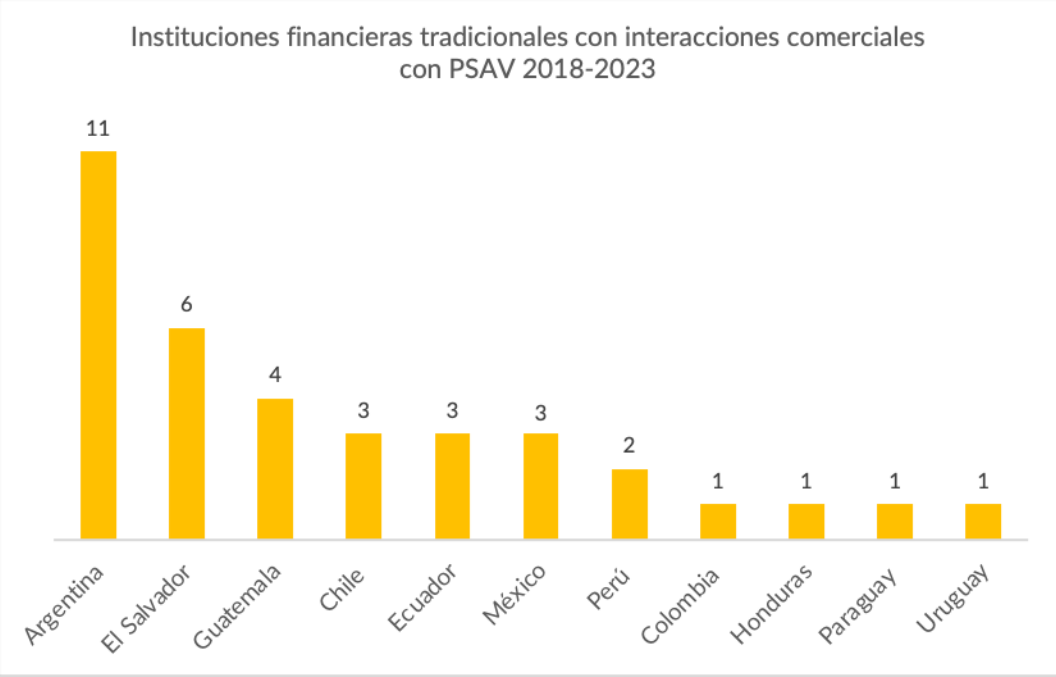


Gráfico 7 Instituciones financieras tradicionales con interacciones comerciales con PSAV por país 2018-2023



71. Cabe agregar que las 189 instituciones financieras que no han tenido actividad comercial con PSAV, indicaron que por política no aceptan como clientes a PSAV, o en su caso, usuarios de AV. En caso de identificarlos, informaron que suelen desvincularlos.

72. Dentro de los servicios y productos que se ofrecen a los PSAV, se analizaron las 36 respuestas afirmativas y se identificó lo siguiente:

- 12 indicaron que actualmente ya no operan con PSAV, en ese sentido, sólo 24 instituciones financieras continúan operando con PSAV.
- Cuatro no aportaron información sustantiva sobre los productos que ofrecen a PSAV.
- Cuatro bancos indicaron que los PSAV tienen acceso a todos los servicios que ofrecen dichas instituciones (uno de Argentina, uno de El Salvador, uno de México y uno de Paraguay).

73. Dentro de los productos y servicios ofrecidos a los PSAV están:

a. Cuentas bancarias. Principalmente cuentas corrientes y cuentas de depósito, incluyendo cuentas a la vista y cuentas monetarias.
b. Servicios de transferencia de fondos internacionales y locales, así como la provisión de tarjetas de crédito.
c. Otros productos y servicios adicionales proporcionados por el banco, adaptados a las necesidades del perfil del cliente. Por ejemplo, para PSAV se ofrece la liquidación de operaciones y el acceso a motores de pago, bajo estrictas regulaciones y requisitos de autorización.

V. PRINCIPALES AMENAZAS

74. El GAFI (FATF, 2013, p.7) define a la amenaza como *"… una persona o grupo de personas, un objeto o una actividad con el potencial de causar daño, por ejemplo, al estado, la sociedad, la economía, etc. En el contexto del lavado de activos y el financiamiento del terrorismo, esto incluye a los delincuentes, los grupos terroristas y sus facilitadores, sus fondos, así como las actividades pasadas, presentes y futuras de lavado de dinero y financiamiento del terrorismo."* Las amenazas pueden evolucionar rápidamente debido a factores externos, como avances tecnológicos, el uso de activos virtuales o cambios en las tácticas de los grupos delictivos.

75. El uso ilícito de AV representa una amenaza emergente en la región (GAFILAT–BCIE, 2024); lo que significa que los países reconocen el uso ilícito de activos virtuales como una amenaza en sus ENR o lo destacan en informes de tipologías, pero, no logran identificar o rastrear estas actividades de manera efectiva (fase de detección), ni están imponiendo consecuencias legales o regulatorias significativas a quienes cometen estos delitos (fase de sanción).

76. Si bien las criptomonedas no representan un riesgo intrínsecamente mayor que los activos tradicionales, sus características únicas pueden facilitar delitos cibernéticos que afecten infraestructuras y servicios críticos (Europol, s.f.). Entre esas características están el anonimato o

pseudonimato, descentralización, inmediatez para procesar las operaciones, alcance global e irreversibilidad.

a. Uso ilícito de activos virtuales a nivel regional

77. En esta sección se presenta una visión integral de los usos ilícitos de los AV. El objetivo es proporcionar información que permita comprender cómo se han utilizado los AV y PSAV con fines ilícitos en la región.

78. A nivel regional, según Chainalysis (2024), en 2023 se observó una tendencia hacia el uso de stablecoins en actividades ilícitas, desplazando a Bitcoin en delitos como estafas y transacciones con entidades sancionadas. Las tácticas de lavado de dinero se diversificaron con un aumento en el uso de puentes cross-chain y mixers como YoMix, mientras que la concentración de fondos ilícitos se desplazó de servicios centralizados a protocolos DeFi, los cuales, por su menor transparencia, facilitan la ocultación de fondos. Estos cambios reflejan una adaptación continua de los delincuentes para evadir la detección, subrayando la necesidad de una mayor diligencia y coordinación para combatir efectivamente los delitos relacionados con los AV y PSAV.

79. Asimismo, según datos de TRM Labs (2024), en 2023, las estafas y fraudes relacionados con criptomonedas ascendieron a 12.5 mil millones de dólares, esto representó un tercio de todos los fondos ilícitos en el ecosistema cripto a nivel mundial. Aunque el volumen total de fondos ilícitos en la blockchain disminuyó un 30%, de 49.5 mil millones de dólares en 2022 a 34.8 mil millones en 2023, algunas tipologías delictivas, como las ventas de drogas en línea, mantuvieron su volumen a pesar del cierre de varios mercados en la darknet. Diversos factores contribuyeron a la reducción general de la actividad ilícita con AV, incluyendo una mayor vigilancia por parte de las empresas, mayor conciencia del fraude entre el público y acciones más agresivas de las autoridades en Estados Unidos y Europa. Sin embargo, se advierte que el aumento en los precios de Bitcoin y otras criptomonedas, junto con crecientes tensiones geopolíticas, podrían incentivar a los delincuentes a explotar el mercado revitalizado.

i. Tipologías regionales

80. El GAFILAT realiza ejercicios bienales de compilación de tipologías de sus miembros. La primera vez que los países aportaron ejemplos de tipologías en los que se daba cuenta del uso ilícito de los AV fue en el reporte de 2017-2018. Se incluyeron dos casos, uno en el que los AV fueron utilizados para lavar recursos provenientes del tráfico ilícito de drogas y otro de una estafa piramidal basada en AV (GAFILAT, 2018, pp. 79 y 81). En el primer caso, los traficantes vendían drogas a través de tiendas de fachada y posteriormente, compraban bitcoin. Mientras que, en la estafa piramidal, una empresa supuestamente realizaba la gestión de un fondo de inversiones, buscando la rentabilidad en moneda virtual y prometía ganancias de 31% al mes, incompatible con las tasas en el mercado; sólo un pequeño porcentaje de los recursos recibidos habría sido remitido a una empresa conocida por negociar monedas virtuales.

81. En el siguiente ejercicio de tipologías, es decir, el de 2019-2020, sólo un caso involucró a PSAV y AV (GAFILAT, 2021, p. 110). El caso era de trata de personas, y los AV eran utilizados como uno de los mecanismos para ocultar el rastro de los recursos provenientes del delito precedente.

82. Ahora bien, en el ejercicio más reciente, esto es, el de 2021-2022, se incorporaron nueve casos:

1 Un caso en el que la utilización de activos virtuales permitió el ingreso de divisas a través de canales marginales (GAFILAT, 2023b, p. 41).
2 Un caso de estafa piramidal en el que se constituyó una empresa con actividad de prestación de servicios a terceros a través de la inversión en el trading de criptodivisas. A través de dicha sociedad, se captaron a más de 50 ahorristas, con la promesa de invertir el dinero en criptomonedas y abonar retornos con rentabilidad extraordinaria (ídem, p. 64).
3 Uso de activos virtuales para disimular los recursos provenientes del tráfico de drogas (ídem, p. 81).
4 Un caso de posible LA por medio de AV (ídem, p. 83).
5 Un caso en el que se identificaron operaciones con AV y que está relacionado con LA, crimen organizado, cohecho, y malversación. (ídem, p. 85).
6 Un caso de estafa utilizando redes sociales y criptoactivos como medio de pago (ídem, p. 87).
7 Un caso en el que se explica el involucramiento de un PSAV y la utilización de varias metodologías de LA detectadas, entre las que destacaba la compra de activos virtuales como medio para ocultar el efectivo de origen desconocido (ídem p. 89).
8 Adicionalmente, se incorporó un caso de trata de personas, tráfico ilícito de migrantes y uso ilícito de AV para fines de LA (ídem, p. 102).
9 Un caso más, en el que es posible que se hayan utilizado PSAV para estratificar fondos, y que está relacionado con narcotráfico, tráfico ilícito de migrantes y estafa (ídem, p. 104).

83. Como se observa, el número de casos relacionados con AV y PSAV ha aumentado en cada ejercicio compilatorio de tipologías, al igual que la complejidad de estos casos. Esto podría indicar una mayor capacidad de las autoridades para detectar y clasificar adecuadamente estas actividades ilícitas. Alternativamente, el incremento en los casos y su complejidad también podría reflejar un crecimiento en el uso de AV y PSAV para fines ilícitos, así como una evolución en las tácticas de los delincuentes para explotar las características de estos activos. No obstante, es necesaria más información y profundidad a fin de determinar con precisión las causas.

Cuadro 2. Tipologías identificadas por Brasil

En su ENR, Brasil identificó 18 tipologías de LA/FT en las que se utilizan nuevas tecnologías (ENCCLA, 2023):

A. Uso inapropiado de proveedores de servicios de activos virtuales

a. Uso inapropiado de proveedores centralizados de servicios de AV para LA
b. Uso indebido de AV
c. Envío ilegal de valores a través de AV
d. Uso indebido de los intercambios descentralizados de AV para LA
e. Uso de aplicaciones DeFi (DEX o cross-chain bridges) para lavado de dinero

B. Uso indebido de las plataformas de crowdfunding
   a. Uso de plataformas de préstamo colectivo para LA
   b. Uso de plataformas de crowdfunding de donaciones para LA
   c. Uso de plataformas de crowdfunding de preventa para LA
   d. Uso de plataformas nacionales de crowdfunding de donaciones para el FT
   e. Uso de plataformas de crowdfunding de donaciones extranjeras que utilizan AV para financiar el terrorismo
C. Sitios de apuestas
   a. Lavado mediante apuestas deportivas virtuales perdedoras y contradictorias
   b. Lavado mediante reversión de apuestas deportivas virtuales
D. Plataformas de juegos en línea
E. Plataformas de transmisión de video
F. Tokens no fungibles
   a. Ventas simuladas de AV o NFT para LA
G. Metaverso
H. Plataformas pares a pares
I. Servicio de tokenización de activos
   a. Tokenización de cuotas de consorcios para LA

84. La UIF de Costa Rica publicó tres casos en su compilación de tipologías de 2023 (ICD, 2023). Dos relacionados con estafas y uno más con secuestro extorsivo. Igualmente se informó que la Sección Especializada contra el Cibercrimen del Organismo de Investigación Judicial, en el 2023 ha identificado un aumento del 80% de casos relacionados a criptomonedas, en comparación con años anteriores, los cuales involucran distintos tipos de delitos que se vienen investigando en los que figura el tema de los criptoactivos, tales como:

- Estafas
- Legitimación de capitales
- Secuestros extorsivos
- Homicidios
- Extorsiones
- Administración fraudulenta
- Violación de comunicaciones electrónicas

ii. Actividades sospechosas identificadas por los sujetos financieros tradicionales en relación con PSAV

85. De las 225 entidades financieras consultadas sobre la detección de operaciones inusuales o actividades sospechosas relacionadas con los PSAV que podrían indicar riesgos de LA/FT, 33 respondieron afirmativamente y 192 no informaron haber identificado tales patrones. Dentro de los patrones de actividad inusual o sospechosa identificada por las entidades financieras relacionados con PSAV están:

- Uso indebido o no autorizado de PSAV y criptomonedas.
- Falta de justificación del origen de fondos o estructura financiera.
- Evasión de controles o regulaciones.
- Actividades irregulares relacionadas con el mercado de divisas y criptomonedas.
- Fraude y riesgos financieros.

86. El número de entidades que han identificado patrones de operaciones inusuales o actividades sospechosas asociadas con los PSAV sugiere la presencia de operaciones no-reguladas o informales de PSAV. Las entidades financieras tradicionales logran identificar intentos deliberados de evadir controles y regulaciones existentes, reflejados en el uso indebido de criptomonedas y la falta de justificación del origen de fondos. Finalmente se indica que, incluso con prohibiciones, las actividades con AV se mantienen de forma sumergida por lo que las medidas existentes no son completamente efectivas y se requieren estrategias más robustas y coordinadas para mitigar estos riesgos.

iii. Reportes de operaciones sospechosas recibidos por las UIF

87. Algunas UIF compartieron las cantidades de ROS recibidos por parte de los PSAV. Dentro de la información proporcionada, se observa que las señales de alerta identificadas son similares a las identificadas por los servicios financieros tradicionales.

88. A manera de ejemplo, la UIF de Perú proporcionó información actualizada sobre los IIFs elaborados.

Tabla 7 Cantidad y monto (en USD) involucrado en IIFs 2019 – agosto 2024 (Perú)

Año	N° IIFs	Monto en USD
2020	2	135.053,00
2021	1	11.645.851,00
2022	9	38.730.376,00
2023	4	7.683.372,00
2024	2	12 .940.165,00
Total	**18**	**71.134.817,00**

Fuente: SBS

Tabla 8 Cantidad y monto involucrado en IIFs por posible delito precedente 2019 – agosto 2024 (Perú)

Delito precedente	N° IIFs	Monto en USD
Delitos contra el orden financiero y monetario	3	46.401.276,00
Delitos Tributarios	1	11.645.851,00
Delitos contra el Patrimonio	13	10.847.525,00
Tráfico Ilícito de Migrantes	1	2.240.165.00
Total general	**18**	**71.134.817,00**

Fuente: SBS

Tabla 9 Cantidad y monto (en USD) involucrado en IIFs por tipología 2019 – agosto 2024

Tipología	N° IIFs	Monto en USD
Uso de intermediarios financieros informales	1	35.600.000,00
Fondos ilícitos o no justificados canalizados a través de productos o instrumentos financieros y/o de inversión	3	13.922.201,00
Uso de sistemas piramidales	1	10.700.000,00
Fraude Informático BEC	11	5.750.629,00
Uso de recursos ilícitos o no justificados en la adquisición de bienes muebles e inmuebles	1	5.060.711,00
Arbitraje cambiario nacional y/o internacional o mediante transporte de dinero ilícito	1	101.276,00
Total	**18**	**71.134.817,00**

Fuente: SBS

b. Principales amenazas de los AV y PSAV

89. Para identificar las amenazas relacionadas con los activos virtuales y PSAV, se consultó a los PSAV, las UIF, AOP, autoridades reguladoras de PSAV y financieras, así como a los sujetos obligados tradicionales. Al recopilar las respuestas fue posible agruparlas en:

A. Amenazas relacionadas con la explotación de las características inherentes de los activos virtuales para la comisión de diferentes tipos de delitos, y,
B. Amenazas en que los activos virtuales se utilizan para facilitar el lavado de recursos y activos provenientes de otros delitos.

Cuadro 3 Amenazas relacionadas con los activos virtuales y PSAV

A. Amenazas relacionadas con la explotación de las características inherentes de los activos virtuales para la comisión de diferentes tipos de delitos.

- Ciberataques y disrupciones para retener fondos y exigir pagos en AV para liberar datos o restaurar sistemas.[16]
- Uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web.
- Fraude y estafas de inversión.

B. Amenazas en que los activos virtuales se utilizan para facilitar el lavado de recursos y activos de otros delitos:

- Tráfico de estupefacientes y psicotrópicos: Uso de AV para financiar o legitimar recursos provenientes del narcotráfico.
- Trata de personas.
- Defraudación tributaria: Contribuyentes aceptan pagos en AV para evadir impuestos, dificultando la identificación del origen territorial de la renta.
- Corrupción: Fondos estatales vinculados al enriquecimiento ilícito podrían ser convertidos a AV.
- Financiamiento del terrorismo.

90. Es de notar que el financiamiento del terrorismo no se identifica como una de las principales amenazas de la región. Sin embargo, con el fin de analizar el nivel de riesgo para FT, es importante considerar este aspecto desde el análisis de las amenazas.

c. Análisis de las amenazas de los AV y PSAV

91. Durante la mesa de trabajo desarrollada en Antigua, Guatemala, los representantes de los países participaron en un ejercicio de ponderación de las amenazas. Para ello realizaron un ranking de probabilidad de materialización de la amenaza utilizando AV; igualmente, establecieron un ranking de acuerdo con el impacto estimado. Con base en ese ranking descrito, en la metodología, del 1 al 8, donde 1 representa la mayor probabilidad o impacto y 8 la menor, se obtuvo el siguiente resultado.

Tabla 10. Ranking de probabilidad e impacto de las amenazas

Amenaza	Ranking probabilidad	Ranking impacto
Fraude y estafas	1	2
Ataques cibernéticos	2	5
Uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web.	3	8
Tráfico de estupefacientes y psicotrópicas	4	1
Defraudación tributaria	5	6

[16] Por ejemplo, los ataques de fuerza bruta, malware, suplantación de identidad y phishing, extorsión y secuestro de información datos o equipos (ransomware).

Trata de personas	6	3
Corrupción	7	4
Financiamiento del terrorismo	8	7

92. Luego, según fue explicado anteriormente en la metodología, se asignaron calificaciones numéricas inversas para reflejar la magnitud, donde la calificación de Probabilidad y de Impacto se resta de 9. Considerando los rankings, anteriores, la calificación quedó de la siguiente forma:

Tabla 11. Calificación de probabilidad e impacto de las amenazas

Amenaza	Calificación probabilidad	Calificación impacto
Fraude y estafas	8	7
Ataques cibernéticos	7	4
Uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web.	6	1
Tráfico de estupefacientes y psicotrópicas	5	8
Defraudación tributaria	4	3
Trata de personas	3	6
Corrupción	2	5
Financiamiento del terrorismo	1	2

93. El puntaje de la amenaza se obtiene multiplicando las calificaciones de probabilidad e impacto. Aplicando esta fórmula se obtiene lo siguiente:

Tabla 12. Puntaje de las amenazas

Amenaza	Calificación de probabilidad	Calificación de impacto	Puntaje
Fraude y estafas	8	7	**56**
Ataques cibernéticos	7	4	**28**
Tráfico de estupefacientes y psicotrópicas	5	8	**40**
Trata de personas	3	6	**18**
Defraudación tributaria	4	3	**12**
Corrupción	2	5	**10**
Uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web.	6	1	**6**
Financiamiento del terrorismo	1	2	**2**

94. A fin de considerar la existencia de información regional específica sobre cómo se utilizan los AV y PSAV para el LA y delitos precedentes, se sumó el factor transversal que coadyuvó a reflejar la falta de información en la materia. En ese sentido, se utilizó una escala numérica del 1 a 3, donde 1 representa la existencia de información suficiente y confiable sobre esta amenaza y su vinculación con los AV y PSAV y 3 es la poca existencia o ninguna información disponible sobre

esta amenaza y su vinculación con los AV y PSAV. En este sentido, se obtuvieron los siguientes valores:

Tabla 13. Puntaje del factor transversal sobre disponibilidad de la información con relación a las amenazas

Factor transversal sobre disponibilidad de la información	
Amenaza	**Puntaje**
Uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web.	3
Tráfico de estupefacientes y psicotrópicas	3
Trata de personas	3
Financiamiento del terrorismo	3
Fraude y estafas	2
Ataques cibernéticos	2
Defraudación tributaria	2
Corrupción	2

95. Como se observa, en ningún caso se consideró que en la región existe información suficiente sobre las amenazas en relación con el uso indebido de los AV.

96. Luego, para obtener la ponderación final del nivel de la amenaza, se suma el factor transversal sobre la disponibilidad de la información en el cálculo inicial del puntaje de la amenaza. Por tanto, al aplicar este factor transversal sobre disponibilidad de la información para cada amenaza se obtiene lo siguiente:

Tabla 14. Puntaje final de las amenazas + el factor transversal sobre disponibilidad de la información

Amenazas	Calificación de probabilidad x impacto	+ Factor transversal	Puntaje final	Acciones
Fraude y estafas	56	2	58	Requieren atención prioritaria y acciones inmediatas de mitigación.
Tráfico de estupefacientes y psicotrópicas	40	3	43	
Ataques cibernéticos	28	2	30	Necesitan medidas preventivas intensivas y seguimiento constante.
Trata de personas	18	3	21	
Defraudación tributaria	12	2	14	Requieren monitoreo regular y acciones preventivas para reducir el riesgo.
Corrupción	10	2	12	
Uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web.	6	3	9	Requiere monitoreo y esfuerzos para mejorar la comprensión y reducir la incertidumbre asociada.
Financiamiento del terrorismo	2	3	5	

97. Esto demuestra que las principales amenazas son: el fraude y estafas que pueden desarrollarse con los AV, el lavado de dinero producto del tráfico de drogas utilizando AV, los ataques cibernéticos a los PSAV y el lavado de dinero producto de la trata de personas utilizando AV. Es de notar que el financiamiento al terrorismo recibe el puntaje más bajo, confirmando que la amenaza para la región sobre este aspecto es mucho menor comparada con los delitos precedentes del lavado de activos.

VI. PRINCIPALES VULNERABILIDADES

98. Respecto a las vulnerabilidades, el GAFI (FATF, 2013, p.7) indica que *"... tal como se utiliza en la evaluación de riesgos, comprende aquellos elementos que pueden ser explotados por la amenaza o que pueden apoyar o facilitar sus actividades. En el contexto de la evaluación de riesgos de lavado de activos y financiación del terrorismo, considerar las vulnerabilidades como algo distinto de las amenazas significa centrarse, por ejemplo, en los factores que representan debilidades en los sistemas o controles de ALA/CFT o en ciertas características de un país. También pueden incluir las características de un sector en particular, un producto financiero o un tipo de servicio que los hacen atractivos para fines de lavado de activos y financiación del terrorismo."*

99. A continuación se presentan las principales vulnerabilidades señaladas por los encuestados y en las mesas de trabajo con el sector público y privado, para lo cual se analizaron las respuestas recibidas agrupándolas por tema. Estas vulnerabilidades se agruparon en las siguientes categorías: desconocimiento y falta de capacitación, marco jurídico insuficiente, falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV, infraestructura tecnológica insuficiente, falta de supervisión efectiva a los PSAV, características inherentes de los activos virtuales.

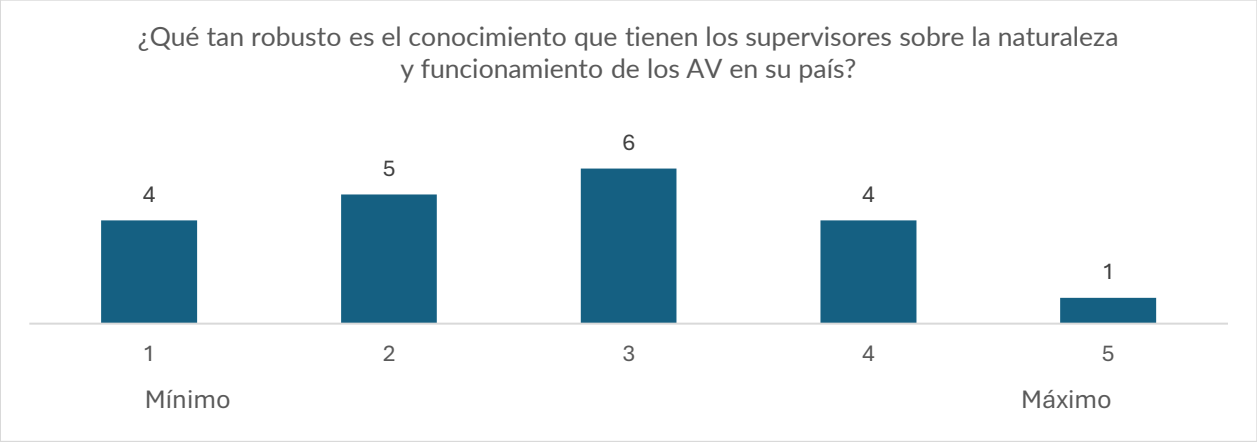
a. Desconocimiento y falta de capacitación

i. Nivel de percepción del conocimiento por parte de los supervisores financieros

100. El primer aspecto que se exploró fue el tema del conocimiento y funcionamiento de los activos virtuales en los países del GAFILAT. Dado que no en todos los casos existe una regulación aplicable o un supervisor designado, se decidió consultar a los supervisores financieros. Estos supervisores tienen contacto directo con el sector financiero tradicional y son quienes podrían conocer mejor las interacciones entre el sector financiero tradicional y los PSAV desde la perspectiva del sector público.

101. Respecto al conocimiento de los supervisores financieros sobre la naturaleza y el funcionamiento de los AV, se pidió a los encuestados que indicaran, usando una escala Likert de 1 a 5, donde 1 era el mínimo y 5 el máximo, qué tan robusto era el conocimiento que poseían los supervisores sobre la naturaleza y el funcionamiento de los AV en su país.

Gráfico 8 Robustez del conocimiento de los supervisores financieros sobre la naturaleza y funcionamiento de los activos virtuales en su país (escala Likert 1-5)



102. Los resultados de la encuesta sugieren que el conocimiento de los supervisores sobre la naturaleza y el funcionamiento de los AV en sus países es generalmente percibido como limitado. La mayoría de las respuestas se agrupan en torno al nivel medio o inferior, muy pocos encuestados consideran que los supervisores tienen un conocimiento alto o muy alto. Esto indica una necesidad de aumentar la capacitación y educación de los supervisores para mejorar su comprensión y, en su caso, capacidad de regulación de los AV.

ii. Nivel de percepción del conocimiento por parte de las UIF

103. Igualmente, las respuestas de las UIF indicaron como desafíos la falta de capacitación especializada y la fluctuación del personal en las UIF. En ese sentido, aún es necesario profundizar el conocimiento y especialización en AV/PSAV, y mejorar la coordinación internacional con otras UIF. La falta de regulación y supervisión de los PSAV en varios países, incluida la falta de un supervisor natural, contribuye a la complejidad del problema.

104. Otros desafíos incluyen la ubicación geográfica de las cuentas y personas naturales vinculadas a los AV, así como el desconocimiento general del tema y la reticencia de los PSAV a colaborar en algunas jurisdicciones. La escasa retroalimentación de las contrapartes internacionales y la ausencia de guías claras para los sujetos obligados sobre cómo llevar a cabo procesos de debida diligencia del cliente (DDC) agravan la situación. Para las UIF, es un desafío no contar con información completa sobre el número de PSAV operativos, ya que dificulta el análisis y la identificación de transacciones sospechosas.

105. No obstante, cabe señalar el trabajo realizado por las UIF para identificar y diseminar señales de alerta, regulaciones, guías y otros documentos relacionados con los AV y los PSAV.

b. Marco jurídico insuficiente

i. Estado de Implementación de la Recomendación 15 del GAFI

106. Los 18 países miembros del GAFILAT han sido evaluados dentro de la cuarta ronda de evaluaciones mutuas, no obstante, la implementación efectiva de los estándares relacionados con los AV ha sido limitada. Cabe aclarar que, por un lado, varios países ya habían sido evaluados cuando la modificación a la Recomendación 15 y la Nota Interpretativa fueron adoptadas, y cuando se aprobaron los criterios para la evaluación de cumplimiento técnico (octubre de 2019). Por otro lado, los países han sido cautelosos al aceptar las operaciones con AV y PSAV, lo que ha ocasionado que se tomen un tiempo prudente para analizar el marco regulatorio a adoptar.

107. Actualmente, de los 18 países cuyos IEM han sido adoptados, las calificaciones de la Recomendación 15 muestran que la mayoría de los países tienen que realizar mejoras de diferente envergadura, pese a los esfuerzos realizados.

Tabla 15. Calificaciones de la Recomendación 15

País	Fecha de calificación*
Recomendación 15 Cumplida	
Guatemala	Octubre de 2018
Honduras	Enero de 2017
Panamá	Enero de 2018
Perú	Febrero de 2019
República Dominicana	Agosto de 2019
Recomendación 15 Mayoritariamente Cumplida	
Cuba	Febrero de 2024
México	Enero de 2021
Paraguay	Noviembre de 2022
Uruguay	Enero de 2020
Recomendación 15 Parcialmente Cumplida	
Argentina	Diciembre 2024
Bolivia	Enero de 2024
Brasil	Diciembre de 2023
Chile	Septiembre de 2021
Colombia	Noviembre 2018
Ecuador	Enero de 2023
El Salvador	Agosto de 2024
Recomendación 15 No Cumplida	
Costa Rica	Enero de 2023

Nicaragua	Enero de 2021

*Los países marcados en color azul aún no han sido evaluados conforme a la actual Recomendación 15 que incluye medidas para los AV y PSAV.

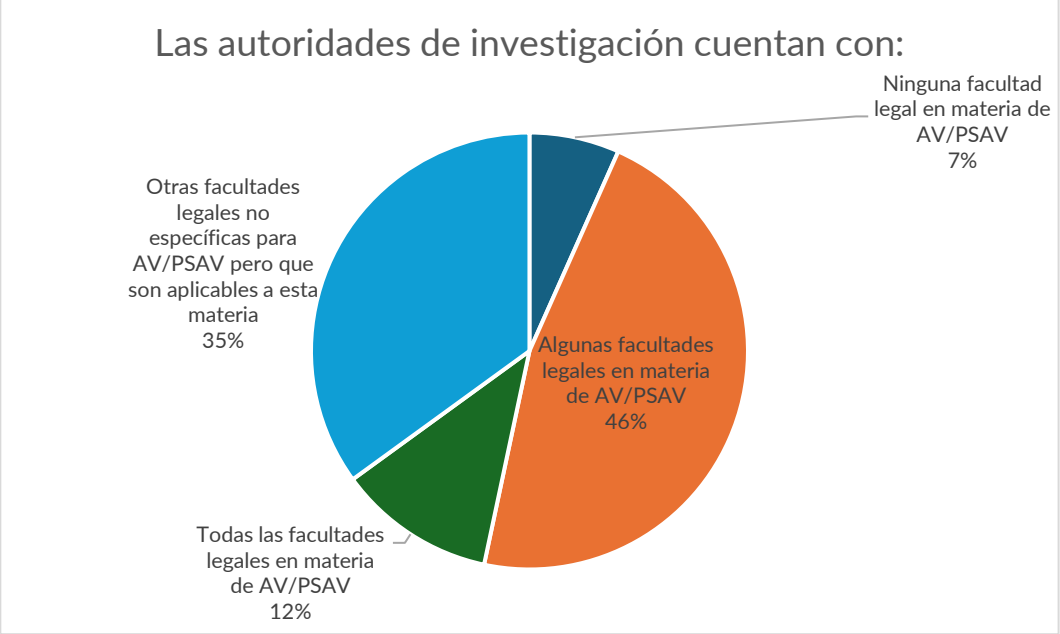
108. Es importante aclarar que siete países fueron evaluados antes de la modificación de la Recomendación 15, la adopción de su nota interpretativa y la publicación de la nueva metodología de evaluación. De ellos, sólo Colombia obtuvo una calificación de parcialmente cumplida, mientras que Guatemala, Honduras, Panamá, Perú y República Dominicana cumplieron completamente, y Uruguay cumplió mayoritariamente. De los diez países evaluados con la metodología ya aprobada en octubre de 2019, sólo Paraguay alcanzó una calificación de mayoritariamente cumplida, mientras que Cuba y México lograron la misma calificación tras procesos de recalificación. En contraste, Argentina, Bolivia, Brasil, Chile, Ecuador, El Salvador, Costa Rica y Nicaragua tienen que abordar deficiencias moderadas y mayores, según corresponda.

109. La diferencia en las calificaciones sugiere la necesidad de continuar mejorando las capacidades regulatorias de los países miembros, con el fin de garantizar la plena implementación de la Recomendación 15 y la adecuada integración de los PSAV en el marco ALA/CFT. En los países evaluados después de octubre de 2019, los retos para cumplir completamente con la Recomendación 15 son significativos, por lo que aún deben enfocarse en mejorar su entendimiento de la operación con activos virtuales, de los PSAV y los riesgos que representan.

ii. Facultades legales de las autoridades de orden público

110. Un aspecto más que se exploró es el de las facultades de las AOP para investigar y procesar casos que involucran AV o PSAV. Para ello, la pregunta fue de elección múltiple como se puede ver en los gráficos siguientes.

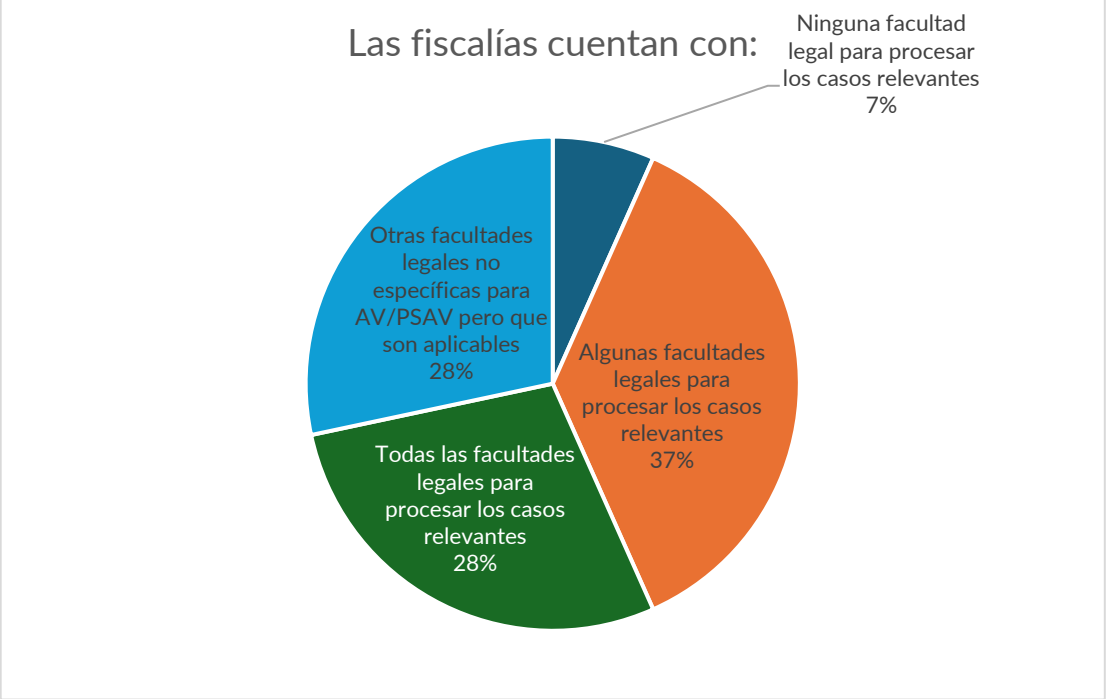
Gráfico 9 Percepción de las facultades legales de las autoridades de investigación para tratar casos de AV/PSAV



111. Una minoría del 7% considera que las autoridades de investigación no tienen ninguna facultad legal para tratar casos de AV/PSAV. El 46% de los encuestados cree que las autoridades de investigación tienen algunas facultades legales específicas para AV/PSAV. Apenas el 12% percibe que las autoridades de investigación cuentan con todas las facultades legales necesarias para abordar los casos de AV/PSAV, aunque esta es una percepción menos común comparada con otras. Finalmente, el 35% considera que las autoridades tienen otras facultades legales generales que, aunque no específicas para AV/PSAV, pueden aplicarse a estos casos.

112. En cuanto a las facultades de la fiscalía, las respuestas indican que, de manera similar a las autoridades de investigación, el 7% considera que la fiscalía no tiene facultades legales para procesar estos casos. Mientras que el 37% de los encuestados cree que la fiscalía tiene algunas facultades legales para procesar casos de AV/PSAV. Cabe resaltar que una porción significativa (28%) piensa que la fiscalía tiene otras facultades legales generales que pueden aplicarse a los casos de AV/PSAV.

Gráfico 10 Percepción de las facultades de las fiscalías para procesar casos de AV/PSAV



113. Los resultados muestran que, si bien existe cierta capacidad legal, puede que no sea completamente adecuada o específica para abordar la totalidad de los desafíos que presentan los casos de AV/PSAV. Tanto para las autoridades de investigación como para la fiscalía, una gran parte de los encuestados considera que solo tienen algunas facultades legales o facultades generales aplicables, pero no específicas y completas para AV/PSAV. Aunque un pequeño porcentaje percibe no tener ninguna facultad legal, la mayoría de las opiniones se dividen entre tener algunas facultades específicas y otras no específicas, pero aplicables. En ese sentido, el marco jurídico de investigación y procesamiento es perfectible, aunque en general no representa necesariamente un impedimento o una vulnerabilidad considerable para abordar casos que involucran AV o PSAV. El marco jurídico podría brindar mayor claridad y especificidad sobre las facultades de las AOP, y reducir así posibles lagunas que afecten la efectividad de las investigaciones y procesamientos.

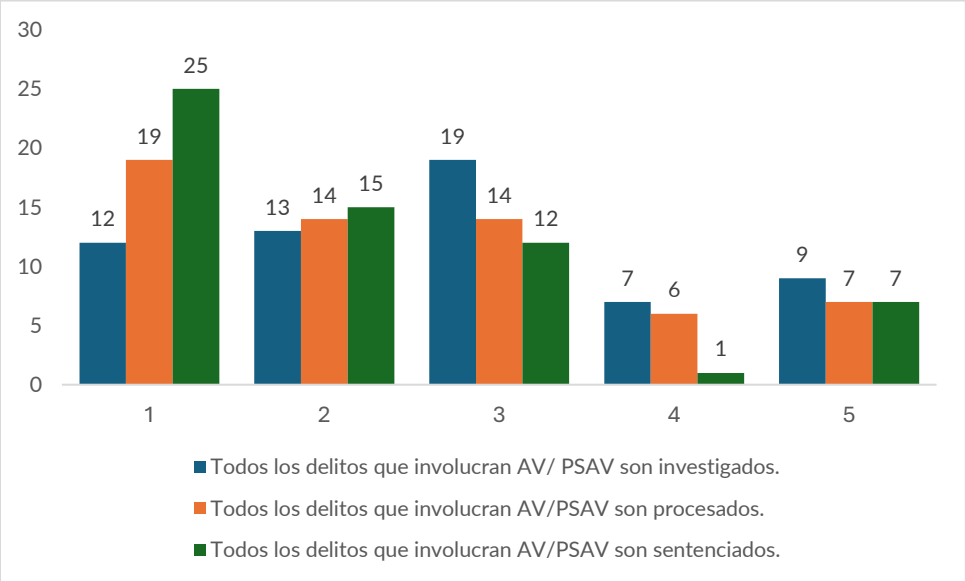
iii. Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV

114. Las autoridades de investigación deben estar en capacidad de enfrentar las amenazas de LA/FT que lleguen a materializarse. Por lo tanto, identificar las vulnerabilidades en la capacidad de investigación y procesamiento de los delitos que involucran activos virtuales y PSAV es fundamental. En ese sentido, la encuesta circulada a las AOP procuró identificar los desafíos que se presentan.

115. En particular, se utilizó una escala de Likert de 1 a 5, donde 1 representaba “totalmente en desacuerdo” y 5 “totalmente de acuerdo”, para formular preguntas a las autoridades de orden público sobre su grado de acuerdo con las siguientes afirmaciones:

- Todos los delitos que involucran AV/PSAV son investigados.
- Todos los delitos que involucran AV/PSAV son procesados.
- Todos los delitos que involucran AV/PSAV son sentenciados.

Gráfico 11 Grado de acuerdo de las AOP sobre la investigación, procesamiento y sentencia de delitos relacionados con AV/PSAV



116. Al comparar los resultados del gráfico anterior, es posible decir lo siguiente:

117. **Todos los delitos que involucran AV/PSAV son investigados:** Las autoridades están generalmente neutrales o en desacuerdo con la afirmación de que todos los delitos que involucran AV/PSAV son investigados. El valor promedio de las respuestas fue de 2.80, lo que indica que las AOP están ligeramente en desacuerdo con la afirmación de que todos los delitos que involucran AV/PSAV son investigados. Las respuestas muestran una percepción mixta entre las autoridades, no obstante, las opiniones no varían de forma extrema. La presencia de respuestas en todos los puntos de la escala sugiere más diversidad en experiencias o percepciones de las autoridades sobre esta etapa en comparación con el procesamiento y la sentencia.

118. **Todos los delitos que involucran AV/PSAV son procesados:** Las autoridades están predominantemente en desacuerdo con la afirmación de que todos los delitos que involucran AV/PSAV son procesados. El promedio de 2.47 de las respuestas muestra un desacuerdo más fuerte en comparación con la investigación e indica que las autoridades no consideran que todos los delitos que involucran AV/PSAV son procesados. Hay una percepción de que muchos delitos no son procesados. La mayoría de las respuestas se concentran en el valor 1 (totalmente en desacuerdo), con una distribución significativa en los valores 2 y 3 (desacuerdo y neutro). Hay pocas respuestas en los valores 4 y 5 (de acuerdo). La alta concentración de respuestas en el valor 1 sugiere una percepción fuerte y generalizada de que muchos delitos no llegan a ser procesados.

119. **Todos los delitos que involucran AV/PSAV son sentenciados:** Las autoridades están mayoritariamente en desacuerdo con la afirmación de que todos los delitos que involucran AV/PSAV son sentenciados. Con un promedio de 2.17, las respuestas reflejan un desacuerdo aún más fuerte respecto a la sentencia de los delitos que involucran AV/PSAV. La respuesta más frecuente es la de "totalmente en desacuerdo", lo que indica que las autoridades perciben que pocos delitos relacionados con AV/PSAV llegan a ser sentenciados. La mayoría de las respuestas se encuentran en el valor 1 (totalmente en desacuerdo), con una distribución significativa en el valor 2 (desacuerdo), con muy pocas respuestas en los valores 3 (neutro), 4 y 5 (de acuerdo). La gráfica refleja una fuerte percepción de ineficacia en la etapa de sentencia de estos delitos, con una clara mayoría de respuestas en el desacuerdo total.

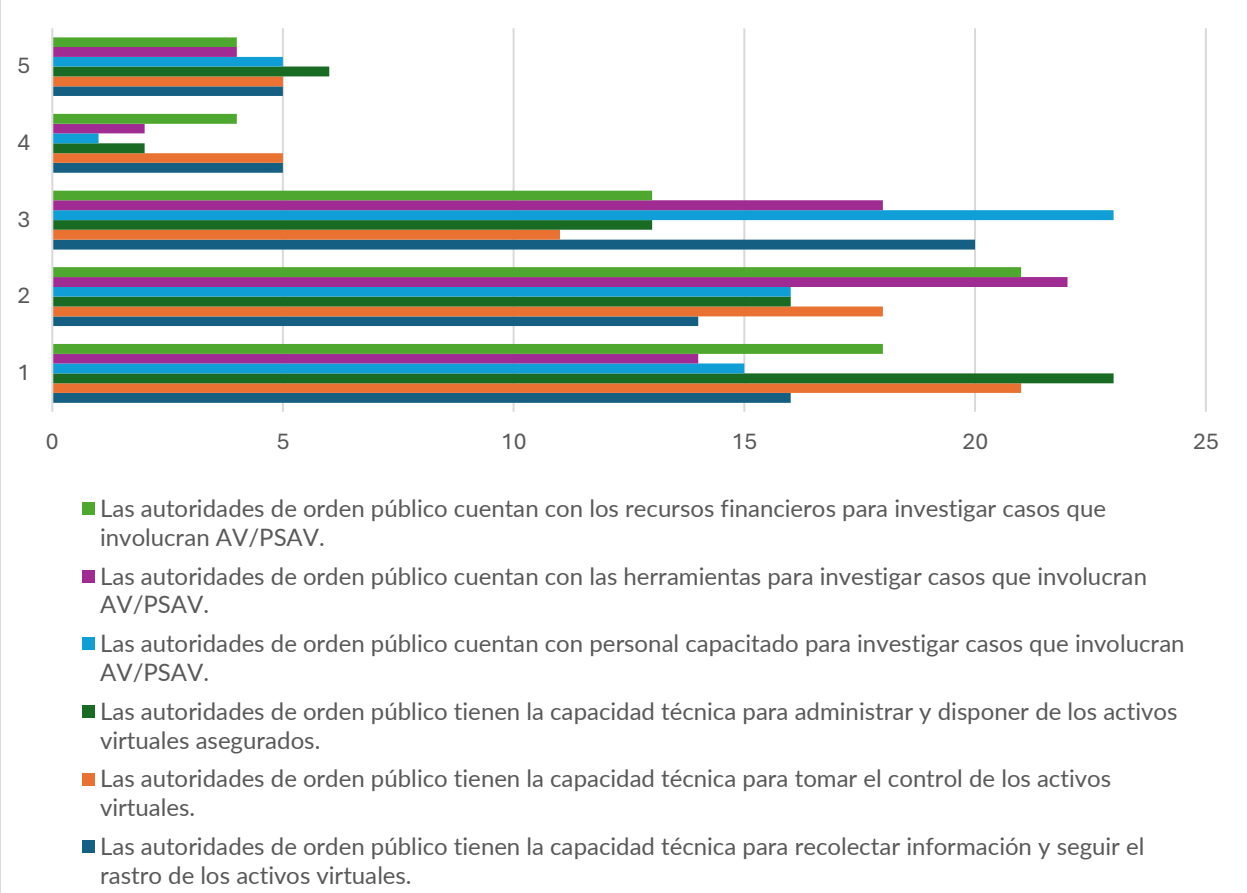
120. Los resultados indican que las autoridades de orden público no están completamente de acuerdo con la efectividad del sistema en cuanto a la investigación, procesamiento y sentencia de los delitos que involucran AV y PSAV. El desacuerdo aumenta progresivamente desde la investigación hasta la sentencia, lo que sugiere que, aunque algunos delitos puedan ser investigados, hay una disminución en la efectividad a medida que los casos avanzan a través del sistema judicial, con menos delitos siendo procesados y aún menos siendo sentenciados. La dispersión moderada en las respuestas indica una variedad de percepciones entre las autoridades, aunque la tendencia general es hacia el desacuerdo.

121. Por otro lado, se evaluaron seis afirmaciones sobre las capacidades técnicas y los recursos de las autoridades de orden público en relación con la investigación y manejo de AV y PSAV. De forma análoga, se utilizó una escala de Likert de 1 a 5 (1 = totalmente en desacuerdo, 5 = totalmente de acuerdo), para recabar el grado de acuerdo con las siguientes afirmaciones:

- Las AOP cuentan con los recursos financieros para investigar casos que involucran AV/PSAV
- Las AOP cuentan con las herramientas para investigar casos que involucran AV/PSAV
- Las AOP cuentan con personal capacitado para investigar casos que involucran AV/PSAV
- Las AOP tienen la capacidad técnica para administrar y disponer de los AV asegurados
- Las AOP tienen la capacidad técnica para tomar el control de los AV
- Las AOP tienen la capacidad técnica para recolectar información y seguir el rastro de los AV

122. Los resultados indican que las autoridades de orden público no se perciben completamente equipadas técnica o financieramente para manejar casos que involucran AV/PSAV. Aunque hay una variabilidad en las respuestas, la tendencia general es hacia el desacuerdo en todas las afirmaciones evaluadas.

Gráfico 12 Grado de acuerdo de las AOP sobre sus capacidades técnicas y recursos en relación con los AV/PSAV



iv. Facultades legales de las UIF

123. Se consultó a las UIF sobre los principales desafíos que enfrentan al monitorear y prevenir actividades ilícitas relacionadas con AV/PSAV. Las respuestas indican que las UIF enfrentan múltiples desafíos en el monitoreo y prevención de actividades ilícitas relacionadas con AV y PSAV. Entre los más destacados se encuentran la falta de un marco regulatorio adecuado y la necesidad de herramientas tecnológicas avanzadas.

124. Las UIF indicaron que la solicitud de información en materia de investigaciones de AV ha sido una práctica común en diversas jurisdicciones, aunque con variaciones en la frecuencia y el alcance de dichas solicitudes. En varios casos, se ha requerido información a los PSAV y a otros sujetos obligados dentro del marco de los análisis llevadas a cabo por las UIF. Estas solicitudes se han dirigido tanto a entidades nacionales como a UIF homólogas y otras autoridades internacionales. Por ejemplo, en Ecuador se ha solicitado información específica a un PSAV identificado. En otros contextos, como en Paraguay, la UIF ha recibido solicitudes de información del Ministerio Público en relación con operaciones con activos virtuales. Además, en investigaciones sobre AV, se ha requerido la verificación de flujos financieros dentro de la blockchain utilizando herramientas de trazabilidad.

125. En contraste, algunas jurisdicciones informan que no se han requerido este tipo de solicitudes. Esto puede deberse a que aún no se han identificado negocios o personas naturales que presten servicios como PSAV en esas áreas. La ausencia de solicitudes también puede reflejar una falta de regulación o de mecanismos formales para abordar el tema.

126. Las respuestas destacan una falta de uniformidad en la práctica de solicitar información sobre AV, influenciada en gran medida por la ausencia de regulación y la identificación de PSAV en cada jurisdicción. Mientras que algunas UIF están activamente solicitando y recibiendo información tanto a nivel nacional como internacional, otras aún no han formalizado estas prácticas.

127. Esta situación resalta la necesidad de desarrollar y armonizar regulaciones y mecanismos de cooperación internacional que faciliten un intercambio de información eficiente y efectivo, facilitando así las investigaciones sobre actividades ilícitas relacionadas con AV. Además, es crucial fortalecer las capacidades técnicas y operativas de las UIF para el uso de herramientas avanzadas de trazabilidad y análisis de blockchain.

c. Capacidades técnicas en relación con los activos virtuales

i. Las autoridades del orden público

128. Respecto a las capacidades técnicas existentes de las autoridades de investigación, se observa en el Gráfico 12 sobre el Grado de acuerdo de las AOP sobre sus capacidades técnicas y recursos en relación con los AV/PSAV, que el promedio de respuesta de 2.48 indica un ligero desacuerdo respecto a la capacidad técnica de las autoridades para recolectar información y rastrear activos virtuales. Con un promedio de 2.25, las autoridades muestran un desacuerdo más fuerte en cuanto a su capacidad para tomar el control de estos activos, reflejando una tendencia clara hacia el desacuerdo. Finalmente, el promedio de 2.20 evidencia un desacuerdo aún mayor sobre su capacidad técnica para administrar y disponer de los activos virtuales asegurados. De tal forma que las percepciones sobre la capacidad técnica para recolectar información y seguir el rastro de los AV resultan ligeramente superiores a las capacidades para tomar el control y administrar estos activos.

ii. Capacidades de las UIF

129. Un elemento crucial por considerar es la capacidad de las UIF, y conocer si han tenido experiencia en la producción de inteligencia relacionada con PSAV. Para ello se consultó si los PSAV reportaban operaciones sospechosas, más allá de considerar las obligaciones que pudieran estar impuestas. Igualmente, se preguntó si habían analizado o compartido información en casos que involucraran PSAV, y si tenían mecanismos de colaboración con los reguladores de PSAV en el país.[17]

[17] Conviene aclarar que sólo algunos países han designado a la autoridad de supervisión de PSAV.

Tabla 16 Experiencia de las UIF con casos que involucran PSAV

Pregunta	Sí	No
¿Los PSAV reportan operaciones sospechosas?	8	8
¿La UIF ha analizado o investigado casos vinculados con PSAV?	10	6
¿La UIF ha compartido información o cooperado con sus homólogas extranjeras en casos que involucran PSAV?	9	7
¿La UIF tiene algún mecanismo de colaboración o intercambio de información con los reguladores y supervisores de los PSAV en el país?	9	7

130. Como se puede ver, incluso en los casos donde los PSAV no reportan operaciones sospechosas, las UIF han tenido que analizar casos que involucran AV y PSAV. Igualmente, algunas UIF de países en los que los PSAV no presentan ROS han debido compartir información o cooperar con sus homólogas extranjeras, o bien, tienen algún mecanismo de colaboración o intercambio de información con los reguladores y supervisores de los PSAV en el país.

Cuadro 4 Informe de inteligencia emitido por la UIF Perú

Entre "el 2016 al 2020, la UIF-Perú emitió un IIF [informe de inteligencia financiera] por un monto de USD 99 mil que incluyó uno de los ROS relacionados con AV. Este IIF estuvo relacionado con el fraude BEC, registrando operaciones internacionales con Venezuela y Colombia, y operaciones nacionales en los departamentos de Lima y Junín. Asimismo, en el citado IIF, se reportaron a siete (7) personas naturales (3 peruanos, 3 venezolanos y 1 colombiano) y una (1) persona jurídica del sector de intermediación financiera."

Fuente: SBS, s.f.b, p. 183

131. Además, algunas UIF han desarrollado estudios estratégicos sobre activos virtuales, como parte de sus planes nacionales ALA/CFT. Estas investigaciones a menudo se apoyan en herramientas públicas o de fuente abierta para realizar análisis detallados.

iii. Coordinación interinstitucional y colaboración

132. Otros dos aspectos fundamentales para analizar son los de cooperación internacional y coordinación interinstitucional, en la medida que se expande la adopción de los AV en la región.

133. Se consultó a las AOP sobre la cooperación y coordinación existente con las autoridades de tecnología o financieras en relación con AV/PSAV y LA/FT. 34 respuestas indicaron que sí existía cooperación y ofrecieron una explicación sobre el tipo de cooperación. Sin embargo, 16 AOP indicaron que no existía este tipo de cooperación y coordinación, 2 no respondieron y 8 dieron respuestas inválidas. Esto indica que aún cabe mejorar el tipo de coordinación y cooperación a fin de mejorar las investigaciones que involucren AV y PSAV.

134. Respecto a los procesos o mecanismos utilizados para compartir datos y conocimientos en casos de investigaciones conjuntas relacionadas con AV y PSAV, 37 AOP indicaron que existen y de forma general, explicaron dichos mecanismos. Por otro lado, 14 indicaron que no existían esos

procesos o mecanismos, aunado a 5 que desconocían si existían, 2 más que no respondieron y 2 que respondieron de forma inválida.

135. En cuanto a requerimientos de información, 32 AOP respondieron que no se ha requerido información en materia de investigaciones de activos virtuales, 2 desconocían si se había requerido y 2 no respondieron. De esa manera, 24 AOP informaron que sí han realizado requerimientos en este sentido.

136. Los datos indican que, si bien existe un grado de coordinación y colaboración interinstitucional en varias jurisdicciones, la falta de uniformidad y la ausencia de mecanismos robustos de compartición de información puede crear vulnerabilidades significativas. Mejorar estos aspectos podría fortalecer las capacidades investigativas y la efectividad en la lucha contra el LA/FT en el contexto de los AV.

137. Al consultar a las UIF sobre su grado de cooperación y coordinación con las autoridades de tecnología y las autoridades financieras o de seguridad pública, las respuestas recibidas indican que el marco normativo específico para la regulación de AV y PSAV se encuentra en desarrollo en muchos países. A pesar de esta situación, se han implementado diversas iniciativas para promover la cooperación y coordinación entre las autoridades tecnológicas, financieras y de seguridad pública en relación con la prevención del LA/FT.

138. Varias jurisdicciones han establecido mecanismos formales e informales de intercambio de información. Por ejemplo, en Chile existe la Mesa Intersectorial contra el Lavado de Activos y el Financiamiento del Terrorismo, que reúne a distintas instituciones públicas para coordinar actividades y estrategias relacionadas con AV/PSAV. En Cuba, la Resolución No. 215 de 2021 creó el "Grupo de Criptoactivos" como órgano asesor del Banco Central, integrado por representantes de varias agencias gubernamentales para evaluar proyectos y políticas relacionadas con criptoactivos.

139. En algunos casos, las UIF han impulsado mesas de trabajo y han coordinado con AOP y ministerios tecnológicos para usar herramientas tecnológicas avanzadas en el rastreo de transacciones en blockchain. En México, las autoridades ALA/CFT han establecido convenios de colaboración y mesas de trabajo que incluyen el intercambio de información y acceso a aplicaciones de inteligencia para la prevención de delitos relacionados con AV/PSAV. Por otra parte, la UIF de El Salvador ha gestionado distintas mesas de trabajo con las AOP, especialmente los supervisores y la Fiscalía General para trabajar casos en conjunto relacionados a AV. Esta práctica ha tenido resultados favorables para el congelamiento de criptomonedas.

d. Infraestructura tecnológica y herramientas insuficientes

i. Recursos para investigar de las autoridades investigativas

140. En cuanto a la disponibilidad de recursos, se consultó a las autoridades de investigación sobre el personal, las herramientas y el aspecto presupuestal más general. Un promedio de 2.42 sugiere un ligero desacuerdo en cuanto a la disponibilidad de personal capacitado para investigar casos relacionados con AV/PSAV, mientras que un promedio de 2.33 refleja una percepción similar respecto a la disponibilidad de herramientas necesarias para dichas investigaciones. Además, el promedio de 2.25 denota un desacuerdo más fuerte sobre la disponibilidad de recursos financieros, lo que destaca la percepción generalizada de una falta de recursos financieros entre las autoridades para investigar casos de AV/PSAV.

141. Con base en lo anterior, es posible decir que hay una percepción de insuficiencia tanto en personal capacitado como en herramientas necesarias para investigar estos casos; aunado a ello, las autoridades también consideran que no cuentan con suficientes recursos financieros para llevar a cabo investigaciones efectivas en esta área. Lo anterior sugiere la necesidad de mejoras significativas en capacitación, herramientas y asignación de recursos para fortalecer las capacidades de las autoridades en este ámbito.

ii. Recursos para las UIF

142. En varias jurisdicciones, se han realizado investigaciones utilizando herramientas disponibles en la web para la trazabilidad de activos a través de la blockchain. Algunos países informan que sus UIF realizan investigaciones tecnológicas específicas en materia de AV y PSAV, a veces en coordinación con la fiscalía o utilizando plataformas tecnológicas de código abierto. Por ejemplo, hay casos donde se ha realizado el análisis de transacciones sospechosas a través de registros de blockchain en internet, estableciendo la trazabilidad y movimientos de los activos virtuales.

143. En contraste, algunas respuestas indican que no se realizan actualmente investigaciones tecnológicas específicas sobre AV debido a la falta de herramientas especializadas. En ciertos países, las UIF carecen de instrumentos tecnológicos necesarios para llevar a cabo tales investigaciones.

144. El análisis de las respuestas a las encuestas destaca la variabilidad en la capacidad de las UIF para realizar análisis avanzados en el ámbito de los AV. Las UIF indicaron que requieren acceso a herramientas especializadas para rastrear y analizar transacciones de AV/PSAV, y enfrentan dificultades debido al uso de tecnologías que ocultan el beneficiario final y la utilización de jurisdicciones no cooperantes.

e. Licenciamiento o registro y supervisión efectiva a los PSAV

i. Reguladores y supervisores FINTECH y PSAV[18]

145. Los reguladores y supervisores de los PSAV son quienes tienen el primer contacto con estos proveedores, por lo que fue fundamental consultarles. Su participación permite identificar áreas que requieran una mayor coordinación, cerrar posibles brechas en la supervisión y garantizar que los marcos regulatorios estén alineados para prevenir actividades ilícitas. Además, la inclusión de reguladores y supervisores especializados facilita la promoción de una cultura de cumplimiento más sólida en el ecosistema de los PSAV. Su conocimiento específico contribuye al desarrollo de políticas que aborden las particularidades del sector de manera efectiva.

146. Los resultados de las encuestas indican que, en varios países de la región, se han implementado regulaciones y directrices específicas para el uso de tecnologías subyacentes como blockchain y tecnología de registro distribuido (DLT, por sus siglas en inglés) lo que refleja un reconocimiento y adaptación a las innovaciones tecnológicas; al mismo tiempo, aún hay necesidad de marcos regulatorios que aborden estas tecnologías.[19]

ii. Reguladores tecnológicos

147. Las autoridades tecnológicas poseen un profundo conocimiento sobre las innovaciones, vulnerabilidades y avances tecnológicos intrínsecos a los AV; lo cual es esencial para identificar y evaluar los riesgos específicos asociados con estas tecnologías. Igualmente, se consideró que los riesgos de ciberseguridad son prominentes en el ámbito de los activos virtuales; por lo que los reguladores tecnológicos pueden aportar perspectivas focalizadas sobre cómo las brechas de seguridad podrían ser explotadas para fines delictivos.

148. De igual forma, conforme al enfoque adoptado, una comprensión efectiva de los riesgos de LA/FT asociados a los AV y PSAV requiere un abordaje multidisciplinario. La inclusión de estas autoridades busca asegurar que los marcos regulatorios integren tanto los aspectos financieros como los tecnológicos, lo cual permite una supervisión más integral y eficaz. Esta participación diversa fomenta la colaboración interinstitucional y el intercambio de información, contribuyendo al fortalecimiento de las estrategias nacionales en materia de ALA/CFT.

149. Cuatro reguladores tecnológicos respondieron a la encuesta, Bolivia, Ecuador, México y Uruguay. Con base en las respuestas recibidas, es posible indicar:

- No existen regulaciones o directrices tecnológicas relacionadas con el uso de tecnologías subyacentes, como blockchain o tecnología de registro distribuido (DLT por sus siglas en inglés).

[18] Debido a que en varios países no existe un regulador de PSAV se optó por ampliar el alcance y solicitar información a los reguladores FINTECH.
[19] Se recibieron 19 respuestas, de 12 países.

- No existe regulación de la tecnología blockchain en términos de seguridad, privacidad y cumplimiento de las leyes ALA/CFT.
- Los reguladores tecnológicos no participan en el otorgamiento de licencias o autorizaciones a empresas que operan con activos virtuales y blockchain en su país.
- Los reguladores tecnológicos no implementan ni han participado en la implementación de programas de educación y concientización dirigidos a la industria tecnológica y a los usuarios de AV para promover buenas prácticas y la identificación de riesgos LA/FT.[20]

iii. Supervisión del sector financiero tradicional

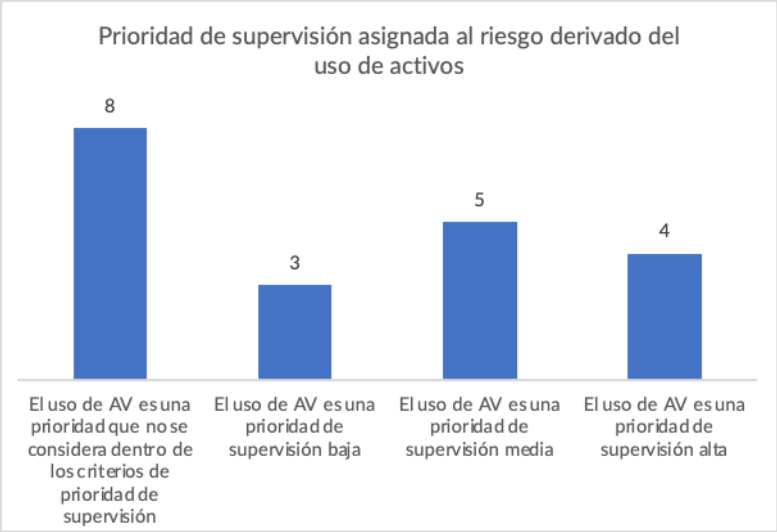
150. Se consideró esencial explorar la prioridad asignada al riesgo derivado del uso de AV en la determinación de prioridades de supervisión del sector financiero tradicional debido a la importancia de la relación entre las instituciones financieras tradicionales y los PSAV. Entre otras cosas, se valoró que los riesgos asociados con los AV pueden afectar indirectamente a las instituciones financieras tradicionales, incluso si no operan directamente con AV o PSAV. Los clientes de estas instituciones pueden interactuar con AV a través de terceros, y no reconocer estos riesgos podría generar puntos ciegos en la gestión de riesgos. Incluir el riesgo de AV en las prioridades de supervisión permitiría detectar tempranamente posibles vulnerabilidades que inicialmente podrían no ser visibles, pero que podrían desarrollarse a medida que se difunde el uso de AV.

151. Como se indicó, se recibieron 20 respuestas de diferentes supervisores financieros, a quienes se les consultó si supervisaban que las instituciones financieras aplicaran medidas de debida diligencia en cuanto a la relación comercial con los clientes usuarios de AV. Las respuestas indican que en 11 casos no se supervisa, y que 9 sí supervisan.

152. En cuanto a la prioridad de supervisión, la mayoría de los supervisores financieros que respondieron la encuesta no consideran el uso de AV como una alta prioridad de supervisión. Esto podría deberse a una variedad de factores, incluyendo la falta de comprensión de los riesgos, la ausencia de marcos regulatorios claros o recursos limitados para la supervisión. Sin embargo, hay una creciente conciencia en algunas áreas sobre la necesidad de supervisar las actividades relacionadas con AV, como lo indica el grupo que las clasifica como una prioridad media o alta.

Gráfico 13 Prioridad de supervisión asignada al riesgo derivado del uso de activos virtuales

[20] Se puede consultar más información en el anexo sobre medidas de ciberseguridad.



153. Respecto a las medidas correctivas y sancionatorias a alguna entidad supervisada en materia de AV, se recibieron únicamente cuatro respuestas. Dentro de las medidas correctivas y sancionatorias implementadas están:

- Multas.
- Programas de control de fiscalización.
- Medidas correctivas dirigidas a las entidades vigiladas con el objetivo de fortalecer la gestión del riesgo LA/FT.
- Medidas preventivas.
- Emisión de recomendaciones para implementar monitoreos diferenciados que aborden las nuevas amenazas en el mercado de AV, así como procesos de identificación que conduzcan a una aplicación efectiva de la regla de viaje o una identificación correcta de los beneficiarios reales en las operaciones financieras.

Cuadro 5 Deficiencias identificadas en la supervisión de entidades financieras tradicionales con clientes de AV y PSAV

Respecto a las deficiencias anotadas en la supervisión de las entidades financieras que operan o tienen clientes usuarios de AV y/o PSAV, cinco supervisores financieros indicaron:

- La ausencia de un marco regulatorio integral para los activos virtuales genera un desconocimiento significativo por parte de las entidades vigiladas y una dependencia excesiva en los originadores y operadores de transacciones criptográficas.
- A diferencia de los entornos financieros tradicionales, donde los factores de riesgo son más fáciles de monitorear, en el mercado criptográfico la información para las entidades financieras depende de la voluntad de sus clientes, dificultando el seguimiento y control de riesgos.
- La naturaleza dinámica e innovadora del mercado de AV complica la implementación de herramientas tecnológicas adecuadas para el monitoreo efectivo, impactando la capacidad para prevenir y mitigar riesgos de manera proactiva.

- La falta de conocimiento específico sobre productos, así como manuales desactualizados de prevención de lavado de activos reflejan una deficiencia en la estructuración de contextos y el empleo de herramientas de monitoreo y validación, lo que requiere una mayor inversión en recursos para gestionar adecuadamente los riesgos.

154. Cabe añadir que siete supervisores financieros indicaron que se han llevado a cabo capacitaciones dirigidas a los sujetos obligados en materia de AV. Estos eventos incluyen sesiones de capacitación con expertos internacionales, campañas de sensibilización, así como eventos tanto virtuales como presenciales.

155. Como se señaló anteriormente, los supervisores financieros desempeñan un papel crucial en la formación de la conducta y cultura del sector financiero tradicional. Por ello, su rol puede facilitar la adaptación proactiva del sector a las innovaciones tecnológicas y a las nuevas formas de operaciones financieras, asegurando así su preparación para los desafíos futuros.

156. Durante la mesa de trabajo de Perú, se conocieron en mayor detalle dos iniciativas regulatorias experimentales enfocadas en los AV y PSAV. En Colombia y Honduras, donde se están implementando estas iniciativas, la regulación de AV y PSAV se encuentra en una etapa preliminar. Estas iniciativas representan enfoques proactivos para interactuar con el sector de AV y PSAV, lo que ha facilitado una comprensión más profunda de sus dinámicas operativas y desafíos específicos. Este enfoque iterativo y colaborativo contribuye a crear un entorno que promueve la innovación, protege los derechos de los usuarios y facilita el abordaje efectivo de los retos que presentan los AV y PSAV.

iv. Colaboración con los supervisores financieros

157. Dentro de las respuestas proporcionadas por los supervisores financieros, las agencias encuestadas indicaron los esfuerzos realizados en materia de cooperación y coordinación entre las autoridades de tecnología, financieras y de AOP en relación con los riesgos de LA/FT de los AV/PSAV. Entre esos esfuerzos destaca el caso colombiano del año 2020, cuando la implementación de un proyecto piloto por parte de entidades vigiladas facilitó la creación de canales de comunicación y coordinación con diversas entidades gubernamentales, incluyendo la Consejería Presidencial, el Ministerio de Hacienda, el Ministerio de Tecnologías de la Información, y otras instituciones clave. Este proyecto permitió la cooperación interinstitucional y el intercambio de información esencial.

158. Por otro lado, para los países de Centroamérica, Colombia y República Dominicana, el Consejo Centroamericano de Superintendentes de Bancos, Seguros y Otras Instituciones Financieras (CCSBSO) ha sido fundamental en el intercambio de experiencias y evaluaciones de amenazas y vulnerabilidades en la región. Particularmente, el Comité Técnico de Prevención de LA/FT ha seguido de cerca los avances normativos en cada país.

159. En Bolivia, la ASFI firmó un convenio de cooperación con la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) para intercambiar información sobre actividades de supervisión y procedimientos sancionadores relacionados con el riesgo de legitimación de ganancias ilícitas y FT.

f. Características intrínsecas de los AV

160. Los PSAV encuestados compartieron sus vulnerabilidades y riesgos operativos, de los cuales se retoman únicamente aquellos relevantes para esta ESR.

- Fallas en la implementación de seguridad. Las debilidades en la implementación de medidas de seguridad, como cifrado inadecuado o autenticación débil, pueden exponer la plataforma a riesgos de seguridad.
- Desarrollo de aplicaciones inseguras. Las vulnerabilidades en el desarrollo de aplicaciones, como fallos de seguridad en códigos, pueden ser aprovechadas por los atacantes para comprometer la seguridad de la plataforma.
- Problemas de privacidad. La recopilación y gestión de grandes cantidades de datos personales pueden plantear riesgos de privacidad si no se implementan adecuadamente medidas de protección de datos.
- Desconocimiento del funcionamiento de la tecnología por parte de grupos vulnerables. La falta de conocimiento respecto a qué son las criptomonedas y cómo funciona esta tecnología tan reciente, en algunas oportunidades puede llevar a los usuarios a creer en información que no es fidedigna, a creer ofertas con recompensas que no son realistas, a actuar impulsivamente, a recibir asesoría por parte de sujetos y empresas sin ninguna autorización para brindar asesoramiento en materia de inversión y, en conclusión, expone al usuario al riesgo de ser víctima de delitos como la estafa.
- Riesgos tecnológicos emergentes. La rápida evolución de la tecnología en el espacio de AV puede presentar nuevos riesgos, como vulnerabilidades de contratos inteligentes o problemas de seguridad en nuevas tecnologías blockchain.

i. Ciberseguridad y protección de datos

161. Aunado a lo anterior, los PSAV encuestados también han adoptado diversas estrategias y prácticas para salvaguardar los datos y fondos de sus usuarios. Entre estas prácticas están:

- Cifrado de extremo a extremo: Protege la confidencialidad de la información tanto en tránsito como en reposo.
- Cifrado SSL/TLS: Garantiza la seguridad en todas las transferencias de datos hacia y desde los usuarios.
- Autenticación multifactorial (MFA): Implementa varios métodos de verificación para acceder a las cuentas de los usuarios, incluyendo la autenticación de dos factores (2FA) como medida obligatoria.
- Políticas de acceso y control de privilegios: Limita los privilegios de usuario para minimizar el riesgo de accesos no autorizados.

- Firewalls y sistemas de prevención de intrusiones: Protegen la red contra ataques externos.
- Segmentación de la red: Minimiza vulnerabilidades y protege la infraestructura de red.
- Almacenamiento en frío y billeteras multifirma: Custodia segura de activos criptográficos, con la mayoría de los fondos en almacenamiento seguro.
- Monitoreo en tiempo real: Detecta y responde rápidamente a actividades sospechosas.
- Planes de respuesta a incidentes: Establece procedimientos para actuar ante brechas de seguridad.
- Entrenamiento en seguridad: Formación continua para empleados y usuarios sobre las mejores prácticas de ciberseguridad.
- Cultura de seguridad: Fomenta una cultura organizacional que prioriza la ciberseguridad.
- Auditorías regulares: Evaluaciones periódicas para identificar y corregir vulnerabilidades.
- Certificaciones de seguridad: Cumplimiento con estándares internacionales como SOC 2 e ISO 27001.
- Políticas de respaldo de datos: Copias de seguridad periódicas para garantizar la recuperación de datos.
- Actualizaciones y parches de seguridad: Mantenimiento continuo de sistemas y aplicaciones para proteger contra vulnerabilidades.
- Herramientas avanzadas de seguridad: Uso de software antivirus, detección de intrusos y monitoreo continuo para mitigar amenazas.

g. Análisis de las vulnerabilidades

162. Todas las vulnerabilidades identificadas por todos los participantes de este estudio fueron agrupadas en temas principales y a continuación se enlistan:

Tabla 17. Análisis de las vulnerabilidades

Vulnerabilidades	Contenido

a. Desconocimiento y falta de capacitación	El desconocimiento generalizado y la falta de capacitación impiden la correcta regulación, supervisión e investigación del sector de AV. Sin una comprensión adecuada, es difícil aplicar un enfoque basado en riesgos y garantizar el cumplimiento de las medidas de ALA/CFT.
	
	Esta vulnerabilidad comprende:
	• Falta de comprensión del sector por parte de:
	  ○ Autoridades gubernamentales.
	  ○ Sector financiero tradicional.
	  ○ Proveedores de Servicios de Activos Virtuales (PSAV).
	  ○ Población en general.
	• Los PSAV carecen de conciencia sobre la importancia del cumplimiento regulatorio.

b. Marco jurídico insuficiente	Sin leyes y regulaciones claras, las autoridades carecen de herramientas legales para supervisar, investigar y sancionar actividades ilícitas. La disparidad normativa dificulta la cooperación nacional e internacional. Esta vulnerabilidad comprende: • Falta de regulación integral en materia de ALA/CFT y operación de PSAV. • Disparidad normativa y ausencia de unificación de criterios a nivel regional. • Carencia de facultades de las autoridades de orden público. • Falta de licenciamiento, registro y supervisión de PSAV. • Marco sancionatorio insuficiente o inadecuado. • Necesidad de normativa prudencial para PSAV.
c. Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV	La incapacidad para investigar y procesar eficazmente los delitos relacionados con AV y PSAV permite que las actividades ilícitas prosperen con facilidad. Esta vulnerabilidad comprende: • Limitaciones en la comprensión del sector y aplicación de la ley a delitos relacionados con AV. • Falta de trabajo articulado entre las fuerzas del orden. • Carencia de personal especializado y recursos adecuados.
d. Infraestructura tecnológica y herramientas insuficientes	Sin la infraestructura tecnológica adecuada, las autoridades y los supervisores no pueden detectar, monitorear ni investigar eficazmente las actividades relacionadas con AV. Esta vulnerabilidad comprende: • Recursos limitados para adquirir herramientas tecnológicas avanzadas. • Infraestructura inadecuada para supervisión e investigación. • Necesidad de herramientas de análisis de blockchain y otras tecnologías relevantes.
e. Falta de supervisión a PSAV	La supervisión inadecuada permite que los PSAV funcionen sin cumplir con las obligaciones legales, aumentando el riesgo de uso indebido de los AV para actividades ilícitas.

	Esta vulnerabilidad comprende: • Los PSAV operan sin supervisión efectiva en materia de ALA/CFT. • Los supervisores carecen de comprensión y experiencia para supervisar el sector de manera efectiva. • Ausencia de reportes por parte de los sujetos obligados.
f. Características intrínsecas de los AV	Si bien estas características facilitan la innovación y eficiencia en el sector financiero, también presentan desafíos significativos para la prevención y detección de actividades ilícitas. Sin embargo, su impacto puede mitigarse si se abordan adecuadamente las vulnerabilidades anteriores. Esta vulnerabilidad comprende: • Anonimato y pseudonimato. • Intercambio Peer-to-Peer (P2P). • Alcance global y velocidad de las transacciones. • Ecosistemas descentralizados (smart contracts y DApps). • Menor costo de las operaciones.

i. Priorización de las vulnerabilidades

163. Los representantes regionales discutieron el orden de importancia de las vulnerabilidades y su prioridad de atención. Con base en esas discusiones y conclusiones, se determinó que el orden de prioridad de las vulnerabilidades es el siguiente.

Tabla 18. Descripción de las vulnerabilidades

Prioridad	Vulnerabilidad	Descripción

1	**Desconocimiento y falta de capacitación**	• Falta de comprensión del sector por parte de:
		  • Autoridades gubernamentales.
		  • Sector financiero tradicional.
		  • Población en general.
		• Los PSAV carecen de conciencia sobre la importancia del cumplimiento regulatorio.

	Marco jurídico insuficiente	• Falta de regulación integral en materia de ALA/CFT y operación de PSAV. • Disparidad normativa y ausencia de unificación de criterios a nivel regional.

		• Carencia de facultades de las autoridades de orden público. • Falta de licenciamiento, registro y supervisión de PSAV. • Marco sancionatorio insuficiente o inadecuado. • Necesidad de normativa prudencial para PSAV.
2	**Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV**	• Limitaciones en la comprensión del sector y aplicación de la ley a delitos relacionados con AV. • Falta de trabajo articulado entre las fuerzas del orden. • Carencia de personal especializado y recursos adecuados.
3	**Infraestructura tecnológica y herramientas insuficientes**	• Recursos limitados para adquirir herramientas tecnológicas avanzadas. • Infraestructura inadecuada para supervisión e investigación. • Necesidad de herramientas de análisis de blockchain y otras tecnologías relevantes.
4	**Falta de supervisión efectiva a los PSAV**	• Los PSAV operan sin supervisión efectiva en materia de ALA/CFT. • Los supervisores carecen de comprensión y experiencia para supervisar el sector de manera efectiva. • Ausencia de reportes por parte de los sujetos obligados.
5	**Características intrínsecas de los AV**	• Anonimato y pseudonimato. • Intercambio Peer-to-Peer (P2P). • Alcance global y velocidad de las transacciones. • Ecosistemas descentralizados (smart contracts y DApps). • Menor costo de las operaciones

164. Abordar las vulnerabilidades relacionadas con el desconocimiento y falta de capacitación; así como con el marco jurídico insuficiente tendrán el mayor impacto transversal. Sin una comprensión adecuada de los AV y la operación de los PSAV, aunado a un marco jurídico integral sólido, es imposible abordar eficazmente las otras vulnerabilidades.

165. La falta de capacidad de investigación y procesamiento de delitos se ubica en segundo lugar, ya que es fundamental que las autoridades posean capacidades y personal altamente calificados en la materia a fin de perseguir y sancionar actividades ilícitas relacionadas con los AV y PSAV para disuadir su ocurrencia.

166. La infraestructura tecnológica y las herramientas son prioritarias para respaldar las funciones de supervisión e investigación. Sin las herramientas adecuadas, incluso con las autoridades capacitadas y con un marco legal sólido, las jurisdicciones se enfrentarían a diversas dificultades.

167. La falta de supervisión a PSAV se considera en cuarto lugar, dado que una supervisión efectiva depende de la comprensión del sector, un marco legal adecuado y contar con los recursos tecnológicos necesarios.

168. Las características intrínsecas de los AV se ubican en último lugar, ya que, aunque presentan desafíos inherentes, su impacto puede mitigarse si se abordan eficazmente las vulnerabilidades anteriores.

ii. Calculando las vulnerabilidades

169. Según la metodología, y en el mismo sentido que las amenazas, se asignaron calificaciones numéricas inversas para reflejar la magnitud de la prioridad, siendo 5 la mayor magnitud y 1 la menor. Por tanto:

Tabla 19. Magnitud de las vulnerabilidades

Vulnerabilidad	Magnitud
Desconocimiento y falta de capacitación	5
Marco jurídico insuficiente	5
Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV	4
Infraestructura tecnológica y herramientas insuficientes	3
Falta de supervisión a los PSAV	2
Características intrínsecas de los AV	1

170. Ahora bien, para obtener el puntaje de las vulnerabilidades, se sumaron las calificaciones del nivel de magnitud que representa cada vulnerabilidad detallada en el cuadro anterior. No obstante, para ejecutar esta sumatoria se realizó un análisis que conllevó a identificar la manera y en qué medida, determinada amenaza puede aprovecharse de ciertos tipos de vulnerabilidades.

Tabla 20. Puntaje de las vulnerabilidades

Amenazas	Vulnerabilidades con mayor interacción respecto de la amenaza	Puntaje de las vulnerabilidades (Sumatoria de las magnitudes)
Fraude y estafas	• Desconocimiento y falta de capacitación • Marco jurídico insuficiente • Infraestructura tecnológica y herramientas insuficientes • Falta de supervisión a los PSAV • Características intrínsecas de los AV	16
Tráfico de estupefacientes y psicotrópicos	• Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV • Infraestructura tecnológica y herramientas insuficientes	8

	• Características intrínsecas de los AV	
Ataques cibernéticos	• Desconocimiento y falta de capacitación • Marco jurídico insuficiente • Infraestructura tecnológica y herramientas insuficientes • Falta de supervisión a los PSAV • Características intrínsecas de los AV	16
Trata de personas	• Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV • Infraestructura tecnológica y herramientas insuficientes • Características intrínsecas de los AV	8
Defraudación tributaria	• Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV • Infraestructura tecnológica y herramientas insuficientes • Características intrínsecas de los AV	8
Corrupción	• Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV • Infraestructura tecnológica y herramientas insuficientes • Características intrínsecas de los AV	8
Uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web.	• Desconocimiento y falta de capacitación • Marco jurídico insuficiente • Infraestructura tecnológica y herramientas insuficientes • Falta de supervisión a los PSAV • Características intrínsecas de los AV	16
Financiamiento del terrorismo	• Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV • Infraestructura tecnológica y herramientas insuficientes • Falta de supervisión a los PSAV • Características intrínsecas de los AV	10

171. Los cálculos del impacto de las distintas vulnerabilidades en la amenaza muestran que las amenazas relacionadas con la explotación de las características inherentes de los activos virtuales para la comisión de diferentes tipos de delitos, como el fraude y estafas, los ataques cibernéticos y el uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web presentan una mayor magnitud de vulnerabilidad con un puntaje de 16. Continúa el financiamiento al terrorismo con un puntaje de 10, y las amenazas de que los AV se utilicen para facilitar el lavado de recursos

y activos de otros delitos, como lo son el tráfico de drogas, la trata de personas, los delitos tributarios y la corrupción obtuvieron un puntaje de vulnerabilidad de 8.

172. De forma particular, en relación con el financiamiento al terrorismo, es de mencionar que a pesar de que en la región este delito no presenta una mayor la amenaza, se reconoce que los AV pueden ser vulnerados para el FT. En este sentido, se identificaron como vulnerabilidades la falta de capacitación e infraestructura tecnológica para investigar el uso de los AV para el FT, así como las debilidades en la supervisión de los PSAV y las características intrínsecas de los AV. No obstante, la magnitud definida para estas vulnerabilidades no está dentro de los primeros lugares.

173. Finalmente, se destaca que, en cierto grado, cualquier amenaza indicada en este análisis puede aprovecharse indistintamente de cualquiera de las vulnerabilidades planteadas, es decir que, este análisis no es taxativo, por lo que cada país puede tener una percepción diferenciada conforme a la aplicación de medidas mitigantes propias y en relación con su contexto y materialidad.

VII. PRINCIPALES RIESGOS

174. Según lo definido en la metodología, el nivel de riesgo se calcula sumando los puntajes obtenidos del análisis de las amenazas y las vulnerabilidades. Una vez aplicada la fórmula, se definieron los niveles de exposición al riesgo de LA/FT de los AV y PSAV según la escala descrita en la sección de la metodología.

175. En ese sentido, se muestra un nivel de riesgo muy alto utilizando AV y PSAV para el LA del producto que deriva de los delitos de fraude y estafas, los ataques cibernéticos, y el tráfico de drogas. El lavado de activos producto de la trata de personas tiene un nivel alto de riesgo. Por su parte, el uso de los AV para LA mediante esquemas de defraudación tributaria, la corrupción y el uso ilícito de mixers (o tumblers) y comercio ilícito a través de la dark web, tiene un nivel de riesgo medio.

176. Finalmente, el financiamiento del terrorismo (FT) refleja un riesgo medio para la región. Si bien en términos generales la amenaza se determina baja, el nivel considerable de vulnerabilidad que presenta actualmente el sector de los AV y los PSAV permite concluir que el riesgo de FT en este sector es medio[21].

[21] El análisis del riesgo realizado en esta ESR de AV relacionado al FT, se encuentra en línea con los "Principios Rectores de Argelia" establecidos mediante la RCSNU S/2025/22 del 9 de enero de 2025. Estos principios no vinculantes estipulan la importancia a nivel global sobre la prevención, detección e interrupción del uso de tecnologías financieras nuevas y emergentes con fines terroristas. En particular, hacen énfasis en la comprensión y evaluación de riesgos de FT en estas tecnologías emergentes tales como los AV, los sistemas de pagos móviles y el crowfunding. Estos principios destacan la importancia de la colaboración pública-privada en la materia, del manejo de inteligencia blockchain y de la regulación y supervisión EBR para los PSAV para evitar fines terroristas y de su financiamiento.

177. Particularmente, este nivel de vulnerabilidad se ve acentuado por el hecho de que las organizaciones terroristas, a menudo, dependen de donaciones de bajo valor que pueden pasar desapercibidas en los sistemas tradicionales de monitoreo. En lo referente a, los servicios ofrecidos por los PSAV —especialmente mediante operaciones peer-to-peer (P2P), plataformas de redes sociales y entornos de finanzas descentralizadas (DeFi)— pueden facilitar este tipo de financiamiento a pequeña escala pero de alto volumen. Esto puede dificultar significativamente su detección sin el uso de herramientas especializadas y una comprensión profunda del funcionamiento y los riesgos del sector.

Tabla 21. Niveles de riesgo

Amenazas	Vulnerabilidades con mayor interacción respecto de la amenaza	Puntaje de la amenaza	Puntaje de las vulnerabilidades (Sumatoria de las magnitudes)	Nivel de riesgo
Fraude y estafas	• Desconocimiento y falta de capacitación • Marco jurídico insuficiente • Infraestructura tecnológica y herramientas insuficientes • Falta de supervisión a los PSAV • Características intrínsecas de los AV	58	16	74
Tráfico de estupefacientes y psicotrópicos	• Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV • Infraestructura tecnológica y herramientas insuficientes • Características intrínsecas de los AV	43	8	51
Ataques cibernéticos	• Desconocimiento y falta de capacitación • Marco jurídico insuficiente	30	16	46

	• Infraestructura tecnológica y herramientas insuficientes • Falta de supervisión a los PSAV • Características intrínsecas de los AV			
Trata de personas	• Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV • Infraestructura tecnológica y herramientas insuficientes • Características intrínsecas de los AV	21	8	29
Defraudación tributaria	• Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV • Infraestructura tecnológica y herramientas insuficientes • Características intrínsecas de los AV	14	8	22
Corrupción	• Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV • Infraestructura tecnológica y herramientas insuficientes • Características intrínsecas de los AV	12	8	20

Uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web.	• Desconocimiento y falta de capacitación • Marco jurídico insuficiente • Infraestructura tecnológica y herramientas insuficientes • Falta de supervisión a los PSAV • Características intrínsecas de los AV	9	16	25
Financiamiento del terrorismo	• Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV • Infraestructura tecnológica y herramientas insuficientes • Falta de supervisión a los PSAV • Características intrínsecas de los AV	5	10	15

VIII. RECOMENDACIONES PARA MITIGAR LOS RIESGOS IDENTIFICADOS

178. Los países miembros del GAFILAT podrían considerar los siguientes elementos para mitigar los riesgos regionales identificados de acuerdo con las prioridades identificadas.

a. Construcción de un conocimiento más sólido y contextualizado

179. **Emprender esfuerzos para construir un conocimiento más sólido y contextualizado como primer paso; sin embargo, no necesariamente debe iniciarse con una evaluación de riesgos formal de manera inmediata.** Las experiencias analizadas evidencian que realizar una "evaluación de riesgos" sin una etapa previa de exploración y acercamiento al conocimiento de los AV y los PSAV puede resultar en documentos con escasa profundidad técnica y operativa. Por ello, antes de emprender un ejercicio formal de evaluación, sería valioso implementar acciones exploratorias preliminares. Estas acciones deberían estar orientadas a recopilar información cuantitativa y

cualitativa, con el propósito de evaluar aspectos como el grado de conocimiento de la población sobre el tema, el nivel de aceptación de estas nuevas tecnologías, y su posible impacto en productos o sectores económicos tradicionales, entre otros.

180. Para abordar la situación y diseñar una solución a medida, los países **podrían considerar las siguientes preguntas**:

- ¿En la jurisdicción, se usan AV? ¿Se pueden pagar bienes o servicios con AV?
- ¿Qué tipo de personas ofrecen este tipo de servicios o promueven su uso?
- ¿Dónde y cómo se ha verificado el uso de AV?
- ¿Se han conocido casos de uso de AV en hechos punibles o actividades de tinte ilícito?
- ¿Qué nivel de conocimiento y comprensión tiene la población general y los actores clave sobre los AV?
- ¿Cuál es el nivel de la demanda de AV como medio de inversión, pago o reserva de valor?
- ¿Qué sectores económicos o sociales están más inclinados a adoptar o rechazar los AV?
- ¿Qué papel juegan las instituciones financieras locales en la promoción, intermediación o rechazo de los AV?
- ¿Qué retos legales o regulatorios han enfrentado los usuarios o proveedores de AV en el pasado?
- ¿Se han presentado investigaciones, litigios o sanciones vinculadas al uso o la oferta de AV?
- ¿Qué actores podrían beneficiarse o ser perjudicados por el uso de AV en actividades ilícitas?
- ¿Existen plataformas tecnológicas o proveedores de infraestructura en la jurisdicción que faciliten el uso o la custodia de AV?
- ¿Qué nivel de preparación técnica tienen los organismos regulatorios, de supervisión o de investigación para abordar los desafíos relacionados con AV?

181. Algunas **actividades sugeridas** pueden ser:

- Encuestas o formularios a sujetos obligados (inclusive a PSAV) sobre los temas indicados en el párrafo anterior.
- Análisis de ROS que contengan información con relación a operativas ligadas a AV.
- Mesas de diálogo con AOP para identificar uso de AV en la comisión de hechos punibles.
- Capacitaciones que conlleven a itinerarios diferenciados de formación conforme al perfil correspondiente (reguladores, supervisores, personal UIF, policías, fiscales y jueces, entre otros)

b. Acercamiento de los reguladores, supervisores y/o autoridades competentes al sector de PSAV

182. **Una vez encaminada la fase de conocimiento preliminar mencionada anteriormente, sería altamente recomendable fomentar un acercamiento directo con los PSAV con el objetivo de conocer al sector doméstico de primera mano y promover una interacción constructiva con los actores relevantes.** Este proceso puede llevarse a cabo mediante la organización de mesas de

trabajo colaborativas o, alternativamente, mediante el establecimiento de un **registro voluntario**. El registro podría extenderse a personas físicas o jurídicas que acepten o promuevan el uso de AV en sus actividades o que, de alguna manera, operen con dichos activos.

183. El enfoque debe centrarse en **cuantificar y conocer a los actores del sector**. Esto permitirá evaluar la materialidad del sector y, a partir de esa base, desarrollar una **evaluación sectorial del riesgo**. La realización de esta evaluación sectorial, fundamentada en un marco metodológico robusto y en la información obtenida directamente de los actores implicados, garantizará un análisis más profundo y contextualizado. De esta manera se evitarán especulaciones sobre la existencia y características de los actores del sector, ya que ellos mismos participarán activamente en el proceso de evaluación.

c. Evaluación sectorial de riesgos

184. **Una vez explorado el sector y sus actores, e, idealmente, habiendo establecido una alianza estratégica, se puede proceder con una evaluación informada de los riesgos que esta actividad representa para el país**. Este análisis debe basarse en un conocimiento sólido de la actividad y su incidencia, con el objetivo de identificar y abordar de manera integral los aspectos críticos relacionados con el uso de AV y el establecimiento de PSAV.

185. **La evaluación debe considerar los siguientes elementos clave:**

- **Tipos de actividades de los PSAV**: Identificar las diferentes modalidades de operación y servicios ofrecidos por estos actores, así como los tipos de AV con los que operen.
- **Amenazas**: Evaluar cómo las amenazas están usando los AV para facilitar delitos o lavar los activos procedentes de otros delitos, y cómo los PSAV están siendo abusados para fines ilícitos.
- **Vulnerabilidades**: Analizar los puntos débiles del sistema que podrían facilitar el uso indebido de activos virtuales.
- **Mitigación de riesgos**: Diseñar estrategias y mecanismos para mitigar los riesgos identificados, asegurando un enfoque equilibrado que promueva la innovación mientras se minimizan los riesgos.

186. Este enfoque permite desarrollar una evaluación robusta, metodológicamente fundamentada, que refleje las particularidades del contexto nacional y establezca una base sólida para la toma de decisiones regulatorias y operativas.

d. Integración de los hallazgos de la evaluación sectorial de riesgos al marco jurídico

187. Con base en la Evaluación de Riesgos realizada, se sugiere que el marco normativo incorpore la realidad observada, establezca reglas claras para los PSAV, y contemple acciones idóneas para mitigar los riesgos identificados. Es fundamental que este marco no solo atienda los riesgos actuales, sino que también incluya disposiciones para abordar los riesgos emergentes, y asegure la protección de la jurisdicción y, de ser posible, de la región frente a los desafíos que plantea el uso de estas nuevas tecnologías.

188. Si bien es fundamental que los países emitan regulaciones y normativas alineadas con los estándares internacionales, la regulación de los PSAV debe estar fundamentada en los hallazgos específicos del proceso de evaluación de riesgos. Esto significa que las particularidades identificadas en el contexto nacional, como las amenazas, vulnerabilidades y riesgos inherentes, deben guiar el diseño normativo.

189. Al responder a estas realidades locales, la regulación no solo será más efectiva en la mitigación de riesgos, sino que también permitirá una implementación más contextualizada y sostenible.

190. Igualmente importante para el marco jurídico, los países deben garantizar que las AOP cuenten con todas las facultades necesarias para investigar, procesar y sancionar las conductas ilícitas relacionadas con el uso de AV y el abuso de los PSAV. Esto implica dotar a las AOP de herramientas legales específicas que permitan una respuesta efectiva frente a actividades criminales identificadas como amenazas.

191. Asimismo, el marco jurídico debe prever procedimientos claros y eficientes para la recolección, análisis y uso de evidencia digital, así como garantizar la cooperación internacional. Además, debe garantizarse que las sanciones previstas sean proporcionales, efectivas y disuasivas.

e. Establecimiento del control prudencial

192. A partir de un conocimiento profundo del sector y de los elementos que configuran la operativa con AV y sus proveedores, es fundamental establecer y delimitar las competencias del organismo supervisor. Este debe contar con capacidades técnicas, operativas y, especialmente en este ámbito, tecnológicas, que permitan un monitoreo efectivo de las actividades relacionadas con AV y sus proveedores.

193. Es imprescindible reconocer la naturaleza financiera de estas actividades, lo que exige supervisores con habilidades para analizar el sector desde una perspectiva económica e integrar estas operaciones dentro de los servicios financieros. Sin embargo, no basta con comprender los riesgos financieros asociados; es igualmente importante garantizar la trazabilidad de las operaciones y aprovechar las ventajas que ofrece la tecnología. Esto requiere una inversión en sistemas avanzados para monitorear las actividades con AV.

194. La supervisión también debe estar estrechamente coordinada con las AOP para aprovechar oportunidades significativas para investigar y perseguir delitos asociados al uso de AV de manera eficiente y efectiva. Este enfoque colaborativo es esencial para garantizar un equilibrio entre innovación tecnológica, seguridad y cumplimiento normativo.

f. Promover la relación entre el sector financiero tradicional y los PSAV

195. Una relación sólida entre el sector financiero tradicional y los PSAV es clave para fomentar un ecosistema financiero inclusivo, innovador y regulado. Se recomienda la promoción de la capacitación continua para el fomento de una cultura de inclusión entre ambos sectores.

196. Un aspecto crítico para fortalecer esta relación es **evitar el *de-risking***, para lo cual es fundamental promover el enfoque basado en riesgos que permita a las entidades financieras tradicionales evaluar a los PSAV individualmente en lugar de aplicar medidas generalizadas que excluyan al sector. El fomento de una relación fluida no solo mejora la comprensión mutua, sino que también ayuda a reducir las percepciones de riesgo y a generar confianza.

197. Para lograr esa relación sólida y segura, se recomienda lo siguiente:

- Los PSAV deben adoptar y mantener las mejores prácticas ALA/CFT.
- Facilitar programas educativos y sesiones de formación para mejorar el entendimiento de la naturaleza y las operaciones de los PSAV, al tiempo que los PSAV interiorizan las expectativas regulatorias y operativas del sector financiero tradicional.
- Creación de **foros de discusión y mesas redondas periódicas** donde representantes de ambos sectores dialoguen, compartan experiencias y trabajen conjuntamente para identificar oportunidades de colaboración y resolver desafíos regulatorios. Estos espacios permiten una mayor comprensión de las capacidades y limitaciones de cada sector, promoviendo soluciones prácticas y colaborativas que eviten el *de-risking* innecesario.

g. Actualización y mejora continua de los mitigadores de riesgo del sector

198. El fortalecimiento continuo de las medidas mitigantes es importante para garantizar la sostenibilidad en la prevención y gestión de riesgos asociados a los AV y a los PSAV. Para ello, es necesario implementar un enfoque estratégico que integre capacitación, innovación tecnológica y especialización institucional.

199. Un componente esencial para la sostenibilidad es la formación constante de los analistas de las UIF y del personal de otras autoridades competentes. Estos programas deben abarcar aspectos técnicos, regulatorios y operativos relacionados con los AV y PSAV, así como temas emergentes en el ámbito de la tecnología financiera. La capacitación debe incluir el análisis de riesgos específicos, la interpretación de transacciones en blockchain y la identificación de tipologías de uso ilícito. Un enfoque continuo asegura que las autoridades estén actualizadas frente a las amenazas y tendencias globales, permitiendo una respuesta más efectiva y proactiva.

200. La integración de herramientas tecnológicas avanzadas, como soluciones de análisis blockchain, mejorará la detección de transacciones sospechosas y el rastreo de los flujos de AV. La inversión en estas herramientas debe ir acompañada de la capacitación adecuada para maximizar su impacto en las labores de supervisión e investigación.

201. La sostenibilidad de las medidas mitigantes también depende de una colaboración activa entre las autoridades nacionales e internacionales. Es crucial establecer canales de comunicación y cooperación entre reguladores, UIF, cuerpos de seguridad y actores del sector privado, fomentando el intercambio de información y mejores prácticas.

202. Finalmente, las medidas mitigantes deben estar sujetas a una evaluación constante para garantizar su efectividad. Esto incluye la revisión periódica de marcos normativos, la actualización de protocolos de supervisión y el ajuste de estrategias en función de los resultados obtenidos y los cambios en el panorama de riesgos, especialmente las amenazas.

203. Todo lo anterior son recomendaciones que los países pueden implementar o continuar fortaleciendo, buscando, por un lado, regular y promover un uso adecuado de los AV y PSAV, y, por otro, generar herramientas preventivas y de detección cuando este sector es abusado para cometer delitos, incluyendo el LA y FT. En la medida que los países fortalezcan sus sistemas ALA/CFT, el riesgo regional podrá ser mejor administrado.

IX. CONCLUSIONES

204. La adopción de AV en la región del GAFILAT muestra una diversidad de casos de uso que varían según las condiciones económicas de cada país. Mientras que, en algunos países, las criptomonedas se utilizan como una herramienta para mitigar la inflación y facilitar las remesas, en otros mercados han evolucionado hacia un vehículo de inversión especulativa. Estas tendencias indican que la adopción de criptomonedas en Latinoamérica continúa en ascenso. A medida que las tecnologías cripto sigan desarrollándose y las economías latinoamericanas enfrenten nuevos desafíos, es probable que se generen nuevos casos de uso adaptados a las necesidades específicas de la región. Las perspectivas futuras para la industria de AV en América Latina muestran una tendencia de crecimiento, lo que anticipa una mayor integración de los activos virtuales (criptomonedas en particular) en el sistema financiero tradicional y un incremento en la adopción y diversificación de inversiones en la región.

205. Existe información extremadamente limitada de fuentes oficiales que informe el número de PSAV, y que permita caracterizar al sector de forma regional sobre los tipos de servicios ofrecidos, volumen transaccional y otras características de estos proveedores.

206. Aún sería deseable contar con información detallada sobre cómo las amenazas utilizan los activos virtuales y los PSAV en la región, no obstante, con los datos provistos es posible mencionar que las principales amenazas identificadas en relación con los AV y los PSAV son:

- Ataques cibernéticos: Ataques de ingeniería social, hackeo, suplantación de identidad (phishing).
- Uso ilícito de mixers (o tumblers) y comercio ilícito a través de la Dark Web.
- Fraude y estafas de inversión.
- Tráfico de estupefacientes y psicotrópicos.

- Trata de personas.
- Defraudación tributaria.
- Corrupción.
- Financiamiento del terrorismo.

207. Las vulnerabilidades están vinculadas fundamentalmente al poco conocimiento del ecosistema de AV y PSAV por parte de todos los actores ALA/CFT, la cual tiene múltiples consecuencias de forma transversal. Las principales vulnerabilidades identificadas son:

- Desconocimiento y falta de capacitación.
- Marco jurídico insuficiente.
- Falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV.
- Infraestructura tecnológica y herramientas insuficientes.
- Falta de supervisión a PSAV.
- Características intrínsecas de los AV.

208. Considerando estas amenazas y vulnerabilidades, se concluye que en la región los AV y PSAV tienen un nivel de riesgo muy alto para el LA del producto que deriva de los delitos de fraude y estafas, los ataques cibernéticos, y el tráfico de drogas. El lavado de activos producto de la trata de personas tiene un nivel alto de riesgo. Por su parte, el uso de los AV para LA mediante esquemas de defraudación tributaria, la corrupción y el uso ilícito de mixers (o tumblers) y comercio ilícito a través de la dark web, tiene un nivel de riesgo medio. En cuanto al uso de AV y PSAV para el FT se refleja un riesgo medio para la región.

209. Por otro lado, un aspecto importante a considerar para los países consiste en la necesidad futura de analizar los riesgos emergentes asociados a AV y PSAV, sobre todo aquellos vinculados a Finanzas Descentralizadas (DeFi), transacciones P2P, entre otros.

210. Adicionalmente, los resultados indican que las entidades financieras tradicionales están logrando detectar actividades informales o no reguladas de los PSAV, lo que resalta la urgencia de una regulación más robusta. Ha habido un aumento en el número de ROS relacionados con AV y PSAV recibidos por las UIF, aunque en aquellos países en los que no están obligados a presentar ROS frecuentemente carecen de información de primera mano proveniente de los PSAV. Este escenario demanda una mejora en los mecanismos de reporte y una mayor cooperación interinstitucional para optimizar la detección y prevención de actividades ilícitas.

211. En general, el sector financiero tradicional tiene una percepción cauta hacia las personas que operan con AV y hacia los PSAV. Esto permite indicar que, los servicios financieros tradicionales en su mayoría aplican medidas de *de-risking*. Esta postura prudencial, aunque orientada a mitigar riesgos de LA/FT, puede tener repercusiones significativas para los PSAV y facilitar la comisión de actividades ilícitas. Ante la restricción de acceso a servicios financieros locales, los propietarios de estos negocios podrían establecer relaciones con entidades financieras en jurisdicciones con marcos regulatorios más favorables o a formar alianzas estratégicas con

empresas del mismo sector en otros países. Este desplazamiento geográfico y la colaboración transnacional conllevan a la implementación de esquemas operativos más complejos, incrementando así la dificultad para supervisar y controlar las actividades financieras, lo que a su vez traslada el riesgo a otras jurisdicciones. Además, esta fragmentación internacional podría facilitar la elusión de controles regulatorios y exacerbar la vulnerabilidad de los sistemas financieros ante actividades ilícitas.

212. Es imperativo que los reguladores y supervisores ALA/CFT asuman un rol más activo en el acercamiento y la colaboración con el sector de PSAV. La reticencia persistente del sector financiero tradicional para colaborar con los PSAV genera puntos ciegos que facilitan la prestación clandestina de servicios, incrementando los riesgos tanto para el público en general como para la detección efectiva de actividades ilícitas.

213. Los PSAV encuestados muestran conocimiento sobre la necesidad de aplicar medidas ALA/CFT, sin embargo, el grado de cumplimiento no puede calificarse, ya que hace falta información que demuestre la madurez del sector desde una perspectiva regional. De conformidad con los resultados de las encuestas, se evidenció la voluntad por parte de los PSAV de integrarse adecuadamente al marco regulatorio en los países de la región. Estos actores muestran capacidad para cumplir con los requisitos ALA/CFT, sin embargo, es esencial que todos establezcan relaciones con pares debidamente registrados o licenciados, implementando políticas y procedimientos ALA/CFT robustos y medidas de mitigación de riesgos.

214. La falta de regulación facilita la operación clandestina de PSAV y favorece la explotación del sector por parte de las amenazas. Esta falta de regulación afecta no solo a la materia de ALA/CFT. Aunque existen acciones regulatorias, es necesario considerar regulaciones más profundas. La disparidad normativa en la región se refleja en requisitos dispares para la actividad de los PSAV, lo que hace que requisitos como la "regla de viaje" no tengan aplicación regional y se dificulte su cumplimiento; y que se intensifiquen problemas como el del “amanecer” (*sunrise issue*[22]) que repercuten en la descoordinación en la implementación.

215. La infraestructura tecnológica insuficiente impide que las autoridades estén en capacidad plena de supervisar e investigar casos en los que se involucran AV. Como se muestra en este informe, particularmente resulta necesario fortalecer la infraestructura tecnológica de las AOP. Las AOP deberían contar con herramientas que permitan realizar análisis e inteligencia de la blockchain, y estar en capacidad de decomisar, tomar el control y administrar los AV.

[22] El "problema del amanecer" se refiere a la adopción desigual de la regla de viaje en las distintas jurisdicciones, debido a retrasos o estándares inconsistentes. El cumplimiento de la Regla de Viaje exige que los PSAV garanticen que ciertos requisitos de información acompañen a los flujos de pago. Sin embargo, dada la falta de una implementación uniforme entre jurisdicciones, es posible que no siempre se dé el caso de que ambos PSAV involucrados en una transacción estén obligados por sus respectivas autoridades nacionales a cumplir, independientemente de la regulación en la jurisdicción beneficiaria. No obstante, hasta que todos los PSAV implementen la Regla de Viaje (es decir, que exista cumplimiento global), los PSAV que operan en, o desde, jurisdicciones que cumplen con la normativa seguirán enfrentando dificultades para ejecutar todas las transacciones de manera conforme. (Traducción no oficial - Box 2.1 What's the Sunrise Issue? - https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/Best-Practices-Travel-Rule-Supervision.pdf)

Adicionalmente, la insuficiencia tecnológica afecta también la posibilidad de prestar cooperación internacional. Las AOP muestran falta de capacidad de investigación y procesamiento de delitos que involucran a los AV y PSAV. Es fundamental que las AOP cuenten con todas las facultades necesarias, capacidades y herramientas para investigar y procesar casos relacionados con AV y PSAV, y que las autoridades judiciales estén adecuadamente capacitadas para juzgar y sentenciar estos delitos.

216. Es fundamental aprovechar la experiencia de las UIF en el análisis de casos y fortalecer la coordinación interinstitucional para abordar de manera integral las actividades ilícitas relacionadas con AV y PSAV.

217. A pesar de las diferencias estructurales entre los activos virtuales y las finanzas tradicionales, los AV y PSAV no necesariamente presentan un riesgo intrínseco mayor que los activos financieros convencionales. Las autoridades han fortalecido sus capacidades para detectar actividades ilícitas relacionadas con AV, lo que se evidencia en el aumento de tipologías identificadas por los países miembros del GAFILAT. No obstante, las tendencias indican una diversificación en las tácticas de LA. Estos cambios reflejan una adaptación continua de los delincuentes para evadir la detección, subrayando la necesidad de una mayor diligencia y coordinación entre las entidades reguladoras y el sector financiero tradicional.

218. El fortalecimiento de las medidas mitigantes relacionadas con los AV y los PSAV requiere un enfoque integral y estratégico para garantizar su efectividad a largo plazo. Como primer paso, es esencial construir un conocimiento sólido y contextualizado. Esto incluye implementar acciones exploratorias preliminares antes de iniciar formalmente evaluaciones de riesgos, como encuestas a actores clave, análisis de reportes de operaciones sospechosas y mesas de diálogo con autoridades de orden público. Estas actividades permitirán recopilar información cuantitativa y cualitativa sobre la incidencia de los AV y los PSAV, identificando las áreas prioritarias de intervención.

219. En paralelo, se recomienda fomentar un acercamiento directo con los PSAV, organizando mesas de trabajo colaborativas y estableciendo registros voluntarios que permitan cuantificar y conocer a los actores del sector. Este acercamiento no solo facilitará una evaluación sectorial de riesgos más profunda y basada en datos reales, sino que también permitirá diseñar estrategias regulatorias alineadas con la realidad del sector. Una vez consolidado este conocimiento, se debe proceder con una evaluación informada de riesgos que aborde las amenazas, vulnerabilidades y estrategias de mitigación necesarias para equilibrar la innovación tecnológica con la prevención de actividades ilícitas.

220. Finalmente, estas medidas deben integrarse en el marco jurídico y en los procesos de supervisión prudencial. La regulación resultante debe ser proporcional y adaptativa, garantizando que las autoridades competentes cuenten con las herramientas legales, técnicas y tecnológicas necesarias para monitorear el sector de manera efectiva. Asimismo, se debe promover la colaboración interinstitucional e internacional para fortalecer la trazabilidad de las operaciones,

combatir las amenazas emergentes y garantizar un enfoque sostenible en la gestión de riesgos asociados a los activos virtuales.

FUENTES Y REFERENCIAS

Bitso. (s.f.a). *Panorama cripto en América Latina: Reporte 2º semestre 2023*. Bitso.

Bitso (s.f.b). *Panorama cripto en América Latina: Reporte 1er semestre 2024*. Bitso

Cárcamo Jiménez, O. J. (17 de abril de 2024). *Estado del ecosistema Fintech en Honduras – Hub de innovación financiera [Diapositivas de presentación]*. Mesa Regional de Trabajo de la ESR de LA/FT de los AV/PSAV - GAFILAT, Perú 2024. Comisión Nacional de Bancos y Seguros. Honduras.

Chainalysis. (2020). *The 2020 Geography of Cryptocurrency Report*. Chainalysis.

Chainalysis. (2021). *The 2021 Geography of Cryptocurrency Report*. Chainalysis.

Chainalysis. (2022). *The 2022 Geography of Cryptocurrency Report*. Chainalysis.

Chainalysis. (2023). *The 2023 Geography of Cryptocurrency Report*. Chainalysis.

Chainalysis (2024). *The 2024 Crypto Crime Report*. Chainalysis.

Comité de Coordinación para la Prevención y Lucha contra el Lavado de Activos, la Financiación del Terrorismo y la Proliferación de Armas de Destrucción Masiva. (s.f.). *2022 Versión Pública -Evaluaciones nacionales de riesgos de lavado de activos y de financiamiento del terrorismo y de la proliferación de armas de destrucción masiva*. Ministerio de Justicia y Derechos Humanos, Argentina.

Cyber Diplomacy Toolbox. (s.f.). *What is Cyber Diplomacy?* Cyber-Diplomacy Toolbox. Consultado el 13 de septiembre de 2024 en https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html.

Department of the Treasury. (2024). 2024 *National Money Laundering Risk Assessment (NMLRA)*. Department of the Treasury, EUA.

Department of the Treasury. (2024a). *2024 National Proliferation Financing Risk Assessment*. Department of the Treasury, EUA.

Department of the Treasury. (2024b). *2024 National Terrorist Financing Risk Assessment*. Department of the Treasury, EUA.

Department of the Treasury. (2024c). *Illicit Finance Risk Assessment of Non-Fungible Tokens*. Department of the Treasury, EUA.

ENCCLA. (2023). *Ação 09/2023: Identificação de tipologias de lavagem de dinheiro e financiamento do terrorismo que se utilizam de novas tecnologias*. Documento no publicado. Brasil.

Egmont Group. (2023). *Public Summary Report on Abuse of Virtual Assets for Terrorist Financing Purposes.* Information Exchange Working Group (IEWG). Egmont Group of Financial Intelligence Units.

Elliptic. (s.f.). *2020 Edition Financial Crime Typologies in Cryptoassets the Concise Guide for Compliance Leaders.* Elliptic.

Elliptic. (s.f.a). *Typologies Report 2023 Preventing Financial Crime in Cryptoassets Using Blockchain Analysis to Mitigate Risk*. Elliptic.

Europol. (s.f.). *Cryptocurrencies and financial crime: A strategic approach to ensure security*. Europol. Consultado el 13 de septiembre de 2024 en https://www.europol.europa.eu/media-press/newsroom/news/cryptocurrencies-and-financial-crime-strategic-approach-to-ensure-security.

Europol, Basel Institute on Governance e Interpol. (2021). *Combating Virtual Assets-Based Money Laundering and Crypto-Enabled Crime. 2021 Recommendations of the Tripartite Working Group on Criminal Finances and Cryptocurrencies*.

Europol y Basel Institute on Governance. (2022). *Seizing the opportunity: 5 Recommendations for Crypto Assets-Related Crime and Money Laundering. 2022 Recommendations of the Joint Working Group on Criminal Finances and Cryptocurrencies.*

Europol, Basel Institute on Governance y European Financial and Economic Crime Centre. (2024). *A race against time: Europol – Basel Institute on Governance recommendations on preventing and combating the criminal use of cryptocurrencies.*

FATF. (2012-2023). *Estándares internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo, y el financiamiento de la proliferación de armas de destrucción masiva* (trad. GAFILAT). GAFILAT.

FATF. (2013). *FATF Guidance National Money Laundering and Terrorist Financing Risk Assessment*. FATF.

Jiménez Benavides, A. M. (17 de abril de 2024). *Experiencias sobre los activos virtuales en El Salvador [Diapositivas de presentación].* Mesa Regional de Trabajo de la ESR de LA/FT de los AV/PSAV - GAFILAT, Perú 2024. Fiscalía General de la República El Salvador.

GAFILAT. (s.f.a). *Informe de amenazas regionales en materia de lavado de activos*. GAFILAT.

GAFILAT. (s.f.b). *Segunda actualización del informe de amenazas regionales en materia de lavado de activos (2017-2018).* GAFILAT. https://www.gafilat.org/index.php/en/biblioteca-virtual/gafilat/documentos-de-interes-17/estudios-estrategicos-17/3861-segunda-

actualizacion-del-informe-de-amenazas-regionales-de-la-del-gafilat-1/file, consultado el 7 de diciembre de 2023.

GAFILAT. (s.f.c). *Tercera Actualización del Informe de Amenazas Regionales en materia de Lavado de Activos (2019-2021)*. GAFILAT. https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/estudios-estrategicos-17/4506-tercera-actualizacion-del-informe-de-amenazas-regionales-2019-2021-del-gafilat/file, consultado el 7 de diciembre de 2023.

GAFILAT. (2018). *Casos y tipologías regionales 2017-2018*. GAFILAT

GAFILAT. (2021). *Informe de Tipologías Regionales de LA/FT 2019-2020*. GAFILAT.

GAFILAT. (2021a). *Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales*. GAFILAT.

GAFILAT. (2023a). *Guía para la Regulación ALA/CFT de Activos Virtuales y Proveedores de Servicios de Activos Virtuales en la Región del GAFILAT*. GAFILAT.

GAFILAT. (2023b). *Informe de Tipologías Regionales de LA/FT 2021-2022*. GAFILAT

GAFILAT – BCIE. (2024). *Cuarta Actualización del Informe de Amenazas Regionales en materia de Lavado de Activos y Financiamiento del Terrorismo*. GAFILAT.

IBM. (s.f.). *Brute force attacks*. IBM Documentation. https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-brute-force-attacks, consultado el 31 de octubre de 2024.

ICD (Instituto Costarricense sobre Drogas). (2023). *Unidad de inteligencia financiera – Tipologías – Riesgos de lavado de dinero y financiamiento del terrorismo apartado especial sobre los activos virtuales*. Gobierno de Costa Rica. https://www.icd.go.cr/portalicd/images/docs/uif/doc_interes/acerca_uif/Compiladotipo2023.pdf

National Institute of Standards and Technology (NIST). (s.f.). *NIST Computer Security Resource Center - Glossary*. https://csrc.nist.gov/glossary/.

Ramírez Leoni, J.D. (17 de abril de 2024). *Avances en la evaluación de riesgos de activos virtuales y PSAV en Guatemala [Diapositivas de presentación]*. Mesa Regional de Trabajo de la ESR de LA/FT de los AV/PSAV - GAFILAT, Perú 2024. Intendencia de Verificación Especial. Guatemala

Reuters. (3 de agosto de 2022). *Honduras launches Bitcoin Valley tourist town Santa Lucia*. Reuters. Consultado el 13 de septiembre de 2024 en

https://www.reuters.com/world/americas/honduras-launches-bitcoin-valley-tourist-town-santa-lucia-2022-07-29/

Rubí, Scarlet. (25 de agosto de 2022). *Bitcoin Valley Honduras*. Radar Latam. Crypto Conexión. Consultado el 13 de septiembre de 2024 en https://cryptoconexion.com/bitcoin-valley-honduras/.

SBS. (s.f.a). *Activos virtuales y proveedores de servicios de activos virtuales: diagnóstico situacional, legislación comparada y exposición a los riesgos de LA /FT en el Perú*. SBS. Perú.

SBS. (s.f.b). *Versión detallada evaluación nacional de riesgos de lavado de activos 2021*. SBS. Perú.

SBS. (16 de abril de 2024). *Riesgo LA/FT de los activos virtuales y proveedores de servicios de activos virtuales [Diapositivas de presentación].* Mesa Regional de Trabajo de la ESR de LA/FT de los AV/PSAV - GAFILAT, Perú 2024. SBS. Perú.

SFC (Superintendencia Financiera de Colombia). (9 de septiembre de 2024). *Innovas FCA: La arena sandbox del supervisor*. SFC. Colombia. Consultado el 13 de septiembre de 2024 en https://www.superfinanciera.gov.co/publicaciones/10114253/innovasfclaareneras andbox-del-supervisor-10114253/.

SFC. (27 de junio de 2024). *Superfinanciera presenta balance del cierre del piloto en el que se probaron operaciones en productos de depósito a nombre de plataformas de criptoactivos*. SFC. Colombia. Consultado el 13 de septiembre de 2024 en https://www.superfinanciera.gov.co/publicaciones/10115218/superfinanciera-presenta-balance-del-cierre-del-piloto-en-el-que-se-probaron-operaciones-en-productos-de-deposito-a-nombre-de-plataformas-de-criptoactivos/

SEPRELAD (Secretaría de Prevención de Lavado de Dinero o Bienes, Unidad de Inteligencia Financiera). (s.f.). *Estudio sectorial de riesgos de LA/FT de activos virtuales y proveedor de servicios de activos virtuales - Año 2020*. SEPRELAD. Paraguay.

SHCP (Secretaría de Hacienda y Crédito Público). (s.f.). *Evaluación nacional de riesgos 2020. Versión Pública*. SHCP. México.

SHCP (Secretaría de Hacienda y Crédito Público). (2023). *Evaluación nacional de riesgos de lavado de dinero y financiamiento del terrorismo 2023*. SHCP. México.

Supelano Mendoza, V.M. (17 de abril de 2024). *Experiencia país [Diapositivas de presentación]*. Mesa Regional de Trabajo de la ESR de LA/FT de los AV/PSAV - GAFILAT, Perú 2024. Unidad de Información y Análisis Financiero. Colombia.

TRM Labs. (2024). *The Illicit Crypto Economy Key Trends from 2023*. TRM Labs.

Anexo 1: Patrones de actividades inusuales o sospechosas identificadas por los sujetos financieros tradicionales

Se consultó a las entidades financieras si habían identificado patrones de operaciones inusuales o actividades sospechosas relacionadas con los PSAV que podrían indicar riesgos de LA/FT. Del total de 225 respuestas recibidas, 33 entidades informaron que sí han identificado patrones de operaciones inusuales o actividades sospechosas; mientras que los 192 restantes no informaron haber identificado tales patrones.

De las 33 entidades que respondieron haber identificado patrones inusuales o sospechosos:

- 16 son entidades que actualmente aceptan clientes usuarios de AV y PSAV.
- 17 tienen una política de no aceptar clientes AV y PSAV.

A pesar de que 17 entidades tienen una política de no aceptar clientes relacionados con AV o PSAV, aun así, han identificado patrones de operaciones inusuales o actividades sospechosas relacionadas con estos. Esto sugiere que, aunque oficialmente no acepten estos clientes, de alguna manera están teniendo contacto con transacciones o actividades vinculadas a los AV y PSAV. Esta situación indica la necesidad de una revisión más exhaustiva de sus políticas y procedimientos para asegurar que se está gestionando adecuadamente el riesgo de LA/FT asociado con estos tipos de activos y servicios.

Dentro de los patrones de actividad inusual o sospechosa identificada por las entidades financieras relacionados con PSAV están:

A. Uso indebido o no autorizado de PSAV y criptomonedas:

- El cliente opera con PSAV en representación de otros clientes, en otras oportunidades no cuenta con la capacidad patrimonial suficiente que justifique la operativa.
- Operaciones realizadas por PSAV a las que se le presta especial atención a la justificación del origen de los fondos, ya que operan por cuenta de terceros.
- Ocultamiento del verdadero objeto social del PSAV.
- PSAV que no declararon su actividad como tal al momento de la vinculación, buscando evadir controles de debida diligencia acordes a su actividad económica.
- Persona natural accionista de PSAV utilizando su cuenta personal para movimientos de empresa de reciente constitución, buscando evadir controles de debida diligencia acordes a la actividad económica de PSAV.
- Empresas del rubro de tecnología que realmente realizan actividad de AV o PSAV sin declararla.
- Operativas de fraude relacionadas con PSAV.

B. Falta de justificación del origen de fondos o estructura financiera:

- Personas naturales que realizan intermediación de cripto, con fondos no justificados y sin debida diligencia de sus clientes.
- Clientes que no pueden respaldar los montos operados ni las operaciones, con actividades comerciales que deberían ingresar por comercio exterior, arbitradores, empresas no residentes, etc.
- Alto número de transacciones de personas naturales sin justificación del origen de los fondos.
- Traslado de fondos desde billeteras electrónicas a cuentas bancarias sin justificación clara de su origen.
- Clientes que realizan múltiples recargas desde la wallet oficial y luego pagan las tarjetas con márgenes cortos de retorno, sin respaldo.

C. Evasión de controles o regulaciones:

- Clientes operando como corredores sin las autorizaciones correspondientes, generando captación de recursos de terceros para inversión en criptomonedas.
- Clientes que administran fondos de terceras personas para *trading* sin autorización.
- Entidades que registran depósitos en ubicaciones distantes sin justificación congruente con la actividad declarada.

D. Actividades irregulares relacionadas con el mercado de divisas y criptomonedas:

- Clientes que venden activos virtuales a distintas personas físicas para hacerse de fondos en el país, en virtud de las condiciones internacionales.
- Clientes con posibles irregularidades cambiarias vinculadas a exportadores de servicios, que a su vez reciben fondos a través de criptomonedas.
- Fraccionamiento de valores, retiros en efectivo, transacciones P2P, giros en comercios de criptomonedas en Gibraltar y Malta. Clientes que adquieren AV a través de productos tradicionales.

E. Fraude y riesgos financieros:

- Ingreso de efectivo para compra de activos digitales vinculado a phishing.
- Operativas de fraude relacionadas con PSAV.

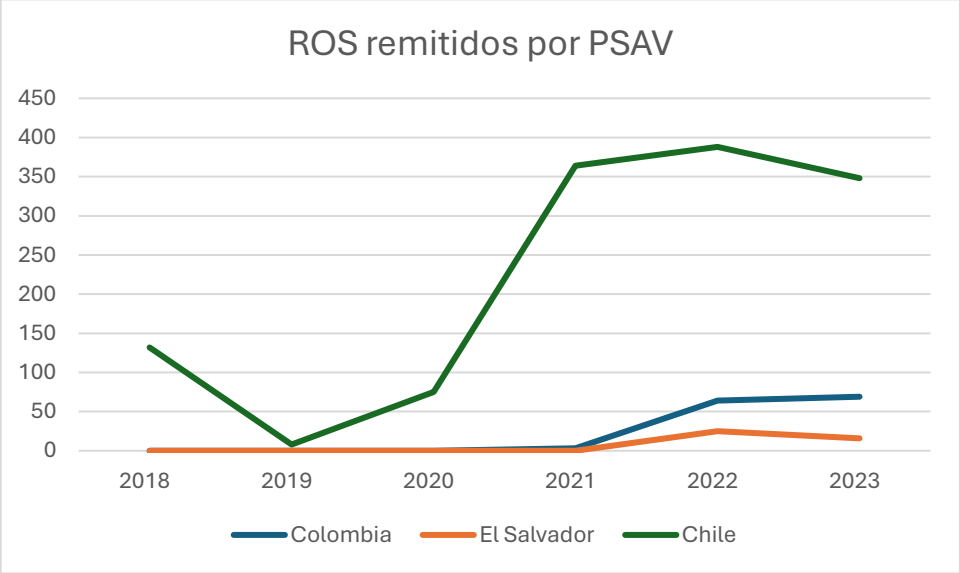
Anexo 2: Señales de alerta identificados por las UIF

Seis UIF, Argentina, Chile, Colombia, El Salvador, Paraguay y Perú, compartieron información estadística sobre el número de ROS presentados por los PSAV por medio de las encuestas, así como sobre los ROS recibidos que están relacionados con AV.

Número de ROS presentados por los PSAV (2018-2023)

Número de ROS presentados por los PSAV						
	2018	**2019**	**2020**	**2021**	**2022**	**2023**
Colombia	0	0	0	3	64	69
El Salvador	0	0	0	0	25	16
Chile	132	8	75	364	388	348
Total	132	8	75	367	477	433

Tendencia de los ROS remitidos por PSAV (2018-2023)



El gráfico anterior muestra que:

- En el caso de Colombia, a partir de 2021 hay un aumento significativo en el número de ROS remitidos por PSAV, comienzan con 3 en 2021 y alcanzan a 69 en 2023. Esto coincide con la emisión de la Resolución 314 de 2021, del 15 de diciembre de 2021, por la cual se impone una obligación de reporte a la UIAF a las empresas que provean servicios de AV.
- El caso de El Salvador es similar, la recepción de ROS comienza a partir de 2022, después de la adopción de Bitcoin como moneda de curso legal en 2021. El incremento inicial en 2022 es notable, la disminución en 2023 podría indicar una mejora en los controles preventivos o cambios en las actividades que generan reportes.
- Chile es el país que muestra la mayor actividad en ROS remitidos por PSAV, con una fluctuación significativa. Se observa un pico en 2021 con 364 reportes, un pequeño incremento en 2022 y una ligera disminución en 2023, aunque se mantienen en niveles

altos. La alta cantidad de reportes puede indicar un entorno con más actividades sospechosas, o bien una mayor efectividad en la identificación y reporte de estas actividades.

- En Paraguay, Argentina y Perú no se observa actividad en el número de ROS remitidos por PSAV en los años analizados. Sin embargo, en el caso de Perú al mes de agosto de 2024 se habían recibido 4 ROS remitidos por PSAV, lo que sería producto de la emisión de la legislación en 2023, y la regulación en 2024, que incluye a los integrantes del sector como sujetos obligados a informar a la UIF.

ROS recibidos que están relacionados con AV

ROS en Costa Rica

La UIF de Costa Rica proporcionó información sobre la realización de un recuento de los ROS relacionados con AV del 2022 al 2024 identificándose al menos 47 casos relacionados. Los casos se cuantifican monetariamente en una cifra de 377 millones de colones y 59.2 millones de dólares, para un total dolarizado de 60 millones de dólares.

1. En la siguiente tabla se muestra la estadística de ROS

ROS CRIPTOACTIVOS 2022-2024*			
Año	**Cantidad**	**Colones**	**Dólares**
2022	21	38 538 536,99	43 650 440,24
2023	16	0	5 787 212,76
2024	10	339 452 094,26	9 815 115,33
Totales	**47**	**377 990 631,25**	**59 252 768,33**

*** Año 2024 al 18/04/2024**

Fuente y elaboración: Unidad de Inteligencia Financiera Costa Rica/ Plataforma SICORE

ROS en Guatemala

En el marco de la segunda actualización de la ENR, se realizó la publicación del Módulo de AV/PSAV, la cual aborda de forma detallada los riesgos a los que se encuentra expuesto el país. Conforme al análisis de la información interna enviada por las Personas Obligadas a la IVE, se identificaron un total de 228 Reportes de Transacciones Sospechosas (RTS) relacionados con el sector de activos virtuales, ascendiendo a un monto de Q2,001.0 millones en el periodo de 2018 a 2023, siendo reportados principalmente por las entidades bancarias (95.2%). Según la información contenida en las descripciones de los reportes, se pudo observar que el 51.3% fue reportado por realizar la compra o venta de activos virtuales y 17.1% por casos relacionados con estafa.

ROS en Honduras

Igualmente, durante la mesa regional de trabajo, se obtuvo información de que la UIF de Honduras identificó haber recibido 59 ROS relacionados con AV entre el 13 de marzo de 2017 y el 11 de abril de 2024. Los ROS involucraban a 58 personas. Derivado de la revisión de esos 59 ROS, se lograron identificar las señales de alerta que se presentan a continuación (Cárcamo Jiménez, 17 de abril de 2024).

Principales señales de alerta identificadas en los ROS relacionados con AV en Honduras

- Operaciones que no armonizan con la actividad económica ni el perfil del cliente.
- Clientes que no reconocen la contraparte de la transacción (ordenante de TT o de LBTR)
- Transferencias internacionales, cartas de crédito, LBTR-ACHs, efectivo recibido, compra de divisas, transacciones locales sin lógica comercial, vinculación con contrapartes (terceros) sin relación comercial.
- Apertura de productos financieros o de inversión por parte de un grupo de personas que presentan características similares, tales como las fechas de solicitud de apertura, cantidades depositadas y retiradas, datos de confirmación y referencias personales y comerciales.
- Transferencias entre cuentas del mismo titular o a favor de otras personas, sin justificación aparente.
- Explicaciones no satisfactorias, a criterio de la Entidad Financiera, sobre la variación significativa de las operaciones del cliente con respecto a su perfil.

ROS en Perú

De acuerdo con información de la SBS, entre 2019 y agosto de 2024, la UIF de Perú recibió un total de 913 ROS relacionados con el uso de criptoactivos, con un monto total involucrado de USD 1 298 millones. Dichos ROS representaban el 0.9% de los ROS recibidos durante dicho periodo, y el 0.6% del monto total asociado. En los 913 ROS, se registraron 1124 operaciones, de las cuales el 38.5% tuvo un alcance internacional relacionado con más de 25 jurisdicciones diferentes. Estados Unidos fue reportado en 258 de las 1124 operaciones, Colombia fue incluida en 147 operaciones, seguida de Canadá con 15 operaciones. En este periodo, se encontraron las siguientes señales de alerta:

Principales señales de alerta identificadas en los ROS que mencionan criptoactivos en Perú 2019-agosto 2024

Señal de Alerta	N° de Apariciones
El cliente realiza frecuentes o significativas operaciones que no guardan relación con la actividad económica declarada y/o con su situación patrimonial y/o financiera, o que sobrepasan los importes con que opera usualmente.	593
El cliente se niega a proporcionar la información solicitada o la información proporcionada es inconsistente o de difícil verificación por parte de las empresas.	215
El cliente realiza operaciones complejas sin una finalidad aparente.	78
Operaciones fraccionadas realizadas a fin de eludir normas u obligaciones de revelación.	49
Transferencias electrónicas por montos significativos hacia personas o negocios que no mantienen cuentas en la empresa.	46

Se toma conocimiento por los medios de difusión pública u otro, según sea el caso, que un cliente (ejecutante y/o beneficiario), está siendo investigado o procesado por el delito de lavado de activos, delitos precedentes, el delito de financiamiento del terrorismo y/o delitos conexos.	36
El cliente presenta una inusual despreocupación respecto de los riesgos que asume o los costos que implican el negocio o transacción que está realizando.	29
El cliente que realiza frecuentemente operaciones por grandes sumas de dinero (depósitos, retiros o compras de instrumentos monetarios, entre otros) y se niega o evita dar información sobre el origen y/o destino del dinero o estas operaciones no guardan relación con su actividad económica.	29

Fuente. SBS

Anexo 3: Medidas de ciberseguridad implementadas por los países

Respecto a la ciberseguridad, en varios países se han implementado diversas iniciativas relacionadas con tecnologías emergentes.

- En Bolivia, la normativa incluye la Ley N°164, el Decreto Supremo N°1793, y el Decreto Supremo N°2514, que establecen lineamientos técnicos en seguridad de la información para el sector público y la creación del Centro de Gestión de Incidentes Informáticos del Estado. Además, Bolivia ha desarrollado la Agenda Digital 2030 y propone la creación de la Agencia Plurinacional de Ciberseguridad para fortalecer la ciberseguridad y la soberanía tecnológica.
- México ha desarrollado la Estrategia Nacional de Ciberseguridad de 2017 y la Estrategia Digital Nacional 2021-2024, enfocándose en la concientización de los riesgos asociados al uso de tecnologías y la necesidad de una cultura general de ciberseguridad. Además, se propuso la "Ley Federal de Ciberseguridad" en 2023, que incluye la creación de una Agencia Nacional de Ciberseguridad y la realización de pruebas de vulneración anuales.
- En Uruguay, existe un Marco de Ciberseguridad que permite la gestión adecuada de los activos de información en empresas y el sector público. Recientes modificaciones legislativas han asignado a la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC) la responsabilidad de diseñar e implementar una estrategia de ciberseguridad en colaboración con el Banco Central del Uruguay y otros operadores públicos y privados.

En cuanto a la cooperación y coordinación entre las autoridades de tecnología, financieras y de seguridad pública en relación con AV/PSAV y LA/FT, las respuestas indican diversas maneras de implementar dicha cooperación.

- En Bolivia, la AGETIC (Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación) coopera con las autoridades competentes conforme a sus requerimientos y competencias.
- En Ecuador, existe el Comité Nacional de Ciberseguridad, que incluye la participación de varios ministerios y genera políticas y lineamientos para combatir la ciberdelincuencia, la ciberdefensa y la ciber diplomacia.
- En México, las autoridades del régimen ALA/CFT cuentan con mecanismos de cooperación y coordinación nacional, como convenios de colaboración e intercambio de información, mesas de trabajo y acceso a productos de inteligencia para la prevención y combate al LA/FT y sus delitos subyacentes, incluidos aquellos relacionados con el uso de activos virtuales.
- En Uruguay, AGESIC colabora de forma permanente con el sector financiero a través de reuniones periódicas con las distintas entidades bancarias del país y ha participado en la redacción de regulaciones relacionadas con el registro de sujetos obligados en materia ALA/CFT.

Anexo 4. Medidas de mitigación implementadas por los PSAV e instituciones financieras

a. Medidas de mitigación implementadas por los PSAV

221. Es importante reconocer que los PSAV están implementado varias medidas de mitigación que, con una buena regulación a nivel nacional, pueden ser fortalecidas. Los 63 PSAV encuestados (100%) indicaron que implementan medidas y tienen políticas ALA/CFT. Estos procedimientos incluyen desde la verificación de identidad mediante tecnologías avanzadas y el monitoreo continuo de actividades, hasta la clasificación de riesgos y el mantenimiento de registros. En algunos casos, se destacó el uso de herramientas digitales para la verificación no presencial, auditorías internas y externas rigurosas, y la especialización en servicios para personas jurídicas.

Cuadro 6 Medidas ALA/CFT más comunes implementadas por los PSAV

A continuación, se detallan las prácticas más comunes y particulares implementadas por los PSAV encuestados para cumplir con las regulaciones y mantener la confianza en el sector.

- DDC y monitoreo continuo
  - Verificación de identidad mediante documentos oficiales, biometría, y validación con bases de datos gubernamentales.
  - Monitoreo de actividades para detectar comportamientos inusuales o sospechosos.
- Evaluación de riesgos
  - Clasificación de riesgos basada en factores asociados al cliente y su actividad económica.
  - Evaluación del perfil del cliente y seguimiento de transacciones para mantener actualizada la información del cliente.
- Documentación y conservación
  - Integración de expedientes electrónicos y físicos con la documentación requerida.
  - Conservación de la información por el plazo legal estipulado.
- Políticas y manuales
  - Manuales de políticas ALA/CFT.
  - Capacitación del personal en temas ALA/CFT.
- Tecnologías y herramientas:
  - Herramientas automatizadas para screening en listas de control y verificación continua.
  - Sistemas de compliance avanzados para revisión de transacciones y monitoreo de listas internacionales.

222. Respecto a las medidas implementadas por los PSAV para verificar la identidad de los usuarios y la legitimidad de sus transacciones; los encuestados indicaron que la verificación de la

identidad y la legitimidad de las transacciones se realiza mediante una combinación de tecnologías y procesos de cumplimiento normativo.

Cuadro 7 Métodos de verificación de la identidad de usuarios y legitimidad de transacciones implementadas por los PSAV encuestados

Los PSAV encuestados indicaron que dentro de los métodos y procedimientos que utilizan para la verificación de la identidad de los usuarios y la legitimidad de sus transacciones están:

- KYC y Biometría: Utilización de procedimientos KYC y herramientas biométricas para verificar documentos de identidad y realizar pruebas de vida (selfies).
- Utilización de proveedores especializados: Empresas como Onfido, Veriff, y Metamap proporcionan servicios de verificación de identidad, utilizando inteligencia artificial para validar documentos y realizar comparaciones biométricas.
- Listas de control: Las identidades se verifican contra listas nacionales e internacionales de sanciones y personas expuestas políticamente (PEPs).
- Sistemas automatizados: Herramientas como Chainalysis y TRM Labs permiten el monitoreo continuo de las transacciones, identificando patrones sospechosos y verificando la legitimidad de las direcciones de wallet.
- Alertas automáticas: Los sistemas generan alertas automáticas para transacciones inusuales, que luego son revisadas por equipos de cumplimiento.
- Aplicación de la regla de "Same Name Account". Algunas plataformas solo permiten transferencias desde y hacia cuentas bancarias asociadas al mismo nombre del titular de la cuenta, lo que garantiza que los fondos provienen y se dirigen al mismo propietario.
- Expedientes digitales: La recopilación y conservación de documentos se realiza de manera digital.
- Clasificación de los clientes en niveles de riesgo (alto, medio, bajo) y aplicación de diferentes niveles de diligencia según su perfil.
- Monitoreo continuo. Seguimiento constante del comportamiento transaccional de los usuarios para detectar cualquier actividad sospechosa o inconsistente con su perfil económico.

223. Revisar la idoneidad de estas políticas y procedimientos es fundamental para mitigar los riesgos específicos de LA/FT por parte de los PSAV. Por ello, es importante que el marco regulatorio y de supervisión permita y motive que el sector implemente las medidas preventivas.

b. Medidas de mitigación implementadas por las instituciones financieras

224. Por su parte, las instituciones financieras también están implementando medidas de mitigación que pueden ser reforzadas con un ambiente regulatorio apropiado para considerar los AV y PSAV. En este sentido, las 24 instituciones que participaron de este estudio que actualmente aceptan clientes usuarios de AV o PSAV indicaron que cuentan con políticas y procedimientos

específicos para mitigar los riesgos asociados con las operaciones que involucran PSAV. Dentro de los procedimientos específicos, mencionaron:

- Políticas de debida diligencia reforzada. Implementación de estándares y políticas específicas para PSAV, con evaluaciones y documentación adicional requerida.
- Monitoreo y evaluación continua. Sistemas de monitoreo continuo, alertas específicas y análisis periódicos adicionales para PSAV.
- Evaluación y segmentación de clientes y rechazo de clientes con bajo nivel de calificación.
- Requisitos de documentación adicional y políticas de conocimiento del cliente específicas para PSAV.
- Controles operacionales y restricciones. Políticas de no manejo de efectivo, restricciones de transferencias y monitoreo reforzado de operaciones.

Cuadro 8 Procedimientos de debida diligencia intensificada para PSAV en instituciones financieras

Dentro de los procedimientos de debida diligencia reforzada implementada por 22 instituciones financieras para el caso de PSAV, se contempla lo siguiente:

- Se aplica una debida diligencia reforzada con la aprobación en comité específico para este tipo de industria.
- Política denominada "Vinculación y monitoreo de los Clientes Especiales." Esta política incluye: completar un cuestionario sobre los controles en materia de ALA/CFT, evaluar las políticas y procedimientos implementados por el PSAV, una entrevista con el equipo de compliance del PSAV, documentación adicional como el manual de ALA/CFT, último informe del revisión externa o auditoría, último informe técnico del oficial de cumplimiento, contar con la autorización relevante.
- Aprobación por la gerencia, previa reunión con los equipos de cumplimiento del cliente. Asimismo, se evalúa su programa ALA/CFT, sus procesos de control y sus manuales de ALA/CFT.
- Análisis de la actividad del cliente para entender y justificar su operatoria, verificación de la composición de la sociedad, sus beneficiarios finales llegando a las personas físicas que poseen más del 10% de su capital social o bien aquellas que tienen el control de las mismas, en la medida que posean alertas en los sistemas de monitoreo se realizan muestreos de su operatoria a fin de entender la razonabilidad de las mismas y se solicita documentación para definir sus perfiles, se actualizan sus legajos de acuerdo al riesgo que representen para la entidad.
- Factores específicos como el tipo de activos utilizados, patrones de transacciones y los ecosistemas en los que operan.
- Visita a las instalaciones para confirmar su existencia y operación, se requieren las autorizaciones de la entidad supervisora local correspondiente para operar en esta jurisdicción, se requiere completar información adicional en la vinculación, por ejemplo, respecto a sus operaciones internacionales, así como documentar su fuente de ingresos, incluyendo además las respectivas validaciones en listas de control local e internacional.

Anexo 5. Entornos regulatorios experimentales: Colombia y Honduras

Durante la mesa de trabajo, se conocieron con mayor detalle dos iniciativas regulatorias experimentales enfocadas en los AV y PSAV. En Colombia y Honduras, donde se están implementando estas iniciativas, la regulación de AV y PSAV se encuentra en una etapa incipiente. Estas iniciativas representan enfoques proactivos para interactuar con el sector de AV y PSAV, lo que ha facilitado una comprensión más profunda de sus dinámicas operativas y de los desafíos específicos que enfrentan. Este enfoque iterativo y colaborativo contribuye a crear un entorno que promueve la innovación, protege los derechos de los usuarios y facilita el abordaje efectivo de los retos que presentan los AV y PSAV.

La arenera - Colombia

La arenera de la Superintendencia Financiera de Colombia (SFC), creada mediante la resolución 031 de 2017 y modificada por la resolución 0143 de 2020, es un entorno controlado diseñado para operar con PSAV. En este espacio, se realizan pruebas piloto para evaluar innovaciones tecnológicas que impactan el sector financiero. Los principales objetivos de la arenera incluyen:

- Probar operaciones de cash-in y cash-out en productos financieros de depósito a nombre de un exchange, utilizando tecnologías innovadoras para la gestión de riesgos y siguiendo lineamientos internacionales.
- Evaluar la efectividad de desarrollos tecnológicos en la verificación de la identidad digital y la trazabilidad de las transacciones empleadas en los procesos de gestión de riesgos.
- Fomentar un espacio de aprendizaje conjunto entre el ecosistema digital y el gobierno nacional, facilitando la colaboración y el entendimiento mutuo para el diseño de regulaciones más efectivas.

Estas iniciativas permiten a la SFC experimentar y adaptar regulaciones que promuevan la innovación tecnológica, aseguren la gestión de riesgos adecuada y protejan los derechos de los usuarios dentro del sector financiero (Supelano Mendoza, 17 de abril de 2024).

En junio de 2024, la SFC (27 de junio de 2024) informó que culminaron las operaciones de prueba en La Arenera para la adquisición (cash-in) y venta (cash-out) de criptoactivos, a través de productos financieros de depósito en Colombia. En el piloto realizado por la SFC, participaron siete alianzas compuestas por entidades vigiladas, junto con plataformas de intercambio de criptoactivos constituidas en el país. Durante este período, se llevaron a cabo operaciones de cash-in y cash-out en productos financieros de depósito a nombre de exchanges, utilizando innovaciones tecnológicas para la gestión de riesgos conforme a los lineamientos del GAFI. Los resultados del piloto demostraron una operación segura sin incidentes que comprometan la continuidad del proyecto, la estabilidad de las entidades participantes o la protección de los consumidores financieros. Además, las plataformas implementaron un sistema de administración de riesgo de LA/FT y herramientas avanzadas para la verificación de identidad digital y la

trazabilidad de transacciones, así como mecanismos robustos de atención al consumidor y divulgación de información sobre los riesgos asociados a los criptoactivos.

Para participar, las plataformas debían estar constituidas en Colombia y utilizar exclusivamente el producto de depósito para recaudar y dispersar recursos en moneda local. Durante el piloto, se permitió la compraventa y almacenamiento de criptoactivos en billeteras digitales, asegurando la identificación del origen, destino y monto de cada transacción sin integrar estos activos al sistema financiero colombiano. Además, las plataformas debían demostrar el uso de herramientas tecnológicas para el conocimiento y seguimiento de clientes y transacciones. Las plataformas que cumplieron con los requisitos lograron operar, garantizando seguridad, transparencia y protección a los usuarios.

Este piloto proporcionó información esencial para futuras iniciativas regulatorias, destacando la importancia de que tanto las entidades vigiladas como el público general comprendan y gestionen adecuadamente los riesgos asociados al uso y transacción de criptoactivos.

Hub de innovación financiera - Honduras

La Comisión Nacional de Bancos y Seguros (CNBS) y el Banco Central de Honduras (BCH) han dirigido el estudio del sector Fintech a través del Hub de Innovación Financiera. Se han identificado seis verticales del ecosistema FinTech con un aproximado de 34 sociedades, entre ellas dos de criptomonedas y tecnología blockchain. El sistema financiero tradicional en Honduras muestra una notable renuencia hacia las Fintech, sustentada en una fuerte cultura basada en los servicios financieros tradicionales. A pesar de este escepticismo, el sector Fintech continúa realizando esfuerzos significativos para lograr una mayor escalabilidad, enfrentándose a limitaciones de fondeo que restringen su crecimiento y expansión. Para superar estos desafíos y promover la innovación financiera, es esencial mantener una coordinación efectiva entre los reguladores. Esta colaboración facilita la creación de un entorno regulatorio más favorable, permitiendo que las Fintech desarrollen soluciones innovadoras que complementen y transformen los servicios financieros convencionales, impulsando así una evolución más dinámica y competitiva del sistema financiero en su conjunto (Cárcamo Jiménez, 17 de abril de 2024).

Bitcoin Valley

Bitcoin Valley es un proyecto iniciado en julio de 2022 en Santa Lucía, Honduras, con el objetivo de promover la adopción de Bitcoin como método de pago dentro de la industria turística. La iniciativa, liderada por la Universidad Tecnológica de Honduras, Blockchain Honduras, Coincaex y el gobierno municipal de Santa Lucía, busca entrenar a al menos 60 empresarios locales en el uso y aceptación de criptoactivos, creando así un ecosistema económico que atraiga a cripto-turistas. Además, Bitcoin Valley pretende expandirse a otras localidades turísticas cercanas y consolidar un corredor turístico innovador en el uso de criptomonedas, alineándose con proyectos similares en El Salvador, Costa Rica y Guatemala.