República de Nicaragua
Consejo Nacional
ALA/CFT/CFP

Resumen Ejecutivo (2021-2024)

EVALUACIÓN DE RIESGOS DE LAVADO DE ACTIVOS, FINANCIAMIENTO AL TERRORISMO Y FINANCIAMIENTO A LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA QUE SURGEN DE ACTIVIDADES DE ACTIVOS VIRTUALES Y OPERACIONES DE PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES

Entre agosto y noviembre del 2024 el Consejo Nacional ALA/CFT/CFP de la República de Nicaragua, bajo la coordinación de la Unidad de Análisis Financiero, desarrolló este proceso evaluativo planteándose como objetivos específicos: conocer la materialidad del uso de AV por la población nicaragüense; delimitar amenazas potenciales del mal uso de estas tecnologías; identificar las vulnerabilidades operativas, tecnológicas, institucionales y relacionadas a la regulación prudencial y supervisión ALA/CFT/CFP que enfrenta el país en la materia; determinar riesgos asociados a los delitos de LA/FT/FP, derivados del aprovechamiento de las vulnerabilidades identificadas por parte de las amenazas delimitadas, y por último, evaluar el grado de exposición que tendría Nicaragua a los riesgos determinados, considerando su probabilidad de ocurrencia y el impacto de sus consecuencias.

En Nicaragua aún no se registran Proveedores de Servicios de Activos Virtuales, aunque se han identificado una cantidad muy baja de personas naturales dedicándose al intercambio entre activos virtuales y moneda fíat y entre diferentes tipos de activos virtuales, utilizando plataformas de PSAV extraterritoriales tanto centralizados como descentralizados; sin embargo, la materialidad de esta actividad en nuestro país es muy baja, con solamente, un 0.3% de la población nacional en uso de carteras digitales de criptomonedas, lo que incluye a negocios que aceptan activos virtuales como medio de pago por los bienes o servicios que brindan; un 0.03% de la población apta para realizar transacciones bancarias realizando operaciones con activos virtuales a través de los productos y servicios financieros tradicionales de la banca y apenas un peso económico del 0.016% en relación al Producto Interno Bruto Nicaragüense; esto coincide con la ubicación de Nicaragua en una escala de baja adopción de criptomonedas (114/155) en el índice global de adopción de criptomonedas de la empresa, hoy por hoy a la vanguardia en análisis de blockchain, Chainalysis. Esto no quiere decir, que los nicaragüenses no usan criptomonedas, el análisis de materialidad reflejó el uso primordial de las así llamadas "monedas estables" (específicamente USDT y USDC) y la criptomoneda génesis, el Bitcoin, para propósitos de inversión, medios de pago y exploración del ecosistema principalmente, y para tal fin utilizan mayormente los exchanges centralizados, Binance, Bybit, Bitget, Coinpay, Kraken y OKX, en orden de favoritismo.

Para la presente evaluación de riesgos, se definieron como fuentes informativas los Informes estadísticos de TRM, Chainalysis y Elliptic, las Guías del GAFI, GAFILAT y de otros organismos internacionales pertinentes, interacción con la comunidad de usuarios, encuestas nacionales de inclusión financiera, Reportes de Operaciones Sospechosas relacionados con usuarios y requerimientos dirigidos a entidades pertinentes del sector público, privado y sociedad civil.

Las amenazas y vulnerabilidades, así como, la definición de la materialidad, fueron objetivamente proporcionadas por cuatro mesas de trabajo y discusión, las que se denominaron: Tecnología Subyacente, Materialidad del Sector, Regulación y Supervisión y Detección e Investigación de Tendencias Criminales, conformadas por un total de 26 miembros que delimitaron como principales amenazas vinculantes y en orden de mayor incidencia a: ***La Estafa***, que ha aumentado en los últimos

dos años; los ciberdelitos de ***Fraude Informático*** (también en aumento), ***Acceso indebido a sistemas informáticos*** y ***daños a sistemas informáticos*** (estos dos últimos investigados en nuestro contexto como **Ransomware**); el ***Lavado de Activos***, considerando su nivel de riesgo moderado en nuestra vigente ENR de LA y; el ***Tráfico de estupefacientes, psicotrópicos y sustancias controladas***, como principal amenaza del país conforme también, a nuestra ENR de LA.

Asimismo, se identificaron las siguientes vulnerabilidades, en orden de mayor atención requerida:

- Utilización de tecnologías y aplicaciones P2P extraterritoriales para realizar criptotrading.
- Controles o herramientas tecnológicas insuficientes para identificar a las personas naturales o jurídicas que lleven a cabo actividades de PSAV sin la autorización o el registro necesario.
- Falta de experiencia y conocimientos en la aplicación de recursos tecnológicos para realizar una adecuada verificación de la tecnología utilizada por los PSAV, tanto para el otorgamiento de licencias como para desarrollar la vigilancia y supervisión.
- Bajos niveles de capacitación en materia de activos virtuales y la tecnología blockchain por parte de las autoridades investigativas y de persecución penal.
- Falta de recursos humanos especializados en materia de activos virtuales y las tendencias criminales de su uso, tanto en el ámbito de detección, como de prevención, investigación y persecución penal.
- Escasez de herramientas tecnológicas para el rastreo oportuno de transacciones en cadenas de bloques y la investigación de casos relacionados a activos virtuales.
- Falta de sensibilización sobre los riesgos que representan las operaciones con AV a los Sujetos Obligados y usuarios en general.
- Nulo registro de Proveedores de Servicios de Activos Virtuales que pudieran brindar información de interés sobre operaciones sospechosas de LA/FT/FP vinculados a AV.
- Ausencia de obligaciones que garanticen la regla de viaje en las transferencias con activos virtuales.
- Falta identificar y evaluar los riesgos de LA/FT/FP que surgen de las actividades de las finanzas descentralizadas y que se aplique un enfoque basado en riesgo para garantizar en base al entendimiento de estos, las medidas de prevención, administración y mitigación.
- Carencia de regulación específica que establezca obligaciones de prevención, detección y reporte de actividades relacionadas con el LA/FT/FP para los PSAV regulados y supervisados por la UAF.
- Insuficiencia de recursos materiales y financieros por parte de las autoridades competentes, para garantizar la regulación, monitoreo y/o supervisión de las actividades de los PSAV.

- Falta de un diagnóstico para valorar si los medios materiales y tecnológicos con que cuentan actualmente los Sujetos Obligados son adecuados para el cumplimiento de los requisitos regulatorios.

El análisis de estas cuatro amenazas versus las trece vulnerabilidades identificadas permitió determinar seis riesgos de LA/FT/FP asociados a Activos Virtuales y PSAV a los que podría enfrentarse el país, los que se detallan a continuación:

Amenazas	Vulnerabilidades	Riesgos	Consecuencias	Nivel
Estafa y Fraude Informático	Falta de recursos humanos especializados en materia de AV y las tendencias criminales de su uso, tanto en el ámbito de detección, como de prevención, investigación y persecución penal.	Incremento de delitos de estafa y fraude informático vinculados a AV difícilmente perseguibles por las Autoridades de Orden Público.	Significativas pérdidas económicas para las víctimas, conjugado con un daño reputacional al sistema de justicia nacional, por no dar una respuesta oportuna a los afectados.	**MEDIO**
	Nulo registro de PSAV que pudieran brindar información de interés sobre operaciones sospechosas de LA/FT/FP vinculados a AV.			
	Falta de sensibilización sobre los riesgos que representan las operaciones con AV a los Sujetos Obligados y usuarios en general.			
Acceso indebido a sistemas informáticos y Daños a sistemas informáticos (Ransomware)	Falta de experiencia y conocimientos en la aplicación de recursos tecnológicos para realizar una adecuada verificación de la tecnología utilizada por los PSAV, tanto para el otorgamiento de licencias como para desarrollar la vigilancia y supervisión.	El Ransomware se posiciona como uno de los principales ciberdelitos en Nicaragua, donde piratas informáticos liberan virus que comprometen e inhabilitan sistemas informáticos sensibles, exigiendo un pago de rescate en AV, que luego son lavados o usados para financiar actos terroristas.	Seguridad jurídica y nacional vulnerada por inhabilitación de objetivos sensibles y primordiales para la estabilidad política, legal, económica y social de la nación.	**ALTO**

Lavado de activos	Falta de un diagnóstico para valorar si los medios materiales y tecnológicos con que cuentan actualmente los SO son adecuados para el cumplimiento de los requisitos regulatorios.	Incapacidad de enfrentar el LA/FT/FP asociados a AV, al no contar con las competencias técnicas, tecnológicas y reglamentarias necesarias para hacerle frente a esta nueva modalidad delictiva.	Introducción a la economía nacional de flujo de criptoactivos ilícitos, contaminando el mercado interno.	**MEDIO**
	Carencia de regulación específica que establezca obligaciones de prevención, detección y reporte de actividades relacionadas con el LA/FT/FP para los PSAV regulados y supervisados por la UAF.			
	Ausencia de obligaciones que garanticen la regla de viaje en las transferencias con AV.			
	Insuficiencia de recursos materiales y financieros por parte de las autoridades competentes, para garantizar la regulación, monitoreo y/o supervisión de las actividades de los PSAV.			
	Falta identificar y evaluar los riesgos de LA/FT/FP que surgen de las actividades de las DeFi y que se aplique un enfoque basado en riesgo para garantizar en base al entendimiento de estos, las medidas de prevención, administración y mitigación.			
	Falta de recursos humanos especializados en materia de AV y las tendencias criminales de su uso, tanto en el ámbito de detección, como de prevención, investigación y persecución penal.			

Tráfico de estupefacientes, psicotrópicos y otras sustancias controladas.	Escases de herramientas tecnológicas para el rastreo oportuno de transacciones en cadenas de bloques y la investigación de casos relacionados a AV.	Aumento de rendimientos ilícitos de Narcotraficantes y Lavadores de Activos que tranzan con AV, por falta de una oportuna y efectiva inteligencia financiera e investigación policial.	Disminución de obstáculos para el Narcotráfico y LA, al evitar la incautación u ocupación de dinero fíat ilícito y por ende un aumento del consumo de drogas.	**MEDIO**
	Bajos niveles de capacitación en materia de AV y la tecnología blockchain por parte de las autoridades investigativas y de persecución penal.			
	Utilización de tecnologías y aplicaciones P2P extraterritoriales para realizar criptotrading.			
	Controles o herramientas tecnológicas insuficientes para identificar a las personas naturales o jurídicas que lleven a cabo actividades de PSAV sin la autorización o el registro necesario.			
	Falta de experiencia y conocimientos en la aplicación de recursos tecnológicos para realizar una adecuada verificación de la tecnología utilizada por los PSAV, tanto para el otorgamiento de licencias como para desarrollar la vigilancia y supervisión.	Personas naturales proveen servicios de AV sin la autorización y regulación debida, siendo indetectables por las autoridades competentes.	Usuarios legítimos desprotegidos ante eventuales abusos o descontrol de estos servicios financieros emergentes, exponiéndose a ser objetos del LA/FT/FP.	**BAJO**
Lavado de Activos	Utilización de tecnologías y aplicaciones P2P extraterritoriales para realizar criptotrading.			
Estafa y Fraude Informático	Controles o herramientas tecnológicas insuficientes para identificar a las personas naturales o jurídicas que lleven a cabo actividades de PSAV sin la autorización o el registro necesario.			

	Falta identificar y evaluar los riesgos de LA/FT/FP que surgen de las actividades de las DeFi y que se aplique un enfoque basado en riesgo para garantizar en base al entendimiento de estos, las medidas de prevención, administración y mitigación.	Los SO no detectan operaciones sospechosas de LA vinculados a AV desarrolladas en protocolos de finanzas descentralizadas, que podrían dirigirse al terrorismo o a individuos o entidades sancionadas por proliferación de armas de destrucción masiva.	Integración en protocolos de finanzas descentralizadas de criptoactivos lavados y/o disfrute de bienes y/o servicios adquiridos mediante la transferencia P2P de criptoactivos ilícitos en pro del FT o FP.	**MEDIO**
Acceso indebido a sistemas informáticos y Daños a sistemas informáticos (Ransomware)	Falta de sensibilización sobre los riesgos que representan las operaciones con AV a los SO y usuarios en general.			
Lavado de activos	Utilización de tecnologías y aplicaciones P2P extraterritoriales para realizar criptotrading.			
Tráfico de estupefacientes, psicotrópicos y otras sustancias controladas.	Nulo registro de PSAV que pudieran brindar información de interés sobre operaciones sospechosas de LA/FT/FP vinculados a AV.			

Como recomendaciones generales de mitigación a los riesgos determinados, se sugieren las siguientes:

a. Reforzar la protección y seguridad informática en la infraestructura tecnológica de las autoridades competentes de investigación y persecución penal, así como de instituciones sensibles para la seguridad jurídica y nacional, de la mano con la actualización de la estrategia nacional de ciberseguridad.

b. Promover eventos formativos permanentes para las autoridades competentes y sujetos obligados, que propicie una comprensión constante de estas tecnologías y su entorno cambiante, así como, la gestión de recursos para la obtención de certificaciones internacionales en esta materia para funcionarios públicos vinculados al enfrentamiento de los delitos de LA/FT/FP.

c. Promover cooperaciones internacionales bilaterales tendientes a que países con más experiencia en la temática compartan sus conocimientos y así ampliar el entendimiento-país sobre estas novedosas operaciones financieras.

d. Divulgar la presente Evaluación de Riesgos al público en general, para lograr una amplia comprensión de la ciudadanía y efectuar publicaciones periódicas advirtiendo a los usuarios sobre los riesgos asociados a las transacciones con AV, las estafas y el fraude informático.

e. Mejorar las capacidades tecnológicas de las autoridades competentes de investigación y persecución penal, que permita perseguir las alertas, indicios y evidencias pertinentes en materia de enfrentamiento al LA/FT/FP asociados a AV y PSAV.

f. Evaluar la pertinencia de que personas naturales (cambistas cripto o intercambiadores) que desarrollan criptotrading como negocio, se sometan al licenciamiento y registro normado por el regulador prudencial de los PSAV.

PARTICIPANTES