REPÚBLICA BOLIVARIANA DE VENEZUELA
VICEPRESIDENCIA SECTORIAL DE ECONOMÍA
SUPERINTENDENCIA NACIONAL DE CRIPTOACTIVOS Y ACTIVIDADES CONEXAS (SUNACRIP)

Caracas, 24 MAR. 2022

211º, 163º y 23º

PROVIDENCIA N° 054 -2022

JOSELIT RAMÍREZ
Superintendente Nacional de Criptoactivos y Actividades Conexas (SUNACRIP)

DIRECTRICES RELACIONADAS CON LOS REPORTES DE ACTIVIDADES SOSPECHOSAS VINCULADOS CON EL USO DE TECNOLOGIAS FINANCIERAS (FINTECH), FORMULADAS POR LA UNIDAD NACIONAL DE INTELIGENCIA FINANCIERA (UNIF)

La Superintendencia Nacional de Criptoactivos y Actividades Conexas, en aplicación de los principios de cooperación interinstitucional y de prevención de operaciones ilícitas, consagrados en el artículo 4 del Decreto Constituyente Sobre el Sistema Integral de Criptoactivos y en ejercicio de la atribución conferida por el numeral 5 del artículo 11 del citado Decreto Constituyente, de velar por el apego del Sistema Integral de Criptoactivos a las disposiciones y mejores prácticas que le resulten aplicables en materia de prevención y control de riesgos de legitimación de capitales, financiamiento al terrorismo y financiación de la proliferación de armas de destrucción masiva, en concordancia con la normativa especial nacional vigente, los Convenios Internacionales suscritos y ratificados por nuestro país relativos a la prevención, administración y mitigación de dichos riesgos, así como en cumplimiento de las Recomendaciones y Estándares Internacionales emitidos por el Grupo de Acción Financiera Internacional (GAFI), informa a todos los Sujetos Obligados del Sistema Integral de Criptoactivos, sometidos a su regulación y supervisión, acerca de las siguientes "DIRECTRICES RELACIONADAS CON LOS REPORTES DE ACTIVIDADES SOSPECHOSAS VINCULADOS CON EL USO DE TECNOLOGÍAS FINANCIERAS (FINTECH), FORMULADAS Y EMITIDAS POR LA UNIDAD NACIONAL DE INTELIGENCIA FINANCIERA (UNIF)", mediante Circular identificada con la nomenclatura UNIF-DDG-DSU-03078, de fecha 27 de octubre de 2021, las cuales son de obligatorio cumplimiento:

De conformidad con lo dispuesto en los artículos 3 y 4 numerales 11 y 12, 8 y 10 del Decreto N° 3.656 de Adecuación de la Unidad Nacional de Inteligencia Financiera (UNIF), publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.522, de fecha 12 de noviembre de 2018, los Convenios y Acuerdos Internacionales suscritos por la República Bolivariana de Venezuela; así como, las Recomendaciones y Estándares Internacionales emitidos por el Grupo de Acción Financiera Internacional (GAFI), relacionados con la lucha contra el lavado de activos (legitimación de capitales para Venezuela), el financiamiento al terrorismo y el financiamiento a la proliferación de armas de destrucción masiva (LC/FT/FPADM), en esta ocasión asociado específicamente con la Recomendación del GAFI No. 15 "Nuevas Tecnologías"; se emiten las siguientes pautas dirigidas a los Sujetos Obligados que desarrollan y/o utilizan Tecnología Financiera (FINTECH) o tienen relaciones de negocios con Instituciones FINTECH, a los fines de fortalecer los mecanismos de monitoreo, detección, análisis y remisión a la UNIF de Reportes de Actividades Sospechosas (RAS) presuntamente vinculados con la LC/FT/FPADM, por la utilización de estos avances tecnológicos.

INTRODUCCION

El desarrollo de las nuevas tecnologías se ha incrementado de forma acelerada en el mundo entero, con propuestas comerciales innovadoras e inclusivas, las cuales han evolucionado de forma disruptiva los modelos de negocio de las Instituciones Financieras tradicionales. El uso de la tecnología digital en actividades financieras y de inversión (Tecnología FINTECH), incluyen nuevos productos dentro de Instituciones Financieras, formas de pago y servicios de almacenamiento de valor.

A continuación se citan ejemplos de Tecnología FINTECH: pasarelas de pago, billeteras virtuales (Wallet), sistemas de pago sin contacto, canales electrónicos a través de la utilización de cajeros automáticos "ATM", tarjetas virtuales prepagadas, equipos de punto de venta físicos y virtuales "POS/MPOS", robot de voz interactivo "IVR", banca por internet aprovechando la plataforma de pago automático o pago electrónico, pago móvil "P2P, P2C y C2P", interfaz de programación de aplicaciones que permiten que productos y servicios se comuniquen con otras aplicaciones (APIs), inteligencia artificial, aplicaciones de teléfonos móviles Inteligentes, tabletas u ordenadores "APPS", computación en la nube "Cloud Computing", datos masivos "Big Data", desarrollo de contratos inteligentes, apertura de cuentas bancarias a través de nuevas tecnologías, soluciones bancarias multiplataformas, entre otros.

El uso de las FINTECH son transversales en los distintos sectores financieros y económicos (bancario, seguros, valores, actividades y profesiones no financieras designadas "APNFD" y los proveedores de servicios de activos virtuales "PSAV"), los cuales conllevan a riesgos

inherentes de ser utilizadas por la Delincuencia Organizada en todas sus modalidades para la LC/FT/FPADM, ya que proporcionan nuevos métodos de transmisión de valor a través de internet con alcance transfronterizo, por cuanto la naturaleza y servicio de los productos permiten movilizar fondos o valores rápidamente a nivel mundial y su tecnología implícita podría facilitar transacciones con seudónimos o anonimato.

De acuerdo a los estándares internacionales, los países desde las Instituciones Financieras, APNFD y PSAV, deben identificar y evaluar los riesgos de LC/FT/FPADM que pudieran surgir con respecto al desarrollo de nuevos productos y prácticas comerciales, incluyendo mecanismos de envío y uso de innovaciones tecnológicas o tecnologías en desarrollo. Para gestionar y mitigar los riesgos que surjan, las naciones deben garantizar que los Sujetos Obligados que desarrollan y/o utilizan Tecnología Financiera (FINTECH) o tienen relaciones de negocios con Instituciones Financieras FINTECH, tengan licencia, sean regulados en materia de Prevención y Control de LC/FT/FPADM y estén sujetos a procesos de supervisión para garantizar el cumplimiento de las medidas relevantes requeridas en las Recomendaciones del GAFI.

En lo que respecta al marco jurídico nacional, la Constitución de la República Bolivariana de Venezuela en su artículo 110 reza lo siguiente: "El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país... Asimismo, el mencionado artículo dispone"... El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La Ley determinará los modos y medios para dar cumplimiento a esta garantía." Adicionalmente, en el artículo 299 de la Carta Magna, señala al Estado conjuntamente con la iniciativa privada para promover el desarrollo armónico de la economía nacional.

En ese orden de ideas, la Unidad Nacional de Inteligencia Financiera (UNIF), con el firme propósito de contribuir con los principios de solidez, transparencia, eficiencia, confiabilidad y sustentabilidad del desarrollo económico y social del sector financiero, APNFD y PSAV; emite directrices relacionadas con: Señales de Alerta, Controles Internos, Riesgos y Reportes de Actividades Sospechosas (RAS), para robustecer los mecanismos de monitoreo, detección, análisis y remisión a la UNIF de los Reportes de Actividades Sospechosas presuntamente vinculados con la LC/FT/FPADM, por la utilización de las FINTECH.

SEÑALES DE ALERTA

A continuación, se detallan un conjunto de indicadores que permitirán identificar comportamientos atípicos vinculados con operaciones realizadas a través de las FINTECH, presuntamente relacionados con la LC/FT/FPADM:

- Clientes o usuarios que realicen operaciones con FINTECH en Instituciones que no cuenten con la debida autorización de funcionamiento emitida por el Ente de Control y Regulación.
- Clientes o usuarios que utilicen FINTECH, los cuales se nieguen o no suministren datos para su identificación y verificación; así como, la del propietario o beneficiario final en caso que sea persona jurídica.
- Clientes o usuarios que presenten documentos de identificación expirados o cuya veracidad no pueda ser convalidada.
- Clientes que se rehúsen o eviten entregar información relacionada con su actividad económica, ocupación o fuente generadora de ingresos.
- Clientes o usuarios que manifiesten robo de identidad o acceso indebido en las cuentas que tienen en las plataformas FINTECH, y que posteriormente se tenga conocimiento que fueron utilizadas para realizar operaciones fraudulentas en línea.
- Clientes que utilicen redes sociales, páginas web o anuncios falsos, para realizar operaciones fraudulentas con FINTECH.
- Clientes o usuarios objeto phishing, smishing, estafas en línea, secuestro de datos, robo de información financiera y confidencial, fuga de datos, malware móvil, ransomware, entre otros riesgos tecnológicos.
- Operaciones con clientes o usuarios que mantengan cuentas y billeteras virtuales anónimas, innominadas o con nombres ficticios.
- Clientes o usuarios con cuentas y billeteras virtuales abiertas para facilitar transacciones con altas sumas de fondos representados en activos virtuales provenientes de billeteras virtuales de los cuales no pueda determinarse los datos de identificación del titular de la contraparte.
- Información pública (noticias criminis, listas de nominación nacional e internacional, entre otras) sobre la presunta relación del cliente o usuarios en actividades de legitimación de capitales, narcotráfico, terrorismo, corrupción gubernamental, fraude y otros delitos conexos investigados por las autoridades del orden público.

- Clientes o usuarios que soliciten servicios de intercambio entre activos virtuales y monedas fiduciarias, una o más formas de activos virtuales, remesas o fondos representados en criptoactivos, directo entre pares (igual a igual), quioscos o cajeros automáticos inteligentes, pagos de terceros desconocidos, emisión, oferta y/o venta de un activo o agentes, que actúen en nombre de terceros.

CONTROLES INTERNOS

Los Sujetos Obligados que se vinculan con las FINTECH, deben adoptar una cultura de cumplimiento e instaurar las políticas y procedimientos integrales de administración de riesgos en materia de Prevención y Control de LC/FT/FPADM, de acuerdo a su naturaleza, tamaño, volumen de operaciones, ubicación geográfica, niveles de riesgo, disponibilidad tecnológica e instrucciones emanadas del Órgano de Control Competente, a los fines de mitigar la posibilidad de ser utilizados como mecanismos para LC/FT/FPADM.

En ese sentido, les corresponderá instaurar procesos y sistemas tecnológicos que permitan hacer un registro cronológico de las transacciones efectuadas a través de la plataforma tecnológica utilizada, identificar el origen y destino de los fondos, la dirección del protocolo de internet (IP) utilizada y el usuario; así como, implementar controles para detectar eventos presuntamente vinculados con fraudes de origen interno y externo, operaciones inusuales y/o sospechosas asociadas a la LC/FT/FPADM.

RIESGOS EN MATERIA DE LC/FT/FPADM VINCULADOS CON EL ECOSISTEMA FINTECH.

- Aumento en la utilización del dinero fiduciario en su representación electrónica o digital (criptoactivos) mediante las FINTECH, en sustitución del papel moneda en efectivo, para adquirir bienes y servicios.
- Acrecentamiento vertiginoso de los proveedores de servicios financieros con Tecnología FINTECH: billeteras virtuales, pasarelas de pago, aplicativos para hacer trading desde equipos electrónicos (tabletas, celulares) y el desarrollo de la tecnología Blockhain en distintas áreas (finanzas, salud, entre otros), sin la debida autorización de parte de los reguladores nacionales e internacionales.
- Aumento de la inclusión financiera digital.
- Uso masivo de las FINTECH para evadir las sanciones del Consejo de Seguridad de las Naciones Unidas y otras inhabilitaciones locales o extranjeras.
- El anonimato inherente en la minería y comercialización de criptomonedas.

- Clientes o usuarios que estén designados en las Listas Ejecutivas de las Resoluciones del Consejo de Seguridad de las Naciones Unidas u otras listas internacionales relacionadas con la LC/FT/FPADM y otros Delitos de la Delincuencia Organizada.
- Clientes o usuarios con volumen de transacciones inusuales, en comparación con lo que pudiese esperarse razonablemente de acuerdo al perfil registrado (no se corresponda con la actividad económica y el nivel de ingresos declarado).
- Clientes o usuarios con nacionalidad o domicilio en países categorizados con riesgo alto en materia de LC/FT/FPADM.
- Clientes, usuarios, personas naturales o jurídicas constituidas o establecidas en países, zonas geográficas y jurisdicciones cuya legislación facilite el secreto bancario o el secreto de registro, insuficientes regulaciones en la materia similares a la República Bolivariana de Venezuela; o que contemplen tributos reducidos o inexistentes (paraísos fiscales).
- Clientes categorizados como PEP´s (Persona Expuesta Políticamente}, con cuentas y billeteras virtuales que traten de evitar el adecuado y completo diligenciamiento de recaudos o no justifiquen adecuadamente el origen de fondos.
- Clientes categorizados como Organizaciones, Fundaciones o Asociaciones sin Fines de Lucro (OSFL), que realicen operaciones mediante Instituciones de Tecnología Financiera, cuya cuantía no guarde relación con el carácter caritativo, religioso, cultural, educativo, social o fraternal indicado en el objeto social, sin justificación alguna del origen de los fondos.
- Clientes o usuarios que ejecuten operaciones con registros de protocolos de internet (IP) distintos a los cotidianos.
- Clientes o usuarios que, al efectuar operaciones consecutivas y estructuradas, eluden entregar información cuando les sea requerida respecto del origen y destino de los fondos.
- Clientes o usuarios que exhiben inusual despreocupación respecto de los riesgos que asumen en las operaciones efectuadas y/o de las comisiones que asumen por las transacciones.
- Clientes o usuarios que realicen operaciones a través de personas jurídicas, de empresas intermedias u otras estructuras jurídicas, sin ningún fundamento claro de índole comercial o de otro tipo, que aumenten innecesariamente la complejidad de la operación o impliquen una falta de transparencia.
- Usuarios que efectúen los pagos mediante operaciones inusuales, complejas o estructuradas.

- Pagos mediante la utilización de billeteras virtuales, pasarelas de pago y/o criptoactivos, en la dinámica criminal de la Delincuencia Organizada.
- Rebeldía de la comunidad FINTECH para estar regulada y supervisada por los Entes Gubernamentales.
- Creación de Desarrollos Financieros (DEFI) descentralizados con tecnología blockchain, que ofrecen acceso a activos virtuales de una forma desregularizada y sin los protocolos de la Política Conozca a su Cliente.
- Utilización de billeteras virtuales para hacer transferencias y remesas internacionales no reguladas y supervisadas por las autoridades venezolanas, ante la imposibilidad de recibir y realizar transferencias de divisas a nivel internacional a través de los bancos tradicionales mediante el Sistema Swift, como consecuencia de las sanciones económicas unilaterales interpuestas por los Estados Unidos de América y sus países aliados.

REPORTES DE ACTIVIDADES SOSPECHOSAS.

La Unidad Nacional de Inteligencia Financiera es el centro para la recepción y análisis de los Reportes de Actividades Sospechosas (RAS) y otra información relevante, presuntamente vinculada con la LC/FT/FPADM y otros delitos determinantes asociados, de acuerdo con lo dispuesto en la Recomendación Nº 29 del GAFI; en concordancia con lo señalado en los artículos 13, 24 y 25 de la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT) y el artículo 2 del Decreto de Adecuación de la UNIF que establece: "La Unidad Nacional de Inteligencia Financiera (UNIF) tiene como objeto centralizar, procesar y analizar los RAS remitidos por los distintos sujetos obligados designados por la Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo, a fin de revelar al Ministerio Publico, información que pueda evidenciar la posible comisión de hechos punibles y la identificación de sus autores y participes, si fuere el caso; así como, la información que requieran para realizar sus investigaciones. De igual manera, en el ejercicio de sus funciones procesará y revelará información de importancia estratégica de naturaleza administrativa de utilidad para la Oficina Nacional Contra la Delincuencia Organizada y Financiamiento al Terrorismo, Entes y Órganos de Control y el cumplimiento de los fines del Estado en general".

En la página web de la UNIF (http://www.unif.gob.ve/unif circulares/), en la sección publicación/circulares se encuentra el Instructivo del Formulario RAS (PE-UNIF-005), publicado mediante la Circular Nº UNIF-DIF-DAE-00028 del 14/02/2019, el cual debe ser tomado en cuenta por los Sujetos Obligados y las Instituciones de Tecnología Financiera (FINTECH) según su contexto y riesgos, para establecer los mecanismos de debida diligencia en la

detección, análisis y reporte oportuno de actividades y operaciones sospechosas en materia de prevención de LC/FT/FPADM. Conviene destacar lo establecido en la Recomendación Nº 21 del GAFI sobre revelación (tipping-off) y confidencialidad, en concordancia con el artículo 14 de la LOCDOFT y el artículo 5 del Decreto de Adecuación de la UNIF.

Por los sustentos esbozados, los Órganos y Entes de Control, así como los Sujetos Obligados y las Instituciones de Tecnología Financiera (FINTECH) con licencia para operar dentro del territorio nacional, deben acatar las pautas indicadas, con especial énfasis en los mecanismos de monitoreo y detección de operaciones inusuales y actividades sospechosas presuntamente vinculadas con la LC/FT/FPADM y otros ilícitos de Delincuencia Organizada.

Cabe resaltar que el incumplimiento de las "DIRECTRICES RELACIONADAS CON LOS REPORTES DE ACTIVIDADES SOSPECHOSAS VINCULADOS CON EL USO DE TECNOLOGÍAS FINANCIERAS (FINTECH), FORMULADAS Y EMITIDAS POR LA UNIDAD NACIONAL DE INTELIGENCIA FINANCIERA (UNIF)", conllevará a la aplicación de las sanciones respectivas, de conformidad con lo previsto en el ordenamiento jurídico nacional.

Esta Providencia entrará en vigencia a partir de su publicación en la Página Web Oficial de la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP).

REPÚBLICA BOLIVARIANA DE VENEZUELA
SUNACRIP
DESPACHO DE LA SUPERINTENDENCIA NACIONAL DE CRIPTOACTIVOS Y ACTIVIDADES CONEXAS

JOSELIT RAMÍREZ
Superintendente Nacional de Criptoactivos
y Actividades Conexas (SUNACRIP)
Decreto Nº 3.471 de fecha 19 de junio de 2018
Gaceta Oficial de la República Bolivariana de Venezuela
Nº 41.422 del 19 de junio de 2018