BOLETÍN INFORMATIVO*

NORMAS

ADMINISTRACIÓN Y FISCALIZACIÓN DE LOS RIESGOS RELACIONADOS CON LA LEGITIMACIÓN DE CAPITALES, EL FINANCIAMIENTO DEL TERRORISMO Y EL FINANCIAMIENTO DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA,

PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES Y A LAS PERSONAS Y ENTIDADES QUE PROPORCIONEN PRODUCTOS Y SERVICIOS A TRAVÉS DE ACTIVIDADES QUE INVOLUCREN ACTIVOS VIRTUALES, EN EL SISTEMA INTEGRAL DE CRIPTOACTIVOS

En la Gaceta Oficial de la República Bolivariana de Venezuela signada con el número 42.110 de fecha 21 de abril de 2021 fue publicado por la Vicepresidencia Sectorial de Economía a través de la Superintendencia Nacional de Criptoactivos y Actividades Conexas Providencia mediante la cual se dictan las Normas relativas a la administración y fiscalización de los riesgos relacionados con la legitimación de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, aplicables a los proveedores de servicios de activos virtuales y a las personas y entidades que proporcionen productos y servicios a través de actividades que involucren activos virtuales, en el Sistema Integral de Criptoactivos.

Establece lo siguiente:

REPÚBLICA BOLIVARIANA DE VENEZUELA
VICEPRESIDENCIA SECTORIAL DE ECONOMÍA
SUPERINTENDENCIA NACIONAL DE CRIPTOACTIVOS Y ACTIVIDADES CONEXAS
Caracas, 21 de abril de 2021
211º, 162º y 22º
PROVIDENCIA N° 044-2021
JOSELIT RAMÍREZ

Superintendente Nacional de Criptoactivos y Actividades Conexas

En ejercicio de las atribuciones conferidas por los artículos 7, 8, 10 y los numerales 2 y 5 del artículo 11 del Decreto Constituyente sobre el Sistema Integral de Criptoactivos, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 41.575, de fecha 30 de enero de 2019, se dictan las siguientes:

NORMAS RELATIVAS A LA ADMINISTRACIÓN Y FISCALIZACIÓN DE LOS RIESGOS RELACIONADOS CON LA LEGITIMACIÓN DE CAPITALES, EL

FINANCIAMIENTO DEL TERRORISMO Y EL FINANCIAMIENTO DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA, APLICABLES A LOS PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES Y A LAS PERSONAS Y ENTIDADES QUE PROPORCIONEN PRODUCTOS Y SERVICIOS A TRAVÉS DE ACTIVIDADES QUE INVOLUCREN ACTIVOS VIRTUALES, EN EL SISTEMA INTEGRAL DE CRIPTOACTIVOS

Por cuanto

El ecosistema de los activos virtuales está evolucionando e incorporando una gama de nuevas tecnologías y servicios asociados a los mismos, así como también está generando nuevos modelos de negocio y tipos de transacciones que conllevan riesgos inherentes de ser utilizados para que delincuentes y terroristas laven sus ganancias o financien sus actividades ilícitas, ya que proporcionan nuevos métodos de transmisión de valor a través de Internet.

Por cuanto

El alcance global de las actividades de los Proveedores de Servicios de Activos Virtuales, así como la naturaleza transfronteriza de los productos y servicios que involucran activos virtuales, permiten movilizar fondos o valores rápidamente a nivel mundial y su tecnología implícita podría facilitar transacciones con seudónimo o anonimato, lo cual hace que los delincuentes puedan querer abusar de los mismos para fines de delincuencia organizada, legitimación de capitales, financiamiento al terrorismo y financiamiento de la proliferación de armas de destrucción masiva.

Por cuanto

Los protocolos subyacentes sobre los cuales se basan varios de los nuevos productos de pago y servicios que involucran activos virtuales, no requieren ni proporcionan identificación y verificación de los participantes y los registros históricos de las transacciones generadas en la cadena de bloques (Blockchain) no están necesariamente asociados con la identidad en el mundo real, lo cual implica mayores riesgos en esta materia, que deben ser identificados y mitigados.

Por cuanto

Es obligación de la República Bolivariana de Venezuela prevenir que el Sistema Integral de Criptoactivos sea utilizado como canal para realizar actividades ilícitas relacionadas con la legitimación de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva y que la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP) está facultada para velar por el apego del mencionado Sistema a las disposiciones y mejores prácticas que le resulten aplicables en materia de prevención, control y fiscalización de dichos riesgos.

Por cuanto

Las actividades, productos y servicios que involucran activos virtuales son susceptibles de ser utilizados indebidamente por la delincuencia organizada, como instrumentos para la legitimación de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, lo cual podría afectar los procesos económicos, políticos y sociales del país,

En virtud de lo anterior:

La Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP), en uso de las atribuciones que le confieren los artículos 7, 8, 10 y los numerales 2 y 5 del artículo 11 del Decreto Constituyente sobre el Sistema Integral de Criptoactivos, resuelve dictar las siguientes normas:

TÍTULO I

CAPÍTULO I

DISPOSICIONES GENERALES

Artículo 1: Esta Providencia tiene por objeto establecer las normas, actuaciones y controles que, como mínimo, deben adoptar y ejecutar los Sujetos Obligados para prevenir y mitigar el riesgo que sus actividades y operaciones sean utilizadas como mecanismos para legitimar capitales provenientes de actividades ilícitas o para financiar el terrorismo o la proliferación de armas de destrucción masiva, tomando en cuenta su nivel de riesgo determinado en base a sus respectivas evaluaciones.

Artículo 2: Esta norma está dirigida a las personas y entidades, públicas y privadas, que proporcionen a terceros productos y servicios a través de actividades que involucren activos virtuales o criptoactivos, en o desde el territorio de la República Bolivariana de Venezuela. Entre los Sujetos Obligados por esta norma se encuentran la Tesorería de Criptoactivos de Venezuela, S.A., que es competente para la comercialización, recaudación y distribución de activos virtuales, así como las Casas de Intercambio de Criptoactivos con licencia para operar en el territorio nacional, las cuales brindan infraestructura para la negociación de activos virtuales. Están incluidos dentro de la categoría de Sujetos Obligados por estas normas, los Proveedores de Servicios de Activos Virtuales, los cuales, según la Guía para un Enfoque Basado en Riesgo de Activos Virtuales y Proveedores de Servicios de Activos Virtuales, elaborada por el Grupo de Acción Financiera Internacional, son definidos de la siguiente manera:

Proveedor de Servicios de Activos Virtuales: Cualquier persona física o jurídica que realice como conducta empresarial, una o más de las siguientes actividades u operaciones, para o en nombre de otro, sea persona natural o jurídica: 1.-) Intercambio entre activos virtuales y monedas fiduciarias, 2.-) Intercambio entre una o más formas de activos virtuales, 3.-) Transferencia de activos virtuales, 4.-) Custodia y/o administración de activos virtuales o de instrumentos que permitan el control sobre activos virtuales y 5.-) Participación y prestación de servicios financieros relacionados con la emisión, oferta y/o venta de un activo virtual.

Entre los Sujetos Obligados por esta norma se encuentran los proveedores de cuentas y billeteras de activos virtuales, así como también quienes, como conducta empresarial, albergan billeteras de terceros, mantienen la custodia o el control de activos virtuales, billeteras o claves privadas de otra persona física o jurídica, así como los propietarios, operadores y administradores de cajeros automáticos de activos virtuales.

Igualmente se encuentran obligados por estas normas, en todo cuanto les resulte aplicable, los propietarios, operadores y administradores de las plataformas tecnológicas y sitios web que, como conducta empresarial, participen en actividades o transacciones, para o en nombre de otro, que involucren activos virtuales y en la prestación de servicios de intermediación, préstamos, comercialización, intercambio y transferencia de valores representados en activos virtuales, que operen en o desde el territorio de la República Bolivariana de Venezuela. Estas plataformas tecnológicas y sitios web deben estar autorizadas por la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP), para operar en o desde el territorio nacional.

Cuando existan diferencias significativas entre las leyes, regulaciones, normas y medidas sobre prevención de LC/FT/FPADM que aplican dichas plataformas tecnológicas y sitios web, conforme a su jurisdicción de origen y las leyes, regulaciones, normas y medidas venezolanas, sus propietarios, operadores y administradores deben implementar las medidas que se establecen en esta Providencia, agregando aquellas contenidas en las normas de su jurisdicción de origen, que resulten más estrictas que las exigidas en la República Bolivariana de Venezuela.

Los Proveedores de Servicios de Activos Virtuales y demás Sujetos Obligados por estas Normas, deben contar con las respectivas autorizaciones o licencias otorgadas por la Superintendencia Nacional de Criptoactivos y Actividades Conexas (SUNACRIP) para operar, ofrecer productos y brindar servicios a terceros, que involucren activos virtuales, en o desde el territorio de la República Bolivariana de Venezuela.

Artículo 3: Los Sujetos Obligados por estas normas deben establecer políticas, métodos y mecanismos internos de control, aprobados por la Junta Directiva o el órgano que ejerza funciones equivalentes, que les permitan prevenir, administrar y mitigar sus riesgos identificados en materia de LC/FT/FPADM, así como también deben demostrar que los han implementado y puesto en práctica, cuando les sea requerido por este Organismo. Igualmente, deben verificar y hacer seguimiento a la implementación efectiva de dichos controles internos e intensificarlos en caso de ser necesario.

Artículo 4: A los efectos de estas normas, los términos indicados en este artículo, tanto en mayúscula como en minúscula, singular o plural, masculino o femenino, tendrán los siguientes significados:

a. Activos Virtuales: Son una representación digital de valor que se puede comercializar o transferir digitalmente y puede utilizarse para fines de pago o inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiduciarias.

b. Armas de Destrucción Masiva: Son aquellas armas diseñadas para matar a una gran cantidad de personas, dirigidas tanto a civiles como a militares, con efectos devastadores en las personas, infraestructura y medio ambiente, tales como las armas nucleares, biológicas y las químicas.

c. Casa de Intercambio de Criptoactivos: Son personas jurídicas que tienen como objetivo brindar la plataforma o infraestructura tecnológica de intermediación y negociación, para que personas naturales y jurídicas puedan realizar operaciones de intercambio y transferencia que involucren activos virtuales.

d. Beneficiario Final: El significado de este término depende del contexto en el que se utilice y puede ser:

d.1. La(s) persona(s) natural(es) que final y efectivamente, en forma directa o indirecta, posee(n) o controla(n) a un cliente o usuario ocasional que sea una estructura o persona jurídica.

d.2 La(s) persona(s) natural(es) que ejerce(n) influencia significativa sobre la cuenta o relación.

d.3. La(s) persona(s) natural(es) en cuyo nombre o beneficio se realiza una transacción.

e. Cliente: Persona natural o jurídica, pública o privada, que adquiere o contrata productos y/o servicios ofrecidos por un Sujeto Obligado, basados en activos virtuales o criptoactivos y sus tecnologías conexas.

f. Factor de Riesgo de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva: Es toda circunstancia o situación que aumenta la probabilidad que el Sujeto Obligado sea utilizado consciente o inconscientemente para dichas actividades delictivas. Estos factores generadores de riesgo permiten identificar y analizar los riesgos y los agentes que los generan, así como diseñar la matriz de riesgo, entre los cuales se encuentran:

o Clientes.

o Productos, negocios y servicios que involucren activos virtuales.

o Canales de distribución.

o Uso de tecnologías nuevas o en desarrollo.

o Tipos de activos virtuales involucrados en las operaciones

g. Financiamiento al Terrorismo: Es el acto de proporcionar, facilitar, resguardar, administrar, colectar o recabar fondos por cualquier medio, directa o indirectamente, con el propósito de que éstos sean utilizados en su totalidad o en parte por un terrorista individual o por una organización terrorista, o para cometer uno o varios actos terroristas, aunque los fondos no hayan sido efectivamente utilizados o no se haya consumado el acto o los actos terroristas.

h. Financiamiento de la Proliferación de Armas de Destrucción Masiva: Es el acto de proporcionar fondos o servicios financieros en cualquier forma o modalidad, que se utilizan, en todo o en parte, para la fabricación, adquisición, posesión, desarrollo, exportación, transbordo, corretaje, transporte, transferencia, almacenamiento o uso de armas nucleares, químicas o biológicas y sus vectores y materiales relacionados (incluidos ambos tecnologías y bienes de doble uso utilizados para fines no legítimos), en contravención de las leyes nacionales y acuerdos internacionales aplicables.

i. Fuentes Creíbles: Se refiere a información que es producida por organismos bien conocidos que generalmente son vistos como de buena reputación y que hacen esta información pública. Además del Grupo de Acción Financiera Internacional (GAFI) y sus homólogos, estas fuentes incluyen, pero no se limitan, a cuerpos supra nacionales o internacionales como el Grupo Egmon de Unidades de Inteligencia Financiera, así como también organismos gubernamentales nacionales. La información suministrada por estas fuentes creíbles no tiene efectos de una ley o reglamento y no debe considerarse como una determinación automática de que algo sea de mayor riesgo.

j. Gobierno Corporativo: Conjunto de reglas que ordenan de forma transparente las relaciones y el comportamiento de la Junta Directiva o del órgano que ejerza función equivalente del Sujeto Obligado, los accionistas, la Gerencia, los clientes, usuarios y otros participantes interesados. Estas reglas también definen los objetivos estratégicos de la institución, los medios, recursos y procesos para alcanzar dichos objetivos, así como los sistemas de verificación del seguimiento de las responsabilidades y controles correspondientes a cada nivel de la estructura de la entidad.

k. Métodos: Son las actuaciones o procedimientos implementados por el Sujeto Obligado para llevar a cabo una determinada actividad en el Sistema Integral de Administración de Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva.

l. Operación Compleja: Aquella que se compone de transacciones o elementos diversos, es decir, que contiene varias operaciones de diferente clasificación, configuradas por un conjunto o unión de éstas. Para determinar las condiciones inusitadas de complejidad de operaciones se debe tener en cuenta la clase de transacción, ya que ésta por su naturaleza puede no ser sencilla, pero para el empleado que opera activos virtuales o criptoactivos, esta situación habitual es convencional. Lo que determina la forma compleja de esta clase de operación, es la orden del cliente o usuario que pueda complicar una transacción normalmente simple.

m. Operación en Tránsito: Aquella por la cual el Sujeto Obligado sirve de escala entre el origen y el destino de la operación, ya sea esta nacional o internacional.

n. Operación Inusual: Aquella cuya cuantía o características no guarda relación con la actividad económica y perfil del cliente o por su número, por las cantidades transadas, o por sus características, se escapan de los parámetros de normalidad establecidos para un rango determinado de mercado.

o. Operación No Convencional: Aquella que no esté de acuerdo o en consonancia con los precedentes, costumbres o usos del ecosistema de los activos virtuales o criptoactivos y que no se ajusta a los procedimientos requeridos en esa clase de operaciones. Esta categoría también se puede aplicar cuando se comprenda que toda operación está integrada por un conjunto de fases, y se omite una o varias de ellas, o se sigue un procedimiento no establecido regularmente por la institución.

p. Políticas: Son los lineamientos generales que deben adoptar los Sujetos Obligados relacionados con el Sistema Integral de Administración de Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva. En cada una de sus etapas y elementos el citado sistema debe contar con unas políticas claras y efectivamente aplicables, dichas políticas deben permitir el eficiente, efectivo y oportuno funcionamiento del citado sistema y traducirse en reglas de conducta y métodos que orienten a la Gerencia en la implementación de controles efectivos.

q. Programa de Cumplimiento: Recopilación del conjunto de políticas, normas, métodos y controles internos implementados por el Sujeto Obligado para mitigar y controlar los riesgos de legitimación de capitales, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva.

r. Riesgos Asociados a la Legitimación de Capitales, el Financiamiento del Terrorismo y el Financiamiento de la Proliferación de Armas de Destrucción Masiva: La posibilidad de sufrir pérdidas, daños o consecuencias perjudiciales, directa o indirectamente, a que están expuestos los Sujetos Obligados, si se materializan en sus actividades y operaciones la legitimación de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. Incluye la posibilidad de sanciones contra los directivos y empleados del Sujeto Obligado, cuando las mencionadas actividades ilícitas hayan sido facilitadas por negligencia, impericia o inobservancia de la ley con que hayan actuado en el desempeño de sus obligaciones; estos riesgos son: reputacional, legal, operativo y de contagio.

s. Riesgo de Contagio: Es la posibilidad de pérdida o daño que un Sujeto Obligado puede sufrir, directa o indirectamente, por una acción o experiencia de un relacionado o asociado. El relacionado o asociado incluye personas naturales o jurídicas que tienen la posibilidad de ejercer influencia sobre el Sujeto Obligado.

t. Riesgo de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva: Es la posibilidad que un Sujeto Obligado sea utilizado directamente o a través de sus actividades y operaciones, como instrumento para la legitimación de capitales, el financiamiento al terrorismo y el financiamiento de la proliferación de armas de destrucción masiva.

u. Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

v. Riesgo Legal: Es la contingencia o posibilidad de pérdida que emana del incumplimiento, por parte del Sujeto Obligado, de las leyes, normas, reglamentos, prácticas prescritas o normas de ética de cualquier jurisdicción en la que lleva a cabo sus actividades.

w. Riesgo Operacional: Es la posibilidad de sufrir daños potenciales y pérdidas, motivados en la forma de organización del Sujeto Obligado y en la estructura de sus métodos de gestión, debilidades en sus controles internos, errores en el procesamiento de sus operaciones, fallas de seguridad e inexistencia o desactualización de sus planes de contingencia del negocio, así como la potencialidad de sufrir pérdidas inesperadas por sistemas inadecuados, fallas administrativas, eventos externos, deficiencias en sus controles internos y sistemas de información originadas, entre otros, por errores humanos, fraudes, incapacidad para responder de manera oportuna o impedir que los intereses del Sujeto Obligado se vean comprometidos de cualquier manera.

x. Riesgo de Reputación: Es la posibilidad de sufrir pérdidas o daños derivados de la opinión negativa ocasionada por la afectación de la imagen de un Sujeto Obligado, al verse involucrado voluntaria o involuntariamente en transacciones o relaciones de negocios ilícitos con clientes o usuarios ocasionales, así como por cualquier otro evento externo.

y. Riesgo Residual o Neto: Es el nivel resultante del riesgo después de aplicar los controles o medidas de mitigación.

z. Segmentación: Es el proceso por medio del cual se lleva a cabo la separación de elementos en grupos homogéneos al interior de ellos y heterogéneos entre ellos. La separación se fundamenta en el reconocimiento de diferencias significativas en sus características (variables de segmentación).

aa. Señales de Alerta: Es el conjunto de indicadores cualitativos y cuantitativos que permiten identificar, oportuna y prospectivamente, comportamientos atípicos de las variables relevantes, previamente determinadas por el Sujeto Obligado.

bb. Sospecha: Aquella apreciación fundada en conjeturas, en apariencias o avisos de verdad (indicios), que determinará hacer un juicio negativo de la operación por quien recibe y analiza la información, haciendo que desconfíe, dude o recele de una persona por la actividad profesional o económica que desempeña, su perfil financiero, sus costumbres o personalidad, así la ley no determine criterios en función de los cuales se puede apreciar el carácter dudoso de una operación. Es un criterio subjetivo basado en las normas de máxima experiencia de hecho.

cc. Sujetos Obligados: A los efectos de estas normas, son las personas públicas y privadas a que hace referencia el artículo 2 de las presentes normas, las cuales se encuentran sometidas a la inspección, supervisión, vigilancia, regulación, control y sanción de la Superintendencia Nacional de Criptoactivos y Actividades Conexas.

dd. Transacción Estructurada: Esquema para intentar evadir los requisitos de reportes o declaraciones que sean fijados por las autoridades competentes, mediante el método de dividir grandes cantidades de fondos o valores representados en activos virtuales, en múltiples montos por debajo del umbral de reporte o declaración. Bajo este esquema, montos relativamente pequeños de fondos o valores representados en activos virtuales pueden ser depositados y movilizados en numerosas cuentas y billeteras virtuales de uno o varios titulares.

ee. Usuarios y usuarias: Toda persona natural o jurídica que, sin ser cliente, eventualmente adquiere o utiliza productos y/o servicios ofrecidos por un Sujeto Obligado, basados en activos virtuales o criptoactivos y sus tecnologías conexas

Artículo 5: A los efectos de estas normas, las siglas y abreviaturas señaladas en este artículo tendrán los siguientes significados:

ABREVIATURA	SIGNIFICADO
DDC:	Debida Diligencia para el conocimiento del Cliente
EBR:	Enfoque Basado en Riesgo
GAFI:	Grupo de Acción Financiera Internacional.
LC/FT/FPADM:	Legitimación de Capitales, Financiamiento al Terrorismo, Proliferación de Armas de Destrucción Masiva
LOCDOFT:	Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo
RAS:	Reporte de Actividad Sospechosa
PCSC:	Política Conozca a su Cliente
PEP:	Persona Expuesta Políticamente
PPAP:	Políticas para la Administración de Riesgos
POA PCLC/FT/EPADM:	Plan Operativo Anual de Prevención y Control de Legitimación de Capitales, Financiamiento al Terrorismo y Proliferación de Armas de Destrucción Masiva.

SIAR LC/FT/DPADM:	Sistema Integral de Administración de Riesgos de legitimación de Capitales, Financiamiento al Terrorismo y proliferación de Armas de Destrucción masiva
SUNACRIP:	Superintendencia Nacional de Criptoactivos y Actividades Conexas
Este Organismo, esta Superintendencia este Ente regulador, este Ente Supervisor	Superintendencia Nacional de Criptoactivos y Actividades Conexas
TCV	Tesorería de Criptoactivos de Venezuela
UNIF::	Unidad Nacional de Inteligencia Financiera

TÍTULO II

ADMINISTRACIÓN INTEGRAL DE RIESGOS DE LC/FT/FPADM

CAPÍTULO I

SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS DE LEGITIMACIÓN DE CAPITALES, FINANCIAMIENTO AL TERRORISMO Y FINANCIAMIENTO DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA (SIAR LC/FT/FPADM)

Artículo 6: El Sujeto Obligado debe formular, adoptar, implementar y desarrollar un Sistema Integral de Administración de Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (SIAR LC/FT/FPADM), soportado en soluciones informáticas y herramientas tecnológicas que, entre otros aspectos, permitan el manejo y análisis de grandes volúmenes de datos, para la toma de decisiones que involucren activos virtuales o criptoactivos. Dicho Sistema Integral debe ser formulado e implementado en concordancia con el nivel de sus riesgos de LC/FT/FPADM, en cumplimiento de las disposiciones legales que rigen la materia y de estas normas

Artículo 7: El SIAR LC/FT/FPADM debe:

1. Brindar capacitación a los empleados del Sujeto Obligado para identificar los riesgos de LC/FT/FPADM y sus factores, detectarlos, mitigarlos y reportarlos, con particular énfasis en la comprensión del manejo de herramientas tecnológicas y soluciones informáticas para la aplicación de medidas y controles en materia de prevención, administración y mitigación de dichos riesgos.

2. Contar con herramientas tecnológicas y soluciones informáticas que faciliten el análisis y manejo de datos e igualmente permitan aplicar medidas y controles de prevención, administración y mitigación de riesgos de LC/FT/FPADM, igualmente, debe contar con el personal suficiente que permita atender en forma oportuna las alertas de actividades sospechosas que arrojen los sistemas de monitoreo.

3. Mantener un enfoque de prevención y control basado en el riesgo, que incluya políticas, normas, métodos y controles internos, matrices de riesgos, sistemas de monitoreo, así como planes operativos, los cuales deben cumplir y ajustarse, en lo que les sea aplicable, al marco jurídico vigente, así como a la normativa, instrucciones y directrices emitidas por este Organismo, al Código de Ética, a las guías y mandatos corporativos, recomendaciones de auditoría, evaluaciones y autoevaluaciones, entre otros, que estén relacionados con la administración de los riesgos de LC/FT/FPADM.

Las mejores prácticas y estándares internacionales constituyen pautas y referencias que se deben tener en cuenta para fortalecer el SIAR LC/FT/FPADM, siempre que no colidan con la normativa nacional vigente.

Artículo 8: Las políticas, métodos, normas y controles internos que adopte e implemente el Sujeto Obligado deben ser incluidos en el respectivo Manual de Administración de Riesgos de Legitimación de Capitales, Financiamiento del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva, el cual será de obligatorio cumplimiento para el Sujeto Obligado.

Artículo 9: Las políticas que adopte el Sujeto Obligado deben cumplir, como mínimo, con los siguientes requisitos:

a. Señalar los lineamientos que adoptará el Sujeto Obligado frente a los factores de riesgo y los riesgos asociados de LC/FT/FPADM.

b. Garantizar la reserva de la información de las personas reportadas.

c. Consagrar la exigencia de que los funcionarios y empleados antepongan el cumplimiento de las normas en materia de administración de riesgos de LC/FT/FPADM al logro de las metas comerciales.

Artículo 10: Los métodos y actuaciones que en esta materia asuma y ejecute el Sujeto Obligado deben cumplir como mínimo con los siguientes requisitos:

a. Identificar la evolución de los perfiles de riesgo de transacciones, clientes, negocios, productos y servicios, actividad económica y activos virtuales involucrados en las operaciones.

b. Implementar las metodologías para la detección y análisis de operaciones inusuales y sospechosas y establecer el proceso para informar de manera oportuna a las autoridades competentes.

c. Establecer los procesos para llevar a cabo un efectivo, eficiente y oportuno conocimiento de los clientes actuales y potenciales, siendo que dichos procesos deben estar soportados en soluciones tecnológicas seguras que permitan identificar a los clientes en forma remota, así como verificar la información suministrada y sus correspondientes soportes.

Artículo 11: El SIAR LC/FT/FPADM tomará en cuenta las tareas básicas que se detallan a continuación:

1. La aplicación de políticas, métodos, normas y controles internos para el adecuado conocimiento de transacciones, clientes, empleados y terceros relacionados, complementado con una constante información, capacitación y entrenamiento del personal del Sujeto Obligado, conforme a las políticas de capacitación previstas en esta Providencia.

2. Control y detección de actividades que se pretendan realizar o se hayan realizado, para dar apariencia de legalidad a operaciones vinculadas a la LC/FT/FPADM, mediante la implementación de controles y herramientas tecnológicas de monitoreo adecuadas, oportunas y efectivas.

3. Reporte oportuno, eficiente y eficaz, de operaciones detectadas que se pretendan realizar o se hayan realizado y que se sospeche estén relacionadas con la LC/FT/FPADM.

4. Conservación por el plazo establecido en estas normas, de todos los archivos, registros de transacciones y documentación, en forma física o digital, derivados de las tareas precedentes, destinados a proporcionar a las autoridades competentes información cuando sea requerido para adelantar sus investigaciones.

5. Resguardo de la información obtenida por medios digitales o físicos, relacionada con las operaciones que involucran activos virtuales o criptoactivos.

Artículo 12: El SIAR LC/FT/FPADM estará integrado por:

1. La Junta Directiva o el órgano que ejerza función equivalente.

2. El Presidente del Sujeto Obligado o quien haga sus veces.

3. El Oficial de Cumplimiento de prevención de legitimación de capitales, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva (en adelante Oficial de Cumplimiento).

Las personas naturales o jurídicas que otorguen créditos o financiamiento o efectúen inversiones mediante recursos o valores propios representados en activos virtuales, no estarán obligados a establecer un SIAR de LC/FT/FPADM, pero estarán obligados a proporcionar a esta Superintendencia los datos estadísticos, estados financieros y demás datos o información periódica u ocasional que esta les solicite.

CAPÍTULO II

OBLIGACIONES Y FUNCIONES DE LA JUNTA DIRECTIVA O EL ÓRGANO QUE EJERZA FUNCIÓN EQUIVALENTE

Artículo 13: La Junta Directiva o el órgano que ejerza función equivalente del Sujeto Obligado, tendrá las siguientes obligaciones y funciones:

1. Asegurar el establecimiento y mantenimiento del SIAR LC/FT/FPADM, proporcionando para ello la infraestructura organizativa, funcional y presupuestaria idónea para que pueda ser eficiente y eficaz.

2. Aprobar las políticas, normas, métodos, planes, programas, controles internos, parámetros de segmentación y cualquier otro instrumento vinculado con la administración de riesgos de LC/FT/FPADM, así como supervisar su cumplimiento.

3. Establecer y aprobar una partida presupuestaria específica e identificable dentro del presupuesto general del Sujeto Obligado, designada anualmente para garantizar la ejecución de las tareas vinculadas con la PCLC/FT/FPADM, dirigiendo especial atención a los programas de capacitación y a la adquisición y mejora de sistemas informáticos y herramientas tecnológicas adecuados para la prevención y mitigación de riesgos de LC/FT/FPADM.

4. Asegurar que el Oficial de Cumplimiento cuente con suficiente autoridad y recursos (humanos, financieros y tecnológicos) para administrar un programa de cumplimiento contra LC/FT/FPADM eficaz, conforme al perfil de riesgo del Sujeto Obligado.

5. Recibir y analizar los informes trimestrales y anuales elaborados por el Oficial de Cumplimiento, relacionados con PCLC/FT/FPADM, tomando las decisiones más significativas y las acciones correctivas, en caso que le sean planteadas deficiencias y debilidades, lo cual debe reflejarse como una función relacionada con el Gobierno Corporativo.

6. Asumir en forma individual y por escrito, el Compromiso Institucional para prevenir la LC/FT/FPADM, el cual deberá estar inserto en el expediente de cada uno de los miembros.

CAPÍTULO III

OBLIGACIONES Y FUNCIONES DEL PRESIDENTE DEL SUJETO OBLIGADO

Artículo 14: El Presidente del Sujeto Obligado o quien haga sus veces, será responsable de:

1. Asegurar que el SIAR LC/FT/FPADM funcione debidamente y que las políticas, normas, métodos y controles internos, así como las decisiones emanadas de la Junta Directiva o el órgano que ejerza función equivalente, sean conocidos y aplicados por las instancias que corresponda.

2. Conocer los informes anuales y trimestrales presentados por el Oficial de Cumplimiento a la Junta Directiva o al órgano que ejerza función equivalente.

CAPÍTULO IV

EL OFICIAL DE CUMPLIMIENTO

Artículo 15: La persona que ejerce el cargo de Oficial de Cumplimiento debe:

1. Ser un empleado de alto nivel, con poder de decisión, que dependa y reporte directamente a la Junta Directiva o al órgano que ejerza función equivalente.

2. Estar jerárquicamente un nivel por debajo del Presidente del Sujeto Obligado o quien haga sus veces, en la estructura organizativa del Sujeto Obligado.

3. Ser una persona de reconocida solvencia moral y ética, conocer la legislación y reglamentación vigente relativa a la materia de PC LC/FT/FPADM, conocer y comprender la estructura del Sujeto Obligado, los negocios, productos y servicios que ofrece, los canales de distribución o comunicación que utiliza, clientes, las tecnologías utilizadas y las nuevas tecnologías o en desarrollo que el Sujeto Obligado pretende utilizar, así como los tipos de activos virtuales involucrados en las operaciones del Sujeto Obligado y los riesgos potenciales de LC/FT/FPADM que están asociados a los mismos.

4. Estar dedicado en forma exclusiva a las funciones de prevención y control de los riesgos relacionados con LC/FT/FPADM

Artículo 16: La autoridad funcional y las decisiones que en el marco de la ejecución de sus actividades ejerza o adopte el Oficial de Cumplimiento, serán de observancia obligatoria por parte de todos los ejecutivos, empleados y unidades del Sujeto Obligado, una vez que dichas decisiones sean aprobadas por la Junta Directiva o el órgano que ejerza función equivalente.

Artículo 17: El Oficial de Cumplimiento tendrá entre sus obligaciones y funciones:

1. Promover el cumplimiento de las políticas, métodos, disposiciones y controles aprobados por la Junta Directiva del Sujeto Obligado, relacionados con el funcionamiento del SIAR LC/FT/FPADM.

2. Conocer los informes, observaciones y recomendaciones en materia de PC LC/FT/FPADM, producto de las inspecciones realizadas por este Organismo y los exámenes practicados por los Auditores independientes, a fin de dar seguimiento a las acciones correctivas relacionadas con las deficiencias o debilidades detectadas.

3. Diseñar un POA PC LC/FT/FPADM, el cual deberá ser presentado a la Junta Directiva o al órgano que ejerza función equivalente, para su aprobación, basado en las políticas, programas, métodos y normas de prevención y control de LC/FT/FPADM

4. Coordinar y supervisar el cumplimiento de la normativa vigente y de los controles internos, por parte de las dependencias que tienen responsabilidad en la ejecución de los planes, programas y normas de prevención y control de riesgos de LC/FT/FPADM.

5. Presentar informes de gestión trimestrales y anuales a la Junta Directiva o al órgano que ejerza función equivalente. Dichos informes periódicos deberán contener como mínimo los siguientes aspectos:

5.1 Diseño de las políticas, métodos, estrategias, planes, programas y normas internas en materia de PC LC/FT/FPADM, así como información de la gestión cumplida.

5.2 Estadísticas relacionadas con:

5.2.1 Número de alertas generadas.

5.2.2 Casos analizados.

5.2.3 Casos pendientes de análisis.

5.3 Descripción de nuevas tendencias o tipologías utilizadas para cometer hechos ilícitos a través del uso de activos virtuales o criptoactivos, sus productos y servicios asociados, a fin de adoptar las medidas orientadas a la mitigación de los riesgos derivados de ellas.

5.4 Recomendaciones para el mejoramiento de los métodos y controles internos adoptados por el Sujeto Obligado en materia de PC LC/FT/FPADM.

6. Elaborar el Programa Anual de Capacitación de acuerdo con lo establecido en esta Providencia, así como otros programas y actividades de capacitación no contempladas en el Programa Anual de Capacitación, que se consideren necesarias o convenientes.

7. Coordinar las actividades de formación y capacitación del personal del Sujeto Obligado, en lo relativo a la legislación, reglamentación y controles internos vigentes, incluyendo los aspectos relativos a la política Conozca a su Empleado, así como las políticas y procedimientos relacionados con la PC LC/FT/FPADM.

8. Desarrollar estrategias comunicacionales de información y sensibilización, dirigidas a los clientes y empleados, en relación con la materia de PC LC/FT/FPADM.

9. Elaborar normas y métodos de verificación de datos físicos o digitales y análisis de información, con la finalidad de desarrollar indicadores que permitan determinar comportamientos transaccionales inusuales o sospechosos de clientes y usuarios, para ser aplicados por el Sujeto Obligado, relacionados con la prevención, control y detección de operaciones sospechosas de LC/FT/FPADM.

10. Analizar las alertas de Actividades Sospechosas, debiendo decidir la pertinencia de elaborar y remitir a la Unidad Nacional de Inteligencia Financiera (UNIF), el formulario denominado Reporte de Actividades Sospechosas (RAS) o archivarlo y hacerle seguimiento al caso, así como dejar constancia en un informe sobre la decisión adoptada y las opiniones que la sustentaron.

11. Enviar a la UNIF los Reportes de Actividades Sospechosas que considere necesario, así como también enviar las respuestas a las solicitudes de información relacionadas con la materia que esta y otras autoridades competentes requieran, dentro de los plazos establecidos por las leyes y comunicaciones de solicitud de información.

12. Informar a la SUNACRIP acerca de las tipologías o modelos de actuación que vaya identificando el Sujeto Obligado en las operaciones de sus clientes, como modus operandi para la LC/FT/FPADM, respetando en todo momento la reserva y confidencialidad de los datos de identificación de las personas naturales o jurídicas involucradas en los Reportes de Actividades Sospechosas a la UNIF.

13. Conocer y evaluar el funcionamiento de los nuevos esquemas de negocio, productos y servicios que involucren activos virtuales o criptoactivos y en caso de considerarlo conducente, recomendar la adopción de medidas de PC LC/FT/FPADM, previo al lanzamiento de dichos nuevos esquemas de negocio, productos y servicios. Esta misma evaluación deberá realizarse en caso que el Sujeto Obligado pretenda utilizar nuevas tecnologías o en desarrollo, debiendo aplicar el Enfoque Basado en Riesgo para mitigar y administrar los riesgos identificados.

14. Mantener las relaciones institucionales con esta Superintendencia y la UNIF, así como con otras autoridades competentes, organizaciones no gubernamentales e instituciones dedicadas a la prevención, represión y control de LC/FT/FPADM.

15. Representar al Sujeto Obligado en convenciones, eventos, foros, comités y actos oficiales nacionales e internacionales relacionados con la materia de PC LC/FT/FPADM, cuando sea designado por la Junta Directiva del Sujeto Obligado.

16. Mantener debidamente actualizados los documentos, formularios e información vinculados con la materia de prevención y control de LC/FT/FPADM, tales como Código de Ética, Compromiso Institucional, Manual para la Administración de Riesgos de LC/FT/FPADM, Ficha de Identificación del Cliente, Declaración Jurada de origen y destino de fondos, entre otros. Los comentarios sobre las acciones realizadas al respecto deberán incluirse en el informe de gestión correspondiente (trimestral o anual) que debe presentar el Oficial de Cumplimiento ante la Junta Directiva o el órgano que ejerza función equivalente del Sujeto Obligado.

17. Solicitar la incorporación activa de cualquier directivo o empleado del Sujeto Obligado, a objeto de ejecutar eficientemente las tareas inherentes al SIAR LC/FT/FPADM.

18. Otras estrictamente relacionadas con la materia de prevención y control de riesgos de LC/FT/FPADM, a juicio de la Junta Directiva o el órgano que ejerza función equivalente del Sujeto Obligado.

19. Evaluar el cumplimiento del POA PC LC/FT/FPADM, con el propósito de asegurar que los objetivos, actividades y tareas incluidas en el mismo se estén cumpliendo adecuadamente. Asimismo, deberá presentar un informe trimestral a la Junta Directiva o al órgano que ejerza función equivalente en relación al cumplimiento del mencionado plan. De igual forma, deberá presentar informes adicionales en caso de sobrevenir circunstancias o eventos imprevistos que afecten el cumplimiento del POA PC LC/FT/FPADM, o ameriten realizar cambios en el mismo.

20. Elaborará el Manual para la Administración de Riesgos de LC/FT/FPADM y lo revisará al final de cada año, a los fines de mantenerlo actualizado de acuerdo a los cambios en la normativa vigente, nuevas tendencias, situación económico financiera del país y cualquier otro factor que pudiese modificar su contenido, las evidencias documentales de la precitada revisión deberán insertarse en el manual. El Oficial de Cumplimiento deberá estar dotado de una estructura organizativa, tecnológica y presupuestaria idónea para que pueda ejecutar sus labores.

Artículo 18: En caso de ausencias temporales del Oficial de Cumplimiento, la Junta Directiva o el órgano que ejerza función equivalente deberá designar un suplente. Estas ausencias temporales no podrán exceder de un lapso de sesenta (60) días continuos, si transcurrido este lapso subsistiere la falta, se considerará falta absoluta.

En caso de falta absoluta, la designación del nuevo Oficial de Cumplimiento deberá efectuarse dentro de los treinta (30) días continuos siguientes a la fecha en que sea declarada la falta absoluta por el Presidente del Sujeto Obligado o quien haga sus veces.

CAPÍTULO V

ANÁLISIS, CONTROL Y DETECCIÓN DE OPERACIONES SOSPECHOSAS DE LC/FT/FPADM

Artículo 19: El análisis, control y detección de operaciones sospechosas de LC/FT/FPADM estará a cargo del área operativa que maneja las plataformas tecnológicas y sistemas informáticos mediante los cuales se proporcionan productos financieros y servicios a través de actividades que involucran activos virtuales o criptoactivos. Dicha área operativa tendrá la misión de analizar, controlar y detectar la posible LC/FT/FPADM en las actividades y operaciones del Sujeto Obligado; le reportará al Oficial de Cumplimiento toda la información relativa a las operaciones o hechos que puedan estar relacionados con la LC/FT/FPADM.

La Junta Directiva o el órgano que ejerza función equivalente implementará las medidas necesarias para que dicha área operativa esté dotada del personal especializado, así como de los recursos materiales, técnicos y el entrenamiento adecuado para el cumplimiento de sus funciones en materia de análisis, control y detección de operaciones sospechosas de LC/FT/FPADM.

Artículo 20: El área operativa encargada del análisis, control y detección de operaciones sospechosas de LC/FT/FPADM tendrá las siguientes obligaciones y funciones:

1. Analizar las señales de alerta emitidas por las herramientas tecnológicas y sistemas informáticos, a los fines de determinar si hay indicios suficientes para calificar los hechos o transacciones como actividades sospechosas de LC/FT/FPADM.

2. Informar al Oficial de Cumplimiento los hechos o transacciones calificados como actividades sospechosas de LC/FT/FPADM, siendo que el Oficial de Cumplimiento deberá informar a la SUNACRIP sobre tipologías o modelos de actuación que vaya

identificando el Sujeto Obligado en las operaciones de sus clientes, como modus operandi para la LC/FT/FPADM, respetando en todo momento la reserva y confidencialidad de los datos de identificación de las personas naturales o jurídicas involucradas en los Reportes de Actividades Sospechosas a la UNIF.

3. Utilizar programas automatizados para el monitoreo de operaciones y la detección de actividades sospechosas de LC/FT/FPADM.

4. Diseñar conjuntamente con el Oficial de Cumplimiento, desarrollar y aplicar los parámetros de segmentación de los diferentes factores de riesgo de LC/FT/FPADM, del Sujeto Obligado.

5. Determinar conjuntamente con el Oficial de Cumplimiento y aplicar las directrices que se otorgarán a las herramientas informáticas utilizadas por el Sujeto Obligado para la emisión de señales de alerta.

6. Establecer con base al conocimiento razonable que se tenga de la operatividad del cliente, listas de exceptuados de las señales de alertas regularmente emitidas por las herramientas informáticas destinadas para tal fin.

7. Asignar las respectivas calificaciones a los diferentes factores de riesgo, considerando las directrices establecidas en esta norma, en concordancia con cualquier base conceptual que el Sujeto Obligado estime prudente aplicar.

8. Analizar los diferentes factores de riesgo de LC/FT/FPADM para evaluarlos y clasificarlos cualitativamente y establecer las medidas de mitigación a ser aplicadas según el nivel de dichos riesgos.

9. Aplicar herramientas tecnológicas que permitan realizar un seguimiento para detectar tendencias, cambios en el perfil financiero y actividades inusuales de las operaciones de los clientes

10. Emitir mensualmente estadísticas relacionadas con:

a. Número de alertas generadas.

b. Casos analizados.

c. Casos remitidos a la UNIF mediante los Reportes de Actividades Sospechosas (RAS) y los casos que se mantendrán bajo seguimiento y evaluación.

d. Casos pendientes de análisis.

e. Tipologías o modelos de actuación que vaya identificando el Sujeto Obligado en las operaciones de sus clientes, como modus operandi para la LC/FT/FPADM, las cuales deben ser informadas a la Sunacrip.

11. Recabar y transmitir la información que, en materia de PC LC/FT/FPADM, se debe enviar a este Organismo, garantizando la calidad de la data y la oportunidad de su remisión

12. Otras a juicio del Oficial de Cumplimiento o de la Junta Directiva o del órgano que ejerza función equivalente del Sujeto Obligado.

CAPÍTULO VI

EXCEPCIÓN PARA LA DESIGNACIÓN DEL OFICIAL DE CUMPLIMIENTO

Artículo 21: El Sujeto Obligado que considere que puede cumplir satisfactoriamente con estas normas sin designar un Oficial de Cumplimiento, podrá presentar ante este Organismo, para su revisión, las justificaciones respectivas, a los fines de evaluar su viabilidad y aprobación.

Artículo 22: En el caso del artículo anterior, el socio, accionista o directivo que desempeñe el cargo de mayor jerarquía, cumplirá adicionalmente las funciones de Oficial de Cumplimiento y asumirá las responsabilidades correspondientes al control, prevención, detección y reporte previstas en esta Providencia.

CAPÍTULO VII

OTROS ELEMENTOS DEL SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS DE LC/FT/FPADM

"SECCIÓN A"

PLAN OPERATIVO ANUAL DE PREVENCIÓN Y CONTROL DE RIESGOS DE LC/FT/FPADM (POA PC LC/FT/FPADM)

Artículo 23: El Sujeto Obligado diseñará anualmente un plan estratégico para prevenir y mitigar los riesgos de LC/FT/FPADM, que se denominará Plan Operativo Anual de Prevención y Control de LC/FT/FPADM (POA PC LC/FT/FPADM), donde se incluirán todas aquellas actividades a desarrollarse durante el ejercicio económico, todo ello, a los fines de garantizar el cumplimiento de las políticas, normas y controles internos en materia de PC LC/FT/FPADM, dicho plan debe ser elaborado durante el último trimestre del año anterior a su ejecución y estará a la disposición de esta Superintendencia los primeros quince (15) días hábiles del año de su vigencia. El referido plan debe ser aprobado por la Junta Directiva o el órgano que ejerza función equivalente.

Asimismo debe incluir, de acuerdo con las necesidades determinadas, la adquisición, implementación o perfeccionamiento de los sistemas informáticos de monitoreo y detección de operaciones inusuales y sospechosas, programas de capacitación para los trabajadores, planes de supervisión y auditoría independiente, perfeccionamiento de mecanismos de control interno, perfeccionamiento de los programas informáticos y desarrollo de soluciones basadas en tecnología para incrementar la eficiencia y eficacia en la administración de los riesgos de LC/FT/FPADM.

La ejecución del POA PC LC/FT/FPADM debe ser flexible y ajustarse a las necesidades del Sujeto Obligado con ocasión de los cambios que experimenten los factores de riesgos asociados a los clientes, productos, negocios y servicios que involucren activos virtuales,

canales de distribución utilizados, uso de tecnologías nuevas o en desarrollo y tipos de activos virtuales involucrados en sus operaciones.

Artículo 24: El POA PC LC/FT/FPADM, a fin de facilitar la emisión de estadísticas que permitan asegurar el control, seguimiento y ejecución de las actividades planteadas, debe contener los aspectos mencionados a continuación:

1. Actividades: Describir las acciones, tareas o labores que el Sujeto Obligado se plantea realizar durante el período de vigencia del POA PC LC/FT/FPADM.

2. Objetivo: Establecer el propósito específico que se espera alcanzar con cada actividad del POA PC LC/FT/FPADM, para fortalecer el SIAR LC/FT/FPADM.

3. Responsables: Indicar la persona o la unidad administrativa responsable de la ejecución de cada actividad del POA PC LC/FT/FPADM.

4. Unidad de medida: Establecer en forma cualitativa las actividades del POA PC LC/FT/FPADM. Por ejemplo: informe, memorando, personas capacitadas, inspecciones, entre otros.

5. Meta: Cuantificar las unidades de medida que se esperan alcanzar con la ejecución del POA PC LC/FT/FPADM.

6. Insumos: Señalar los recursos que serán aplicados en la ejecución de las actividades previstas en el POA PC LC/FT/FPADM (humanos, materiales, técnicos, entre otros).

7. Tiempo de ejecución: Señalar la fecha de inicio y culminación de cada actividad planteada.

8. Indicadores: Identificar el nombre del indicador, descripción del indicador, responsable del indicador, frecuencia de medición, meta efectiva esperada, fórmula de cálculo, área responsable del seguimiento del indicador.

Artículo 25: El Oficial de Cumplimiento debe elaborar un informe sobre la ejecución del POA PC LC/FT/FPADM, por lo menos trimestralmente, el cual señalará el porcentaje de cumplimiento de cada aspecto de su contenido. Este documento debe formar parte de los informes anuales y/o trimestrales que el Oficial de Cumplimiento presentará a la Junta Directiva del Sujeto Obligado o al órgano que ejerza funciones equivalentes; adicionalmente, debe actualizar este informe a la fecha de cualquier auditoría o inspección de este Ente Regulador.

"SECCIÓN B"

CÓDIGO DE ÉTICA Y EL COMPROMISO INSTITUCIONAL

Artículo 26: El Sujeto Obligado debe adoptar un Código de Ética, de carácter general, el cual incluirá aspectos concernientes a la prevención y control de los riesgos de LC/FT/FPADM y el consumo de drogas, de obligatorio conocimiento y cumplimiento para todo su personal, que permita crear un clima de elevada moral y poner en práctica

medidas encaminadas a aumentar la sensibilidad de su personal ante los efectos y riegos de la LC/FT/FPADM.

Artículo 27: El Código de Ética será aprobado por la Junta Directiva o el órgano que ejerza función equivalente y estará disponible para los funcionarios de este Organismo durante las inspecciones que practique, asimismo, deberá remitirlo el Sujeto Obligado a esta Superintendencia, para su revisión, en caso que le sea requerido.

Artículo 28: El Código de Ética deberá ser publicado en la intranet del Sujeto Obligado, se debe hacer entrega de un ejemplar a cada uno de los trabajadores del Sujeto Obligado y archivar en el respectivo expediente del trabajador la constancia de su recepción.

Artículo 29: Todos los miembros de la Junta Directiva o del órgano que ejerza función equivalente (principales y suplentes) del Sujeto Obligado, deberán asumir individualmente por escrito un Compromiso Institucional, donde declaren su identificación y fidelidad con las metas y valores éticos de la organización en materia de PC LC/FT/FPADM, el cual debe actualizarse anualmente y archivarse en el respectivo expediente de los referidos miembros.

"SECCIÓN C"

MANUAL DE ADMINISTRACIÓN DE RIESGOS DE LEGITIMACIÓN DE CAPITALES, FINANCIAMIENTO AL TERRORISMO Y FINANCIAMIENTO DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA (MANUAL AR LC/FT/FPADM)

Artículo 30: El Sujeto Obligado debe diseñar políticas, normas y métodos para mitigar y controlar los riesgos en materia de LC/FT/FPADM, los cuales serán consolidados en un Manual de Administración de Riesgos de LC/FT/FPADM, que podrá ser elaborado en formato físico o digital y debe ser aprobado por la Junta Directiva o el órgano que ejerza función equivalente. Dicho Manual debe ser diseñado considerando las características propias del Sujeto Obligado, así como los diferentes productos y servicios que ofrece a sus clientes, entre otros aspectos pertinentes.

El alcance de dichas políticas, normas, métodos y controles internos debe estar acorde con la dimensión, estructura, riesgos y complejidad del Sujeto Obligado, por tanto, la elaboración del referido Manual deberá basarse en una evaluación previa de los riesgos de LC/FT/FPADM del Sujeto Obligado, siendo que dicha evaluación deberá mantenerse a disposición de esta Superintendencia para las revisiones que considere necesarias.

Artículo 31: El Manual de Administración de Riesgos de LC/FT/FPADM deberá contener como mínimo los siguientes aspectos, en lo aplicable:

1. Información y especificaciones de las herramientas tecnológicas y sistemas informáticos utilizados por el Sujeto Obligado para el monitoreo y la detección de actividades sospechosas de LC/FT/FPADM y flujograma de los procesos de dichos sistemas y herramientas.

2. Indicación de las medidas de seguridad para el acceso y manejo de las herramientas tecnológicas y sistemas informáticos utilizados por el Sujeto Obligado para el monitoreo y la detección de actividades sospechosas de LC/FT/FPADM.

3. Estructura Organizacional del SIAR LC/FT/FPADM, especificando los deberes de cada uno de los actores que lo conforman.

4. Políticas y actuaciones para la administración del riesgo de LC/FT/FPADM, detallando la metodología para su administración (identificación, calificación, control interno, mitigación y monitoreo de los riesgos).

5. Normas y métodos para la aplicación de la Política Conozca su Cliente.

6. Normas y métodos para la aplicación de la Política Conozca su Empleado.

7. Normas y métodos para la aplicación de la Política Conozca sus Terceros Relacionados.

8. Métodos de detección y Reporte de Actividades Sospechosas.

9. Trámites para las notificaciones periódicas a esta Superintendencia.

10. Trámites para satisfacer las solicitudes de información de las autoridades.

11.Métodos para la parametrización de los factores de riesgo y la asignación de categorías de riesgo. Deberá indicarse cuales son los parámetros y factores aplicados.

12.Metodología para la realización de la Evaluación de Riesgos de LC/FT/FPADM

13.Señalar la obligación de mantener por cinco (05) años, en forma física o digital, la información y registros que comprueben la realización de las operaciones, que permitan la reconstrucción de las transacciones y transferencias y la identificación de sus códigos o referencias, así como la determinación del tipo de activo virtual y moneda fiduciaria involucrados. Asimismo, establecer la obligación de mantener por el mismo lapso, en forma física o digital, la información y registros que comprueben las relaciones de negocios de los clientes, así como la información exigida para su identificación.

Esta obligación de mantenimiento abarca muy especialmente la obtención, registro y conservación de la información sobre el originador y el beneficiario de transferencias e intercambios que involucren criptoactivos.

14.Señalar la obligación de aplicar medidas de seguridad de la información en formato digital, que garanticen su integridad e inviolabilidad.

15.Políticas y métodos para la administración de riesgos de LC/FT/FPADM aplicables a las relaciones de custodia, administración y fideicomiso que involucren activos virtuales o instrumentos virtuales que permiten el control sobre activos virtuales, en caso que el Sujeto Obligado brinde este tipo de servicios.

16.Políticas y métodos para la administración de riesgos de LC/FT/FPADM aplicables a las transacciones digitales y las operaciones de intercambio y transferencia que involucren activos virtuales, en caso que el Sujeto Obligado brinde este tipo de servicios.

17.Políticas y métodos para la administración de riesgos de LC/FT/FPADM aplicables a la participación y prestación de servicios relacionados con la emisión, oferta y/o venta de activos virtuales y las políticas y actuaciones concernientes a la administración de riesgos de LC/FT/FPADM aplicables a relaciones con Personas Expuestas Políticamente.

18.Políticas, normas y métodos de administración y mitigación de riesgos específicos de que las operaciones y servicios del Sujeto Obligado sean utilizados para financiar actividades terroristas y la proliferación de armas de destrucción masiva.

19.Señalar la prohibición para los Sujetos Obligados y sus empleados o trabajadores, de advertir o revelar a los clientes o a terceros, sobre verificaciones, notificaciones o reportes efectuados a la UNIF u otras autoridades.

20. Normas y actuaciones para la aplicación de las Resoluciones del Consejo de Seguridad de la Organización de las Naciones Unidas (ONU), relativas a la prevención y represión del terrorismo, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, así como para el congelamiento o bloqueo preventivo de fondos y activos virtuales relacionados con personas o entidades designadas por estar vinculadas con dichas actividades

Los Sujetos Obligados deben reportar a la UNIF información sobre los activos virtuales congelados o bloqueados preventivamente y las acciones ejecutadas en cumplimiento de las referidas Resoluciones del Consejo de Seguridad de la Organización de las Naciones Unidas (ONU).

El Manual de Administración de Riesgos de LC/FT/FPADM deberá ser revisado periódicamente por el Oficial de Cumplimiento, a fin de mantenerlo actualizado de acuerdo a los cambios en la normativa vigente, nuevas tendencias, situación económico-financiera del país y cualquier otro factor que pudiese modificar su contenido. Las evidencias documentales de la precitada revisión deberán insertarse en el manual.

TÍTULO III

POLÍTICAS, MEDIDAS Y CONTROLES PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE LC/FT/FPADM

CAPÍTULO I

Artículo 32: En sus métodos o procesos para gestionar sus riesgos de LC/FT/FPADM, el Sujeto Obligado debe aplicar un Enfoque Basado en Riesgo (EBR) que comprenda los siguientes pasos:

1. Identificar riesgos: La gestión comienza por identificar los riesgos de la organización, entendiendo por organización la misma y su contexto, comprendiendo sus necesidades y las de sus partes interesadas.

2. Analizar y evaluar riesgos: Una vez identificados los riesgos, deben prevenirse estimando la posibilidad de que ocurran y sus consecuencias.

3. Toma de acciones: Luego de realizada la evaluación, se deben definir las acciones de mejora que hagan frente a estos riesgos que se han identificado y cuantificado, integrándolas e implantándolas en los procesos del sistema de gestión.

4. Evaluación de las acciones ejecutadas: La etapa final consiste en evaluar la eficacia y efectividad de las acciones ejecutadas, mediante el seguimiento y la revisión.

Existen diversas herramientas para evaluar los riesgos, sin embargo, el Sujeto Obligado aplicará la metodología que considere conveniente de acuerdo a los factores de riesgos que le son propios.

Artículo 33: Los Sujetos Obligados deben identificar y evaluar los riesgos de LC/FT/FPADM que surgen de sus actividades y operaciones que involucran activos virtuales, sus productos y servicios asociados, además, deben ejecutar medidas encaminadas a prevenir, gestionar y mitigar tales riesgos efectivamente, bajo un Enfoque Basado en los Riesgos identificados, el cual implica que las medidas para prevenir y mitigar dichos riesgos sean proporcionales a los mismos.

Antes de lanzar nuevos productos, servicios y adoptar nuevas prácticas comerciales, nuevos mecanismos de entrega o utilizar tecnologías nuevas o en desarrollo, los Sujetos Obligados deben hacer la respectiva identificación y evaluación de los riesgos de LC/FT/FPADM asociados y ejecutar medidas para gestionarlos y mitigarlos, igualmente deben gestionar y mitigar los riesgos derivados de participar en actividades que implican el uso de tecnologías que propendan al anonimato o en mecanismos y tecnologías que ofusquen u oculten la identidad del remitente, destinatario, titular o beneficiario efectivo de activos virtuales. Si el Sujeto Obligado no puede administrar y mitigar adecuadamente los riesgos que implica participar en tales actividades, entonces no debe involucrarse o participar en las mismas.

Artículo 34: El Sujeto Obligado debe efectuar, durante el último trimestre del ejercicio económico, la evaluación anual de su nivel de riesgo, aplicable para el siguiente período y someterla a la aprobación de la Junta Directiva o del órgano que ejerza función equivalente.

No obstante, los Sujetos Obligados deben estar atentos a los nuevos acontecimientos que involucren activos virtuales, a los fines de actualizar oportunamente su nivel de riesgo.

Los métodos utilizados para la evaluación anual del nivel de riesgo deben incluirse en el Manual de Administración de Riesgos de LC/FT/FPADM. El resultado de dicha evaluación deberá permanecer en el Sujeto Obligado a disposición de este Organismo

durante las inspecciones o cuando éste lo solicite, asimismo, la citada evaluación servirá de base para el diseño y actualización de su Manual de Administración de Riesgos de LC/FT/FPADM, el cual constituye un elemento relevante que incide en el Gobierno Corporativo del Sujeto Obligado.

Artículo 35: El Sujeto Obligado debe realizar anualmente y documentar, su evaluación de riesgos de LC/FT/FPADM, considerando las variaciones de los factores que influyen en los niveles de riesgo, tales como introducción de nuevos modelos de negocio, productos y servicios, nuevos mecanismos de entrega, nuevos clientes, mejoras en los equipos tecnológicos, uso de tecnologías nuevas o en desarrollo, entre otros.

Partiendo de esta evaluación, el Sujeto Obligado debe aplicar un Enfoque Basado en el Riesgo, a fin de asegurar que las medidas para prevenir o mitigar los riesgos de LC/FT/FPADM sean proporcionales a los riesgos identificados y para la asignación eficaz de recursos, siendo que, frente a riesgos mayores, los Sujetos Obligados deben ejecutar medidas intensificadas o mejoradas para administrar y mitigar tales riesgos y cuando estos sean menores, pueden aplicar medidas simplificadas. No se permiten medidas simplificadas si existen sospechas de LC/FT/FPADM.

Artículo 36: El Sujeto Obligado aplicará las categorías de riesgo en todas las áreas de negocios, atendiendo a los diferentes factores de riesgo de LC/FT/FPADM relacionados con sus empleados, clientes, canales de distribución que utilice, modelos de negocio, productos y servicios que ofrece, estructura y tamaño de la entidad, uso de tecnologías nuevas o en desarrollo, tipos de activos virtuales involucrados en sus operaciones. Dichas categorías quedan establecidas en: a) Riesgo Bajo, b) Riesgo Moderado y c) Riesgo Alto.

Artículo 37: El Sujeto Obligado aplicará factores o categorías relevantes que deben ser considerados de Alto Riesgo, sin perjuicio de los que adicionalmente puedan incluirse y calificarse en esta categoría, de acuerdo con los métodos de calificación de riesgo de LC/FT/FPADM propios de cada Sujeto Obligado, o conforme lo instruya una autoridad con competencia en la materia, o según las mejores prácticas internacionales de prevención y control de LC/FT/FPADM; para tal fin deberá considerar los siguientes factores o categorías, los cuales se mencionan a título meramente enunciativo y no taxativo:

1. Clientes y actividades económicas de Riesgo Alto: Personas con las siguientes características o dedicadas a los siguientes tipos de negocios o actividades:

a. Organizaciones Sin Fines de Lucro que principal y habitualmente se dediquen a la recolección de fondos, tanto representados en dinero fiduciario como en activos virtuales, para diversos fines.

b. Personas Expuestas Políticamente (PEP), incluyendo a familiares cercanos, asociados y estrechos colaboradores de dichas personas.

c. Personas jurídicas y estructuras jurídicas constituidas o establecidas en países, zonas geográficas o jurisdicciones que posean un sistema fiscal diferenciado entre residentes y

nacionales, cuya legislación facilita el secreto bancario o el secreto de registro, carezca de tratados internacionales en materia de PC LC/FT/FPADM, o no aplican regulaciones contra la legitimación de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva similares a las vigentes en la República Bolivariana de Venezuela o que las mismas sean insuficientes, así como también que contemplen tributos reducidos o inexistentes (paraísos fiscales).

d. Personas jurídicas o estructuras jurídicas constituidas o establecidas en zonas libres o francas, o cuya situación geográfica sea cercana a los centros de consumo, producción o tránsito de drogas ilícitas, o en zonas o territorios que frecuentemente son menciona.

e. Clientes no residentes.

f. Sociedades mercantiles que tengan accionistas nominales o esté representado su capital social en acciones de tipo al portador.

g. Clientes que participan en negocios o actividades que utilizan cuantías elevadas de dinero en efectivo.

h. Personas jurídicas o estructuras jurídicas que son vehículos de tenencia de activos personales.

i. Sociedades civiles o mercantiles cuyas estructuras de participación o titularidad parecen ser inusuales o complejas, con respecto al carácter de las actividades que desarrollan.

2. Productos y servicios de Riesgo Alto:

a. Servicios de intercambio entre activos virtuales y monedas fiduciarias,

b. Servicios de intercambio entre una o más formas de activos virtuales,

c. Servicios de transferencia electrónica y envío de remesas o fondos representados en criptoactivos.

d. Servicios que facilitan intercambios directos entre pares (igual a igual).

e. Servicios que facilitan intercambios a través de quioscos o cajeros automáticos.

f. Servicios o actividades que involucren seudónimos o transacciones anónimas y pagos recibidos de terceros desconocidos.

g. Custodia y servicios de administración de criptoactivos o de instrumentos virtuales que permiten el control sobre criptoactivos.

h. Participación y prestación de servicios financieros relacionados con la emisión, oferta y/o venta de un activo virtual.

i. Cuentas y billeteras virtuales abiertas a nombre de intermediarios o agentes que actúan en nombre de terceros.

3. Canales de distribución o mecanismos de entrega de Riesgo Alto:

a. Operaciones virtuales por internet, que conllevan negocios o transacciones que no son efectuados “cara a cara” y no implican la presencia física de las partes.

b. Cajeros Automáticos.

c. Negocios o transacciones a través de agentes o intermediarios.

4. Países, jurisdicciones y zonas geográficas de Riesgo Alto:

Los Sujetos Obligados por estas normas deben considerar como de Riesgo Alto los siguientes factores geográficos y aplicar en consecuencia medidas de Debida Diligencia Intensificada a aquellas relaciones comerciales, transacciones y operaciones con personas naturales y jurídicas procedentes de los siguientes países, jurisdicciones y zonas geográficas calificadas como de Riesgo Alto:

a. Países, zonas geográficas y jurisdicciones identificadas por el Grupo de Acción Financiera Internacional (GAFI) u otras fuentes verosímiles (como los Informes de Evaluación Mutua y los Informes de Seguimiento, por ejemplo), como de Alto Riesgo, No Cooperadores, con sistemas o regulaciones inadecuados, mínimos o inexistentes en materia de prevención y control de riesgos de LC/FT/FPADM, o con deficiencias estratégicas para combatir el lavado de dinero, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, así como las jurisdicciones, países y zonas geográficas sujetos a un llamado a la acción o colocados bajo un mayor monitoreo y supervisión.

b. Países, zonas geográficas y jurisdicciones identificados por la Organización de las Naciones Unidas como de alta incidencia en la producción, tráfico y consumo de drogas ilícitas y en el tráfico de personas.

c. Países, zonas geográficas y jurisdicciones señalados por fuentes creíbles como poseedores de niveles significativos de percepción relacionada con el fenómeno del crimen organizado.

d. Países, zonas geográficas y jurisdicciones identificados por los Sujetos Obligados de acuerdo con su experiencia, por el historial de transacciones monitoreadas, por los reportes de organismos especializados en la lucha contra la delincuencia organizada y por la cantidad de Reportes de Actividades Sospechosas detectadas que guarden relación con ese determinado país, zona geográfica o jurisdicción.

5. Tipo de activo virtual involucrado.

El riesgo de LC/FT/FPADM inherente a los criptoactivos resulta incrementado en los casos de activos virtuales cuyas características y tecnologías asociadas conllevan exposición a anonimizadores del Protocolo de Internet (IP) y a otros mecanismos susceptibles de ofuscar las transacciones, los flujos y contrapartes, así como de ocultar la fuente de los fondos representados en criptoactivos o de inhibir la capacidad para identificar a clientes y usuarios propietarios de los mismos.

Todos los factores o categorías relevantes anteriormente mencionados a título simplemente enunciativo y no taxativo, deben ser considerados de Alto Riesgo por los Sujetos Obligados y conllevan la necesidad de aplicar respecto de ellos medidas de Debida Diligencia Intensificada.

Artículo 38: El Sujeto Obligado puede considerar, entre otras, las siguientes variables específicas mencionadas a título enunciativo, no taxativo, que pueden modificar el nivel de riesgo que haya determinado para un cliente o una transacción en particular:

1. El propósito de la relación comercial puede influir en el nivel de riesgo evaluado, por ejemplo, las cuentas y billeteras virtuales que son abiertas para facilitar transacciones de consumidores tradicionales, pueden presentar un menor riesgo que las cuentas y billeteras virtuales abiertas para facilitar transacciones con altas sumas de fondos representados en activos virtuales de una entidad comercial desconocida.

2. La cantidad de activos virtuales que deposite un cliente o el volumen de las operaciones realizadas. El volumen de transacciones inusualmente grandes, en comparación con lo que pudiese esperarse razonablemente del cliente, puede ser un indicador que deba ser clasificado como Riesgo Alto, aun cuando inicialmente no haya sido clasificado como tal. A la inversa, los bajos niveles de transacciones realizadas por un cliente que haya sido clasificado como de riesgo alto, pueden permitir que el Sujeto Obligado trate al cliente como de menor riesgo.

3. Las relaciones de larga duración, con contacto frecuente con los clientes a lo largo de las mismas, presentan menos riesgos desde el punto de vista de LC/FT/FPADM.

4. El nivel de regulación y régimen de supervisión al que esté sometido el cliente. Un cliente de un Sujeto Obligado, que se encuentre ubicado en un país, zona geográfica o jurisdicción donde existan normas adecuadas en materia de prevención y control de LC/FT/FPADM, o que forma parte de un grupo cuya sociedad matriz lo somete a una regulación y supervisión adecuada, presentará menos riesgos en esta materia que un cliente no regulado o sometido únicamente a una regulación mínima en materia de prevención y control de LC/FT/FPADM.

5. El uso por parte de los clientes, de empresas intermediarias u otras estructuras, sin ningún fundamento claro de índole comercial o de otro tipo, o que aumenten innecesariamente la complejidad de la operación o impliquen una falta de transparencia. Dichas estructuras aumentarán el riesgo en materia de LC/FT/FPADM, a menos que se considere que sean lo suficientemente transparentes y se justifique su utilización.

CAPÍTULO II

POLÍTICAS, MEDIDAS Y CONTROLES PARA LA ADMINISTRACIÓN DE RIESGOS DE LC/FT/FPADM DERIVADOS DE LOS CLIENTES

Artículo 39: Los Sujetos Obligados se abstendrán de iniciar o mantener relaciones económicas y prestar servicios o ejecutar actividades, operaciones y transacciones que

involucren activos virtuales, con personas naturales o jurídicas cuya identidad no pueda ser determinada plenamente, o lo estén con nombres ficticios, o con claves o números que sustituyan la verdadera identidad y no resulte posible establecer la identidad real del cliente o usuario; tampoco podrán mantener cuentas y billeteras virtuales anónimas, innominadas o con nombres obviamente ficticios. Igualmente se abstendrán de realizar operaciones con usuarios ocasionales no identificados, o cuando exista sospecha de LC/FT/FPADM, o cuando tengan dudas acerca de la veracidad o idoneidad de la información suministrada.

Los Sujetos Obligados deben establecer por todos los medios posibles la verdadera identidad de sus clientes, beneficiarios finales y de los terceros participantes en las actividades, servicios y transacciones que involucren activos virtuales.

Los Sujetos Obligados, en función de la naturaleza de sus negocios y del riesgo inherente a sus operaciones, deben implementar políticas, normas, métodos y controles internos para desarrollar adecuada y continuamente, una Política de Debida Diligencia para el Conocimiento del Cliente (DDC), siempre aplicando las disposiciones mínimas que se señalan en esta Providencia

El adecuado conocimiento del cliente permitirá establecer razonablemente su nivel de riesgo de LC/FT/FPADM, considerando factores tales como los antecedentes del cliente, su país de origen, si ocupa un cargo relevante en el sector público o privado, las cuentas y billeteras virtuales vinculadas, actividad de negocios u otros indicadores de riesgo. Sobre la base de sus propios criterios, el Sujeto Obligado debe evaluar si un cliente presenta un riesgo mayor de LC/FT/FPADM y si existen circunstancias que pudieran llevarle a establecer que determinados clientes presenten un riesgo de LC/FT/FPADM de menor nivel.

Es importante que la política de aceptación del cliente no sea demasiado restrictiva y termine negando el acceso del público en general a los servicios del Sujeto Obligado.

Artículo 40: Los Sujetos Obligados deben diseñar y ejecutar procesos efectivos de Debida Diligencia para el conocimiento del Cliente (DDC), para establecer y mantener relaciones comerciales con sus clientes, para realizar transacciones ocasionales que involucren activos virtuales por encima del umbral mínimo de un mil Euros (1.000 EUR), o cuando exista sospecha de LC/FT/FPADM, o cuando se tengan dudas sobre la veracidad o idoneidad de los datos de identificación del cliente obtenidos previamente.

Las medidas de Debida Diligencia del Cliente comprenden, entre otros aspectos, identificar al cliente y verificar su identidad, así como también la del propietario o beneficiario final en caso que el cliente sea persona jurídica. La verificación de la identidad del cliente puede efectuarse mediante bases de datos, información o documentación confiable de fuentes independientes.

Los Sujetos Obligados podrán aplicar medidas de Debida Diligencia para la identificación y verificación de la identidad del cliente, no cara a cara, sino corroborando

la información de identidad recibida del cliente (como su nombre, dirección, número de identificación nacional, fecha de nacimiento, correo electrónico, número telefónico, por ejemplo), con información en bases de datos públicas o de terceros o con información de fuentes confiables e independientes.

Los Sujetos Obligados también podrán aplicar las siguientes medidas de Debida Diligencia para el Conocimiento del Cliente:

- Rastrear las direcciones de Protocolo Internet (IP) de los equipos usados por el cliente y llevar un registro de dichas direcciones.

- Buscar en la web para corroborar información de actividad coherente con el perfil de transacciones del cliente.

- Examinar las transacciones llevadas a cabo a lo largo de la relación comercial, para asegurar que las transacciones que se realizan sean consistentes con el conocimiento que se tiene sobre el cliente, su actividad comercial y su perfil de riesgo, incluyendo, cuando sea necesario, la fuente de los fondos involucrados en operaciones con activos virtuales o criptoactivos.

- Efectuar la identificación de las demás partes involucradas en las operaciones y la de los usuarios ocasionales.

El proceso de DDC también incluye entender la estructura de titularidad y control de los clientes que sean personas jurídicas o estructuras jurídicas, así como comprender el propósito y el carácter que se pretende dar a la relación comercial y obtener más información en situaciones de mayor riesgo, para aumentar el grado de conocimiento que se tenga del cliente y sus actividades.

Artículo 41: Para las transferencias de activos virtuales por montos mayores a un mil Euros (1.000 EUR) o su equivalente, los Sujetos Obligados deben incluir en las mismas:

a. Nombre del originador y del beneficiario

b. Un número de cuenta o billetera virtual para cada uno, cuando dichas cuentas o billeteras virtuales se usen para procesar la transacción o en ausencia de cuenta o billetera, un único número de referencia de la transacción que permita rastrearla.

c. Dirección del originador o su número de identidad nacional o el número de identificación del cliente o la fecha y lugar de su nacimiento.

Los Sujetos Obligados, al realizar transferencias de activos virtuales por montos mayores a un mil Euros (1.000 EUR) o su equivalente, deben transmitir de inmediato y de forma segura, la información requerida del originador y del beneficiario. Esta información requerida debe ser enviada simultáneamente o concurrentemente, con la transferencia misma del activo virtual.

Tanto el Sujeto Obligado ordenante de la transferencia, como el Sujeto Obligado beneficiario de la misma, deben conservar esta información requerida y ambos deben

tomar las medidas para congelar sin demora fondos y activos virtuales que son propiedad o estén controlados o que estén a disposición, directa o indirectamente, o para el beneficio de personas y entidades designadas por las Resoluciones del Consejo de Seguridad de las Naciones Unidas que exhortan a los Estados miembros a prevenir y reprimir el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. Se debe informar a la UNIF acerca de los fondos y activos virtuales congelados, así como las acciones realizadas en cumplimiento de dichas Resoluciones.

Los Sujetos Obligados no deben realizar transacciones u operaciones con personas y entidades designadas por las referidas Resoluciones del Consejo de Seguridad de la Organización de las Naciones Unidas.

Por cuanto no todas las transferencias de activos virtuales involucran a dos Sujetos Obligados, en aquellos casos en que la transferencia involucre a un solo Sujeto Obligado en cualquier extremo de la misma, este último debe cumplir con los requisitos relacionados con la información requerida con respecto a su cliente (el originador o beneficiario, según sea el caso).

Artículo 42: Los Sujetos Obligados intermediarios que faciliten las transferencias de activos virtuales como elemento intermedio de una cadena de transferencias, deben acompañar a la transferencia con la información del originador, del beneficiario y asegurarse que esta información requerida se transmita a lo largo de la cadena de transferencias, debiendo mantener su registro.

Esta información requerida del originador y del beneficiario no necesita ser comunicada como parte (como incorporada) de la transferencia en blockchain u otra plataforma de registro distribuida, el envío de esta información requerida, al Sujeto Obligado beneficiario, puede ser por un proceso totalmente distinto del de la cadena de bloques y de registro distribuido, siendo que cualquier tecnología, solución de software o herramienta es aceptable, siempre que permita cumplir con esta obligación en forma efectiva, inmediata y segura.

Artículo 43: Los Sujetos Obligados intermediarios deben identificar y reportar transacciones sospechosas, tomar medidas de congelamiento y evitar transacciones u operaciones con personas y entidades designadas por las Resoluciones del Consejo de Seguridad de las Naciones Unidas que exhortan a los Estados miembros a prevenir el Financiamiento del Terrorismo y de la Proliferación de Armas de Destrucción Masiva.

Artículo 44: Si durante el establecimiento o en el curso de la relación comercial o cuando se realizan transacciones, el Sujeto Obligado sospecha o tiene motivos razonables para sospechar, que las transacciones están relacionadas a LC/FT/FPADM, o existan dudas sobre la veracidad o idoneidad de los datos de identificación del cliente obtenidos, se debe tratar de identificar y verificar la identidad del cliente y del beneficiario final, independientemente del umbral arriba designado y hacer un Reporte de Actividad Sospechosa a la UNIF.

Artículo 45: El Sujeto Obligado aplicará la Política Conozca a su Cliente (PCSC) de manera diferenciada, de acuerdo con la sensibilidad y nivel de riesgo de LC/FT/FPADM, conforme a sus propios métodos o procesos de evaluación de riesgos y en consideración a circunstancias y factores de riesgos, cuando el nivel de riesgo sea:

a. Alto, le corresponde una DDC intensificada.

b. Moderado, le corresponde una DDC mejorada.

c. Bajo, le corresponde una DDC estándar.

Las medidas de DDC intensificadas para mitigar los riesgos potencialmente más altos, pueden consistir, entre otras, en:

1. Actualizar los datos de identificación del cliente y verificarlos con información existente en bases de datos de terceros u otras fuentes fiables.

2. Obtener información adicional sobre el cliente, el beneficiario final y la naturaleza prevista de la relación comercial o sobre el carácter que se pretende dar a esta última.

3. Rastrear las direcciones Protocolo de Internet (IP) de los equipos usados por el cliente y llevar un registro de dichas direcciones.

4. Buscar en internet información que corrobore las actividades del cliente de manera consistente con su perfil de transacción.

5. Obtener información sobre la fuente u origen de los fondos o valores representados en activos virtuales del cliente que son utilizados para realizar intercambios, transferencias y actividades que involucren activos virtuales, así como obtener información sobre la fuente de riqueza del cliente y los motivos o razones de las transacciones y transferencias intentadas o realizadas.

6. Incrementar el grado y variar la naturaleza del seguimiento o monitoreo de la relación comercial y efectuar el examen de las transacciones y transferencias llevadas a cabo, para asegurar que las mismas sean consistentes con el conocimiento que tiene el Sujeto Obligado sobre el cliente, su actividad comercial y el perfil de riesgo.

7. Examinar los antecedentes y el propósito de las transacciones u operaciones complejas, inusuales grandes y los patrones inusuales de transacciones, que no tengan un propósito económico o lícito aparente.

8. Para las transacciones y transferencias ocasionales por montos mayores al umbral de un mil Euros (1.000 EUR) o su equivalente, limitar la fuente de los fondos fiduciarios a una cuenta bancaria o tarjeta de crédito a nombre del cliente.

Artículo 46: El Sujeto Obligado debe:

1. Determinar el nivel de riesgo del cliente al momento que se establece la relación de negocios y actualizarlo cuando considere que existan elementos suficientes para ello. El universo de clientes debe evaluarse globalmente cada doce (12) meses, a fin de aplicar el

nivel apropiado de DDC en cada caso y mantener consistencia entre los métodos o procesos aplicados. La calificación del cliente podrá modificarse al momento que las características del cliente experimenten cambios significativos con respecto a la información aportada al Sujeto Obligado, ya sea al inicio de la relación comercial, como producto de la actualización efectuada por éste o como consecuencia del cambio de su perfil transaccional que haya generado las alertas respectivas.

2. Poner en práctica medidas y controles apropiados para mitigar el riesgo potencial de LC/FT/FPADM, de aquellos clientes que se hayan determinado de Riesgo Alto.

3. Establecer registros individuales, en forma física o digital, de cada uno de sus clientes, con el fin de obtener y mantener actualizada la información necesaria para determinar fehacientemente su identificación y las actividades económicas a las que se dedican. Asimismo, debe adoptar parámetros de segmentación, a los efectos de definir el perfil financiero del cliente, de modo que dicho perfil facilite la identificación de las operaciones inusuales o sospechosas, siendo que una adecuada segmentación permitirá determinar el rango en el cual se desarrollan normalmente las operaciones que realizan los clientes y las características del mercado en que participan.

4. Mantener actualizados los datos de los clientes.

5. Aplicar medidas de DDC cuando exista sospecha de LC/FT/FPADM, siendo prudente llevar a cabo en estos casos actualización de datos del cliente, solicitud de información que avale sus operaciones, declaraciones juradas, entre otros que se considere convenientes, siempre y cuando tales medidas no constituyan una alerta sobre la investigación, en tales casos, corresponderá efectuar un Reporte de Actividades Sospechosas a la UNIF y participar a la SUNACRIP acerca de la tipología o modelo de actuación relacionada con dicha actividad sospechosa. Estas participaciones o notificaciones a la SUNACRIP se harán respetando en todo momento la reserva y confidencialidad de los datos de identificación de las personas naturales o jurídicas involucradas en los Reportes de Actividades Sospechosas a la UNIF.

Artículo 47: Los Sujetos Obligados podrán identificar de forma remota (no presencial) a sus clientes y usuarios, a través de sistemas tecnológicos de identificación digital idóneos, confiables e independientes, con lo cual se facilita la inclusión financiera y se reducen costos para los Sujetos Obligados. Dichos sistemas deben permitir el mantenimiento de registros en formato digital, de las gestiones de Debida Diligencia del Cliente realizadas a través de ellos y además deben ser auditables y transparentes.

Cuando los Sujetos Obligados utilicen sistemas tecnológicos para identificación digital remota, deberán asegurarse que los métodos implementados sean acordes con los estándares para la identificación remota de clientes aplicados en la industria financiera.

Por cuanto los organismos, instituciones, empresas e institutos que forman parte del sector público son considerados como factores de bajo riesgo en materia de LC/FT/FPADM, conforme a los estándares internacionales y mejores prácticas, los

Sujetos Obligados podrán aplicar medidas simplificadas de Debida Diligencia del Cliente para el establecimiento y mantenimiento de relaciones comerciales con dichas entidades públicas y para el manejo de las cuentas y billeteras virtuales de las cuales aquellos sean titulares.

Artículo 48: El Sujeto Obligado podrá efectuar la verificación de la identidad del cliente, mediante:

a.Personas naturales venezolanas y extranjeras residentes en el país, a través de la cédula de identidad laminada.

b. Personas naturales extranjeras no residentes en el país, mediante el pasaporte vigente.

c. Personas jurídicas, a través de:

c1. El Registro de Información Fiscal (RIF) expedido por el Servicio Nacional Integrado de Administración Aduanera y Tributaria (SENIAT).

c2. Copias de los documentos constitutivos de la persona jurídica, sus estatutos sociales y de las modificaciones posteriores que guarden relación con su estructura accionaria y de control, debidamente inscritos en el registro correspondiente. Si la persona jurídica está constituida fuera del territorio nacional, dichos documentos deben estar legalizados y/o apostillados, según corresponda.

Los Sujetos Obligados deberán identificar y verificar la información referente al beneficiario final de sus clientes que sean personas jurídicas, lo cual incluye a las personas naturales que ejercen el control de las mismas, ya sea por participación accionaria u otro medio.

Artículo 49: El Sujeto Obligado cuando tenga indicios o certeza que los clientes no actúan por cuenta propia, solicitará la presentación del poder debidamente autenticado y legalizado o apostillado, según corresponda y deberá recabar la información necesaria que permita conocer tanto la identidad de los representantes, apoderados y autorizados, como de las personas por cuenta de las cuales actúan.

Artículo 50: El Sujeto Obligado debe elaborar y mantener, en forma física o digital, un expediente del cliente con la información consignada por el cliente, el cual contendrá:

1. Para personas naturales:

a. Copia de la cédula de identidad o del pasaporte del cliente, según corresponda.

b. Ficha de Identificación del Cliente.

c. Declaración jurada del origen lícito de los fondos o valores representados en sus activos virtuales, siempre y cuando no esté inserta en el cuerpo de la Ficha de Identificación del Cliente.

d. Constancias de las acciones de verificación inicial y periódica realizadas por el Sujeto Obligado, de acuerdo con el nivel de riesgo determinado para el cliente.

e. Claves públicas, direcciones o cuentas del cliente.

f. Cualquier otro documento o información relacionada con el cliente y sus actividades, que el Sujeto Obligado estime pertinente.

2. Para personas jurídicas:

a. Copia del documento constitutivo y de los estatutos sociales, debidamente inscritos en el Registro correspondiente y de sus posteriores modificaciones relacionadas con su estructura accionaria y de control. Si la persona jurídica está constituida fuera del territorio nacional, dichos documentos deben estar legalizados y/o apostillados, según corresponda.

b. Copia del Registro de Información Fiscal (RIF).

c. Ficha de identificación del cliente persona jurídica.

d. Ficha de identificación de las personas naturales que establecen la relación de negocios en representación del ente jurídico.

e. Declaración jurada del origen lícito de los fondos o valores representados en sus activos virtuales, siempre y cuando no esté inserta en el cuerpo de la ficha de identificación del cliente.

f. Constancias de las acciones de verificación inicial y periódica realizadas por el Sujeto Obligado en concordancia con el nivel de riesgo determinado para el cliente.

g. Claves públicas, direcciones o cuentas del cliente.

Artículo 51: Este Organismo podrá elaborar un Formato Único de Ficha de Identificación del Cliente, tanto para persona natural como para persona jurídica, el cual podrá ser suministrado a los Sujetos Obligados a través de Comunicado o Circular con su respectivo instructivo, no obstante, el Sujeto Obligado podrá incorporar información adicional en el citado formato, de acuerdo a su política de administración de riesgos.

Artículo 52: El Sujeto Obligado, de acuerdo al nivel de riesgo de sus potenciales o nuevos clientes, deberá emplear diferentes métodos para verificar la identidad y los datos aportados por éstos, siendo que a mayor nivel de riesgo utilizará métodos más pormenorizados o estrictos, los cuales pueden incluir la solicitud de información adicional, el contacto con el cliente, las comunicaciones, la verificación independiente de la identidad del cliente a través de una comparación de la información suministrada por el cliente con la información obtenida por una empresa consultora o de investigación, o en una base de datos pública u otra fuente confiable e independiente.

Artículo 53: El Sujeto Obligado debe asegurarse de la calidad de la información relacionada con la captura de datos de la Ficha de Identificación del Cliente y sus

actualizaciones, fundamentándose en los principios de integridad, disponibilidad, confidencialidad y no repudio.

Artículo 54: El Sujeto Obligado incluirá en su Manual de Administración de Riesgos de LC/FT/FPADM las normas y métodos para la verificación de los datos aportados por sus clientes, de acuerdo al nivel de riesgo asignado a cada tipo de cliente.

Los Sujetos Obligados deben verificar la identidad del cliente y del beneficiario final, antes o durante el curso del establecimiento de la relación comercial o al realizar transacciones para usuarios ocasionales. En los casos en que resulte esencial no interrumpir la realización normal de los negocios y operaciones, los Sujetos Obligados pueden completar la verificación tan pronto como sea razonablemente factible luego del establecimiento de la relación, adoptando procesos para manejar el riesgo bajo condiciones especiales para el uso de productos y servicios que involucren activos virtuales, antes de completar las labores de verificación.

Quedan exceptuadas del proceso de verificación las cuentas y billeteras virtuales que sean destinadas al pago de nómina de los trabajadores, de los sectores público y privado, siempre y cuando los datos sean proporcionados oficialmente por los patronos respectivos. Así mismo, las cuentas y billeteras virtuales de las personas jubiladas y pensionadas abiertas por mandato del órgano competente del Estado que proporciona estos beneficios, quedarán exceptuadas de la verificación de sus datos.

Artículo 55: Si durante el curso de las gestiones de Debida Diligencia realizadas para iniciar relaciones comerciales con un nuevo cliente o cuando el sujeto obligado actualice los datos de sus clientes, el empleado del Sujeto Obligado detecta o sospecha falsedad, contradicción o incongruencias en la información aportada por el cliente, negará el servicio solicitado y hará del conocimiento de su supervisor inmediato esta situación, con el fin de determinar las acciones procedentes en estos casos.

Artículo 56: Cuando existan suficientes indicios para presumir la falsedad de algunos de los datos aportados por el cliente, después de haberse prestado un servicio o ejecutado una actividad que involucre activos virtuales, el Oficial de Cumplimiento analizará el caso y de considerarlo procedente, este último informará la situación a la UNIF, mediante el formulario Reporte de Actividades Sospechosas, así como también indicará los datos verdaderos en relación al cliente, si los hubiera obtenido.

Artículo 57: El Sujeto Obligado debe tener precaución y adoptar medidas mejoradas o intensificadas de DDC, en los siguientes casos:

1. Prestación de servicios o ejecución de actividades, operaciones y transacciones que involucren activos virtuales, para niñas, niños y adolescentes, así como para personas con discapacidad y entredichos.

2. Apertura de nueva cuenta o billetera virtual por parte de un cliente previamente vinculado a una cuenta o billetera virtual, sin una causa que aparentemente lo justifique.

Artículo 58: El Sujeto Obligado verificará la identidad de los usuarios ocasionales de acuerdo a estas normas, cuando se establezca cualquier relación de negocios o se intente efectuar operaciones de cualquier índole, o ante cualquier transacción que no implique la vinculación formal con el Sujeto Obligado.

Artículo 59: El Sujeto Obligado exigirá estampar las huellas dactilares de los dedos pulgar y/o índice de la mano derecha o en su defecto los de la mano izquierda, siempre que sea posible, en los comprobantes correspondientes, a las personas que utilicen servicios que involucren activos virtuales brindados a través de canales de distribución físicos (taquillas).

Artículo 60: El Sujeto Obligado podrá aceptar la cédula de identidad laminada como único requisito para los ciudadanos que participen en procesos de incorporación de la población al Sistema Integral de Criptoactivos propiciados por el Estado venezolano, como parte de sus políticas públicas de inclusión social, mediante la apertura de cuentas y billeteras virtuales u otras políticas o medidas estatales. En los procesos de incorporación de la población al Sistema Integral de Criptoactivos propiciados por el Estado venezolano, como parte de sus políticas públicas de inclusión social, el Sujeto Obligado aplicará medidas de mitigación de los riesgos de LC/FT/FPADM basadas principalmente en el monitoreo, seguimiento y revisión de las cuentas y billeteras virtuales y del volumen y frecuencia de las transacciones realizadas a través de ellas.

Artículo 61: Los Sujetos Obligados conservarán en forma física o digital, durante un período mínimo de cinco (05) años, la información, registros y soportes correspondientes que comprueben la realización de las operaciones y las relaciones de negocios de los clientes y usuarios ocasionales, así como la información y registros obtenidos a través de medidas de DDC exigidos para la identificación de los clientes, los cuales pueden ser necesarios para la reconstrucción de operaciones y relaciones de negocio, por las autoridades competentes, en las labores de inteligencia financiera. Estos registros deben ser suficientes para permitir la reconstrucción de transacciones individuales, incluyendo identificación de las partes, carácter y fecha de la operación, los montos y tipos de activos virtuales involucrados, clase y número de identificación de las cuentas y billeteras virtuales involucradas, de manera tal que ofrezcan evidencia, de ser necesario, para el procesamiento de actividades criminales. Dicho periodo transcurrirá de la siguiente manera:

1. Los documentos relativos a la identificación de clientes y usuarios, a partir del día en que finalice la relación.

2. Los documentos que acrediten una operación, a partir de la ejecución de ésta.

3. Los Reportes de Actividades Sospechosas, a partir de su remisión a la UNIF.

Esta obligación de mantenimiento abarca muy especialmente la obtención, registro y conservación de la información sobre el originador y el beneficiario de transferencias e intercambios que involucren activos virtuales.

La información obtenida a través de medidas de Debida Diligencia del Cliente y los registros de transacciones que deben ser mantenidos por los Sujetos Obligados, deben incluir:

a. Datos relacionados con la información de las partes relevantes,

b. Las claves públicas (o identificadores equivalentes),

c. Direcciones o cuentas y billeteras involucradas (o equivalentes identificadores), siendo necesario recabar además información adicional que permita asociar la dirección, cuenta o billetera, a una persona real o física.

d. La naturaleza y fecha de la operación y

e. Las cantidades involucradas.

Artículo 62: El Sujeto Obligado debe establecer métodos y controles internos eficientes que permitan obtener cualquier información requerida, en un plazo no mayor de setenta y dos (72) horas.

CAPÍTULO III

POLÍTICAS, MEDIDAS Y CONTROLES PARA LA ADMINISTRACIÓN DE RIESGOS DE LC/FT/FPADM DERIVADOS DE LOS EMPLEADOS

Artículo 63: El Sujeto Obligado debe formular e implementar la Política Conozca su Empleado, que incluya los trámites de reclutamiento y selección del personal (nuevos ingresos), verificando los datos e información por ellos aportados, así como las referencias de trabajos anteriores.

El Sujeto Obligado debe elaborar y mantener en forma física o digital un expediente del empleado que permanecerá en la dependencia encargada de la gestión del talento humano, el cual contendrá la información exigida para su ingreso, así como:

a. Constancia de verificación de los datos y referencias aportados al momento de establecerse la relación laboral.

b. Certificados y soportes que evidencien la participación del empleado en actividades de capacitación relacionadas con la materia de prevención y control de LC/FT/FPADM.

c. Declaración de conocimiento.

Artículo 64: Cuando el Sujeto Obligado tenga indicios suficientes para considerar que alguno de sus empleados pudiera estar incurso en la presunta comisión de delitos previstos y sancionados en nuestra legislación, cometidos en el marco de sus actuaciones vinculadas con la relación laboral, tiene la obligación de realizar el procedimiento de denuncia establecido en la normativa que regula el procedimiento penal.

El Sujeto Obligado deberá realizar las investigaciones necesarias a través de su Gerencia de Seguridad o Unidad equivalente y documentar la averiguación como paso previo a la formalización de la denuncia.

CAPÍTULO IV

CAPACITACIÓN DEL PERSONAL

Artículo 65: Con el objeto de prevenir las operaciones de LC/FT/FPADM, el Sujeto Obligado deberá diseñar, financiar, desarrollar e implementar un Programa Anual de Capacitación de PC LC/FT/FPADM, ajustado a su perfil operacional y conforme a sus riesgos en materia de LC/FT/FPADM. Este plan estará dirigido a todo el personal, directivos, ejecutivos, empleados, representantes y autorizados, según las responsabilidades y actividades que desempeñe cada grupo.

Artículo 66: Para el diseño del Programa Anual de Capacitación de PC LC/FT/FPADM el Sujeto Obligado debe considerar la audiencia a la cual va dirigido y tomar en cuenta las funciones específicas de cada área del Sujeto Obligado. Dicho programa deberá contemplar los siguientes aspectos:

1. Los nuevos ingresos deberán recibir obligatoriamente una inducción y sensibilización en esta materia.

2. Capacitación que permita al personal comprender las particularidades que en esta materia se presentan en las áreas sensibles del Sujeto Obligado.

3. Capacitación especializada y altamente tecnificada para el Oficial de Cumplimiento y el personal del área operativa que maneja las plataformas tecnológicas y sistemas informáticos, quienes deben recibir capacitación periódica que sea relevante y adecuada, en razón de los cambios en las exigencias de los organismos reguladores y en los nuevos métodos y técnicas de LC/FT/FPADM utilizados por la delincuencia organizada.

4. Asistencia a eventos que brinden información y capacitación sobre prevención, control y administración de riesgos de LC/FT/FPADM, para directivos y empleados relacionados con las funciones de prevención, control y administración de riesgos de LC/FT/FPADM.

Artículo 67: El Sujeto Obligado debe documentar el cumplimiento de sus programas de capacitación y llevar registros (físicos o digitales) de los mismos, los cuales estarán a la disposición de este Organismo cuando lo requiera y deberán permanecer en los archivos del Sujeto Obligado por un período mínimo de diez (10) años, contados a partir de la fecha de haberse realizado la capacitación, debiendo contener la siguiente información:

1. Lugar, fecha, programa y contenido detallado e identificación de los instructores de cada capacitación.

2. Copias del contrato, propuesta de servicios, facturas y resumen curricular de los instructores

3. Lista de asistencia que identifique: fecha, nombre del evento, identificación y firma del participante, indicación del área a la cual pertenece el trabajador dentro de la estructura del Sujeto Obligado.

4. Copias de constancias, certificados o soportes de las actividades de capacitación impartidas o recibidas en materia de PC LC/FT/FPADM.

5. Constancias de la asistencia de directivos y empleados a eventos nacionales e internacionales relacionados con el tema de prevención, control y administración de riesgos de LC/FT/FPADM, incluyendo nombre del evento, lugar y fecha, contenido del programa e identificación de los asistentes por el Sujeto Obligado y sus cargos.

Artículo 68: (Declaración de Conocimiento) El Sujeto Obligado diseñará un documento que deberán suscribir individualmente los directivos y trabajadores, donde declaren haber recibido información y capacitación sobre prevención y administración de los riesgos de LC/FT/FPADM en cada oportunidad en la cual se imparta dicha capacitación y donde se especifique su contenido. Del citado documento se debe mantener evidencia física o digital y debe estar a disposición de esta Superintendencia cuando así lo requiera.

CAPÍTULO V

MEDIDAS Y CONTROLES DE NATURALEZA TECNOLÓGICA, PARA LA ADMINISTRACIÓN DE RIESGOS DE LC/FT/FPADM DERIVADOS DE ACTIVIDADES Y SERVICIOS QUE INVOLUCRAN ACTIVOS VIRTUALES

Artículo 69: Los Sujetos Obligados deberán utilizar herramientas tecnológicas con la capacidad técnica necesaria que les permita brindar adecuadamente sus servicios y efectuar en forma segura las operaciones y transacciones que involucren activos virtuales, así como dar cumplimiento a las normas relativas a la seguridad de la información, a la prevención y administración de riesgos de LC/FT/FPADM y a la prestación de servicios que involucren activos virtuales que sean emitidas por este Organismo.

Las herramientas para prevenir y mitigar riesgos de LC/FT/FPADM en materia de activos virtuales, deben ser tecnológicas, porque las plataformas para prestar servicios y ejecutar actividades de intercambio, transferencia y administración que involucren activos virtuales, son sitios web.

Artículo 70: Los Sujetos Obligados deben contar con herramientas tecnológicas que permitan mitigar los riesgos de LC/FT/FPADM, monitorear eficazmente operaciones y rastrear los fondos o valores representados en activos virtuales.

Dichas herramientas tecnológicas deben hacer posible la identificación de las contrapartes en las transacciones y operaciones con activos virtuales e igualmente, deben mostrar y conservar información precisa sobre el originador y el beneficiario en los movimientos y transferencias de activos virtuales y sus mensajes relacionados; del mismo modo, deben garantizar que esta información permanezca en la transferencia electrónica o mensaje relacionado, a lo largo de toda la cadena de pago o transacciones.

Las referidas soluciones o herramientas deben ser eficaces y eficientes, estar basadas en tecnología que mejore potencialmente el cumplimiento en materia de administración de riesgos de LC/FT/FPADM y deben permitir al Sujeto Obligado monitorear o rastrear los

movimientos y transferencias de activos virtuales, con el propósito de detectar aquellas que carezcan de la información requerida sobre el originador y/o beneficiario y tomar las medidas apropiadas, asimismo, deben permitir el registro de las transacciones y la conservación de los registros de las mismas.

Artículo 71: El Sujeto Obligado deberá:

1. Prestar especial atención a cualquier riesgo de LC/FT/FPADM que surja de la utilización de las nuevas tecnologías o en desarrollo, que dificulten la identificación y verificación de la identidad del cliente o usuario y adoptar las medidas para impedir su utilización con fines ilícitos. Asimismo, debe abstenerse de usar tecnologías o mecanismos que favorezcan el anonimato u oculten la identidad del remitente, destinatario, titular o beneficiario final de activos virtuales.

2. Contar con sistemas de monitoreo que le permitan llevar a cabo una diligencia debida constante sobre la relación comercial y examinar las transacciones efectuadas en el transcurso de esa relación, para asegurarse que las transacciones que se lleven a cabo estén acordes con el conocimiento que tiene el Sujeto Obligado acerca del cliente, sus negocios y su perfil en cuanto a riesgos de LC/FT/FPADM. Los sistemas de monitoreo de la relación comercial y de las operaciones deben estar acompañados de herramientas que permitan identificar alertas que actúen automáticamente como indicadores para ayudar a detectar actividades sospechosas de LC/FT/FPADM y reportarlas a la UNIF.

La presencia de un indicador de alerta de actividad sospechosa debe dar lugar a un mayor control, seguimiento y examen por parte del Sujeto Obligado y la presentación de un Reporte de Actividad Sospechosa cuando corresponda. En todo caso, el cliente y usuario pueden siempre proporcionar explicaciones para justificar el indicador de alerta.

Las herramientas tecnológicas que se usen para el monitoreo de transacciones específicas y de la relación comercial (continuo), deben permitir detectar patrones de transacciones irregulares, comportamientos inusuales o poco comunes que puedan sugerir una actividad u operación potencialmente sospechosa, así como facilitar la identificación de cambios en el perfil del cliente.

3. Implementar sistemas tecnológicos con capacidad para detectar las transacciones que se realicen y emitir señales de alerta que incluyan, entre otros aspectos, la frecuencia con que ingresan a la cuenta y/o billetera virtual fondos o valores representados en activos virtuales.

Artículo 72: Queda prohibido a los Sujetos Obligados prestar servicios con mezcladores, volteadores y anonimizadores del protocolo de internet (IP), que reducen la transparencia de las transacciones, así como también queda prohibido usar herramientas tecnológicas o prácticas operacionales susceptibles de ocultar u ofuscar la fuente y los flujos de los fondos representados en activos virtuales o inhibir la capacidad para identificar a los clientes y usuarios.

CAPÍTULO VI

POLÍTICAS, MEDIDAS Y CONTROLES PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE LC/FT/FPADM DERIVADOS DE LAS PERSONAS EXPUESTAS POLÍTICAMENTE Y DE LA PRESTACIÓN DE SERVICIOS DE CUSTODIA Y/O ADMINISTRACIÓN DE ACTIVOS VIRTUALES O DE INSTRUMENTOS VIRTUALES QUE PERMITAN EL CONTROL SOBRE ACTIVOS VIRTUALES

Artículo 73: El Sujeto Obligado debe tomar medidas razonables para mitigar el riesgo de participar, deliberada o involuntariamente, en el encubrimiento o en la realización de transacciones, operaciones o transferencias que involucren ingresos, fondos o valores representados en activos virtuales, derivados de actos de corrupción, por parte de figuras políticas nacionales o extranjeras, funcionarios públicos de alto nivel y su círculo de colaboradores.

Artículo 74: El Sujeto Obligado debe diseñar, establecer y aplicar métodos de DDC cuando mantenga relaciones comerciales con personas que son o han sido considerados bajo el perfil de una Persona Expuesta Políticamente, bien sea esta un cliente o un beneficiario final de movimientos, intercambios o transferencias que involucren activos virtuales.

El Sujeto Obligado debe implementar sistemas apropiados que permitan:

a. Determinar si el cliente o el beneficiario final es o fue una Persona Expuesta Políticamente.

b. La identificación de los riesgos y el diseño de controles eficaces para la adecuada gestión de los riesgos derivados de las Personas Expuestas Políticamente (sean clientes o beneficiarios finales).

c. El monitoreo de las transacciones efectuadas en las cuentas y billeteras virtuales de las Personas Expuestas Políticamente, cuyos controles deben estar basados en su nivel de riesgo.

Artículo 75: El Sujeto Obligado, de acuerdo con el nivel de riesgo y los procedimientos de Debida Diligencia para el conocimiento del Cliente (DDC), cuando se vincule con un individuo calificado como PEP, debe asegurar como mínimo lo siguiente:

1. Identificación del titular de la cuenta y billetera virtual y del beneficiario de los movimientos, intercambios y transferencias de activos virtuales que se generen desde las mismas.

2. Obtención de información directamente del individuo relacionada a su condición de PEP.

3. Identificación del país de residencia del titular de la cuenta y billetera virtual, calificado como PEP.

4. Obtención de información para establecer la fuente de la riqueza de la Persona Expuesta Políticamente y el origen de los fondos o valores representados en los activos virtuales del sujeto calificado como PEP.

5. Verificación de referencias para determinar si el individuo es ó fue un PEP.

6. Obtención de información relacionada con las terceras personas que tengan acceso y/o autorización para el manejo de la cuenta y billetera virtual del individuo calificado como PEP.

7. Hacer esfuerzos razonables para revisar fuentes públicas de información relacionada con el individuo calificado como PEP.

8. Llevar a cabo un monitoreo continuo intensificado de la relación comercial. Las medidas y controles aplicables a los sujetos calificados como PEP deben aplicarse también a los miembros de su familia y asociados cercanos.

Artículo 76: El Sujeto Obligado que preste servicios de custodia y/o administración de activos virtuales o de instrumentos virtuales que permitan el control sobre activos virtuales, debe diseñar e implementar medidas y controles que contribuyan a mitigar los riesgos de LC/FT/FPADM, de conformidad con la naturaleza de estos servicios. Dichas medidas deben contemplar como mínimo:

a. Recabar y conservar información adecuada, exacta y oportuna sobre las relaciones comerciales en las cuales prestan estos tipos de servicios, que incluya identificación de las partes involucradas (contratantes de los servicios, beneficiarios finales y cualquier otra persona que ejerza el control final efectivo sobre la relación), así como la ejecución de medidas razonables para verificar la identidad de dichas personas.

b. Recabar y conservar la mayor cantidad de información posible acerca del origen, propósito y destino de los fondos o valores representados en los activos virtuales objeto de la relación.

CAPÍTULO VII

MEDIDAS Y CONTROLES PARA LA ADMINISTRACIÓN DE RIESGOS RELACIONADOS CON EL FINANCIAMIENTO AL TERRORISMO

Artículo 77: El Sujeto Obligado debe aplicar un Enfoque Basado en Riesgos a la prevención y mitigación de los riesgos relacionados con el financiamiento al terrorismo, el cual tomará en cuenta las siguientes consideraciones:

1. El financiamiento al terrorismo tiene similitudes y diferencias cuando se compara con la legitimación de capitales y los riesgos que genera pudieran ser detectados tomando en consideración lo siguiente:

1.1. El bajo valor que puedan presentar las transferencias y transacciones involucradas.

1.2 El hecho que los fondos o valores involucrados, representados en activos virtuales, pudiesen provenir de fuentes legales.

1.3. La naturaleza de la fuente de los fondos o valores representados en activos virtuales puede variar de acuerdo con el tipo de organización terrorista.

2. Cuando los fondos o valores involucrados representados en activos virtuales se derivan de una actividad delictiva, los mecanismos de monitoreo tradicionales que se usan para identificar la legitimación de capitales pueden ser también adecuados para identificar el financiamiento al terrorismo, aunque la actividad indicativa de sospecha no aparente estar conectada con este delito.

3. Cuando las transacciones y transferencias se realizan en pequeñas cantidades y se aplica un Enfoque Basado en Riesgos, podría considerarse que la transacción es de mínimo riesgo en cuanto a legitimación de capitales, lo cual no aplica para el delito de financiamiento al terrorismo.

4. Cuando los fondos o valores involucrados representados en activos virtuales provienen de una fuente legal, es necesario indagar con mayor minuciosidad para determinar que pudieran ser usados para el financiamiento del terrorismo.

5. Las acciones de los terroristas pueden aparentar inocencia, como sería la compra de materiales y pago de servicios (por ejemplo: químicos de venta libre y común, un vehículo, entre otros).

6. Las transferencias y transacciones de fondos o valores representados en activos virtuales, de o para terroristas, derivados de actividades delictivas y aquellos procedentes de fuentes legítimas, pueden no presentar los mismos rasgos que la legitimación de capitales convencional.

7. No es responsabilidad del Sujeto Obligado el determinar el tipo de actividad criminal que esté realizando el cliente, su deber es reportar la actividad sospechosa oportunamente a la UNIF y participar a la SUNACRIP las tipologías o modelos de actuación que vaya identificando el Sujeto Obligado como modus operandi para el financiamiento del terrorismo. Estas participaciones o notificaciones a la SUNACRIP se harán respetando en todo momento la reserva y confidencialidad de los datos de identificación de las personas naturales o jurídicas involucradas en los Reportes de Actividades Sospechosas a la UNIF.

Artículo 78: El Sujeto Obligado, para detectar actividades de financiamiento al terrorismo, tendrá en cuenta las siguientes medidas y procedimientos:

1. Monitoreo sobre las transferencias y transacciones que involucren originadores y/o beneficiarios (individuos u organizaciones) ubicados en países, jurisdicciones o áreas geográficas designados según las listas emanadas del Consejo de Seguridad de la Organización de Naciones Unidas, por estar vinculados con actividades terroristas.

2. Monitoreo que permita identificar transferencias y transacciones relacionadas con personas naturales o jurídicas que han sido identificadas en otras jurisdicciones o países como elementos vinculados con organizaciones o actividades terroristas o su financiamiento.

3. Control interno y señales de alerta basados en las tipologías detectadas y difundidas por las autoridades nacionales o de otras jurisdicciones, relacionadas con el financiamiento de actividades terroristas.

4. Las medidas y procedimientos acordados por el Consejo de Seguridad de las Naciones Unidas, así como las normativas emitidas por los órganos nacionales competentes con motivo a éstas.

Artículo 79: El Sujeto Obligado debe prestar especial atención a las operaciones y actividades que presenten características que puedan indicar que los fondos o valores involucrados representados en activos virtuales pudieran estar relacionados con el financiamiento al terrorismo, debe someterlas a un exhaustivo análisis y en los casos que el Sujeto Obligado lo considere procedente y califique la operación como sospechosa, deberá elaborar y remitir a la UNIF el Reporte de Actividades Sospechosas y participará a la SUNACRIP las tipologías o modelos de actuación que vaya identificando como modus operandi para el financiamiento del terrorismo. Estas participaciones o notificaciones a la SUNACRIP se harán respetando en todo momento la reserva y confidencialidad de los datos de identificación de las personas naturales o jurídicas involucradas en los Reportes de Actividades Sospechosas a la UNIF.

CAPÍTULO VIII

MEDIDAS Y CONTROLES PARA LA ADMINISTRACIÓN DE RIESGOS RELACIONADOS CON EL FINANCIAMIENTO DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA

Artículo 80: El Sujeto Obligado debe establecer políticas, normas y métodos orientados a prevenir que flujos de fondos o valores representados en activos virtuales sean orientados, a través de sus transacciones y servicios, al financiamiento de la investigación y desarrollo de las armas de destrucción masiva. Se requiere la aplicación de una Debida Diligencia del Cliente (DDC) y de herramientas que permitan el cabal conocimiento de los clientes y usuarios ocasionales, sus operaciones y relacionados, para determinar oportunamente su vinculación directa o indirecta con personas, organizaciones o gobiernos que se encuentren desarrollando, fabriquen y/o comercialicen Armas de Destrucción Masiva, de acuerdo a las Resoluciones emitidas por el Consejo de Seguridad de la Organización de las Naciones Unidas.

Artículo 81: Para la administración de sus riesgos relacionados con el financiamiento de la proliferación de armas de destrucción masiva, el Sujeto Obligado deberá cumplir con políticas y métodos similares a los establecidos en el Capítulo anterior de esta Providencia, para la administración de los riegos relacionados con el financiamiento al terrorismo.

TÍTULO IV

LAS AUDITORÍAS

Artículo 82: El Sujeto Obligado debe contar con la función de Auditoría independiente, a los fines de comprobar el nivel de cumplimiento de la normativa vigente y la efectividad de los planes, programas, métodos y controles internos adoptados para prevenir, controlar, detectar y reportar operaciones que se presuman relacionadas con la LC/FT/FPADM.

Artículo 83: La función de Auditoría independiente desempeña un rol importante, pues permite evaluar objetivamente la gestión y los controles del riesgo de LC/FT/FPADM, proporcionando de manera oportuna a la Junta Directiva o al órgano de dirección que haga sus veces, información sobre la efectividad del cumplimiento de las políticas y métodos de PC LC/FT/FPADM.

Las Auditorías al programa de cumplimiento contra LC/FT/FPADM deben ser efectuadas anualmente, siendo una práctica responsable que el Sujeto Obligado realice Auditorías de cumplimiento en proporción a su perfil de riesgo de LC/FT/FPADM. Los auditores del programa de cumplimiento contra LC/FT/FPADM deben realizar pruebas para verificar el cumplimiento específico de la LOCDOFT, otras normas vigentes y evaluar los sistemas de información de gestión pertinentes.

La Auditoría debe basarse en el riesgo y sus programas de evaluación variarán según el tamaño del Sujeto Obligado, su complejidad, el alcance de sus actividades, su perfil de riesgo, la calidad de sus funciones de control y el uso que hace de la tecnología. Un programa de Auditoría basado en riesgo efectivo cubrirá todas las actividades del Sujeto Obligado.

El alcance de las evaluaciones de Auditoría variará según la valoración de los riesgos. Las pruebas deben ayudar a la Junta Directiva y a la Gerencia a identificar las áreas que presentan debilidades y que requieren revisiones más estrictas.

Las pruebas de Auditoría deben evaluar todos los aspectos exigidos por la normativa aplicable a la prevención y control de los riesgos de LC/FT/FPADM, incluyendo lo siguiente, a menos que el alcance de la revisión se circunscriba a un área o actividad particular:

1. Evaluación global del SIAR LC/FT/FPADM.

2. Evaluación de la efectividad del programa de cumplimiento contra LC/FT/FPADM contenido en el Manual de Administración de Riesgos de LC/FT/FPADM.

3. Revisión de la autoevaluación de riesgos del Sujeto Obligado.

4. Evaluación de los esfuerzos de la Gerencia para implementar las medidas correctivas señaladas en las observaciones formuladas por esta Superintendencia y en las auditorías previamente realizadas.

5. Revisión del Programa Anual de Capacitación en cuanto a su alcance y contenido.

6. Revisión de la efectividad de los sistemas de monitoreo y detección de actividades sospechosas de estar relacionadas con la LC/FT/FPADM. Los auditores no podrán tener acceso a la información relacionada con los casos que se investiguen o que hayan sido reportados a las autoridades como actividades sospechosas de estar relacionadas con la LC/FT/FPADM.

Artículo 84: Los Sujetos Obligados deberán exigir a los auditores la presentación de un "Informe Anual Sobre Prevención y Control de Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva", en relación al cumplimiento de los deberes establecidos en las Providencias, Normativas y Circulares emitidas por la SUNACRIP y otras autoridades competentes, relativas a los riesgos de LC/FT/FPADM; dicho Informe deberá contener las respectivas conclusiones y recomendaciones.

Para la preparación y elaboración de este Informe, los auditores no podrán tener acceso a la información relacionada con los casos que se investiguen o que hayan sido reportados a las autoridades como actividades sospechosas de estar relacionadas con LC/FT/FPADM.

Los Sujetos Obligados deberán remitir su "Informe Anual Sobre Prevención y Control de Riesgos de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva" a la UNIF y a la SUNACRIP, dentro de los noventa (90) días calendarios siguientes al cierre del ejercicio anual.

Artículo 85: Aquellas operaciones detectadas por los auditores, que a su criterio constituyen actividades sospechosas, deberán ser informadas al Oficial de Cumplimiento, quien las evaluará y decidirá si deben ser reportadas a la UNIF.

Artículo 86: Cuando este Organismo considere deficiente el Informe presentado por el auditor o los auditores, podrá exigir al Sujeto Obligado el cambio de éstos. Artículo 87: En el caso que el o los auditores emitan un pronunciamiento desfavorable en relación al cumplimiento, por parte de los Sujetos Obligados, de sus obligaciones previstas en la LOCDOFT, en esta Providencia y en las demás normas que resulten aplicables en materia de PC LC/FT/FPADM, esta Superintendencia podrá practicar una inspección especial para comprobar la exactitud del dictamen emitido y exigir las acciones correctivas correspondientes.

TÍTULO V

NOTIFICACIONES PERIÓDICAS A ESTA SUPERINTENDENCIA

Artículo 88: El Sujeto Obligado remitirá a esta Superintendencia, vía electrónica, notificaciones de las transacciones, intercambios y transferencias realizadas por sus clientes y usuarios, que involucren criptoactivos, por montos iguales o superiores a los que sean establecidos por este Organismo. Este Ente Supervisor informará los datos que debe contener y las características técnicas de las mencionadas notificaciones.

Artículo 89: Los Sujetos Obligados participarán a esta Superintendencia, lo siguiente:

1. Identificación de las personas naturales y jurídicas que sean accionistas del Sujeto Obligado, así como la composición accionaria de las personas jurídicas que sean titulares de acciones representativas de su capital social.

2. Identificación de los miembros de la Junta Directiva o del órgano que ejerza función equivalente, así como información general de tales personas.

3. Datos de identificación de todas las cuentas y billeteras virtuales que posean cada uno de sus clientes.

4. Información de las transferencias e intercambios de activos virtuales efectuados por sus clientes y usuarios, a partir de los montos o umbrales que sean establecidos por esta Superintendencia.

5. Los saldos de las cuentas y billeteras virtuales de sus clientes. El Sujeto Obligado debe remitir la información antes señalada con los datos, características técnicas y periodicidad que sean establecidos en la normativa que emita para tal fin esta Superintendencia.

TÍTULO VI

REPORTE A LA UNIF DE LAS OPERACIONES QUE SE PRESUMAN COMO DE LC/FT/FPADM Y NOTIFICACIÓN A LA SUNACRIP DE LAS TIPOLOGÍAS O MODELOS DE ACTUACIÓN

Artículo 90: El Sujeto Obligado debe:

1. Conservar la información de las transacciones, intercambios y transferencias efectuadas que involucren activos virtuales, así como reportar a la UNIF aquellas operaciones que se consideren sospechosas de LC/FT/FPADM, tomando en cuenta su cuantía, frecuencia, continuidad, entre otros factores e informar a la SUNACRIP acerca de las tipologías o modelos de actuación que vaya identificando el Sujeto Obligado como modus operandi para la LC/FT/FPADM. Estas notificaciones a la SUNACRIP acerca de dichas tipologías o modelos de actuación se harán respetando en todo momento la reserva y confidencialidad de los datos de identificación de las personas naturales o jurídicas involucradas en los Reportes de Actividades Sospechosas a la UNIF.

2. Colaborar de forma oportuna y expedita con los órganos del Poder Público, autoridades administrativas, judiciales y de investigación con competencia en materia de prevención, control y represión de los delitos de LC/FT/FPADM, atendiendo adecuada y diligentemente sus requerimientos. El secreto profesional o confidencialidad debida no es oponible a las solicitudes de información formuladas por las autoridades, ni a los reportes y notificaciones que efectúe el Sujeto Obligado por iniciativa propia ante la sospecha de la comisión de los citados delitos.

Artículo 91: La comparación de una operación identificada como inusual, no convencional, compleja o estructurada, con la información que se tenga del cliente y las

indagaciones que se realicen o se hayan realizado sin alertar al cliente, podrán determinar si dicha operación debe clasificarse o no como sospechosa. Este proceso de análisis y posterior reporte deberá realizarse con la mayor celeridad posible, en virtud de la naturaleza expedita de las operaciones y actividades que involucran activos virtuales o criptoactivos.

Artículo 92: En la oportunidad que el Oficial de Cumplimiento decida reportar casos de actividades sospechosas de estar vinculadas con LC/FT/FPADM, deberá remitir el correspondiente Reporte de Actividades Sospechosas (RAS) a la UNIF y notificar a la SUNACRIP acerca de la tipología o modelo de actuación relacionada con la actividad sospechosa, utilizando para ello los medios que se determinen, siendo que la notificación a la SUNACRIP de la tipología o modelo de actuación se hará respetando en todo momento la reserva y confidencialidad de los datos de identificación de las personas naturales o jurídicas involucradas en los reportes a la UNIF. Para los efectos de estos reportes y notificaciones, no se requiere tener certeza que se trata de una actividad delictiva, o de que los fondos o valores representados en los activos virtuales provengan de ese tipo de actividad, sólo es necesario que se considere que son actividades sospechosas, basándose en la experiencia y en los análisis que se hayan realizado.

El citado reporte no se considera una denuncia penal y no requiere de las formalidades y requisitos de este modo de proceder, ni acarrea responsabilidad penal o civil contra el Sujeto Obligado y sus empleados o para quien lo suscribe; los clientes no podrán invocar las reglas de confidencialidad o intimidad vigentes, para exigir responsabilidades civiles o penales a los empleados o al Sujeto Obligado, por la revelación de cualquier información, siempre que ésta última reporte la existencia de fundadas sospechas de buena fe a las autoridades competentes, aun cuando la actividad presuntamente delictiva o irregular no se hubiera realizado.

Los Reportes de Actividades Sospechosas a la UNIF y las notificaciones a la SUNACRIP, se acompañarán con toda la información que le sirva de soporte y la que determine la UNIF y la SUNACRIP.

Artículo 93: El Sujeto Obligado, a fin de evitar un reporte inoficioso, debe recabar toda la información posible que sustente razonable y suficientemente los elementos de juicio que establezcan sin lugar a dudas la emisión de un RAS; la responsabilidad de dicha emisión reside en las revisiones efectuadas por el Sujeto Obligado y en las decisiones que finalmente adopte el Oficial de Cumplimiento, por lo tanto, se debe minimizar la elaboración de Reportes de Actividades Sospechosas que constituyan falsos positivos, que no estén suficientemente documentados, o que con base en una evaluación de todas las variables existentes se determine que no se justifica el reporte.

Este Ente Regulador podrá aplicar sanciones ante la emisión de notificaciones y reportes incompletos o evaluados deficientemente.

Artículo 94: El Sujeto Obligado, cuando tenga conocimiento que alguno de sus clientes ha sido reseñado en noticia criminis, notificará de ello a la UNIF, siendo que el

conocimiento de una noticia criminis no debe provocar un Reporte de Actividad Sospechosa de manera automática sobre la persona investigada. En estos casos el Sujeto Obligado deberá analizar la información que tenga sobre el cliente y sus actividades, procediendo a efectuar dicho Reporte sólo si detecta indicios o sospechas que sus actividades pueden estar relacionadas con los delitos de LC/FT/FPADM, en caso contrario, podrá informar a la UNIF que no se encontraron elementos de juicio para reportar sus actividades como sospechosas. En aquellos casos, cuando en el curso de sus operaciones los Sujetos Obligados recaben elementos adicionales de un cliente que haya sido reportado, podrán enviar informes complementarios.

Artículo 95: El Sujeto Obligado prestará especial atención y creará métodos y normas internas de prevención, control y mitigación de riesgos de LC/FT/FPADM, para ser aplicados a las relaciones de negocios, transferencias y transacciones de sus clientes, con personas naturales y jurídicas ubicadas en regiones, zonas o territorios cuya legislación es estricta en cuanto al secreto bancario, de registro o comercial, o no aplican regulaciones contra LC/FT/FPADM similares a las vigentes en la República Bolivariana de Venezuela, o que las mismas sean insuficientes. Cuando dichas transacciones, intercambios y transferencias de activos virtuales no tengan en apariencia ningún propósito que las justifique, serán objeto de un minucioso examen y si a juicio del Oficial de Cumplimiento fueren clasificadas como actividades sospechosas, los resultados de dicho análisis deberán ser enviados de inmediato a la UNIF, por vía electrónica, utilizando el formulario Reporte de Actividades Sospechosas.

Artículo 96: Cuando un cliente o usuario solicite efectuar una operación, intercambio o transferencia de la cual exista indicio o presunción que está relacionada con LC/FT/FPADM, el trabajador del Sujeto Obligado deberá negarle la prestación del servicio solicitado.

En caso que el Sujeto Obligado no pudiera cumplir con los requisitos de DDC aplicables a clientes y usuarios, podrá, previo cumplimiento de las formalidades legales y contractuales, terminar la relación comercial o decidir no vincularse comercialmente con éstos.

Lo anterior deberá informarse de inmediato, a través de los canales internos, al Oficial de Cumplimiento, quien decidirá su reporte a la UNIF, a través del Reporte de Actividades Sospechosas.

Artículo 97: El Sujeto Obligado debe implementar sistemas tecnológicos que permitan la mayor cobertura y alcance posible a sus dispositivos de control para facilitar la detección de operaciones inusuales o sospechosas, tales sistemas como mínimo incluirán las siguientes capacidades:

1. Acceso a todas las operaciones efectuadas en todas las cuentas y billeteras virtuales de los clientes, con el fin de consolidar la información relacionada con las transferencias, intercambios y transacciones efectuadas por un mismo cliente, incluyendo todos los servicios criptofinancieros brindados por el Sujeto Obligado.

2. Emitir reportes de las personas que hayan efectuado transferencias de activos virtuales, operaciones de intercambio entre activos virtuales e intercambios entre activos virtuales y monedas fiduciarias, durante un mismo mes calendario, con la correspondiente sumatoria de las cantidades transferidas o transadas, de tal manera que se pueda realizar el análisis correspondiente para detectar operaciones inusuales o sospechosas.

3. Detectar las operaciones inusuales o sospechosas y emitir señales de alerta, en tiempo real o con frecuencia no mayor de treinta (30) días continuos.

4. Determinar la existencia de clientes que presenten un número significativo (anormal) de productos, servicios, cuentas y billeteras que involucren activos virtuales, sin justificación, con base a sus características operativas o la información declarada al momento de vincularse.

5. Seguimiento intensificado de la relación con aquellos clientes clasificados como de Riesgo Alto y monitoreo continuo de sus operaciones, intercambios y transferencias que involucren activos virtuales.

Artículo 98: El Sujeto Obligado debe prestar especial atención a las informaciones obtenidas a través de diferentes fuentes, tales como:

1. Medios de comunicación social.

2. Organismos gubernamentales nacionales e internacionales.

3. Asociaciones gremiales.

4. Otros Organismos Reguladores.

5. Clientes, usuarios y usuarias.

6. Investigaciones policiales y judiciales.

7. Internet.

Los Sujetos Obligados deben incluir en sus mecanismos de control interno, la revisión periódica de las mencionadas fuentes, a fin de obtener la información referente a casos particulares, últimas tendencias o tipologías de LC/FT/FPADM, o cualquier otra información relevante para fortalecer el SIAR LC/FT/FPADM, estableciendo los métodos para la divulgación interna de la información, por medio de mensajes electrónicos, reuniones periódicas o por cualquier modo efectivo considerado por el Sujeto Obligado.

Aunque estas fuentes contienen información útil, el Sujeto Obligado no deberá elaborar automáticamente un Reporte de Actividades Sospechosas, sin antes haber indagado si existe una explicación razonable sobre las actividades financieras que realiza la persona mencionada en la fuente de información y adicionalmente haber evaluado el perfil de riesgo de dicha persona.

Artículo 99: Las políticas y métodos preventivos que diseñe y adopte el Sujeto Obligado para protegerse de las actividades de LC/FT/FPADM, deben incluir los sistemas de cajeros automáticos utilizados para realizar intercambios entre activos virtuales y monedas fiduciarias, de forma igualmente efectiva a las que se toman en relación a las otras operaciones y servicios que involucran activos virtuales. Los programas de capacitación, los sistemas de control interno y de auditoría, deben tomar en cuenta de manera apropiada el riesgo del uso de los cajeros automáticos por parte de la delincuencia organizada para legitimar capitales provenientes de sus actividades ilícitas, así como para financiar el terrorismo y financiar la proliferación de armas de destrucción masiva.

Artículo 100: Cuando este Ente Regulador o los organismos competentes soliciten información al Sujeto Obligado sobre un cliente o sus operaciones, dentro de las limitaciones establecidas en las leyes, el Sujeto Obligado realizará sus mejores esfuerzos para establecer mecanismos coordinados que permitan la investigación, seguimiento e intercambio de información sobre las presuntas operaciones de LC/FT/FPADM que estén siendo objeto de investigación por parte de los mencionados organismos.

La recepción de una solicitud de información o el conocimiento de una noticia criminis, no debe provocar un Reporte de Actividad Sospechosa de manera automática sobre la persona investigada. En estos casos el Sujeto Obligado deberá analizar la información que tenga sobre el cliente y sus actividades, procediendo a efectuar dicho Reporte sólo si detecta indicios o sospechas que sus actividades puedan estar relacionadas con los delitos de LC/FT/FPADM. En caso contrario, podrá informar a la UNIF que no se encontraron elementos de juicio para reportar sus actividades como sospechosas.

Artículo 101: La información solicitada por los Órganos Jurisdiccionales, el Ministerio Público, los Organismos Policiales y de investigación, o por esta Superintendencia, se remitirá incluyendo los detalles solicitados sobre las operaciones realizadas, anexando copia de los documentos necesarios que permitan la verificación de la información suministrada, siendo el plazo para cumplir con esta obligación, el que se establezca en el oficio de requerimiento para cada caso.

Artículo 102: El Sujeto Obligado, cuando elabore y envíe una comunicación que responda a los requerimientos de información realizados, deberá tomar en consideración los siguientes aspectos:

1. El acuse de recibo de la solicitud de información deberá estar sellado con la identificación del Sujeto Obligado en un lugar visible, donde se pueda observar claramente el nombre, apellidos y la cédula de identidad del empleado que recibe, así como la fecha y hora de su recepción.

2. Responder de manera individual cada solicitud de información y no responder varias solicitudes mediante una misma comunicación.

3. Hacer referencia a la fecha y número completo, sin omitir letras, ni números, de la circular, oficio o solicitud que se responde (resaltar en negrillas esta información).

4. Indicar de forma clara y detallada el tipo de respuesta emitida (afirmativa o negativa).

5. La información remitida debe estar suscrita, sellada y certificada por el representante de la unidad correspondiente que efectúa el suministro de la data o información requerida. 6. Responder en los plazos establecidos.

Artículo 103: Los montos o umbrales que puedan ser establecidos por la UNIF para la utilización de los formularios de Reportes de Actividades Sospechosas, no implican que operaciones de menor cuantía no puedan ser utilizadas por organizaciones delictivas para intentar legitimar capitales, financiar el terrorismo o la proliferación de armas de destrucción masiva, por ello, los Sujetos Obligados deben reportar estas actividades (operaciones de menor cuantía) en caso que las consideren sospechosas.

Artículo 104: El Sujeto Obligado debe instruir a sus empleados y directivos, a los fines de no advertir o revelar a los clientes involucrados, que se han realizado verificaciones o que se ha notificado o reportado a las autoridades actividades que puedan dar indicios de estar relacionadas con LC/FT/FPADM. El Sujeto Obligado no podrá negarles asistencia a dichos clientes ni suspender sus relaciones con ellos ni cerrar sus cuentas y billeteras virtuales, mientras duren las fases del proceso de investigación policial o judicial, a menos que exista autorización para ello, emanada del Juez competente. Asimismo, deberán incrementar las acciones de vigilancia sobre sus cuentas y billeteras virtuales y mantener informada a la UNIF sobre las operaciones sospechosas que se efectúen en ellas.

Artículo 105: El Sujeto Obligado podrá condicionar preventivamente la movilización de cuentas, billeteras virtuales y la prestación de servicios criptofinancieros o que involucren activos virtuales, cuando exista presunción razonable que sus titulares o los beneficiarios de las operaciones y/o servicios se encuentren vinculados con hechos relacionados con LC/FT/FPADM.

En ese caso deberá, dentro de las 96 horas siguientes a la aplicación del condicionamiento, tomar las medidas internas a objeto de esclarecer los hechos que generaron tal presunción y en el supuesto de haber suficientes elementos vinculados a LC/FT/FPADM, hacer el reporte respectivo a la UNIF e informar a la SUNACRIP acerca de las tipología o modelo de actuación relacionados con la actividad sospechosa.

Artículo 106: Este Organismo, así como la UNIF, podrán solicitar el condicionamiento señalado en el artículo anterior, cuando existan suficientes elementos de riesgo en materia de LC/FT/FPADM que haga necesario tomar tal medida a objeto de impedir que las cuentas, billeteras virtuales y los servicios criptofinancieros o que involucren activos virtuales sean utilizados como medio de consumación de tales delitos.

TÍTULO VII

LAS CASAS DE INTERCAMBIO Y LOS PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES DEL EXTERIOR Y LA ADMINISTRACIÓN DE SUS RIESGOS DE LC/FT/FPADM

Artículo 107: Las Casas de Intercambio y los Proveedores de Servicios de Activos Virtuales domiciliados en el exterior, con operaciones en o desde el territorio de la República Bolivariana de Venezuela, deberán someterse a estas normas en todo cuanto les sea aplicable, así como a los mecanismos de control que establezca este Organismo. Cuando existan diferencias significativas entre las leyes, regulaciones, normas y medidas sobre prevención de LC/FT/FPADM que aplican conforme a su jurisdicción de origen y las leyes, regulaciones, normas y medidas venezolanas, deben implementar las medidas que se establecen en esta Providencia, agregando aquellas contenidas en las normas de su jurisdicción de origen, que resulten más estrictas que las exigidas en la República Bolivariana de Venezuela.

Las Casas de Intercambio, los Proveedores de Servicios de Activos Virtuales y las plataformas tecnológicas y sitios web que, como conducta empresarial participen, para o en nombre de terceros, en actividades o transacciones que involucren activos virtuales y en la prestación de servicios de intermediación, préstamos, comercialización, intercambio y transferencia de valores representados en activos virtuales, que estén domiciliados o situados en el exterior, para poder efectuar operaciones o prestar servicios en o desde el territorio de la República Bolivariana de Venezuela, deberán someterse a esta Providencia y a las demás normas nacionales que rigen la materia, en cuanto les sean aplicables.

TÍTULO VIII

ACTUACIÓN DE LA SUPERINTENDENCIA NACIONAL DE CRIPTOACTIVOS Y ACTIVIDADES CONEXAS

Artículo 108: La Superintendencia Nacional de Criptoactivos y Actividades Conexas, cuando lo considere necesario, podrá actualizar los montos de las operaciones, intercambios y transferencias que involucren activos virtuales, a partir de los cuales deben ser realizadas las notificaciones señaladas en esta Providencia, lo cual será informado oportunamente a los Sujetos Obligados.

Asimismo, en su condición de Ente Rector del Sistema Integral de Criptoactivos, ejercerá sus amplias facultades de supervisión, dentro del marco legal y constitucional, para procurar el cumplimiento de las presentes Normas por parte de los Sujetos Obligados y el apego de dicho Sistema Integral a las disposiciones que le resulten aplicables en materia de prevención y control de riesgos de LC/FT/FPADM.

Artículo 109: Esta Superintendencia podrá establecer montos máximos diarios, semanales, mensuales o con cualquier otra periodicidad que se estime conveniente, para las operaciones de intercambio y transferencia de activos virtuales que se realicen a través de los servicios brindados por los Sujetos Obligados.

Asimismo, este Organismo podrá establecer límites máximos de frecuencia o periodicidad que estime convenientes, para las operaciones de intercambio y transferencia de criptoactivos que se realicen a través de los servicios brindados por los

Sujetos Obligados e igualmente podrá establecer límites máximos a la cantidad de activos virtuales que pueden estar depositados en cuentas y billeteras virtuales.

TÍTULO IX

RÉGIMEN SANCIONATORIO

Artículo 110: El incumplimiento de las obligaciones y normas establecidas por esta Providencia podrá ser sancionado conforme a la normativa vigente que resulte aplicable para el momento del incumplimiento o infracción.

TÍTULO X

DISPOSICIONES FINALES

Artículo 111: Esta Providencia entrará en vigencia a los noventa (90) días continuos contados a partir de la fecha de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Para revisar el contenido completo, pulse aquí o siga el siguiente vínculo: http://www.imprentanacional.gob.ve/

Se advierte que el vínculo anterior podría estar deshabilitado para el acceso fuera del Territorio de la República Bolivariana de Venezuela.

21 de abril de 2021