MANUAL

SISTEMA DE AUTOCONTROL Y GESTIÓN DEL RIESGO DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO - SAGRILAFT

CONFIDENCIAL

CÚCUTA - COLOMBIA

Contenido

1. INTRODUCCIÓN 4
2. OBJETIVO 4
3. ALCANCE 4
4. MARCO NORMATIVO LA/FT 4
4.1. NORMAS INTERNACIONALES 4
4.2. ORGANISMOS INTERNACIONALES Y NACIONALES QUE LUCHAN CONTRA LA/FT: 6
4.3. NORMAS NACIONALES 7
4.4. NORMATIVIDAD APLICABLE A LA EMPRESA: 9
5. MARCO CONCEPTUAL 10
6. CLASIFIACION DE LOS EVENTOS DE RIESGO OPERATIVO 16
7. POLÍTICA INTEGRAL DE GESTION DE RIESGOS 16
8. POLÍTICA PARA LA GESTION DEL RIESGO DE LA/FT 17
9. ESTRUCTURA ORGANIZACIONAL PARA LA GESTION DE RIESGOS LA/FT 20
9.1 JUNTA DE SOCIOS 21
9.3 REPRESENTANTE LEGAL 22
9.4 OFICIAL DE CUMPLIMIENTO 23
9.5 COMITÉ LA/FT 25
9.6 DEMAS COLABORADORES 26
10. CARACTERÍSTICAS DE LOS FACTORES DE RIESGO ASOCIADOS A LOS CRYPTOACTIVOS 27
11. PROCESO PARA LA ADMINISTRACIÓN Y GESTION DEL RIESGO DE LA/FT 28
10.1ESTABLECER EL CONTEXTO 29
11.2IDENTIFICACIÓN DEL RIESGO 30
11.3ANÁLISIS DEL RIESGO 30
11.4MATRIZ DE NIVEL DE RIESGO 31
11.5CRITERIOS DE MEDICIÓN 31
11.6NIVEL DE RIESGO 34

CONFIDENCIAL

11.7VALORACIÓN DEL RIESGO 35
11.8PLAN DE TRATAMIENTO 36
12. OBJETIVO COMERCIAL – CLIENTES 37
12.1NO PARAÍSO FISCAL 39
13. CONOCIMIENTO Y VINCULACIÓN (Debida Diligencia) 40
13.1ASOCIADOS, SOCIOS Y ACCIONISTAS: 40
13.2EMPLEADOS CON VINCULO LABORAL O CONTRACTUAL: 41
13.3PROVEEDORES Y CLIENTES: 41
Persona jurídica (Corporativo B2B). 42
Persona natural (Individual P2P). 43
13.4ESTUDIO DE CONFIABILIDAD: 46
13.5ACTUALIZACIÓN DE LA DOCUMENTACIÓN E INFORMACIÓN DE CLIENTES Y PROVEEDORES 49
13.6DEBIDA DILIGENCIA INTENSIFICADA: 49
14. IDENTIFICACIÓN Y ANALISIS DE OPERACIONES INUSUALES Y SOSPECHOSAS 50
14.1OPERACIONES INUSUALES: 50
14.2OPERACIONES SOSPECHOSAS: 51
15 MECANISMO DE DETECCIÓN Y SEÑALES DE ALERTA 52
15.1SEÑALES DE ALERTA: 52
15.2SEGUIMIENTO ELECTRÓNICO DE LAS OPERACIONES 54
16 REPORTE DE OPERACIÓN SOSPECHOSA (ROS) – UIAF 54
17 SANCIONES Y PENALIDADES 57

CONFIDENCIAL

1. INTRODUCCIÓN

En ACTIVOS DIGITALES S.A.S., somos conscientes que **El Lavado de Activos y la Financiación del Terrorismo** son flagelos de carácter mundial que atentan contra la integridad de los mercados de activos virtuales y del sistema financiero, al ser utilizados para el manejo de recursos ilícitos, poniendo en riesgo la continuidad de los negocios.

En razón de lo anterior la compañía ha implementado un Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo (SAGRILAFT) basado en las mejores prácticas de seguridad y autocontrol, y procedimientos que permiten identificar, medir, analizar, monitorear y controlar los eventos internos o externos que impidan el normal desarrollo de las operaciones, tendientes a prevenir el uso de la empresa, de sus asociados, de sus clientes, de sus asociados, de sus proveedores y/o de sus colaboradores como instrumentos para el Lavado de Activos y la Financiación del Terrorismo (LA/FT).

2. OBJETIVO

Establecer medidas, procedimientos y protocolos de “PREVENCIÓN y CONTROL” encaminados a evitar que la ACTIVOS DIGITALES S.A.S. sea utilizada por sus grupos de interés para dar imagen de legalidad a dineros provenientes de actividades ilícitas o que dichos recursos financien actividades terroristas.

3. ALCANCE

Este manual aplica para todos los procesos de la compañía a nivel nacional, que resulten vulnerables de LA/FT o que mayor nivel de exposición al riesgo por contagio tengan, comprendiendo todas las etapas de identificación, valoración y tratamiento de los riegos, de acuerdo al Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación Del Terrorismo (SAGRILAFT) implementado por la compañía.

4. MARCO NORMATIVO LA/FT

4.1. NORMAS INTERNACIONALES

Convención de la Organización de la Naciones Unidas (ONU): contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópica (Viena 1988): Promueve la cooperación entre los países miembros de la ONU a fin de que puedan hacer frente con mayor eficacia a los diversos aspectos del tráfico ilícito de estupefacientes y sustancias sicotrópicas que tengan una dimensión internacional.

CONFIDENCIAL

Comité de Basilea declaración de principios (1988): Estableció políticas y procedimientos de conocimiento del cliente para evitar que los Bancos y otras instituciones financieras pueden ser utilizadas sin saberlo como intermediarios para las transferencias o el depósito de fondos Originados en actividades Criminales.

40 Recomendaciones del GAFI: El Grupo de Acción Financiera Internacional (GAFI) es un ente intergubernamental establecido en 1989 por los Ministerios y sus jurisdicciones Miembro. El mandato del GAFI es fijar estándares y promover la implementación efectiva de medidas legales, regulatorias y operativas para combatir el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación y otras amenazas a la integridad del sistema financiero internacional.
En colaboración con otras partes involucradas a nivel internacional, el GAFI también trata de identificar vulnerabilidades a nivel nacional para proteger el sistema financiero internacional de usos indebidos.

El Grupo EGMONT: es la instancia que reúne a las Unidades de Inteligencia Financiera UIF del mundo. El 9 de junio de 1995, representantes de 24 países y 8 organizaciones internacionales se reunieron en el Palacio de EGMONT en Bélgica para discutir sobre las organizaciones especializadas en la lucha contra el lavado de dinero, conocidas en ese entonces, como “disclosures receiving agencies”, que correspondían a las actuales UIF.

El principal objetivo del grupo es facilitar el intercambio de información entre las UIF de los países miembro, con el fin de combatir los delitos de Lavado de Activos y Financiación del Terrorismo. Así mismo, el Grupo promueve la firma de acuerdos interinstitucionales, conocidos como Memorandos de Entendimiento, para facilitar el intercambio de información bilateral. A diciembre de 2007 la UIAF ha suscrito estos acuerdos con sus homólogas en 32 países.

Grupo de acción financiera de Sudamérica. GAFILAT: El Grupo de Acción Financiera de Latinoamérica (GAFILAT) es una organización intergubernamental de base regional que agrupa a 16 países de América del Sur, Centroamérica y América del Norte para combatir el lavado de activos y la financiación del terrorismo, a través del compromiso de mejora continua de las políticas nacionales contra estos delitos y la profundización en los distintos mecanismos de cooperación entre los países miembros.

Se creó formalmente el 8 de diciembre de 2000 en Cartagena de Indias, Colombia, mediante la firma del Memorando de Entendimiento constitutivo del grupo por los representantes de los gobiernos de nueve países: Argentina, Bolivia, Brasil, Chile, Colombia, Ecuador, Paraguay, Perú y Uruguay. Posteriormente se incorporaron como miembros plenos México (2006), Costa Rica, Panamá (2010), Cuba (2012), Guatemala, Honduras y Nicaragua (2013).

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional: En diciembre de 2000, al suscribir en Palermo (Italia) la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, la comunidad

CONFIDENCIAL

internacional demostró la voluntad política de abordar un problema mundial con una reacción mundial. Si la delincuencia atraviesa las fronteras, lo mismo ha de hacer la acción de la ley. Si el imperio de la ley se ve socavado no sólo en un país, sino en muchos países, quienes lo defienden no se pueden limitar a emplear únicamente medios y arbitrios nacionales.

El propósito de la presente Convención es promover la cooperación para prevenir y combatir más eficazmente la delincuencia organizada transnacional.

Ley USA PATRIOT: es una ley federal de Estados Unidos. Fue aprobada por una abrumadora mayoría tanto por la Cámara de Representantes como por el Senado estadounidense para después ser promulgada por el presidente de los Estados Unidos George W. Bush el 26 de octubre de 2001, después de los atentados del 11 de septiembre de 2001.

El objetivo de esta ley es ampliar la capacidad de control del Estado en aras de combatir el terrorismo, mejorando la capacidad de las distintas agencias de seguridad estadounidenses al coordinarlas y dotarlas de mayores poderes de vigilancia contra los delitos de terrorismo. Asimismo, la ley también promulgó nuevos delitos y endureció las penas por delitos de terrorismo.

4.2. ORGANISMOS INTERNACIONALES Y NACIONALES QUE LUCHAN CONTRA LA/FT:

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL GAFI: (G-7) -1989.

GAFI: Grupo de Acción Financiera Internacional sobre el blanqueo de capitales, establecido en 1989 por el G7, y en abril de 1990 dio a conocer sus Cuarenta Recomendaciones.

Grupo EGMONT: 1995 (Bélgica)

GAFISUD: Grupo de Acción Financiera de Sudamérica -2000.

GAFIC: El Grupo de Acción Financiera del Caribe, establecido como resultado de una serie de reuniones convocadas en Aruba en mayo de 1990 y en Jamaica en noviembre de 1992.

CTDE: Comité contra el Terrorismo – Resolución 1373 de 2001

UNODC: Oficina de Naciones Unidas contra la Droga y el Delito.

CICAD: Comisión Interamericana para el Control del Abuso de Drogas.

CCICLA: Comisión de Coordinación Interinstitucional Contra Lavado de Activos 1995

CONFIDENCIAL

UIAF: Unidad de Información y Análisis Financiero. Ley 526 de 1999
FISCALIA GENERAL DE LA NACIÓN: en 1991 con la promulgación de la nueva Constitución Política y empezó a operar el 1 de julio de 1992.

4.3. NORMAS NACIONALES

En Colombia se han desarrollado algunas leyes y/o normas nuevas para enfrentar los delitos de Lavado de Activos y la Financiación del Terrorismo que se pueden derivar del comercio de servicios de activos virtuales, articulando las entidades gubernamentales y estatales, con el sector financiero:

Estatuto orgánico del sistema Financiero (1993): Las instituciones sometidas al control y vigilancia de la Superintendencia Financiera o quien haga sus veces, estarán obligadas a adoptar medidas de control apropiadas y suficientes, orientadas a evitar que en la realización de sus operaciones puedan ser utilizadas como instrumento para el ocultamiento, manejo, inversión o aprovechamiento en cualquier forma de dinero u otros bienes provenientes de actividades delictivas o destinados a su financiación, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos vinculados con las mismas.

Esas instituciones deberán adoptar mecanismos y reglas de conducta que deberán observar sus representantes legales, directores, administradores y funcionarios, con los siguientes propósitos: Conocer adecuadamente la actividad económica que desarrollan sus clientes, establecer la frecuencia, volumen y características de las transacciones financieras de sus usuarios y reportar de forma inmediata y suficiente a la Unidad de Información y Análisis Financiero cualquier información relevante sobre manejo de activos o pasivos u otros recursos, cuya cuantía o características no guarden relación con la actividad económica de sus clientes.

Extinción de dominio en Colombia: es un mecanismo jurídico establecido por la Ley 1708 del 20 de enero de 2014, esta establece y permite el embargo de bienes privados que hayan sido utilizados o destinados para actividades ilícitas, para esto se debe llevar un debido proceso donde se analiza el afectado, la actividad ilícita de la cual se le esté implicando y el bien mueble o inmueble que entraría en embargo.

Estatuto Anticorrupción o la Ley 1474 de 2011: “Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”

Esta ley endurece las penas o las hace más gravosas de acuerdo a la Ley 793 de 2003, en lo que respecta a casos de corrupción de índole trasnacional, como son el “Lavado de Activos”, solicitando a las empresas del sector financiero y mercado de valores a reforzar los procedimientos y los controles que eviten que sus administradores se vean involucrados en investigaciones penales.

CONFIDENCIAL

Código Penal Colombiano – Ley 599 de 2000: Artículo 323. Lavado de activos. El que adquiera, resguarde, invierta, transporte, transforme, custodie o administre bienes que tengan su origen mediato o inmediato en actividades de extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, delitos contra el sistema financiero, la administración pública, o vinculados con el producto de los delitos objeto de un concierto para delinquir, relacionadas con el tráfico de drogas tóxicas, estupefacientes o sustancias sicotrópicas, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre tales bienes, o realice cualquier otro acto para ocultar o encubrir su origen ilícito incurrirá, por esa sola conducta, en prisión de seis (6) a quince (15) años y multa de quinientos (500) a cincuenta mil (50.000) salarios mínimos legales mensuales vigentes.

Ley 526 de 1999 – Creación de la UIAF: Por la cual se crea la Unidad de Información y Análisis Financiero. La Unidad tendrá como objetivo la prevención y detección de operaciones que puedan ser utilizadas como instrumento para el ocultamiento, manejo, inversión o aprovechamiento en cualquier forma de dinero u otros bienes provenientes de actividades delictivas o destinados a su financiación, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos vinculados con las mismas, prioritariamente el lavado de activos y la financiación del terrorismo.

Ley 970 de 2005 - Convención de las Naciones Unidas contra la Corrupción", adoptada por la Asamblea General de las Naciones Unidas: La finalidad de la presente Convención es: a) Promover y fortalecer las medidas para prevenir y combatir más eficaz y eficientemente la corrupción; b) Promover, facilitar y apoyar la cooperación internacional y la asistencia técnica en la prevención y la lucha contra la corrupción, incluida la recuperación de activos; c) Promover la integridad, la obligación de rendir cuentas y la debida gestión de los asuntos y los bienes públicos.

Ley 1121 de 2006: Por la cual se dictan normas para la prevención, detección, investigación y sanción de la financiación del terrorismo y otras disposiciones.

Las instituciones sometidas al control y vigilancia de la Superintendencia Financiera o quien haga sus veces, estarán obligadas a adoptar medidas de control apropiadas y suficientes, orientadas a evitar que en la realización de sus operaciones puedan ser utilizadas como instrumento para el ocultamiento, manejo, inversión o aprovechamiento en cualquier forma de dinero u otros bienes provenientes de actividades delictivas o destinados a su financiación, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos vinculados con las mismas.

Ley 1108 de 2006: Por medio de la cual se aprueba la “Convención Interamericana contra el Terrorismo”, suscrita en la ciudad de Bridgetown, Barbados, el tres (3) de junio de dos mil dos (2002), en el trigésimo segundo período ordinario de sesiones de la Asamblea General de la Organización de los Estados Americanos.

CONFIDENCIAL

Ley 1330 de 2009: Por el cual se adiciona la Ley 793 de 2002 y se establece el trámite abreviado y el beneficio por colaboración, teniendo por objeto la aplicación de mecanismos que permitan imprimir celeridad y proferir decisiones definitivas sobre los bienes sometidos al trámite de extinción del dominio.

Ley 1453 de 2011: Por medio del cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de la infancia y la adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad.

Decreto 3420 de 2004: Por el cual se modifica la composición y funciones de la Comisión de Coordinación Interinstitucional para el Control del Lavado de Activos y se dictan otras disposiciones. CCICLA, creada por el Decreto 950 de 1995.

Decreto 2669 de 2012: Por el cual se reglamenta la actividad de fáctoring que realizan las sociedades comerciales, se reglamenta el artículo 8 de la Ley 1231, se modifica el artículo 5 del Decreto de 2006 y se dictan otras disposiciones.

Resolución 114 de 2007: Por la cual se impone a las personas naturales, sociedades comerciales y empresas unipersonales dedicadas de manera profesional en el territorio nacional a la compraventa y/o compraventa mediante consignación de vehículos automotores nuevos y/o usados, la obligación de reportar de manera directa a la Unidad de Información y Análisis Financiero.

Circular Externa 100-004 de 2009 de la Superintendencia de Sociedades: Prevención del Riesgo de Lavado de Activos y Financiación del Terrorismo (LA/FT).

Decreto 1497 de 2002: En desarrollo del artículo 9º de la Ley 526 de 1999, la Unidad de Información y Análisis Financiero podrá solicitar a cualquier entidad pública, salvo la información reservada en poder de la Fiscalía General de la Nación, la información que considere necesaria para el cumplimiento de sus funciones.

Guía para la Debida Diligencia de la OCDE para empresas comercializadoras de minerales en Colombia 2019: La Guía de Debida Diligencia de la Organización de Cooperación y de Desarrollo Económico (OCDE) es reconocida como principal herramienta para la gestión responsable y transparente de las cadenas de suministro de los minerales, promoviendo compromiso empresarial sostenible dentro del sector minero.

4.4. NORMATIVIDAD APLICABLE A LA EMPRESA:

Resolución 314 de 2021: Por la cual se impone la obligación de reporte a la UIAF a las Empresas y Personas Naturales que provean servicios de activos virtuales en Colombia,

CONFIDENCIAL

adoptando lo establecido por el GAFI (Grupo de Acción Financiera Internacional) en la recomendación No. 15.

Capítulo X de la Circular Básica Jurídica de la Superintendencia de Sociedades: La Superintendencia de Sociedades, en cumplimiento de su política de supervisión por riesgos ha identificado que una de las contingencias a las que están expuestas las Empresas sujetas a su inspección, vigilancia y control, está en la probabilidad de incurrir en actividades de lavado de activos y de financiamiento del terrorismo (en adelante "LA/FT").

5. MARCO CONCEPTUAL

ACTIVOS VIRTUALES: Un activo virtual es una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar para pagos o inversiones. Los activos virtuales no incluyen representaciones digitales de monedas Fiat, valores y otros activos financieros que ya están cubiertos en otras partes de las Recomendaciones del GAFI.

PROVEEDOR DE SERVICIOS DE ACTIVOS VIRTUALES – PSAV: Significa cualquier persona física o jurídica que no esté cubierta en ningún otro lugar en virtud de las recomendaciones y que, como negocio, realiza una o más de las siguientes actividades u operaciones para o en nombre de otra persona física o jurídica:

1. Intercambio entre activos virtuales y monedas Fiat;
2. Intercambio entre una o más formas de activos virtuales;
3. Transferencia de activos virtuales;
4. Custodia y/o administración de activos virtuales o instrumentos que permitan el control sobre activos virtuales; y
5. Participación y provisión de servicios financieros relacionados con la oferta de un emisor y/o venta de un activo virtual.

CRYPTOACTIVO: El término "criptoactivo" mismo se refiere a un espectro amplio de productos digitales que se emiten de forma privada con tecnología similar (criptografía y, a menudo, registros distribuidos) y que se pueden almacenar y comercializar utilizando principalmente billeteras digitales y bolsas.

AMENAZA: La probabilidad de ocurrencia de un evento potencialmente desastroso, asociado a un evento físico de origen natural, socio - natural o provocado por los seres humanos (antrópica), durante cierto período de tiempo en un sitio dado.

ANALISIS DE RIESGOS: también conocido como evaluación de riesgos o PHA por sus siglas en inglés. Process Hazards Analysis, es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir.

CONFIDENCIAL

AUTOCONTROL: Es la voluntad del funcionario y los administradores para detectar, controlar y gestionar de manera eficiente y eficaz los riesgos a los que está expuesta la empresa.

ADMINISTRACION DE RIESGOS: es la disciplina que combina los recursos financieros, humanos, materiales y técnicos de una empresa, para identificar o evaluar los riesgos potenciales y decidir cómo manejarlos con la combinación óptima de costo – efectividad.

ACTIVIDAD ILICITA: Se trata de todo acto que, de alguna forma, rompe alguna regla o hace un daño de gran importancia a alguien. Lo contrario a ese término es lo lícito, palabra que hace referencia a la cualidad que tiene una persona u objeto por no esconder nada o no haber llevado a cabo un acto de dudosos fines.

ACTOS CRIMINALES: el acto criminal es definido como un acto voluntario que se realiza para herir o asesinar a alguien de alguna u otra forma, también es conocida como una conducta que es condenable.

BLANQUEO DE CAPITALES: también conocido como lavado de dinero o lavado de capitales) es el conjunto de mecanismos o procedimientos orientados a dar apariencia de legitimidad o legalidad a bienes o activos de origen delictivo.

CAPITALES ILICITOS: Bienes, riqueza y medios de producción que fueron adquiridos por medios o actividades contrarios a la ley.

CODIGO DE CONDUCTA: es el conjunto de reglas que establecen la manera y forma de comportamiento que se espera de los miembros de la empresa y cuáles son las conductas inadecuadas que no pueden ser permitidas, tomando en cuenta las metas y los objetivos estratégicos de la compañía.

CIIU: es la clasificación industrial internacional Uniforme elaborada y divulgada por la oficina de estadísticas de la Organización de las Naciones Unidas (ONU); con el objeto de satisfacer las necesidades de los que buscan datos económicos, clasificados conforme a categorías de las actividades económicas.

CONOCIMIENTO DEL CLIENTE: procedimiento para la Prevención, Seguridad y Control y la identificación plena, confiable, y la vinculación de forma Segura a la compañía a CLIENTES, y la verificación de la información suministrada por estos, los cuales deben ser aplicados con diligencia y responsabilidad, que permitan relaciones contractuales de confianza a largo plazo.

CONTROL DE RIESGO: Implementación de políticas, procedimientos y estándares para la gestión de los riesgos.

CONFIDENCIAL

DECLARACION DE OPERACIONES EN EFECTIVO: control que permite el registro de información para verificar la identidad del cliente y la naturaleza de las transacciones en efectivo realizadas y que superen los montos mínimos establecidos.

DECLARACION DE ORIGEN DE FONDOS: Información suministrada de manera voluntaria por el cliente, sobre el origen o la proveniencia de sus recursos.

DEBIDA DILIGENCIA (DUE DILIGENCE - KyC): Equivale a ejecutar algo con suficiente cuidado. Existen dos interpretaciones en la utilización de este concepto en la actividad empresarial. La primera se concibe como el actuar con el cuidado que sea necesario para reducir la posibilidad de llegar a ser considerado culpable por negligencia y de incurrir en las respectivas responsabilidades administrativas, civiles o penales. La segunda, de contenido más económico y más proactivo, se identifica como el conjunto de procesos necesarios para poder adoptar decisiones suficientemente informadas.

EVENTO: Evento es un término que hace referencia a un hecho dado inesperadamente y modifica las circunstancias que rodean al mismo.

EVALUACION DEL RIESGO: Proceso utilizado para medir los parámetros de la probabilidad de que un evento adverso ocurra (y la gravedad del mismo) sobre el ser humano o sobre el medio ambiente como consecuencia de la exposición a un agente causal.

ENRIQUECIMIENTO ILICITO: delito relacionado con el incremento patrimonial de un individuo sin la justificación del mismo, relacionándose con actividades punibles como el cohecho, el tráfico de influencias en el sector público y el narcotráfico, entre otros.

FUENTE DE RIESGO: elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo.

FINANCIACIÓN DEL TERRORISMO (FT): Es el proceso por medio del cual se obtienen los bienes, recursos o activos de procedencia ilícita o licita para realizar actividades terroristas. Delito descrito en el artículo 345 del Código Penal. Apoyo económico a las personas que fomentan actos terroristas, fondeo o inyección de capital.

FRECUENCIA: número de evento o resultados por unidad de tiempo definido.

FACTORES DE RIESGO: agente generador de riesgo de Lavado de Activos y financiación del terrorismo.

GESTION DE RIESGO: se define como el proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de los eventos o ataques, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse.

CONFIDENCIAL

GRUPO DE ACCIÓN FINANCIERA GAFI: Organismo intergubernamental establecido en 1989, cuyo mandato es fijar estándares y promover la implementación efectiva de medidas legales, regulatorias y operativas para combatir el lavado de activos, la financiación del terrorismo y la proliferación y otras amenazas a la integridad del sistema financiero.

IDENTIFICACION DE RIESGOS: proceso para reconocer si existe un peligro y definir su capacidad de impacto o daño.

LISTA OFAC: Office of Foreign Assets Control Agencia del Departamento del Tesoro de Los Estados Unidos de Norteamérica, conocida popularmente como “Lista Clinton”.

LAVADO DE ACTIVOS (LA): Son todas las acciones para dar apariencia de legalidad a recursos de origen ilícito con el fin de introducirlos en la economía a través del sector real o el sector financiero. En la mayoría de los países del mundo esta conducta es considerada delito y también se conoce como lavado de dinero, blanqueo de capitales, legitimación de capitales, entre otros. Delito que comete toda persona que busca dar apariencia de legalidad a bienes o dinero provenientes de alguna de las actividades descritas en el artículo 323 del Código Penal.

LISTAS RESTRICTIVAS (nacionales e internacionales): Relación de personas y empresas que de acuerdo con el organismo que las publica pueden estar vinculadas con actividades de lavado de activos o de financiación del terrorismo, como lo son las listas del Consejo de Seguridad de las Naciones Unidas, que son vinculantes para Colombia. Son listas de control que alertan sobre la presencia de un evento de riesgo relacionado con el registro de personas naturales o jurídicas que han sido vinculadas o condenadas por estar relacionadas con situaciones o procesos judiciales que tienen que ver con el lavado de activos o la financiación del terrorismo, o delitos conexos a los mencionados. Adicionalmente pueden ser consultadas las listas OFAC, INTERPOL, Policía Nacional, entre otras.

MATRIZ DE RIESGO: Herramienta para clasificar y visualizar el riesgo mediante la definición de rangos para la consecuencia y la probabilidad.

MANUAL ADMINISTRACION DEL RIESGO: Documento que establece las políticas, la estructura organizacional, las estrategias y los procesos y procedimientos aplicables en el desarrollo, implementación, seguimiento y control en el Sistema de Administración de riesgo.

MONITOREO: proceso mediante el cual se reúne, observa, estudia y emplea información para luego poder realizar un seguimiento de un programa o hecho particular.

OFICIAL DE CUMPLIMIENTO: funcionario del alto nivel de la empresa designado por el Represéntate Legal de la compañía que tiene como objetivo; verificar el oportuno y estricto cumplimiento de las normas legales establecidas para la prevención y detección de los riesgos asociados a los delitos de Lavado de Activos y/o La Financiación del Terrorismo.

CONFIDENCIAL

OPERACIONES DE BLANQUEO: Actividades fraudulentas que tienen como objetivo el ocultar el origen de recursos o dinero ilícito.

OPERACIÓN INTENTADA: Se configura cuando se tiene conocimiento de la intención de una persona natural o jurídica de realizar una operación sospechosa, pero ésta no se perfecciona por cuanto quien intenta llevarla a cabo desiste de la misma, o porque los controles establecidos o definidos no permitieron realizarla. Estas operaciones tienen que ser reportadas única y exclusivamente a la UIAF.

OPERACIÓN INUSUAL: es aquella operación que por su cuantía o características no guardan relación con la actividad económica del cliente, o que, por su número, por las cantidades transadas o por sus características particulares, se salen de los parámetros de normalidad establecidas por la entidad respectiva.

OPERACIÓN SOSPECHOSA: es toda operación realizada por una persona natural o jurídica, que por su número, cantidad o características no se enmarca dentro de los sistemas y practicas normales de los negocios de una industria o sector determinado y que de acuerdo con los usos y costumbres de la actividad que se trate, no haya podido ser razonablemente justificada.

PROBABILIDAD: Posibilidad de que ocurra un evento o resultado específico, medida por la relación entre los eventos o resultados específicos y el número total de eventos o resultados posibles.

PEPS: PERSONAS EXPUESTAS PÚBLICAMENTE: Personas nacionales o extranjeras que por su perfil o por las funciones que desempeñan pueden exponer en mayor grado a la empresa, al riesgo de LA/FT, tales como: personas que por razón de su cargo manejan recursos públicos, o tienen poder de disposición sobre éstos o gozan de reconocimiento público.

PITUFEO: consiste en utilizar muchas personas haciendo transferencias bancarias pequeñas a distintas cuentas bancarias de personas físicas o jurídicas. Al realizar las transferencias de cantidades mínimas de control bancario por la agencia tributaria del país implicado se hace difícil de seguir el rastro de estas transferencias y fácilmente se pierde la pista de todas las transacciones.

REPRESENTANTE LEGAL: es la facultad otorgada por la ley a una persona para obrar en nombre de otra, recayendo en ésta los efectos de tales actos. El ejercicio de esa representación puede ser obligatorio para el representante, dándole la potestad de celebrar o ejecutar contratos propios del negocio.

RIESGO DE LA/FT: Es el posible impacto negativo, la posibilidad de pérdida o daño que pueden sufrir la empresa, por su propensión a ser utilizadas directamente o a través de sus operaciones para la comisión de delitos por parte de sus asociados, usuarios o clientes, y

CONFIDENCIAL

como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades. También se derivan riesgos por el hecho de no efectuar los reportes correspondientes ante la UIAF.

RIESGOS ASOCIADOS AL LA/FT: Son los riesgos asociados a través de los cuales se materializa el riesgo de LA/FT: estos son: reputacional, legal, operativo y de contagio, que son los riesgos a los que se exponen las organizaciones, con el consecuente efecto económico negativo que ello puede representar para su estabilidad financiera.

RIESGO OPERATIVO: Es la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores.

RIESGO LEGAL: Es la posibilidad de pérdida en que incurre ACTIVOS DIGITALES S.A.S., de ser sancionada, multada u obligada a indemnizar daños como resultado de incumplimiento de normas o regulaciones y obligaciones contractuales. El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

RIESGO REPUTACIONAL: Es la posibilidad de pérdida en que incurre la empresa por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la compañía y sus prácticas de negocios, que puede causar pérdida de clientes, disminución de ingresos o procesos judiciales.

RIESGO INHERENTE: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

RIESGO RESIDUAL: Nivel resultante del riesgo después de aplicar los controles. Es el riesgo que queda, una vez se han instrumentado los controles pertinentes para su tratamiento. En todo caso exige un permanente monitoreo para observar su evolución.

SAGRILAFT: Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación Del Terrorismo, el cual se instrumenta a través de etapas y elementos interrelacionados de forma organizada y metódica.

SEÑALES DE ALERTA: Son circunstancias particulares relacionadas con el proceso de los actos propios advertidas al interior de la organización y que puede ameritar un reporte ante la UIAF. Son hechos, situaciones, eventos, cuantías y demás información que la empresa determine como relevantes, a partir de los cuales se puede inferir la posible existencia de un hecho o situación que escapa a lo que en el desarrollo de la prevención y control del riesgo de LA/FT, se ha determinado como normal.

CONFIDENCIAL

UNIDAD DE INFORMACIÓN Y ANÁLISIS FINANCIERO UIAF: Es una unidad Administrativa Especial, de carácter técnico, adscrita al Ministerio de Hacienda y Crédito Público, creada por la Ley 526 de 1999, modificada por la Ley 1121 de 2006, que tiene por objetivo la prevención y detección de operaciones que puedan ser utilizadas para el lavado de activos y la financiación del terrorismo. Así mismo, impone obligaciones de reporte de operaciones a determinados sectores económicos.

6. CLASIFIACION DE LOS EVENTOS DE RIESGO OPERATIVO

Evento: Presencia o cambio de un conjunto particular de circunstancias

Fraude Interno: Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la compañía o incumplir normas o leyes, en los que está implicado, al menos, un empleado o administrador de la compañía.

Fraude Externo: Actos realizados por una persona externa a la compañía, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.

Relaciones Laborales: Actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y, en general, la legislación vigente sobre la materia.

Clientes: Los Clientes son personas naturales o jurídicas con las que se establece y mantiene una relación de tipo legal o contractual para la prestación de un servicio o el suministro de cualquier producto propio de la actividad institucional.

Daños a Activos Físicos: Pérdidas derivadas de daños o perjuicios a activos físicos de la compañía.

Fallas Tecnológicas: Pérdidas derivadas de incidentes por fallas tecnológicas.

Ejecución y Administración de Procesos: Pérdidas derivadas de errores en la ejecución y administración de los procesos.

7. POLÍTICA INTEGRAL DE GESTION DE RIESGOS

Ante la importancia que tiene ACTIVOS DIGITALES S.A.S., en especializarse como fondo de inversión, mediante la comercialización de servicios de activos virtuales, a nivel internacional, mediante el uso de tecnologías vanguardista para el aseguramiento de los intangibles o fungibles y la debida diligencia para vincular o tener relaciones de tipo contractual y comercial con proveedores, clientes, asociados y colaboradores **CONFIABLES**, se ha implementado el Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo (SAGRILAFT) basado en las mejores prácticas de seguridad y autocontrol, y procedimientos que permiten identificar, medir,

CONFIDENCIAL

analizar, monitorear y controlar los eventos internos o externos que impidan el normal desarrollo de las operaciones, tendientes a prevenir el uso de la empresa, de sus asociados, de sus clientes, de sus proveedores y/o de sus colaboradores como instrumentos para el Lavado de Activos y la Financiación del Terrorismo (LA/FT).

8. POLÍTICA PARA LA GESTION DEL RIESGO DE LA/FT

Es deber de ACTIVOS DIGITALES S.A.S., sus órganos de administración, de gestión, de control, Oficial de Cumplimiento, colaboradores responsables en los procesos de contratación y demás colaboradores, aplicar de forma estricta la ejecución de las siguientes políticas:

8.1 ACTIVOS DIGITALES S.A.S., promulga y expone su compromiso institucional para cumplir con las disposiciones legales y reglamentarias que en materia de prevención y control del LA/FT han determinado o llegaren a determinar las autoridades y organismos de vigilancia y control pertinentes y las que por iniciativa propia se establezcan dentro de la compañía.

8.2 El marco conceptual, políticas, lineamientos y metodologías de la Gestión del Riesgo de LA/FT se encuentran dentro del Sistema de Autocontrol y Gestión del Riesgo de Lavado De Activos y Financiación del Terrorismo (SAGRILAFT) implementado por ACTIVOS DIGITALES S.A.S., entendido este como el conjunto de tareas sistemáticas para planear, hacer, verificar y actuar frente al riesgo.

8.3 Los administradores, representante legal, directivos y todos los colaboradores de ACTIVOS DIGITALES S.A.S., deben comprometerse a prevenir que la empresa sea utilizada como instrumento para el ocultamiento, manejo, inversión o aprovechamiento, en cualquier forma, de dinero u otros bienes provenientes de actividades ilícitas relacionadas con LA/FT.

8.4 Los administradores, representantes legales, directivos y todos los colaboradores deben comprometerse a prevenir que la empresa tenga vínculos con personas naturales y/o jurídicas relacionadas con actividades de LA/FT y a detectar y reportar las operaciones que se pretendan realizar o se hayan realizado, para intentar dar apariencia de legalidad a operaciones vinculadas a LA/FT.

8.5 Es deber del Representante Legal generar y respaldar el aprendizaje permanente de la compañía, mediante el conocimiento sistemático y actualizado de las mejores prácticas, en relación con la gestión de los riesgos en compañía del Oficial de Cumplimiento nombrado.

8.6 El Oficial de Cumplimiento deberá comunicar de manera oportuna los riesgos de la compañía y el estado de las acciones implementadas para su control a nivel

CONFIDENCIAL

estratégico de la organización, así como a la Junta de Socios, los entes reguladores y de control interno y externo.

8.7 El Oficial de Cumplimiento en conjunto con el Representante Legal de ACTIVOS DIGITALES S.A.S., son los responsables de asignar los roles y responsabilidades para la implementación y desarrollo del Sistema de Autocontrol y Gestión del Riesgo de Lavado De Activos y Financiación del Terrorismo (SAGRILAFT) en cada una de las áreas y a los colaboradores que considere pertinentes de acuerdo con su estructura organizacional.

8.8 El Representante legal está en la obligación de asignar los recursos humanos, financieros, técnicos, tecnológicos y logísticos que sean necesarios para la gestión del riesgo LA/FT. El Oficial de Cumplimiento deberá contar con las facultades y recursos necesarios para el adecuado ejercicio de sus funciones.

8.9 El proceso de Cumplimiento en cabeza de su Oficial de Cumplimiento es el encargado de ejecutar el análisis del riesgo LA/FT a los que está expuesta la compañía y de conformidad con este hacer una debida gestión en materia de prevención cumpliendo con la **DEBIDA DILIGENCIA** como lo exige la ley.

8.10 Todos los colaboradores de ACTIVOS DIGITALES S.A.S., están en la obligación de cumplir las políticas, procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento del Sistema de Autocontrol y Gestión del Riesgo de Lavado De Activos y Financiación del Terrorismo (SAGRILAFT), orientando sus acciones a la mitigación de los riesgos e identificación de operaciones inusuales, estando obligados a reportar al proceso de Cumplimiento acerca de cualquier situación u operación inusual o sospechosa de la cual tengan conocimiento directa o indirectamente. Para ello se ha destinado como medio formal el buzón de correo electrónico: cumplimientoactivosdigitales@gmail.com

8.11 Es deber del Representante Legal de la compañía, de sus socios y directivos velar por el mejoramiento continuo del sistema, con la finalidad de prevenir situaciones que impacten significativamente a la empresa.

8.12 ACTIVOS DIGITALES S.A.S., se abstendrá de realizar operaciones con Bancos comerciales o con entidades financieras no constituidas legalmente en Colombia y a nivel Internacional, que no tengan presencia física en algún país, de igual manera no tendrá relación comercial alguna con empresas ubicadas en países o jurisdicciones que adolecen de políticas adecuadas para controlar y prevenir el lavado de activos y la financiación del terrorismo.

8.13 Los colaboradores de ACTIVOS DIGITALES S.A.S., no suministraran información sobre aquellos clientes o proveedores que hayan efectuado o intenten efectuar operaciones sospechosas, es decir, se debe guardar total reserva de la información cuando se trate de reportes a la Unidad de Información y Análisis Financiero - UAIF.

CONFIDENCIAL

8.14 La organización no podrá realizar ninguna operación comercial o celebrar algún tipo de contrato si un potencial proveedor, cliente o alguno de sus accionistas mayoritarios, representantes legales o miembros de junta directiva u órgano equivalente o nuevo colaborador aparece registrado en las listas SDNT (Lista Clinton) o en la Lista de Terroristas emitida por la organización de Naciones Unidas (Lista ONU), la empresa deberá realizar las actividades necesarias para terminar la relación comercial y no podrá realizar ninguna nueva operación con él.

8.15 Los administradores, representantes legales y directivos deben comprometerse en crear y fortalecer una cultura organizacional orientada a anticipar y gestionar los riesgos de LA/FT de la organización y a crear en los empleados una cultura de autocontrol, mediante habilidades en la identificación y valoración de riesgos operativos, jurídicos y reputacionales a los cuales puede verse expuesta la organización y su recurso humano, por lo cual estos temas serán prioritarios en los procesos de formación del talento humano. Para ello, ACTIVOS DIGITALES S.A.S., destinará los recursos que considere pertinentes en formación y generación de campañas sobre la importancia y la naturaleza de la gestión del riesgo de LA/FT, difusión de políticas y prácticas deseables, controles internos y difusión de casos internos y externos.

8.16 Es deber del Oficial de Cumplimiento en coordinación con el área de Gestión Humana socializar y capacitar a todo el personal que ingrese a la compañía, sobre la importancia de las políticas contra el Lavado de Activos y Financiación del Terrorismo adoptadas por la compañía y su impacto.

8.17 El proceso de Cumplimiento evaluará los riesgos de LA/FT asociados a la definición de nuevos productos, el ingreso de nuevos clientes, asociados y accionistas y la incursión a nuevos mercados, para ello utilizará la metodología de la que habla este manual y demás mecanismos para identificar, valorar y monitorizar los riesgos.

8.18 Bajo ninguna circunstancia, la compañía podrá iniciar operaciones o celebrar algún tipo de contrato con algún proveedor, cliente, asociado o colaborador sin que el proceso de Cumplimiento haya realizado la verificación en las respectivas listas restrictivas.

8.19 El proceso de Cumplimiento periódicamente realizará un monitoreo en medios de comunicación e internet para identificar nuevas políticas, modalidades, tipologías, vulnerabilidades, riesgos y grupos delictivos.

8.20 El proceso de Cumplimiento semestralmente deberá realizar la efectividad de los controles implementados en la mitigación de los riesgos de LA/FT por cada proceso, con el fin de realizar los ajustes necesarios o incorporar nuevos controles, que permitan llevar los riesgos a niveles de exposición ACEPTABLES.

CONFIDENCIAL

8.21 Es deber del Oficial de Cumplimiento presentar a la Junta de Socios por lo menos una vez cada semestre, el informe relacionado con la administración y gestión de los riesgos de LA/FT.

8.22 Es deber del Oficial de Cumplimiento garantizar el reporte oportuno de las operaciones comerciales que sean llevadas a cabo por ACTIVOS DIGITALES S.A.S., ante la UIAF de acuerdo a los plazos y tiempos establecidos por esta entidad, de igual manera todas las operaciones que resulten sospechosas e inusuales, de acuerdo a los siguientes tipos de reportes:

a) Reporte de operaciones sospechosas – ROS: se debe enviar a la UIAF de forma inmediata, cuando se tenga conocimiento de una operación que genere sospecha para la entidad.

b) Reporte de ausencia de operaciones sospechosas: el envío del reporte a la UIAF debe realizarse mensualmente.

c) Reporte de PSAV Clientes Res 314 – mensualmente.

d) Reporte de PSAV Transacciones Res 314 – mensualmente.

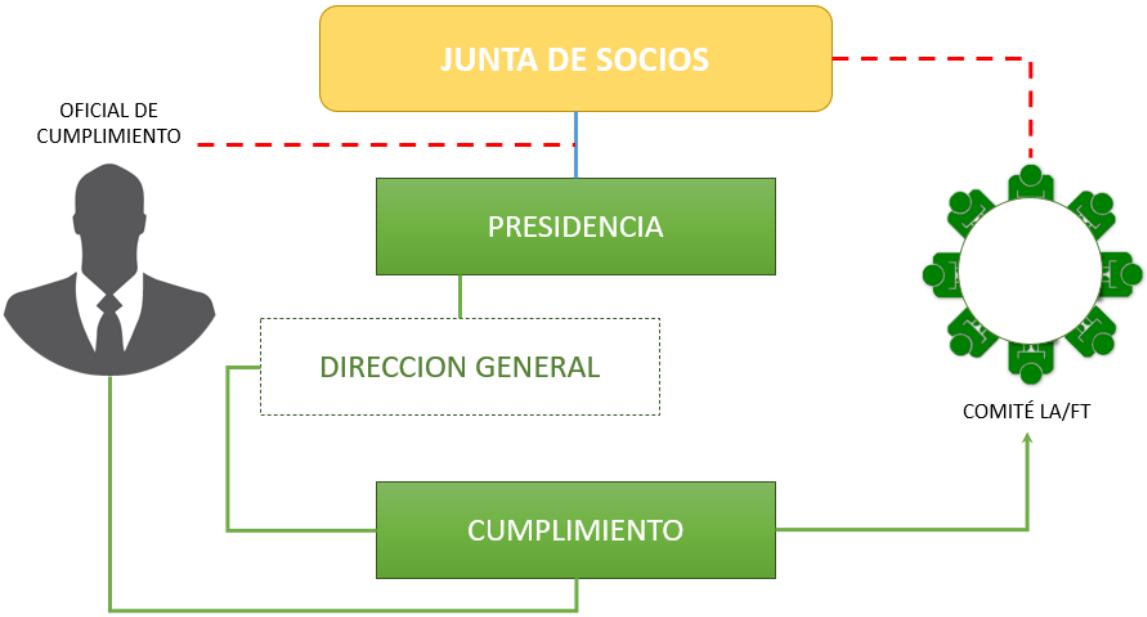
e) Reporte de ausencia de transacciones de PSAV: el envío del reporte a la UIAF se realiza mensualmente.

9. ESTRUCTURA ORGANIZACIONAL PARA LA GESTION DE RIESGOS LA/FT

En ACTIVOS DIGITALES S.A.S., somos conscientes de la necesidad de contar con responsabilidades claras e individuales en cada proceso y para cada colaborador en lo que respecta a las Políticas definidas en este manual, por esta razón Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo (SAGRILAFT) cuenta con el apoyo de una estructura organizacional del nivel estratégico, quienes determinan las siguientes funciones, adicionales a las propias de cada cargo, de acuerdo al manual de funciones:

CONFIDENCIAL

ESTRUCTURA ORGANIZACIONAL PARA LA GESTION DE RIESGOS LA/FT



9.1 JUNTA DE SOCIOS

La Junta de Socios de ACTIVOS DIGITALES S.A.S., como máximo órgano rector en materia de Gestión del Riesgo LA/FT, se compromete a asumir las siguientes Políticas:

- Aprobar mediante acta de la Asamblea General de Socios el Sistema de Administración de Riesgos LA/FT que implementará la compañía.
- Fijar las políticas, definir los mecanismos e instrumentos que se aplicarán en relación con la gestión de riesgo del LA/FT.
- Pronunciarse respecto de cada uno de los informes presentados por el Oficial de Cumplimiento y/o Representante Legal, de acuerdo a la gestión y la Administración de los riesgos LA/FT, contenidos en este manual.
- Destinar los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente el Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo (SAGRILAFT).

- Designar el Oficial de Cumplimiento para liderar el Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo (SAGRILAFT).

- Aprobar los procedimientos para el conocimiento y vinculación de forma segura para Clientes, proveedores y colaboradores.

- Aprobar el Manual para la Gestión de los Riesgos de LA/FT y sus actualizaciones.

- La Junta de Socios en conjunto con el Representante Legal deben efectuar seguimientos permanentes a los riesgos LA/FT identificados en la compañía y determinar el direccionamiento estratégico y los niveles de riesgo que están dispuestos a asumir.

- La Junta de Socios establece que el mismo director de Cumplimiento será el mismo Oficial de Cumplimiento, quien asumirá todas las funciones relacionadas con la Gestión y Administración de los Riesgos de LA/FT.

9.2 REVISORÍA FISCAL

La Revisoría Fiscal deberá establecer unos controles que le permitan evaluar el cumplimiento de las instrucciones contenidas el **Capítulo X de la Circular Básica Jurídica de la Superintendencia de Sociedades y la Resolución No. 363 de noviembre de 2008 de la UIAF**, o cualquier otra norma que la modifique, complemente o sustituya; e informar al Representante Legal, el Oficial de Cumplimiento y la Junta Directiva cuando considere necesario el resultado de su evaluación del cumplimiento de las normas e instrucciones sobre esta materia.

9.3 REPRESENTANTE LEGAL

El Representante Legal de ACTIVOS DIGITALES S.A.S., en concordancia con las otras funciones propias de su cargo, contenidas en su portafolio de gestión, deberá cumplir a cabalidad con las siguientes funciones adicionales:

- Diseñar y someter a aprobación de la Junta de Socios el Manual del Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo (SAGRILAFT). y sus actualizaciones.

- Velar por el cumplimiento efectivo de las Políticas establecidas en este manual, para la Administración y gestión de los riesgos de LA/FT.

- Asegurar que cada una de las etapas del Sistema de administración de riesgos de LA/FT se cumplan de cara a la normatividad vigente que regulan esta materia.

CONFIDENCIAL

- Velar por que se implementen los procedimientos adecuados para la administración de riesgos de LA/FT, que permitan evitar de manera oportuna que la Empresa o alguna de sus partes interesadas sean utilizados como herramientas para legitimar dinero proveniente de actividades ilícitas.

- Garantizar los recursos técnicos, físicos, humanos y tecnológicos para implementar y mantener en funcionamiento el Sistema de Administración de Riesgo para la prevención y control del lavado de activos y financiación del terrorismo – SAGRILAFT.

- Aprobar los criterios, metodologías y procedimientos para el conocimiento y vinculación de forma segura de Proveedores, Clientes y Colaboradores.

- Adoptar las decisiones a que haya lugar, previa validación o autorización otorgada por la Junta de Socios en cuanto a la exclusión de clientes, proveedores y colaboradores según el caso, y en cuanto a la terminación unilateral de relaciones comerciales o contractuales con personas relacionadas con el LA/FT, de conformidad con los informes presentados por el Oficial de cumplimiento.

9.4 OFICIAL DE CUMPLIMIENTO

ACTIVOS DIGITALES S.A.S., deberá asignar la función de Administrador de Riesgos a un funcionario que tenga y acredite conocimientos en Gestión de Riesgos, esta persona deberá demostrar que ha tenido capacitación específica en prevención y control de lavado de activos y la Financiación del Terrorismo.

El Oficial de Cumplimiento tendrá las siguientes responsabilidades:

- Verificar el oportuno y estricto cumplimiento de las normas legales establecidas para la prevención y detección del Lavado de Activos y la Financiación del Terrorismo.

- Implementar y desarrollar los procedimientos generales y específicos que considere adecuados para hacer más efectiva la prevención y detección de estas conductas.

- Velar por el adecuado funcionamiento de la totalidad de los mecanismos e instrumentos específicos diseñados dentro del Sistema de administración de riesgos – SAGRILAFT.

- Realizar los estudios necesarios para determinar si una operación inusual reviste el carácter de sospechosa;

- Reportar en forma inmediata y suficiente a la Unidad de Información y Análisis Financiero (UIAF), las operaciones sospechosas realizadas u operaciones

CONFIDENCIAL

intentadas y rechazadas que tengan características que les otorguen el carácter de sospechosas, en el momento en que sean detectadas, así como la ausencia de las mismas de acuerdo a la normatividad vigente en esta materia.

- Informar a la Junta de Socios sobre las posibles fallas u omisiones en los controles para la prevención de Lavado de Activos y Financiación, que comprometan la responsabilidad de los funcionarios y de la Empresa.

- Presentar trimestralmente a la Junta de Socios, informes detallados acerca del cumplimiento de las labores a su cargo, en los cuales deben referirse como mínimo a los siguientes aspectos:

    1. Las políticas y programas desarrollados para cumplir su función y los resultados de la gestión realizada;

    2. Los resultados de la retroalimentación dada por la UIAF sobre el cumplimiento de las normas de prevención de Lavado de Activos.

    3. Uso de los documentos publicados por las autoridades de inspección, control o vigilancia, en especial por la UIAF, en materia de prevención de Lavado de Activos.

    4. El cumplimiento que se ha dado en relación con el envío de los reportes a las diferentes autoridades, en particular respecto a la oportunidad y calidad de la información.

    5. Las políticas y programas adoptados para la actualización de la información de los clientes y el avance que se haya logrado sobre el tema en cada uno de los productos y servicios ofrecidos por la Empresa.

    6. La efectividad de los mecanismos e instrumentos de control y las medidas adoptadas para corregir las fallas.

    7. Las tendencias que se observen en las operaciones reportadas como sospechosas y las medidas adoptadas para la administración del riesgo asociado a estas.

    8. Los casos específicos de incumplimiento por parte de los colaboradores de ACTIVOS DIGITALES S.A.S., así como los resultados de las órdenes impartidas por la Junta de Socios.

    9. Los correctivos que considere necesarios, incluidas las propuestas de actualización o mejora de los mecanismos e instrumentos de protección.

CONFIDENCIAL

- Diseñar y coordinar los planes de capacitación necesarios, para que los diferentes funcionarios de la Empresa estén debidamente informados y actualizados en la gestión del riesgo de Lavado de Activos. El diseño y coordinación de los planes de capacitación sobre el tema de prevención y detección como mínimo una vez al año.

- Atender y coordinar cualquier requerimiento, solicitud o diligencia de autoridad judicial o administrativa en materia de prevención y detección de Lavado de Activos y la Financiación del Terrorismo.

- Colaborar con el Representante Legal en el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para la oportuna detección de las operaciones inusuales.

- Evaluar los informes presentados por la Auditoria Interna o quien ejecute sus funciones similares o haga sus veces, y los informes que presente el Revisor Fiscal y adoptar las medidas del caso frente a las deficiencias informadas.

- Diseñar las metodologías de segmentación, identificación, medición y control del SAGRILAFT.

- Elaborar y someter a la aprobación de la Junta de Socios, los criterios objetivos para la determinación de las operaciones sospechosas, así como aquellos para determinar cuáles de las operaciones efectuadas por usuarios serán objeto de consolidación, monitoreo y análisis de inusualidad.

9.5 COMITÉ LA/FT

Este comité deberá sesionar de manera BIMESTRAL y sus actividades deberán llevarse a cabo en la Dirección General de la empresa. Harán parte de este comité los siguientes funcionarios:

- El presidente y/o el Representante Legal
- El director de Riesgos
- El Oficial de Cumplimiento
- El Asesor Jurídico
- El Líder de Proceso - según requerimiento

El objetivo de este comité consiste en evaluar los casos y/o riesgos materializados que por su impacto pueden poner en riesgo la seguridad de las operaciones o en el peor de los casos, la continuidad del negocio, de igual manera el comité deberá determinar mediante la metodología de voto individual las cancelaciones unilaterales de contratos y acuerdos comerciales con proveedores, clientes y/o colaboradores que resultasen inmersos en actividades del Lavado de Activos y la Financiación del Terrorismo.

CONFIDENCIAL

Adicional a lo anterior, deberán evaluar las respuestas emitidas por los Representantes Legales de proveedores, clientes y/o colaboradores, previamente solicitados por el Oficial de Cumplimiento, de los que se hayan identificado reportes negativos en las respectivas listas.

Las actividades o funciones de este comité son:

- Revisar los informes de Auditoria, con el fin de identificar malas prácticas por parte de los clientes, proveedores y colaboradores, que pongan en riesgo la seguridad de las operaciones, y en ese mismo sentido generar las medidas a que haya lugar.

- Evaluar y valorar los informes presentados por el Oficial de Cumplimiento sobre las operaciones inusuales, sospechosas e intentadas durante el periodo comprendido.

- Validar las operaciones inusuales detectadas por los colaboradores con el fin de determinar si estas constituyen una operación sospechosa, y en ese mismo sentido reportar a la UIAF o no.

- Analizar los casos de incumplimiento por parte de colaboradores a la Política de gestión de riesgos y así mismo determinar las sanciones a que haya lugar.

9.6 DEMAS COLABORADORES

En ACTIVOS DIGITALES S.A.S., consideramos el factor humano, como una de las herramientas más vulnerables que tienen las empresas para ser utilizada por los delincuentes que buscan dar apariencia de legalidad a dineros provenientes del narcotráfico, por esta razón la cultura de gestión del riesgo de LA/FT, deberá hacer parte integral de los procesos de formación y capacitación de cada uno de nuestros colaboradores.

Los colaboradores tendrán las siguientes responsabilidades:

- Conocer los riesgos y cumplir las políticas y procedimientos de LA/FT que son inherentes a sus actividades y ser responsables por adelantar una eficiente gestión, control y reporte interno de los mismos, lo cual debe formar parte de la evaluación de desempeño de cada colaborador.

- Participar activamente en las capacitaciones y cursos obligatorios u opcionales que sobre la gestión de riesgos de LA/FT sean puestos a disposición de los colaboradores.

- Evitar y en todo caso reportar todo conflicto de interés, propio o de terceros, que pueda presentarse en cuanto a su responsabilidad frente a la gestión de los riesgos de LA/FT.

CONFIDENCIAL

10. CARACTERÍSTICAS DE LOS FACTORES DE RIESGO ASOCIADOS A LOS CRYPTOACTIVOS

El Grupo de Acción Financiera Internacional (GAFI) ha identificado tres métodos principales a través de cuales las organizaciones criminales lavan activos:

1. Uso del sistema financiero
2. El movimiento físico de dinero
3. El movimiento físico de mercancías a través del comercio
4. ¿Uso de nuevos métodos de pago y criptos?

Sin embargo, existen mitos respecto a los criptoactivos o activos digitales:

¡Bitcoin no es anónimo!
▪ Todas las transacciones son públicas y visibles en el blockchain
▪ Mejor dicho, es seudónimo, como email
▪ Cualquiera clave pública puede ser localizada hasta el propietario original
▪ La persona que compró dos pizzas el 22 de mayo 2010, con la clave pública "1XPTgDRhN8RFnzniWCddobD9iKZatrvH4" es la misma persona que envió 1,300 bitcoins a "1DvSvCnRsHdrA76PnD1j58wAeUFnhTaux" el noviembre 15 2010

Sin embargo, este cambio por más que obedezca a un avance tecnológico supone un riesgo de lavado de activos ya que el Blockchain, o cadena de bloques en su traducción; es un sistema de codificación que permite transacciones digitales bajo el anonimato de los usuarios que operan a través de él, dando pie a la verdadera revolución del dinero.

De acuerdo con la definición del Banco Central Europeo, las monedas virtuales son "la representación digital de valor no emitida por un banco central ni por una autoridad pública, ni necesariamente asociada a una moneda fiduciaria, pero aceptada por personas físicas o jurídicas como medio de pago y que puede transferirse, almacenarse o negociarse por medios electrónicos."

Dentro de estas monedas se encuentra el Bitcoin (la primera moneda virtual conocida en 2009), que dio inicio a la creación de muchas otras como el Bitcoin Cash, Litecoin, Decoin, Ripple, entre otras; creándose más de mil monedas virtuales a hoy; las cuales son llamadas también Criptomonedas.

Estas operan bajo la tecnología Blockchain, cuya estructura como bien se indicó, es una cadena de bloques, que contiene una información, un número de identificación único del bloque, y número del bloque anterior, por lo que quedan conectados los bloques de información entre sí, formando una cadena. Los números de identificación se generan según el contenido de los bloques, por tanto, no pueden ser modificados.

CONFIDENCIAL

Dicha cadena de bloques se encuentra “vigilada” por todos los usuarios que se encuentran en la red, y al detectarse la modificación de algún dato, ésta se rompería. La base de datos donde se encuentran grabadas las operaciones es generada por una red de usuarios especiales llamados “mineros”, encargados de resolver difíciles algoritmos para validar las transacciones, guardando y generando nuevos bloques, hasta que finalmente llega la información al usuario que deberá ser entregada. Estos mineros cobran una llamada “comisión” de un porcentaje por dicha labor.

Bajo este modelo de operación, el riesgo de lavado de activos crece porque al operar bajo el anonimato y estar autorreguladas por los mismos usuarios de la red, no es posible identificar los beneficiarios finales de dichas transacciones, el origen lícito de los recursos, identificar las jurisdicciones de los remitentes y destinatarios, ni detectar operaciones de montos inusuales.

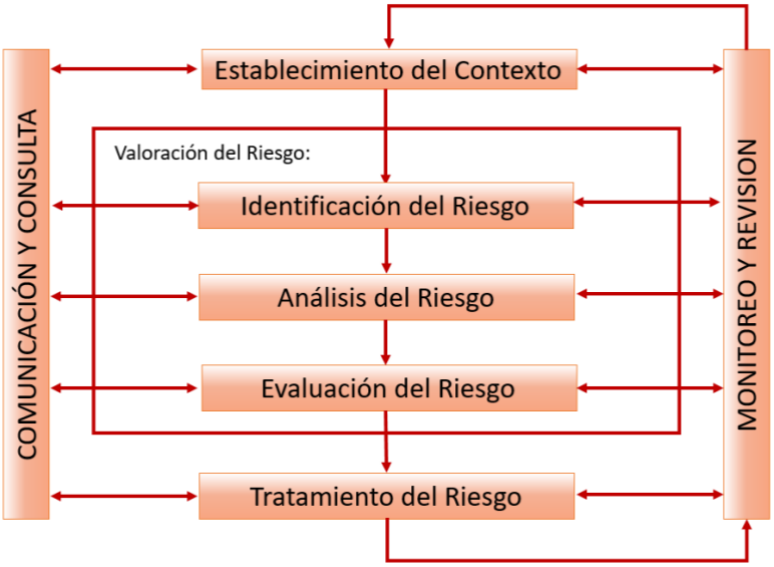
En definitiva, no es posible realizar una debida diligencia sobre los usuarios, lo cual representa la existencia de una mayor posibilidad en la materialización del riesgo de lavado de activos y financiación al terrorismo.

Sin embargo, en ACTIVOS DIGITALES SAS cuenta con un Sistema de Autocontrol y Gestión del Riesgo de Lavado de Activos y Financiación del Terrorismo (SAGRILAFT), aplicado y en marcha que propende por solo ejecutar relaciones de intercambio comercial con activos virtuales con terceros que sean visibles y puedan ejecutar de manera libre y espontanea actividades de debida diligencia (KyC).

11. PROCESO PARA LA ADMINISTRACIÓN Y GESTION DEL RIESGO DE LA/FT

El Sistema de Administración de Riesgo de Lavado de Activos y la Financiación del Terrorismo de la Empresa (SAGRILAFT) toma como marco de referencia la Norma NTC ISO 31000:2009, Gestión del Riesgo (antes NTC 5254:2004) y las 40 recomendaciones del Grupo de Acción Financiera Internacional sobre el blanqueo de Capitales (GAFI), estableciendo etapas o pasos sistemáticos e interrelacionados a través de los cuales ACTIVOS DIGITALES S.A.S., administra el riesgo de LA/FT, alineándose al modelo general de la gestión del Riesgo.

CONFIDENCIAL



10.1 ESTABLECER EL CONTEXTO

Define la relación entre la Empresa y su entorno, identificando las fortalezas, debilidades, oportunidades y amenazas de la compañía que pueden generar riesgos, afectando el cumplimiento de los objetivos de la Empresa.

Este contexto involucra todos los aspectos; financieros, operativos, legales, reputacionales, y de las demás funciones de la compañía, identificando el mercado objetivo de la Empresa, sus competidores, proveedores y clientes, clasificándolos como partes interesadas primordiales para el desarrollo normal de los negocios.

Las partes interesadas pueden ser aquellas personas que están, o perciben estar afectados por una decisión o actividad:

- Los Accionistas
- Los Gerentes
- Los colaboradores con vínculo contractual
- Las Empresas o canales en los que se apoya la empresa
- Los Proveedores de bienes y servicios
- Comerciales o contrapartes del negocio
- Entidades reguladoras y Organizaciones gubernamentales

CONFIDENCIAL

11.2 IDENTIFICACIÓN DEL RIESGO

En esta etapa se identifican y se enlistan las fuentes de riesgos y los eventos que pueden tener impacto en el logro de cada uno de los objetivos estratégicos trazados por la Empresa. Estos eventos pueden retrasar el logro de estos objetivos.

La identificación debe incluir todos los aspectos de los riesgos, estén o no bajo el control de la Empresa., sin embargo, tendrán prelación los procesos y subprocesos de la compañía que sean vulnerables a los riesgos LA/FT.

Una vez identificado lo que pueda suceder e identificados los riesgos, se debe hacer un análisis de estos, deben separarse los menores o aceptables, de los más riesgosos y por supuesto dar información para que ayude en la evaluación y tratamiento de estos.

Evento o incidente: circunstancia que ha ocasionado o podría haber ocasionado un impacto.

Impacto (¿Cuál y Cuanto daño nos puede causar?): Las derivaciones que puede ocasionar a la Empresa la materialización del riesgo.

Causa: (Que y porque): Serie de situaciones o características de originan la aparición de un peligro o un evento.; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos, fallecimiento, sanciones, pérdidas de herramientas técnicas.

Factores de Riesgo (internos o externos): Porque puede suceder? Son los medios, las circunstancias y agentes generadores de riesgo, aquí se incluye el análisis de las vulnerabilidades.

Herramientas Técnicas: Para identificar los riesgos ACTIVOS DIGITALES S.A.S., implementa listas de verificación, juicios basados en la experiencia y los registros. El enfoque utilizado dependerá de la naturaleza de las actividades que se revisa, los tipos de riesgos, el contexto organizacional y el propósito del estudio de gestión de Riesgo.

11.3 ANÁLISIS DEL RIESGO

Con el fin de determinar si los riesgos identificados requieren de algún tipo de control o tratamiento, se debe considerar los eventos de Riesgo LA/FT combinando los conceptos de PROBABILIDAD e IMPACTO. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: No. de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

CONFIDENCIAL

Al no disponer de datos históricos de probabilidad e impacto confiables de los riesgos identificados, la valoración o medición de estos riesgos se hará de manera subjetiva a cargo de las personas responsables en la Gestión de Riesgos, sin embargo, para evitar estos juicios de carácter subjetivo, se debe tomar información de fuentes y técnicas relacionadas; entre ellas se destacan los conceptos de expertos, la literatura asociada al LA/FT y los registros anteriores.

Una vez identificados los riesgos, se debe realizar una socialización sobre los resultados con el líder del proceso y sus colaboradores, que permita determinar si los riesgos efectivamente corresponden a su proceso.

11.4 MATRIZ DE NIVEL DE RIESGO

Para poder valorar los riesgos, se debe partir de un análisis cualitativo que presenta en forma descriptiva la magnitud de las consecuencias y un análisis cuantitativo que contempla valores numéricos que contribuyen a la calidad en la exactitud de la calificación y evaluación de los riesgos.

Para adelantar el análisis del riesgo se deben considerar los siguientes aspectos en la matriz de Nivel de Riesgo:

IMPACTO	5 Catastrófico	5	10	15	20	25
	4 Severo	4	8	12	16	20
	3 Moderado	3	6	9	12	15
	2 Menor	2	4	6	8	10
	1 Insignificante	1	2	3	4	5
		1 Altamente Improbable	2 Improbable	3 Posible	4 Probable	5 Frecuente
		PROBABILIDAD				

11.5 CRITERIOS DE MEDICIÓN

Los impactos y probabilidades se combinan para producir un nivel de riesgo.

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.

CONFIDENCIAL

Se debe calificar cada uno de los Riesgos según la matriz de acuerdo a las siguientes especificaciones:

Tabla de Probabilidades:

CRITERIOS MEDICIÓN PROBABILIDAD			
RANGO PROBABILIDAD	**POSIBILIDAD**	**PROBABILIDAD MATEMÁTICA**	**VALOR**
Casi cierto	Ocurra la mayoría de veces	> 90%	**5**
Muy probable	Posiblemente ocurra varias veces	60,1% - 90%	**4**
Probable	Alguna posibilidad que el evento ocurra	40,1% - 60%	**3**
Improbable	Insignificante posibilidad que el evento ocurra	10,1% - 40%	**2**
Rara Vez	Puede ocurrir en circunstancias excepcionales	< 10%	**1**

Tabla de Consecuencias o Impacto:

CRITERIOS MEDICIÓN CONSECUENCIA/IMPACTO		
CATEGORÍA	**DESCRIPCIÓN**	**VALOR**
Catastrófico	Perdida de la vida, Enorme pérdida financiera, Cierre de la Organización.	**5**
Mayor	Sanciones de tipo legal, Perjuicios extensivos, Perdida de capacidad de producción, Perdida financiera mayor, Cancelación de licencias de funcionamiento, NO Renovación de certificaciones de calidad, Daño reputacional con retiro de clientes, Demandas.	**4**
Medio	Requiere atención por parte de la Organización, Perdida financiera alta, se deben generar planes de acción o mejora, pérdida de ingresos.	**3**
Menor	Tratamiento de primeros auxilios, no revisten gravedad, se debe realizar seguimiento para que el riesgo este controlado, perdida financiera media.	**2**
Insignificante	Sin perjuicios, baja pérdida financiera.	**1**

Lista de ponderación de Impactos:

NIVEL	CLASIFICACIÓN	TIPO DE IMPACTO				
		ECONÓMICO*	X PROCESO	LEGAL	REPUTACIONAL	X CONTAGIO*
1	**Insignificante**	0,1% - 1%	Reproceso de 1 a 2 horas	No conformidades u observaciones de Auditoría Interna	Al interior de la Empresa	Cuando alguno de los funcionarios del nivel de acción o de mandos medios de la Empresa, que se vea involucrado en actividades relacionadas con LA/FT, o que hayan sido reportados en alguna Lista restrictiva.
2	**Menor**	1,00001% - 2%	Reproceso de 3 a 4 horas	Llamados de atención de Revisoría Fiscal y/o Auditorías externas	A nivel del Gremio	Cuando alguno de los funcionarios del nivel de táctico o de jefaturas de la Empresa, que se vea involucrado en actividades relacionadas con LA/FT, o que hayan sido reportados en alguna Lista restrictiva.
3	**Moderado**	2,00001% - 3%	Reproceso de 5 a 8 horas	Llamados de atención o amonestaciones por parte de entidades de Control	A nivel de las Entidades de Control	Cuando alguno de los funcionarios del nivel de Gerencial, Aliados y Proveedores Estratégicos de la Empresa, que se vea involucrado en actividades relacionadas con LA/FT, o que hayan sido reportados en alguna Lista restrictiva.
4	**Severo**	3,00001% - 4%	Reproceso de 9 a 16 horas	Sanciones y/o Multas por parte de entidades de Control	A nivel del Cliente	Cuando algún integrante de La Junta Directiva, Representante Legal, Revisor Fiscal y Oficial de Cumplimiento de la Empresa, que se vea involucrado en actividades relacionadas con LA/FT, o que hayan sido reportados en alguna Lista restrictiva.
5	**Catastrófico**	4,00001% - 5%	Reproceso superior a 17 horas	Intervención de Entidades de Control	A nivel de los Medios de Comunicación	Cuando algún socio o Accionista de la Empresa, que se vea involucrado en actividades relacionadas con LA/FT, o que hayan sido reportados en alguna Lista restrictiva.

CONFIDENCIAL

***** El impacto económico se calcula de multiplicar el porcentaje por el monto movilizado mes de la Empresa.

***** El impacto por Contagio solo aplica para los casos de LA/FT

11.6 NIVEL DE RIESGO

La Evaluación del Riesgo: Compara los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la compañía al riesgo. Para realizar la Evaluación del Riesgo se debe tener en cuenta la posición del riesgo en la siguiente Matriz, teniendo en cuenta que la Junta de Socios ha determinado dar un grado de **ACEPTACIÓN** a todos los riesgos por debajo del nivel de 5 en la Matriz del Riesgo, claro está, después de aplicados los controles sobre los riesgos inherentes, quedando el riesgo residual.

NIVEL DE EXPOSICIÓN		
Categ.	**N. Riesgos**	
Extremo (13 - 25)	Se requiere acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la Alta Dirección o Junta de Socios	**Inaceptable**
Alto (6 - 12)	Requiere atención de la gerencia del o los procesos involucrados. Planes de tratamiento requeridos, implementados y reportados a la Alta Gerencia.	
Moderado (3 - 5)	La responsabilidad gerencial debe ser especificada. Administrado con procedimientos normales de control.	**Aceptable**
Bajo (2)	Se administra con procedimientos rutinarios. No se requiere ninguna acción.	
Muy Bajo (1)		

De acuerdo a lo anterior, los riesgos que se ubiquen en la franja entre 1 al 5, corresponden a la ZONA DE RIESGO aceptada por la compañía, los ubicados por encima de este nivel se ubicarán en la zona de riesgo **INACEPTABLE** para la empresa, donde se requieren planes de tratamiento inmediatos, tal cual se identifica en el siguiente mapa:

CONFIDENCIAL

IMPACTO						
	5 Catastrófico	MODERADO	ALTO	EXTREMO	EXTREMO	EXTREMO
	4 Severo	MODERADO	ALTO	ALTO	EXTREMO	EXTREMO
	3 Moderado	MODERADO	MODERADO	ALTO	ALTO	EXTREMO
	2 Menor	BAJO	MODERADO	MODERADO	ALTO	ALTO
	1 Insignificante	MUY BAJO	BAJO	MODERADO	MODERADO	MODERADO
		1 Altamente Improbable	2 Improbable	3 Posible	4 Probable	5 Frecuente
		PROBABILIDAD				

NIVEL INACEPTABLE

NIVEL ACEPTABLE

11.7 VALORACIÓN DEL RIESGO

La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo frente a los controles existentes, con el objetivo de establecer prioridades para su manejo y fijación de políticas.

Para adelantar esta etapa es necesario identificar los puntos de control existentes en los diferentes procesos que se desarrollan en la Empresa, los cuales permiten obtener información que faciliten la toma de decisiones. Para realizar la valoración es necesario tener en cuenta su clasificación:

Controles Preventivos: Aquellos que actúan para eliminar las causas del riesgo y previenen su ocurrencia o materialización.

Controles Correctivos: Aquellos que permiten tanto el restablecimiento de la actividad después de ser detectado un evento no deseable como la modificación de las acciones que propiciaron su ocurrencia.

Los controles deben ser:

- Operativos (Modelos operativos actualizados)
- De seguridad (R. G. S.) Security o seguridad
- Administrativos (Insurance o seguro – Safety o protección)

CONFIDENCIAL

Además, es necesario valorar si los controles descritos se encuentran documentados, si se están aplicando en la actualidad y si son efectivos para minimizar el riesgo y ponderarlos según la siguiente tabla:

CRITERIOS	VALORACIÓN DEL RIESGO
¿No existen controles?	Se mantiene el resultado de la evaluación antes de controles.
¿Los controles existentes no son efectivos?	Se mantiene el resultado de la evaluación antes de controles
¿Los controles existentes son efectivos, pero no están documentados?	Cambia el resultado a una casilla inferior de la matriz de evaluación antes de controles (el desplazamiento depende de sí el control afecta el impacto o la probabilidad)
Los controles son efectivos y están documentados?	Pasa a casilla inferior (el desplazamiento depende de sí el control afecta el impacto o la probabilidad).

Una vez ha respondido todas las preguntas se procede a realizar la valoración, así:

Calificados y evaluados los riesgos, estos deberán ser analizados frente a los controles existentes para cada riesgo, acto seguido se deben ponderar según la tabla establecida, teniendo en cuenta las respuestas a las preguntas anteriormente formuladas (los controles se encuentran documentados, se aplican y son efectivos).

Para las etapas de análisis del riesgo (calificación y evaluación) y valoración del riesgo, se documenta en el Formato RISK-FOR-001 MAPA DE RIESGOS. (Anexo 1.).

11.8 PLAN DE TRATAMIENTO

Una vez identificados y valorados los riesgos, y ejercidos los controles iniciales se debe proceder a generar el plan de acción para cada riesgo que se ubica dentro de la ZONA INACEPTABLE en su Nivel de Exposición, dando alcance a los siguientes aspectos:

Acciones: Actividades conjuntas y sistemáticas que permitirán que las probabilidades de materialización del riesgo identificado se reduzcan.

Responsables: funcionarios encargados de aplicar los planes de acciones descritos en el formato RISK-FOR-001 MAPA DE RIESGOS. (Anexo 1.). Líderes y/o Coordinadores de proceso (Nivel estratégico y Táctico).

CONFIDENCIAL

Seguimiento: Fechas establecidas para el inicio y la finalización de los planes de acción establecidos. (Revisión de avances y efectividad de las acciones en la valoración del Riesgo).

12. OBJETIVO COMERCIAL – CLIENTES

ACTIVOS DIGITALES S.A.S. tiene dentro de sus objetivos comerciales; la comercialización de servicios de activos virtuales con destino a los mercados locales e internacionales para personas jurídicas o naturales que acrediten documentación correspondiente. Para ello ha establecido un modelo comercial liviano en su estructura de costos, pero seguro, que le permite al pequeño empresario invertir en activos virtuales y otros proyectos productivos de origen legal, garantizando la plena identidad de los terceros, el origen de sus fondos y el cumplimiento de los DDHH y DIH en las poblaciones donde se ubican los títulos mineros de sus proveedores.

Si bien la idea central puede permitir la inclusión de estos pequeños empresarios y que requieran proteger sus capitales de inversión; en ACTIVOS DIGITALES S.A.S. somos conscientes que a nivel nacional e internacional existen algunas actividades vulnerables o que presentan un mayor factor de riesgos al Lavado de Activos y/o La Financiación del Terrorismo, a las cuales en caso de ser requeridos para invertir o comercializar activos virtuales, se deberán ejercer mayores controles sobre el origen y destino de los recursos, sumado a compromisos robustos en materia de prevención del Riesgo de LA/FT.

A continuación, se relacionan las actividades económicas que mayor vulnerabilidad presentan al Lavado de Activos y/o la Financiación del Terrorismo:

A. Corporaciones, fundaciones o entidades sin ánimo de lucro.

B. Personas Políticamente expuestas (PEP).

C. Entidades que realizan actividades económicas de alto riesgo:

- Empresas o personas que comercialicen productos controlados por la Dirección Nacional de Estupefacientes.
- Hoteles y Agencias de viaje
- Cambistas profesionales y casas de cambio
- Casas de Empeño
- Casinos y negocios de Apuestas
- Comercializadoras/arrendadoras de vehículos automotores, embarcaciones y aeronaves
- Comercializadoras bajo el esquema de ventas multinivel o piramidal
- Comercializadoras de armas, explosivos o municiones
- Constructoras

CONFIDENCIAL

- Comercializadoras o agencias de bienes raíces
- Entidades Deportivas
- Estaciones de Gasolina
- Comercializadoras de antigüedades, joyas, metales y piedras preciosas, monedas, objetos de arte y sellos postales
- Prestamistas
- Sector Transportador
- Transportadores de dinero o de valores
- Empresas ubicadas en zonas Francas. (negocios que realizan operaciones de comercio exterior)
- Empresas dedicadas a la transferencia o envío de fondos o remesas
- Operadores Cambiarios fronterizos
- Campañas políticas o políticos en campaña
- Religiosos misioneros
- Extranjeros de estadía temporal en el país
- Ganaderos
- Piscicultores
- Galerías de Arte
- Organizaciones no gubernamentales (ONG)
- Rentistas de Capital (Las personas que se dedican a prestar dinero a particulares).

Todas estas actividades deberán ser clasificadas en la siguiente matriz, de acuerdo a su nivel de criticidad que tenga un mayor factor de riesgo de Lavado de activos y La Financiación del Terrorismo, para esta clasificación se establecieron cuatro criterios:

CRITERIOS - FACTOR DE RIESGO		
NIVEL	**DESCRIPCIÓN**	**RANGO**
BAJO	Actividades económicas con un **factor de riesgo bajo** con relación con Actividades de Lavado de activos o La Financiación del Terrorismo.	(1 - 2)
MEDIO	Actividades económicas con **moderado factor de riesgo** de Lavado de activos y Financiación del Terrorismo, de acuerdo a la experiencia nacional e internacional de actividades vulnerables al LA/FT.	(3 - 5)
ALTO	Son consideradas actividades económicas altamente **vulnerables** al Lavado de Activos y La Financiación del Terrorismo.	(6 - 12)
EXTREMO	Son todas las actividades económicas que **mayor nivel de exposición** a actividades de Lavado de activos y Financiación del terrorismo presentan.	(13 - 25)

CONFIDENCIAL

12.1 NO PARAÍSO FISCAL

ACTIVOS DIGITALES S.A.S. de acuerdo a la normatividad vigente, determina el paraíso fiscal como una zona geográfica con un régimen tributario de impuestos bajos o nulos que atrae a residentes y capital extranjero, ya que su presión fiscal es inferior a la habitual en el resto de países.

En caso de identificar clientes con asiento fiscal en estos territorios, los controles se aplicarán de acuerdo al impacto que puedan generar en el negocio, teniendo como referencia la siguiente tabla de calificación:

CRITERIOS MEDICIÓN CONSECUENCIA/IMPACTO					
VARIABLES	**CATEGORÍA**				
	1. Sin impacto relevante	2. Bajo impacto	3. Impacto moderado	4. Impacto crítico	5. Impacto muy crítico
NO Paraíso Fiscal	Tener asiento fiscal cualquier país diferente a los mencionados en las categorías anteriores.	Tener asiento fiscal en los siguientes países: Perú o Uruguay	Tener asiento fiscal en los siguientes países: Albania, Andorra, Armenia, Aruba, Belice, Bermuda, Bosnia y Herzegovina, Botsuana, Cabo Verde, Islas Caimán, Islas Cook, Curazao, Islas Feroe, Fiyi, Macedonia, Groenlandia, Guernsey, Hong Kong, Isla de Man, Jamaica, Jersey, Jordania, Liechtenstein, Malasia y Labuan, Maldivas, Mauricio, Montenegro, Marruecos, Nauru, Nueva Caledonia, Niue, Omán, Qatar, San Vicente y las Granadinas, San Marino, Seychelles, Suiza, Serbia, Suazilandia, Taiwán, Tailandia, Turquía y Vanuatu.	Tener asiento fiscal en los siguientes países: Panamá.	Tener asiento fiscal en los siguientes países: Bahréin, Barbados, Corea del Sur, Emiratos Árabes Unidos, Granada, Guam, Islas Marshall, Macao, Mongolia, Namibia, Palau, Santa Lucía, Samoa, Samoa Americana, Trinidad y Tobago, y Túnez.

13. CONOCIMIENTO Y VINCULACIÓN (Debida Diligencia)

13.1 ASOCIADOS, SOCIOS Y ACCIONISTAS:

De acuerdo a la Política integral de gestión de riesgo de LA/FT, la compañía establece las siguientes directrices para el ingreso o vinculación de accionistas:

Cuando se presente la necesidad que un socio o accionista vaya a transferir sus acciones o cuotas a un tercero, ellos mismos deberán dar inicio al proceso de conocimiento de la persona o empresa a la cual se le pretenden transferir sus acciones, solicitando la información a la que hace referencia el procedimiento: “SEG-POL-001 POLÍTICAS DE SEGURIDAD PARA EL CONOCIMIENTO, SELECCIÓN Y VINCULACIÓN DE PROVEEDORES Y CLIENTES”, diligenciando el formato “KyC Natural person - ACTIVOS DIGITALES S.A.S.” y anexando los siguientes documentos con el ánimo de conocer al nuevo accionista:

- Certificado de existencia y representación legal con vigencia no superior a 30 días, expedido por la Cámara de Comercio. (Original).
- Fotocopia del Registro Único Tributario - RUT
- Fotocopia del documento de identidad al 150% del Representante Legal. (Solo si aplica).
- Estados financieros certificados o dictaminados por contador público.
- Relación de socios (Nombres completos y cedulas), asociados y accionistas que tengan más del 5% de su capital social o aportes.
- Declaración de renta de último periodo disponible.
- 02 referencias comerciales
- 02 referencias Bancarias

Los accionistas o socios de la Empresa solo transferirán sus acciones o aportes a personas naturales o jurídicas con reconocida y suficiente idoneidad de tipo moral, judicial, penal y fiscal, de igual manera se deberán de abstenerse de realizar tal transacción si existen dudas sobre la procedencia o legitimidad de sus recursos.

Los accionistas o socios de la Empresa bajo ninguna circunstancia podrán transferir sus acciones o aportes a personas naturales o jurídicas que figuren o este reportadas en listas de criminales o terroristas o que este vinculados de manera indirecta con estos, (En especial lista de la OFAC y Naciones Unidas), en ese mismo sentido ACTIVOS DIGITALES S.A.S. no podrá registrar transferencias de acciones o aportes a personas o empresas que figuren en estas listas.

KyC Natural person - ACTIVOS DIGITALES S.A.S.
https://forms.gle/qPaZo5cRVwTB2SPa7

KyC Legal Person - ACTIVOS DIGITALES SAS.
https://forms.gle/zym6HvXWoNPa9J5e7

CONFIDENCIAL

13.2 EMPLEADOS CON VINCULO LABORAL O CONTRACTUAL:

Antes de realizar la contratación del personal, ya sea de manera directa o por medio de una empresa temporal, se debe contar con un concepto "CONFIABLE", en el proceso de estudio de confiabilidad, el cual deberá contener como mínimo las siguientes validaciones:

- Lista OFAC
- Lista de las Naciones Unidas
- Antecedentes Judiciales (Fiscalía)
- Antecedentes Judiciales (Policía Nacional)
- Antecedentes Disciplinarios (Procuraduría)
- Antecedentes Fiscales (Contraloría)
- Antecedentes Contables (BDME)

Adicional a las validaciones anteriores, la Empresa deberá cumplir con los siguientes filtros de seguridad antes de dar inicio al proceso de contratación:

- Referenciación (laboral, académica, personal, gremial)
- Visita domiciliaria
- Financial Scored (Cifin – Datacredito, etc.) *
- Examen de poligrafía (Pre-empleo)
- Prueba (SPA)

*En caso de reportes negativos, se puede viabilizar el ingreso con la presentación del respectivo acuerdo de pago con la entidad reportante.

En caso de identificar conceptos "NO FAVORABLES" o anotaciones que condicionen el ingreso del colaborador, la Empresa deberá abstenerse de dar inicio al proceso de contratación.

13.3 PROVEEDORES Y CLIENTES:

ACTIVOS DIGITALES S.A.S. estableció mecanismos y procedimientos de Prevención, Seguridad y Control para la identificación plena y confiable, y la vinculación de forma Segura a la compañía a PROVEEDORES y CLIENTES, y la verificación de la información suministrada por estos, los cuales deben ser aplicados con diligencia y responsabilidad, que permitan relaciones contractuales de confianza a largo plazo.

Una vez la Empresa haya autorizado el producto o servicio ofertado por el Proveedor, o el cliente haya aceptado la oferta comercial presentada; Los procesos de Operaciones y/o Comercial solicitarán al Proveedor o Cliente el diligenciamiento del formato "RISK-FOR-001 CONOCIMIENTO Y VINCULACIÓN DE CLIENTES Y PROVEEDORES" **(ESTE**

CONFIDENCIAL

DOCUMENTO NO PODRÁ SER DILIGENCIADO POR ALGÚN COLABORADOR DE LA COMPAÑÍA).

Persona jurídica (Corporativo B2B).

Anexo al documento anterior, el Proveedor y/o Cliente seleccionado deberá adjuntar los siguientes soportes:

1. Copia del documento de identificación del Representante Legal

2. Certificado de Existencia y Representación Legal inferior a 30 días

3. Certificación accionaria inferior a 30 días, con indicación de los accionistas de más del 5% de participación y a su vez los accionistas de otras personas jurídicas hasta poder determinar el beneficiario final."

4. Resolución de facturación actualizada o vigente.

5. Copia del documento de identidad y tarjeta profesional del contador o revisor fiscal que firma certificación accionaria, certificado de la Junta Central de Contadores.

6. RUT Actualizado con “Actividad Económica” descrita en el portafolio de servicios.

7. Si el proveedor tiene una condición especial tributaria (1429, cooperativa, etc.) adjuntar respectiva resolución de la DIAN que acredite tal condición."

8. Estados financieros con NIIF con notas aclaratorias.

9. Referencia Bancaria, inferior a 30 días.

10. Referencias Comerciales (03), inferior a 30 días.

11. Certificado de Origen de fondos (firmados en original y huella del representante legal).

12. Certificado de antecedentes del contador y revisor fiscal.

13. Afiliación a la Seguridad Social de los trabajadores.

14. Últimas 3 declaraciones de renta, últimas 3 declaraciones de IVA.

15. Declaración bajo gravedad de juramento de origen de los fondos (socios, accionistas, asociados).

16. Informe de visita de la última fiscalización de DIAN (si la tiene)

CONFIDENCIAL

17. Estructura Corporativa (Nombres directivos y responsables).

18. Sistema de atención a usuarios (PQRS).

19. Diagrama de flujos - presentación con el modelo de negocio, estableciendo en primer lugar un Diagrama de Flujo de como funciona la empresa y los servicios que prestará a Activos Digitales S.A.S.

20. Esquema de proveedores y sus funciones.

21. Esquema de KyC.

22. Manual de prevención de lavado de dinero.

23. Reportes ante UIAF (Últimos 3)

Persona natural (Individual P2P).

Anexo al documento anterior, el Proveedor y/o Cliente seleccionado deberá adjuntar los siguientes soportes:

1. Copia del documento de identificación del Representante Legal

2. Copia del documento de identidad y tarjeta profesional del contador o revisor fiscal que firma y certifica estados financieros y proyecta el pago de impuestos, certificado de la Junta Central de Contadores.

3. RUT Actualizado con “Actividad Económica” descrita en el portafolio de servicios.

4. Referencia Bancaria, inferior a 30 días.

5. Referencias Comerciales (03), inferior a 30 días.

6. Certificado de Origen de fondos (firmados en original y huella del representante legal, certificado por contador Publico).

7. Certificado de antecedentes del contador y revisor fiscal.

8. Afiliación a la Seguridad Social.

9. Últimas 3 declaraciones de renta.

10. Reportes ante UIAF (Últimos 3) o entidad similar fuera de Colombia.

CONFIDENCIAL

La Unidad de Cumplimiento deberá confrontar los datos del Proveedor y/o clientes y los proporcionados en los formatos de vinculación y documentos de representación legal; de sus socios, asociados o accionistas mayoritarios (que tengan una participación igual o mayor al 5% del capital social), sus representantes legales y sus miembros de junta directiva u órgano que haga sus veces, en internet (ej. Google, etc.), y mínimo en las siguientes listas y/o bases de datos abiertas y cerradas:

LISTAS y PEPS (Personas expuestas política y socialmente)
Listas vinculantes
1. Department of State list of Foreign Terrorist Organizations FTO Lista Departamento de Estado EEUU Organizaciones extranjeras terroristas FTO
2. EU Consolidated list of sanctions Lista Unión Europea de organizaciones terroristas
3. EU Consolidated list of sanctions terrorism Lista Unión Europea de personas catalogadas como terroristas
4. UN Security council list Lista Consejo de Seguridad de la ONU
Listas restrictivas
1. Lista Panama Papers Lista personas y empresas vinculadas al escándalo Panama Papers
2. The Arms Export Control Act (AECA) Ley de Control de Exportación de Armas (AECA)
3. World Bank Listing of Ineligible Firms and Individuals Empresas sancionadas Banco Mundial
4. Comité de Sanciones del Grupo BID Comité BID empresas sancionadas por prácticas fraudulentas, corruptas, colusorias, coercitivas u obstructivas
5. Consolidated Canadian Autonomous Sanctions List Lista Consolidada de sanciones autonomas de Canada
6. EEUU Denied Persons List BIS Lista de Personas prohibidas a exportar EEUU
7. EEUU Entity List BIS Lista Entes prohibidos a recibir mercancias EEUU
8. Foreign Corrupt Practices Act List EEUU Lista Ley de Prácticas Corruptas en el Extranjero FCPA EEUU
9. List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (CAPTA List)
10. OFAC Foreign Sanctions Evaders (FSE) List OFAC Lista de evasores de sanciones extranjeras (FSE)
11. UK HM Treasury sanctions list Lista de entes sancionados Gran Bretaña
12. OFAC Non-SDN Iranian Sanctions Act (NS-ISA) List OFAC Lista de la Ley de sanciones iraníes no SDN (NS-ISA)
13. O□ce of Foreign Assets Control OFAC OFAC Lista Clinton
14. Lista OSFI Canada Lista Ofice of the Superintendent of Financial Institutions Canada
15. OFAC Non-SDN Palestinian Legislative Council (NS-PLC) list Lista del Consejo Legislativo Palestino no SDN (NS-PLC)
16. OFAC Sectoral Sanctions Identifications (SSI) List OFAC Lista de identificaciones de sancionadas sectoriales (SSI)
17. EEUU Unverified List BIS Entes no elegibles para recibir artículos sujetos a las Regulaciones de la Administración de Exportaciones EEUU
18. OFAC Non-SDN Menu-Based Sanctions List (NS-MBS List) OFAC Lista de sanciones basada en menús no SDN (Lista NS-MBS)
Noticias criminales
1. Noticias extraditados Corte Suprema de Justicia

CONFIDENCIAL

2. Noticias Policía Nacional LAFT
3. Actividades corruptas o illegales Insight Crime
4. Lista de Personas y Grupos Terroristas Guardía Civil Española
5. Interpol Red notices Boletines Rojos Interpol
6. DSS Most Wanted DSS (Diplomatic Security Service) más buscados
7. ICE Most Wanted ICE (Immigration and Customs Enforcement) más buscados
8. UK Most Wanted Gran Bretaña más buscados
9. Noticias Fiscalía General de la Nación LAFT
10. Noticias Presidencia LAFT
11. Fugitivos DEA Fugitivos más buscados por la DEA
12. Enviromental Protection Agency (EPA) Fugitives Fugitivos Agencia de Protección del medio Ambiente EEUU (EPA)
13. CBI Most Wanted CBI (Central Bureau of Investigation) más buscados
14. FBI Most Wanted FBI (Federal Bureau of Investigation) más buscados
15. UE EUROPOL Most Wanted EUROPOL más buscados
Boletines
1. Boletín de deudores de la Contraloría General de la nación Deudores Contraloría general de la nación reporte trimestral
2. Contadores sancionados Junta Central de Contadores JCC Contadores sancionados JCC
3. Entes Sancionados SECOP Entes sancionados por contratación pública SECOP
4. Boletines Superintendencia Financiera
5. Boletines Superintendencia Solidaria
6. Proveedores ficticios DIAN
7. Noticias Procuraduría General de la Nación
8. Boletines Superintendencia de Industria y Comercio
9. Boletines Superintendencia de Sociedades
PEPS (Colombia)
1. Relacionados a PEPS Colombia
2. Magistrados y funcionarios Consejo de Estado
3. Magistrados y funcionarios Consejo Superior de la Judicatura
4. Magistrados y funcionarios Corte Suprema de Justicia
5. Embajadas en el exterior
6. funcionarios de alto nivel Fuerzas Militares
7. funcionarios públicos nivel municipal, alcaldes y concejales
8. funcionarios partidos políticos y candidatos no elegidos
9. Candidatos elecciones 2019
10. Magistrados y funcionarios Consejo Nacional Electoral
11. Magistrados y funcionarios

CONFIDENCIAL

12. Embajadas en Colombia			
13. Estructura de Gobierno			
14. funcionarios públicos alto nivel gobernaciones y asambleas			
15. funcionarios públicos alto nivel del orden nacional			
16. Colombia			
PEPS Internacionales			
1. Alemania	10. Argentina	19. México	28. Países Bajos
2. Bélgica	11. Bielorrusia	20. Noruega	29. Otros
3. Bolivia	12. Brasil	21. Paraguay	30. Polonia
4. Canadá	13. Chile	22. Perú	31. República de El Salvador
5. Costa Rica	14. Cuba	23. República Bol. de Venezuela	32. República de Honduras
6. Ecuador	15. España	24. República de Guatemala	33. Suecia
7. Estonia	16. Finlandia	25. República de Panamá	34. Venezuela
8. Francia	17. Islandia	26. Uruguay	
9. Letonia	18. Lituania	27. Nicaragua	

En caso que el Proveedor y/o Cliente o alguno de los accionistas mayoritarios, representantes legales o miembros de junta directiva u órgano equivalente figuren en las anteriores listas y su concepto sea “A CONSIDERACION” o “NO CONFIABLE” la decisión de vinculación debe ser trasladada al comité de LA/FT al que hace referencia este documento, donde se definirá la vinculación o no del proveedor o cliente.

Nota: para mayor información consultar el documento “SEG-POL-001 POLITICAS DE SEGURIDAD PARA EL CONOCIMIENTO, SELECCIÓN Y VINCULACION DE PROVEEDORES Y CLIENTES”.

13.4 ESTUDIO DE CONFIABILIDAD:

La Empresa definió una matriz de evaluación de 7 aspectos fundamentales para el conocimiento veraz y confiable del proveedor o cliente con el que se desea iniciar una relación comercial, dichos aspectos tendrán una valoración sobre 3 niveles de aceptación: CONFIABLE, A CONSIDERACIÓN y NO CONFIABLE, el cual se obtiene de manera cuantitativa al ponderar el valor en una escala de medición de 1 a 3 a los hallazgos o reportes identificados en las consultas realizadas contra la cantidad de aspectos evaluados:

CONFIDENCIAL

Aspectos a evaluar:

ASPECTOS A EVALUAR	EVALUACION	CRITERIOS DE MEDICION	HALLAZGOS
1. MUGSHOTS.COM	1	Sin reportes	NO COINCIDENCIAS
2. LISTA CLINTON - OFFICE OF FOREING ASSETS CONTROL (OFAC)	1	Sin reportes	NO COINCIDENCIAS
3. ONU - RESOLUCIONES CONSOLIDGADAS NACIONES UNIDAS	1	Sin reportes	NO COINCIDENCIAS
4. PEPS INTERNACIONALES	1	Sin reportes	NO COINCIDENCIAS
5. USA STATE - BUSCADOS DEPARTAMENTO DE ESTADO	1	Sin reportes	NO COINCIDENCIAS
6. U.S MARCHALS SERVICE	1	Sin reportes	NO COINCIDENCIAS
7. MOST WANTED USA ATF	1	Sin reportes	NO COINCIDENCIAS
8. SANCIONES BANCO INTERAMERICANO DE DESARROLLO - BID	1	Sin reportes	NO COINCIDENCIAS
9. CONSOLIDATED SCREENING LIST	1	Sin reportes	NO COINCIDENCIAS
10. DEA	1	Sin reportes	NO COINCIDENCIAS
11. EUROPE MOST WANTED FUGITIVES	1	Sin reportes	NO COINCIDENCIAS
12. EUROPEAN UNION EXTERNAL ACTION SANCTION LIST	1	Sin reportes	NO COINCIDENCIAS
13. AUTORIDAD REGULADORA DE LA INDUSTRIA FINANCIERA (FINRA)	1	Sin reportes	NO COINCIDENCIAS
14. ICE USA WANTED	1	Sin reportes	NO COINCIDENCIAS
15. INTERPOL	1	Sin reportes	NO COINCIDENCIAS
16. LISTE UNIQUE FRANCE - SANCTIONS LIST	1	Sin reportes	NO COINCIDENCIAS

CONFIDENCIAL

17. THE WORLD BANK - DEBARRED FIRMS AND INDIVIDUALS	1	Sin reportes	NO COINCIDENCIAS
18. HISTÓRICO DE NOTICIAS - INFOMACIÓN REPUTACIONAL	1	Sin reportes	NO COINCIDENCIAS
19. PANAMÁ PAPERS	1	Sin reportes	NO COINCIDENCIAS
20. LISTA PRIVADA INTERNACIONAL ASIA	1	Sin reportes	NO COINCIDENCIAS
21. USA.GOV - GUÍA EN LÍNEA PARA INFORMACIÓN Y SERVICIOS DEL GOBIERNO	1	Sin reportes	NO COINCIDENCIAS
22. VIOLACIONES REGULATORIAS USA - VIOLATIONS TRACKER	1	Sin reportes	NO COINCIDENCIAS
NIVEL DE ACEPTACION	3,85%	**CONFIABLE**	

Criterios de medición:

CRITERIOS MEDICIÓN - HALLAZGOS Y/O REPORTES	
1	Sin reportes
2	Reportes leves / moderados
3	Reportes negativos

Nivel de aceptación:

CATEGORIA	NIVEL DE ACEPTACION
>16%	NO CONFIABLE
14,1,1% - 16%	A CONSIDERACION
<14%	CONFIABLE

CONFIDENCIAL

III. NIVEL DE ACEPTACIÓN DEL CLIENTE O PROVEEDOR	
CONFIABLE	Todos los miembros de la Empresa evaluada deben tener una calificación final del 14% c/u, lo que representa que no se identificaron reportes negativos en las consultas y se debe continuar con el proceso de vinculación.
A CONSIDERACIÓN	Si uno de los miembros de la Empresa evaluada tiene una calificación superior al 14% su concepto se cataloga como "A CONSIDERACIÓN", la decisión de vinculación o continuidad de la relación comercial deberá ser trasladada al comité de Análisis LA/FT, quienes determinarán si los reportes identificados ponen en riesgo la Seguridad de la compañía.
NO CONFIABLE	Si dos (02) o más miembros de la Empresa evaluada tiene una calificación superior al 14% su concepto se cataloga como "NO CONFIABLE", de igual manera si uno solo de los miembros de la Empresa evaluada tiene una calificación superior o igual al 16% su concepto se cataloga como "NO CONFIABLE", la decisión de vinculación o continuidad de la relación comercial deberá ser trasladada al comité de Análisis LA/FT, quienes determinarán si los reportes identificados ponen en riesgo la Seguridad de la compañía.

13.5 ACTUALIZACIÓN DE LA DOCUMENTACIÓN E INFORMACIÓN DE CLIENTES Y PROVEEDORES

Es deber de la Empresa adelantar un proceso de actualización de información y documentación de los proveedores y clientes en un periodo **no** superior a dos años, para lo cual deberá diligenciar nuevamente los formatos de conocimiento y vinculación, de igual manera la Empresa deberá nuevamente hacer la validación de las consultas a la que hace referencia el punto 13.3 y 13.4 de este documento.

Las coincidencias evidenciadas ya sea en la consulta en batch o masiva que se realiza mes a mes, o en esta actualización, estos serán llevador al comité extraordinario de LAFT, quien determinara por el grado de impacto de las coincidencias, si termina la relación comercial con la persona o cliente, o si en su defecto solicita explicación formal sobre la coincidencia, respuesta que también deberá ser analizada por el comité de cumplimiento, una vez sea remitida por el cliente, en un termino no superior a 15 días hábiles. En caso de no recibir respuesta en dicho tiempo, el comité de LAFT quedara facultado para dar por terminada la relación comercial y/o contractual.

13.6 DEBIDA DILIGENCIA INTENSIFICADA:

La Debida Diligencia Intensificada obedece a un conocimiento mas amplio de los clientes, proveedores, socios y/o colaboradores que estén dentro de las actividades económicas que

CONFIDENCIAL

mayor vulnerabilidad presentan al Lavado de Activos y/o la Financiación del Terrorismo, descritas en el numeral *12. OBJETIVO COMERCIAL – CLIENTES* de este manual.

De igual manera, la Debida Diligencia Intensificada a los PEP se extenderán a (i) los cónyuges o compañeros permanentes del PEP; (i) los familiares de las PEP, hasta el segundo grado de consanguinidad, segundo de afinidad y primero civil; (iii) los Asociados Cercanos.

Además de las medidas normales ya mencionadas, el procedimiento de conocimiento de la Contraparte, en el proceso de Debida Diligencia Intensificada se deben: (i) obtener la aprobación de la instancia o empleado de jerarquía superior para la vinculación o para continuar con la relación contractual; (ii) suscribir un manifiesto de seguridad y entendimiento para la aplicación de políticas de prevención contra el Lavado de activos y/o la Financiación del terrorismo, el cual deberá ser firmado por el Representante Legal de la entidad a vincularse.

De igual manera el solicitante deberá allegar el certificado de Beneficiarios finales de su entidad y si este compuesto por personas jurídicas, estas a su vez deberán entregar el mismo documento, que permita conocer las personas naturales finales beneficiarias de los dividendos o rentas de los negocios.

Finalmente, es deber del asesor encargado de dicha vinculación, programar una visita de control a las instalaciones del cliente o proveedor, dando cobertura a los aspectos enunciados en el formato RISK-FOR-003 VISITA A PROVEEDORES Y/O CLIENTES CRÍTICOS, acompañado de mínimo 6 fotografías, el cual deberá ser firmado por el funcionario encargado de dirigir la visita y finalmente remitirse a la Unidad de Cumplimiento.

El resultado de estas revisiones deberá ser llevadas a un comité extraordinario de LAFT, donde se validará si se da o no continuidad al solicitante o si se requiere algún documento adicional.

14. IDENTIFICACIÓN Y ANALISIS DE OPERACIONES INUSUALES Y SOSPECHOSAS

14.1 OPERACIONES INUSUALES:

Son inusuales las transacciones cuya cuantía o características no guardan relación con la actividad económica del cliente, o que por su número, por las cantidades transadas o por sus características particulares, se salen de los parámetros de normalidad establecidas por la Empresa, más exactamente se hace referencia a una serie de factores que denotan una falta de consistencia, coherencia, firmeza, periodicidad y estabilidad respecto a una operación bancaria, financiera, contractual o de otra índole que suscita sospecha sobre su solidez.

CONFIDENCIAL

De igual manera una operación o transacción se considera inusual, cuando cumple al menos uno de los siguientes aspectos:

- No guardan relación con la actividad económica del emisor o receptor de la transacción o se salen de los parámetros de control definidos por la Empresa.
- Operaciones de las cuales no se han emitido explicación o justificación razonable.
- La presencia de algunas de las señales de alerta definidas.
- La identificación de posibles tipologías de transacciones de LA/FT, establecidas por la UIAF y organismos internacionales para los servicios de traslado y administración de valores.
- El receptor de los valores está incluido en listas restrictivas implementadas por la Empresa.

14.2 OPERACIONES SOSPECHOSAS:

Son todas las operaciones realizadas por una persona natural o jurídica, que por su número, cantidad o características no se enmarca dentro de los sistemas y practicas normales de los negocios de una industria o sector determinado y que de acuerdo con los usos y costumbres de la actividad que se trate, no haya podido ser razonablemente justificada.

Estas operaciones una vez sean detectadas por los colaboradores deberán ser reportadas mediante un ROS “Reporte de Operación Sospechosa”, no se requiere tener la certeza de que dicha operación corresponde a una actividad ilícita, así como tampoco se debe tipificar el tipo penal o que los recursos empleados en la operación provienen de actividad ilícitas.

Solo se requiere el diligenciamiento del formato RISK-FOR-002 REPORTE EVENTO DE RIESGO, por no corresponder el ROS a una denuncia penal, el mismo no tiene que ser firmado. Dicho formato aplica tanto para operaciones inusuales, como sospechosas.

Estos reportes serán analizados y estudiados por el proceso de Riesgos y Seguridad, para determinar si se debe reportar o no a la Unidad de Información y Análisis Financiero (UIAF), los colaboradores deben de tener en cuenta las siguientes consideraciones para realizar el reporte interno de este tipo de operaciones:

- Para remitir un Reporte no es necesario tener la certeza de que se trata de una actividad delictiva, solo basta con considerar de manera PRESUMIBLE de que se trata de una transacción sospechosa.

- El ROS no constituye una denuncia penal.

- El ROS es totalmente reservado y el manejo de cada caso es de carácter CONFIDENCIAL.

CONFIDENCIAL

15 MECANISMO DE DETECCIÓN Y SEÑALES DE ALERTA

Durante las etapas de vinculación de nuevos clientes y proveedores y/o la programación de pagos o traslados de efectivo a terceros, los colaboradores involucrados podrán detectar operaciones inusuales, de acuerdo a las señales de alerta ya referidas en este documento, y reportarlas al director nacional de Riesgos y Seguridad mediante el formato RISK-FOR-002 REPORTE EVENTO DE RIESGO, con el fin de que el Oficial de Cumplimiento determine si se trata o no de una Operación Sospechosa.

Las Operaciones inusuales que se identifiquen y sean reportadas durante el mes, serán analizadas en el Comité de LA/FT al que se hace referencia en el punto 9.5 del presente Manual, quienes evalúan estos reportes y establecen si se tratan de Operaciones Sospechosas y en ese mismo sentido autorizar el reporte ante la Unidad de Información y Análisis Financiera (UIAF).

En caso de que el director nacional de Riesgos y Seguridad, previo análisis, determina que la operación reportada debe ser analizada de manera inmediata por el comité de LA/FT, debido a su capacidad de daño o posible consecuencia de alto impacto para la Empresa, convocara a una sesión extraordinaria, la cual deberá llevarse a cabo en el menor tiempo posible.

15.1 SEÑALES DE ALERTA:

ACTIVOS DIGITALES S.A.S. cuenta con alertas parametrizadas en su sistema o software transaccional, estas señales son situaciones, montos, cuantías, indicadores, dobles validaciones, nuevos destinatarios no vinculados y demás información que la Empresa determine como relevante, a partir de los cuales se puede inferir como operaciones o transacciones que se salen de los parámetros de prevención y control establecidos por la compañía.

De igual manera la Empresa realiza monitoreos constantes y permanentes, identificando eventos en los cuales se pueda inferir la posible existencia de una operación anormal, permitiendo a la compañía minimizar el riesgo de ser víctima de actividades de Lavado de Activos y/o Financiación del Terrorismo, y de esta manera blindar o proteger el buen nombre y la Reputación de la Empresa.

Al momento de efectuar el proceso de vinculación de clientes o proveedores, se deben tener en cuenta las siguientes señales de alerta, con el fin de detectar si las operaciones tienen características de inusuales y así poder reportar al director nacional de Riesgos y comprobar la efectividad para contrarrestar las operaciones de Lavado de Activos:

Personas naturales y Jurídicas que:

CONFIDENCIAL

- Tienen nuevos propietarios, las empresas o acciones han sido adquiridas con dificultades económicas, cambian su naturaleza y presentan en corto plazo grandes rentabilidades.
- Perciben ingresos no operacionales superiores a los propios de su actividad comercial.
- Tienen un capital suscrito muy bajo y/o un objeto social muy amplio.
- Tienen en común, gerentes, administradores o representantes legales con otras personas jurídicas o empresas Outsourcing.
- Actúan a nombre de otra persona o razón social, ocultando la real identidad del socio, propietario o representante legal del cliente o proveedor.
- Realizan varias transacciones a fin de que no les sea requerido soportes que declaren la procedencia del efectivo.
- Realizan múltiples operaciones en efectivo en una misma entidad financiera o en diferentes sucursales.
- Las operaciones o transacciones realizadas superan las relacionadas con su actividad comercial.
- Diligencian los formatos con letra ilegible o con enmendaduras.
- Suministran información falsa, de difícil verificación o insuficientes.
- Se molestan cuando se les solicita una identificación detallada y/o el diligenciamiento de algunos formatos.
- Intento de soborno o dinero a un colaborador de la Empresa, con el ánimo de no entregar información.
- Se niega a entregar información respecto a su ubicación actual, residencia y lugares de trabajo, manifestando estar en varias partes o ser difícil de ubicar.
- Registra como dirección de su Empresa, nomenclatura que coincide con las de otras empresas que no guardan relación o vinculo aparente.
- Las referencias personales y Bancarias no pueden ser verificadas.
- Los clientes que aumentan considerablemente sus ingresos sin explicación adecuada.
- Lista de personas que según información de uso publico

Colaboradores de la Empresa que:

- Realizan internamente un sin número de transacciones intentando evadir los controles internos.
- Tienen un estilo de vida superior al nivel de sus ingresos.
- Se muestran celosos ante el manejo de sus clientes por parte de otros compañeros.
- No aceptan sus periodos de vacaciones, no permiten que existan vacíos que representen cambios en su actividad diaria.
- Cambian constantemente de lugar de residencia.
- Se ausentan del lugar de trabajo con frecuencia.
- Laboran más horas de las establecidas y concurren a la oficina en horarios no habituales.
- Asesores comerciales con desconocimiento de clientes frecuentes.
- Asesores comerciales que no soportan debidamente la información en las etapas de conocimiento y vinculación de clientes.

CONFIDENCIAL

- Asesores comerciales que vienen de otras entidades con clientes cautivos con manejo exclusivo y dedicado por parte de ellos.

15.2 SEGUIMIENTO ELECTRÓNICO DE LAS OPERACIONES

ACTIVOS DIGITALES S.A.S. cuenta con una plataforma tecnológica (SIT – Sistema Integrado de Transacciones), donde se realizan la totalidad de las transacciones (Ingresos y salidas de valores), detallando el monto, la cantidad, el origen, el destinatario, la ubicación, los códigos, etc., permitiendo con ello, establecer alertas de modo tal que el proceso de Riesgos y Seguridad realice el monitoreo diariamente con el fin de identificar posibles actividades sospechosas y así mismo reaccionar de manera oportuna evitando la materialización de estos riesgos.

16 REPORTE DE OPERACIÓN SOSPECHOSA (ROS) – UIAF

El reporte de operaciones Sospechosas es una herramienta primordial para poder contrarrestar acciones de Lavado de Activos y/o financian actividades del Terrorismo y otras acciones delictivas. Por esta razón se hace necesario hacer un reporte ante la entidad de control, de manera oportuna y clara, que facilite la evaluación de cada situación reportada y en ese mismo sentido, trasladar dicha información a las autoridades competentes encargadas de generar acciones de tipo judicial.

Para el cumplimiento de la claridad de la información reportada por parte de la Empresa, se hace imperativo que el comité de LA/FT tenga en cuenta las siguientes instrucciones para el diligenciamiento del reporte:

a) Se debe realizar una descripción de los hechos, de manera organizada, clara y completa, indicando (donde aplique) la forma en que se relacionan las personas naturales o jurídicas, no se puede olvidar suministrar los nombres y apellidos completos y/o identificación de las personas reportadas y en lo posible los datos de ubicación como ciudad, municipio, direcciones, teléfonos, etc.

b) Hay que tener en cuenta en la medida de lo posible un ordenamiento cronológico de los eventos y la participación de cada persona o agente, esto ayuda al entendimiento de los mismos.

c) Mencione las características de la operación por las cuales se considera como sospechosa. Adicionalmente, mencione cualquier irregularidad que haya detectado con las personas o transacciones implicadas en la operación sospechosa. No omita ningún dato conocido de la operación e indique cualquier hecho adicional que contribuya al análisis de la misma.

CONFIDENCIAL

d) Se debe sugerir la importancia del reporte (alta, media o baja), considerando los hechos y su similitud con tipologías conocidas de Lavado de Activos y Financiación del Terrorismo. Se deben considerar especialmente las tipologías identificadas por el GAFI (Grupo de Acción Financiera Internacional) y la UIAF.

e) Para determinar la importancia de la operación reportada, el comité de LA/FT considerar entre otras, la presencia de los siguientes elementos:

- Incremento patrimonial o de las operaciones no justificado o por fuera de los promedios del respectivo sector o actividad económica, de acuerdo con el SAGRILAFT implementado por la entidad.
- Presunto uso indebido de identidades, por ejemplo: uso de números de identificación inexistentes, números de identificación de personas fallecidas, suplantación de personas, alteración de nombres.
- Presentación de documentos o datos presuntamente falsos.
- Actuación en nombre de terceros y uso de empresas aparentemente de fachada.
- Relación con personas vinculadas o presuntamente vinculadas a actividades delictivas.
- Relación con bienes de presunto origen ilícito.
- Fraccionamiento y/o inusualidades en el manejo del efectivo.

f) Se debe identificar el reporte que se considera urgente, sugiriendo así la prontitud con la cual se debería actuar respecto del mismo. En tal sentido, por ejemplo, un reporte será urgente cuando:

- Sea inminente la disposición, transferencia o retiro de recursos vinculados a una presunta actividad de lavado de activos y/o financiación del terrorismo.
- Sea inminente el empleo de recursos en la realización de actividades terroristas u otras delictivas.
- Cuando sea imperativa, a juicio del comité de LA/FT, la intervención de las autoridades para evitar la disposición, transferencia o circulación de recursos, en cualquier forma, presuntamente vinculados a operaciones de lavado de activos y/o financiación del terrorismo.

CONFIDENCIAL

g) Realice una descripción de los hechos, de manera organizada, clara y completa, indicando (donde aplique) la forma en que se relacionan personas, productos financieros, transacciones, instituciones financieras y demás agentes de la operación sospechosa.

h) Tenga en cuenta en la medida de lo posible un ordenamiento cronológico de los eventos y la participación de cada persona o agente, si esto ayuda al entendimiento de los mismos.

i) Mencione las características de la operación por las cuales se considera como sospechosa.

j) Es oportuno mencionar cualquier irregularidad que se haya detectado con las personas o transacciones implicadas en la operación sospechosa.

k) Si la Empresa recibió alguna declaración, explicación, justificación u otro, que los implicados hayan dado y que se relacionen con la operación sospechosa, se debe mencionar e indicar la forma en que se hizo (escrita, verbal, a partir de un requerimiento formal de la Empresa, otros) y allegar los soportes correspondientes a la operación.

l) Precisar si se solicitó al cliente actualización de datos o aclaración sobre los hechos respectivos, e indicar la forma en que se hizo (escrita, verbal, a partir de un requerimiento formal de la Empresa, otros).

m) Mencionar si la operación sospechosa se relaciona con algún reporte realizado anteriormente por la Empresa o con otras operaciones.

n) Es importante no omitir ningún dato conocido de la operación y mencionar cualquier hecho adicional que pueda contribuir al análisis de la misma.

o) Tratándose de reportes referidos a clientes, se deben suministrar además los siguientes datos:

- Características y montos de los ingresos y egresos, así como la información patrimonial, en caso de poseerse.
- Descripción del perfil financiero del cliente de acuerdo con lo establecido en el Sistema de Administración de Riesgo LA/FT de la Empresa.
- Comparación del cliente con el sector económico al cual pertenece, de acuerdo con la segmentación contemplada en el Sistema de Administración de Riesgo LA/FT de la Empresa.
- Enunciar, además de los productos vinculados a la operación sospechosa, los otros que posea el cliente en la Empresa, distinguiendo entre unos y otros.

p) Se debe indicar el procedimiento empleado para la detección de la operación reportada, ilustrando los motivos por los cuales fue inicialmente calificada como inusual y las razones

CONFIDENCIAL

por las cuales se determinó que era sospechosa. Si el procedimiento lo incluyó, se debe enunciar la tipología identificada o la señal de alerta activada en el Sistema de Administración de Riesgo LA/FT de la Empresa.

q) Finalmente, la Empresa debe relacionar los soportes correspondientes que expliquen la operación reportada. Esta información puede consistir en soportes de pago de premios, soportes de compra de fichas, documentos de vinculación a la Empresa (formularios y anexos), declaraciones de cambio, declaraciones de importaciones, declaraciones de exportaciones, contratos del cliente, entre otros.

17 SANCIONES Y PENALIDADES

- El incumplimiento de las políticas y directrices aquí establecidas por parte de los colaboradores de la Empresa, pueden acarrear las sanciones de acuerdo lo establecido en el Código Sustantivo Laboral Colombiano y el Reglamento Interno de Trabajo de la Empresa, sin perjuicio de las consecuencias de tipo legal a que hubiere lugar.

- El representante legal y el comité disciplinario son la autoridad máxima al interior de la Empresa, responsable de deliberar sobre las conductas de incumplimiento por parte de colaboradores y en ese mismo sentido determinar el tipo de sanción a que haya lugar.

ELABORO	REVISO	APROBÓ
Héctor Fabio Blandón Posada Oficial de Cumplimiento	**Norman Xavier Luna** Representante Legal **Daniela Velásquez** Representante Legal (S)	**Norman Xavier Luna** Representante Legal **Daniela Velásquez** Representante Legal (S)

CONFIDENCIAL

FECHA 13 de feb. de 2024	**FECHA** 13 de feb. de 2024	**FECHA** 13 de feb. de 2024

CONFIDENCIAL