



**VIGILANCIA  
ACOSTA LTDA.**

una empresa del  **grupo altum**

# **MANUAL DEL SISTEMA INTEGRAL DE PREVENCIÓN Y CONTROL DEL RIESGO DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO (SIPLAFT) GI-MN-02**

<b>CONTROL DE CAMBIOS</b>		
<b>FECHA</b>	<b>VERSIÓN</b>	<b>DESCRIPCIÓN</b>
16/02/2018	00	Elaboración del documento
01/05/2020	01	Actualización logo y esquema del documento

<b>REVISÓ</b>	<b>APROBÓ</b>
<b>William Aponte</b> Oficial de Cumplimiento	<b>Harold Castaño Celis</b> Representante Legal
Documento aprobado mediante Acta No. 161 del 2018	

## TABLA DE CONTENIDO

	<b>Pág.</b>
1. OBJETIVO	3
2. ALCANCE	3
3. DEFINICIONES	3
4. POLÍTICAS	6
4.1. Metodología de implementación del SIPLAFT	6
4.2. Políticas para la prevención y control del riesgo de LA/FT	6
4.3. Comunicación de la política	7
5. PROCEDIMIENTOS PARA LA PREVENCIÓN Y CONTROL DEL RIESGO DE LA/FT	7
5.1. Procedimiento para la gestión del riesgo de LA/FT	7
5.1.1. Identificación	7
5.1.2. Análisis / Evaluación	8
5.1.3. Tratamiento	9
5.1.4. Monitoreo	10
5.2. Atención de solicitudes de autoridades competentes	10
5.3. Conocimiento de clientes y proveedores	10
5.3.1. Proveedores	11
5.3.2. Clientes	11
5.3.3. PEPs	12
5.4. Conocimiento de socios	12
5.5. Conocimiento de los empleados	12
5.6. Determinación del monto máximo de efectivo	14
5.7. Procedimiento para el control del riesgo de LA/FT	14
5.7.1. Herramientas para identificar Operaciones Inusuales o Sospechosas	14
5.7.1.1. Identificación de Operaciones Sospechosas	14
5.7.1.2. Recolectar información y reportar la Operación Sospechosa	14
5.7.2. Reportes a la UIAF	15
5.7.2.1. Reportes de Operaciones Intentadas y Operaciones Sospechosas	15
5.7.2.2. Reportes de transacciones en efectivo	16
5.7.2.3. Otros reportes	16
5.7.2.4. Responsabilidad del reporte	16
6. FUNCIÓN DE LOS ADMINISTRADORES DEL SIPLAFT	16
7. ESTRUCTURA ORGANIZACIONAL	18
8. SANCIONES	18
9. PROGRAMAS DE CAPACITACIÓN	19
10. DOCUMENTACIÓN	19
11. DOCUMENTOS RELACIONADOS	20
12. CONTROL DE CAMBIOS	20

## **MANUAL DEL SISTEMA INTEGRAL DE PREVENCIÓN Y CONTROL DEL RIESGO DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO (SIPLAFT)**

### **1. OBJETIVO**

Establecer los lineamientos y controles adoptados por VIGILANCIA ACOSTA LTDA que permitan prevenir y minimizar la probabilidad de pérdida o daño en que pueda incurrir la empresa por su propensión a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas.

### **2. ALCANCE**

Los elementos descritos en el presente documento contienen todos los lineamientos establecidos frente a la Prevención y Control del Riesgo de Lavado de Activos y Financiación del Terrorismo los cuales son aplicables a todas las actividades realizadas por VIGILANCIA ACOSTA LTDA en desarrollo de su objeto social.

### **3. DEFINICIONES**

Actividades ilícitas: Son aquellas conductas o actividades que de conformidad con una norma vigente ostentan el carácter de ilícitas, esto es, contra derecho.

Administradores: De conformidad al artículo 22 de la Ley 222 de 1995, son administradores, el representante legal, el liquidador, el factor, los miembros de juntas o consejos directivos y quienes de acuerdo con los estatutos ejerzan o detenten esas funciones.

Contraparte: Personas naturales o jurídicas con las cuales VIGILANCIA ACOSTA LTDA tiene vínculos de negocios, contractuales o jurídicos de cualquier orden (accionistas, socios, empleados, clientes y proveedores de bienes y/o servicios).

Control del riesgo de LA/FT: Comprende la implementación de políticas, procesos, prácticas u otras acciones existentes que actúan para minimizar el riesgo LA/FT en las operaciones, negocios o contratos que realice la organización.

Debida diligencia: Equivale a ejecutar algo con suficiente cuidado. 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. También es definida como el conjunto de procesos necesarios para poder adoptar decisiones suficientemente informadas.

Evento: Incidente o situación de LA/FT que ocurre en la organización durante un intervalo particular de tiempo.

Financiación del terrorismo: Delito que comete toda persona que incurra en alguna de las conductas descritas en el artículo 345 del Código Penal, modificado por el artículo 16 de la Ley 1453 de 2011.

Fuentes de riesgo: Son los agentes generadores de riesgo de LA/FT en una organización y se deben tener en cuenta para identificar las situaciones que puedan generarle este riesgo en las operaciones, negocios o contratos que realiza.

Gestión del riesgo de LA/FT: Consiste en la adopción de políticas que permitan prevenir y controlar el riesgo LA/FT.

Grupo de Acción Financiera Internacional (GAFI): Organismo intergubernamental cuyo propósito es elaborar y promover medidas para combatir el lavado de activos.

Herramientas: Son los medios que utiliza la organización para prevenir que se presente el riesgo de LA/FT y para detectar operaciones intentadas, inusuales o sospechosas. Dentro de dichas herramientas se deben mencionar, entre otras, las señales de alerta, indicadores de operaciones inusuales, programas para administración de riesgos organizacionales y hojas electrónicas de control.

LA/FT: Lavado de Activos y Financiación del Terrorismo.

Lavado de activos: 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, modificado por el artículo 33, Ley 1474 de 2011, modificado por el artículo 11, Ley 1762 de 2015.

Listas restrictivas nacionales e internacionales: Relación de personas y organizaciones que de acuerdo con el organismo que las publica, pueden estar vinculadas con actividades de lavado de activos o financiación del terrorismo, como lo son las listas del Consejo de Seguridad de las Naciones Unidas, que son vinculantes para Colombia. Adicionalmente, pueden ser consultadas por Internet las listas OFAC, Interpol, Policía Nacional, entre otras.

Monitoreo: Es el proceso continuo y sistemático mediante el cual se verifica la eficiencia y la eficacia de una política o de un proceso, mediante la identificación de sus logros y debilidades para recomendar medidas correctivas tendientes a optimizar los resultados esperados. Es condición para rectificar o profundizar la ejecución y para asegurar la retroalimentación entre los objetivos, los presupuestos teóricos y las lecciones aprendidas a partir de la práctica.

Operación intentada: Se configura cuando se tiene conocimiento de la intención de una persona natural o jurídica de realizar una operación sospechosa, pero no se perfecciona por cuanto quien intenta llevarla

a cabo desiste de la misma o porque los controles establecidos o definidos por la organización no permitieron realizarla. Estas operaciones también deberán reportarse de forma inmediata a la UIAF.

Operación inusual: Es aquella cuya cuantía o características que no guardan relación con la actividad económica ordinaria o normal de la organización o, que por su número, cantidad o características no se ajusta a las pautas de normalidad establecidas por la organización para un sector, una industria o una clase de contraparte.

Operación sospechosa: Es aquella que por su número, cantidad o características no se enmarca dentro de los sistemas y prácticas normales de los negocios, de una industria o de un sector determinado y, además, que de acuerdo con los usos y costumbres de la actividad que se trate, no ha podido ser razonablemente justificada. Cuando se detecten esta clase de operaciones, deben ser reportadas de manera inmediata a la UIAF.

Personas Expuestas Políticamente (PEPs): Son personas nacionales o extranjeras que por razón de su cargo manejan recursos públicos, o tienen poder de disposición sobre estos o gozan de reconocimiento público. Las PEP extranjeras son individuos que cumplen o a quienes se les han confiado funciones públicas prominentes en otro país, como por ejemplo los Jefes de Estado o de Gobierno, políticos de alto nivel, funcionarios gubernamentales o judiciales de alto nivel o militares de alto rango, ejecutivos de alto nivel de corporaciones estatales, funcionarios de partidos políticos importantes. Las PEP domésticas son individuos que cumplen o a quienes se les han confiado funciones públicas prominentes internamente, como por ejemplo los Jefes de Estado o de Gobierno, políticos de alto nivel, funcionarios gubernamentales o judiciales de alto nivel o militares de alto rango, ejecutivos de alto nivel de corporaciones estatales, funcionarios de partidos políticos importantes. Las personas que cumplen o a quienes se les han confiado funciones prominentes por una organización internacional se refiere a quienes son miembros de la alta gerencia, es decir, directores, subdirectores y miembros de la junta o funciones equivalentes.

Políticas: Son los lineamientos, orientaciones o aspectos que fundamentan la prevención y el control del riesgo de LA/FT en la organización. Deben hacer parte del proceso de gestión del riesgo de LA/FT.

Reportes externos: Son reportes que deben hacer las organizaciones ante la UIAF, esto es, ROS (negativos o positivos) y transacciones en efectivo (negativas y positivas).

Reportes internos: Son aquellos que se manejan al interior de la empresa y pueden ser efectuados por cualquier empleado o miembro, que tenga conocimiento de una posible operación inusual o sospechosa.

Riesgo de LA/FT: Es la posibilidad de pérdida o daño que puede sufrir una organización al ser utilizada para cometer los delitos de lavado de activos o financiación del terrorismo.

Señales de alerta: Hechos, situaciones, eventos, cuantías, indicadores cuantitativos y cualitativos, razones financieras y demás información que la entidad determine como relevante, a partir de los cuales

se puede inferir oportuno y/o prospectivamente la posible existencia de un hecho o situación que escapa a lo que la organización determine como normal.

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 como objetivo la prevención y detección de operaciones que puedan ser utilizadas para el lavado de activos o la financiación del terrorismo.

#### 4. POLÍTICAS

##### 4.1. Metodología de implementación del SIPLAFT

- El SIPLAFT implementado en VIGILANCIA ACOSTA LTDA está fundamentado en la metodología de Administración de Riesgos adoptada por la empresa la cual se encuentra formalizada a través del documento PA-MSIPLAFT-01– Manual de Administración de Riesgos de Vigilancia Acosta Ltda.

##### 4.2. Políticas para la prevención y control del riesgo de LA/FT

VIGILANCIA ACOSTA LTDA implementará los lineamientos, reglas de conducta y procedimientos que orientarán su actuación con miras a evitar situaciones vulnerables para la consolidación de delitos LA/FT. Dichas políticas se deben traducir en una administración de riesgos que contemple lo siguiente:

- El SIPLAFT será de conocimiento de todos los funcionarios de VIGILANCIA ACOSTA LTDA, para lo cual el Oficial de Cumplimiento determinará los medios para el efecto y las modalidades para su actuación.
- El SIPLAFT, aplicará en el contexto interno y externo de VIGILANCIA ACOSTA LTDA tanto en lo misional como en los procesos de apoyo administrativo.
- Los trabajadores de VIGILANCIA ACOSTA LTDA deben asegurar el cumplimiento del presente Manual, para prevenir y controlar conductas relacionadas con la ocultación o legalización de delitos de LA/FT y, con ello minimizar riesgos en las operaciones de la empresa.
- Los procedimientos que se implementen son de obligatoria observancia para todos los trabajadores de VIGILANCIA ACOSTA LTDA. Estos procedimientos permiten identificar operaciones inusuales o sospechosas.
- Todos los trabajadores y directivos de VIGILANCIA ACOSTA LTDA., deben reportar en forma inmediata al Oficial de Cumplimiento, los hechos o circunstancias que consideren vulneradoras de una adecuada Administración de Riesgo de LA/FT.
- La inobservancia de estas medidas dará lugar a los procedimientos disciplinarios internos previstos, sin perjuicio de las actuaciones ante los organismos de control y judiciales a que haya lugar.
- VIGILANCIA ACOSTA LTDA, aplicará la reserva de información de acuerdo a las normas actuales.

- El SIPLAFT al generar información en forma oportuna para atender las demandas de información interna y de los órganos de control, tendrá un carácter prioritario en su operación y la consolidación de la información que produce.
- VIGILANCIA ACOSTA LTDA., se abstendrá de ejercer cualquier actividad comercial, sin importar su cuantía, con personas jurídicas o naturales vinculadas a actividades ilícitas; adicionalmente prohibirá las operaciones, actividades, negocios o contratos sin el debido reconocimiento de los clientes.
- La Junta Directiva, Gerencia General, el Oficial de Cumplimiento y demás empleados de VIGILANCIA ACOSTA LTDA., responderán por las obligaciones y responsabilidades que les sean aplicables en lo referente a la aplicación del SIPLAFT.
- Se observará la prudencia y secreto para con los empleados en lo referente a la información remitida a la UIAF sobre las operaciones que se consideren sospechosas.
- Todos los funcionarios de VIGILANCIA ACOSTA LTDA., tiene la obligación de leer, comprender y poner en práctica los procedimientos contenidos en el presente Manual.
- Se debe anteponer la observancia de los principios éticos y el cumplimiento de las normas antes que el logro de las metas de los servicios.

#### **4.3. Comunicación de la política**

Las políticas y procedimientos descritos en el presente documentos serán comunicados a todos los empleados, socios, directivos y demás partes interesadas a través de los medios establecidos para ello como lo son intranet, correo electrónico institucional, capacitación y demás que VIGILANCIA ACOSTA LTDA., disponga para tal fin.

### **5. PROCEDIMIENTOS PARA LA PREVENCIÓN Y CONTROL DEL RIESGO DE LA/FT**

#### **5.1. Procedimiento para la gestión del riesgo de LAFT**

La administración de eventos de riesgo de LA/FT se realizará alineado con la metodología de administración de riesgos adoptada por VIGILANCIA ACOSTA LTDA., y documentado en los formatos establecidos para tal fin (Documento maestro gestión de riesgo).

La metodología contempla las etapas descritas a continuación<sup>1</sup>:

##### **5.1.1. Identificación**

- 
- <sup>1</sup> El detalle de la metodología para la gestión del riesgo puede ser consultado en el documento PA-MSIPLAFT-01– Manual de Administración de Riesgos de Vigilancia Acosta Ltda.

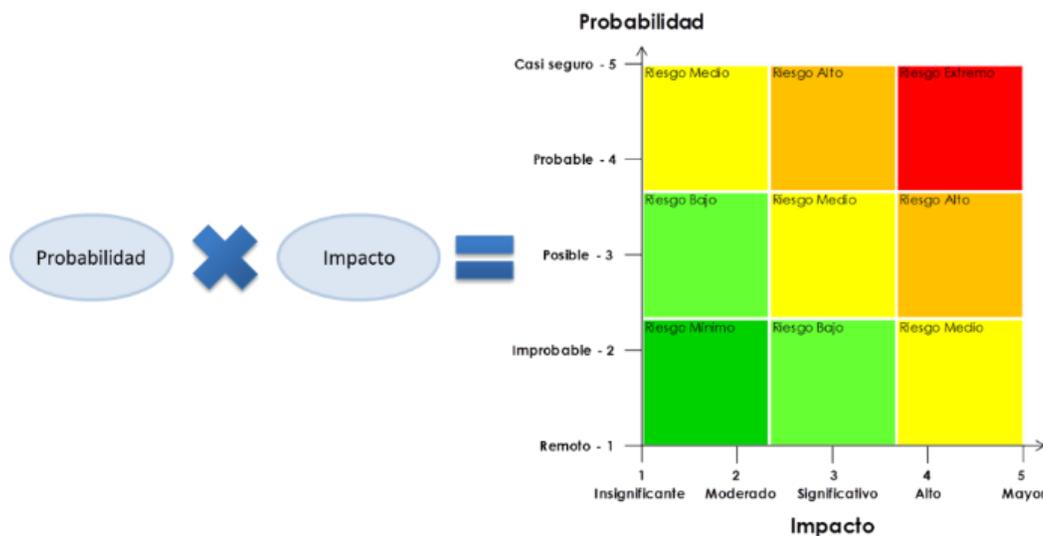
Reconocer los eventos de riesgo de LA/FT asociados al desarrollo del objeto de negocio de la Organización en cada uno de sus procesos.

### 5.1.2. Análisis / Evaluación

Medir la probabilidad y el impacto de ocurrencia de los eventos de riesgo de LA/FT identificados.

VIGILANCIA ACOSTA LTDA., realiza una medición semi-cuantitativa, ya que combina variables cualitativas y cuantitativas, para establecer la probabilidad y el impacto de la potencial materialización del riesgo.

La combinación de Probabilidad e Impacto dará lugar a la valoración del riesgo así:



Para la medición del nivel de riesgo inherente como residual de cada uno de los riesgos identificados, se deberá evaluar su probabilidad e impacto. Como resultado de esta etapa se realiza la medición del riesgo, teniendo en cuenta las siguientes consideraciones:

**Medición Riesgo Inherente:** El riesgo inherente es la medición de los riesgos propios sin tener en cuenta el efecto de los controles. La consolidación de los riesgos inherentes identificados, generan el perfil de riesgo inherente.

**Medición Riesgo Residual:** El riesgo residual es el nivel restante de riesgo luego de evaluar la efectividad de los controles. La medición del riesgo residual se hará una vez se haya evaluado los controles, utilizando como base la siguiente matriz de calificación de riesgo residual.

	PRIMER CONTROL				SEGUNDO CONTROL			
	BAJO	MEDIO	ALTO	EXTREMO	BAJO	MEDIO	ALTO	EXTREMO
<b>Fuerte</b>	MÍNIMO	BAJO	MEDIO	ALTO	MÍNIMO	MÍNIMO	BAJO	MEDIO
<b>Moderado</b>	MÍNIMO	BAJO	MEDIO	EXTREMO	MÍNIMO	BAJO	MEDIO	ALTO
<b>Débil</b>	BAJO	MEDIO	ALTO	EXTREMO	BAJO	MEDIO	ALTO	EXTREMO

### 5.1.3. Tratamiento

Implementar medidas de control a fin de mitigar el riesgo.

Con base en lo anterior, se seleccionan e implementan medidas o planes de tratamiento para modificar el nivel de riesgo, bien sea actuando sobre un impulsor de riesgos, actuando sobre el control actual y/o incrementando los controles.

A continuación se definen las opciones de tratamiento de los riesgos:

Opciones para el Tratamiento del Riesgo		Tipo de Control	Concepto	Características
EVITAR			Es eludir el riesgo, decidiendo no ejecutar la actividad o eliminando el escenario, al cual está asociado el riesgo.	No siempre es aplicable por las características del escenario analizado. Esta opción es riesgos puede adoptarse desconociendo o calculando mal los beneficios de la actividad eliminada frente al riesgo para evitarlo.
CONTROLAR	Disminuir Probabilidad	Controles Preventivos	Atacan los factores de riesgo para evitar que la amenaza se materialice, es decir, para evitar que el riesgo se presente.	Controlar un riesgo implica implementar controles para minimizar o eliminar sus componentes, es decir su probabilidad y su impacto.
	Mitigar Impacto (Consecuencia)	Controles Detectivos	Registran la materialización de la amenaza, es decir, la ocurrencia del riesgo.	
		Controles Correctivos	Actúan directamente en la reducción de las pérdidas y se complementan con los controles detectivos.	

ACEPTAR	Es la decisión consciente de la entidad de tomar el riesgo, bien sea porque este tiene un nivel de severidad aceptable o porque la relación costo / beneficio de los controles no es óptima.	
TRANSFERIR	Es la decisión de entregarle a un tercero parte o la totalidad del riesgo, para que éste lo asuma.	

Los planes derivados del tratamiento del riesgo son registrados en la matriz de riesgo, documentando la actividad a realizar, responsable, las fechas de implementación y seguimiento hasta el cierre de la acción de mejora.

#### 5.1.4. Monitoreo

Es la verificación periódica de los elementos del sistema para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos.

En esta etapa se realizan las siguientes actividades:

- Evaluación periódica de los controles y de las exposiciones a eventos de riesgo operativo.
- Identificación de los niveles de riesgos residuales y de los niveles aceptables establecidos por la Organización.
- Monitorear el funcionamiento del proceso (actividades y controles) para establecer cambios en el mismo y consecuencias sobre el perfil de riesgo.
- Actualización periódica de los perfiles de riesgo y de las exposiciones a eventos de riesgo operativo.

El monitoreo es realizado a la totalidad de los procesos con una periodicidad anual.

#### 5.2. Atención de solicitudes de autoridades competentes

VIGILANCIA ACOSTA LTDA., atenderá a través del Oficial de Cumplimiento la entrega oportuna y veraz de la información que soliciten las autoridades competentes (UIAF, Fiscalía, DIAN, entre otros) en conjunto con el Revisor Fiscal y/o la Junta Directiva.

#### 5.3. Conocimiento de clientes y proveedores

VIGILANCIA ACOSTA LTDA., realizará el conocimiento de clientes, proveedores, terceros o contrapartes de acuerdo a los lineamientos establecidos al interior de sus procesos de tal manera que le permita acreditar una debida diligencia y cumplimiento de los requerimientos emitidos por los organismos de control frente a la gestión y prevención del riesgo de LA/FT. Para esto VIGILANCIA ACOSTA LTDA.,

verificará la identidad de todos sus clientes y proveedores mediante la revisión de la información que estime conveniente para tal fin. Dicha verificación deberá quedar debidamente documentada con fecha y hora de análisis para efectos probatorios de debida diligencia.

Lo descrito anteriormente, se encuentra formalizado al interior de VIGILANCIA ACOSTA LTDA., mediante los procedimientos relacionados a continuación los cuales permiten efectuar un seguimiento al comportamiento de los vinculados logrando identificar señales de alerta u operaciones inusuales por parte de clientes o proveedores.

### 5.3.1. Proveedores

El procedimiento ha establecido para su proceso de vinculación de proveedores / contratistas las siguientes actividades:

- El proveedor / contratista debe diligenciar el formato PA-MSIPLAFT-01-F02 – Identificación de proveedores. anexando la siguiente documentación la cual será revisada y verificada:
  - Original del certificado de existencia y representación legal expedido por la Cámara de Comercio o por la entidad competente (vigencia no superior a tres meses).
  - Fotocopia del número de identificación tributaria NIT o documento de identidad.
  - Fotocopia documento de identidad del representante legal.
- El posible proveedor será consultado en listas restrictivas.
- La verificación de la documentación debe quedar soportada por quien realiza la consulta con firma, fecha y hora.

La actualización de la información de proveedores se realizará con una periodicidad semestral para proveedores críticos, o anual para proveedores con una evaluación de criticidad media o baja.

### 5.3.2. Clientes

El procedimiento ha establecido las siguientes actividades para la verificación y registro de clientes:

- Solicitar el diligenciamiento por parte del cliente del formato PA-MSIPLAFT-01-F01 Registro información de clientes.
- Solicitar al cliente los documentos que acrediten su existencia y representación legal.
- Una vez recolectada la información anteriormente mencionada y con el fin de verificar los antecedentes comerciales de los potenciales clientes, se lleva a cabo la verificación en la base de datos del software adquirido para tal fin (software de consulta de 1.817 listas a nivel mundial), cuyo resultado se registra en la casilla correspondiente en el formato PA-MSIPLAFT-01-F01 Registro información de clientes; en caso que un cliente aparezca reportado, VIGILANCIA ACOSTA LTDA., se

abstendrá automáticamente de continuar con el trámite de formalización del contrato u oferta comercial.

- Anualmente se verifica la base de datos del software de los clientes actuales de la organización, para lo cual se toma como base de consulta un certificado de existencia y representación legal expedido por la autoridad competente, cuyo resultado se registra en el formato PA-MSIPLAFT-01-F03 - Actualización información de clientes.
- Los clientes de origen público se excluyen de la aplicación del procedimiento de selección de cliente, ya que se presume su honorabilidad por su misma naturaleza, es por ello que no se diligencia el formato PA-MSIPLAFT-01-F01 Registro información de clientes.

### 5.3.3. PEPs:

Para el caso de posibles vinculados que por su perfil o razón de su cargo manejan recursos públicos, ostentan algún grado de poder público o gozan de reconocimiento público o por las funciones que desempeñan tengan algún grado de impacto social (PEPs) que puedan exponer en mayor grado de riesgo de LA/FT a VIGILANCIA ACOSTA LTDA, la decisión de establecer la relación deberá ser tomada por la Junta Directiva o Representante Legal contando con información suficiente que respalde el origen de los recursos.

### 5.4. Conocimiento de socios

Frente al conocimiento de los socios, VIGILANCIA ACOSTA LTDA., mantendrá actualizada la información de los miembros de la Junta de Socios. Cuando ingresen o se generen cambios en los socios se deberá tener los siguientes controles con el fin de garantizar la seguridad en la empresa:

- Documento de identidad.
- Verificación en listas.
- Verificación de procedencia de recursos.

Para verificar la procedencia de recursos del socio se deben solicitar los soportes de declaración de renta o escrituras de propiedades, certificados bancarios, entre otros.

La periodicidad del control establecida es al ingreso del socio y actualización cada año. El estudio de seguridad deberá contener la fecha, hora y firma de la persona que lo realizó.

## 5.5. Conocimiento de los empleados

Para el conocimiento de sus empleados VIGILANCIA ACOSTA LTDA., establece los mecanismos descritos a continuación para la verificación de los antecedentes de los trabajadores y/o candidatos:

- Todo aspirante debe pasar por estudio de seguridad consistente en: establecimiento de plena identidad, verificación de certificado de la PONAL, del certificado de la PROCURADURIA, verificación de documentos de estudio, verificación de documentos de identificación, referenciación en empresas, visita domiciliaria, prueba de polígrafo según el caso y exámenes médicos de ingreso y complementarios según el caso. Los responsables del proceso deben velar porque cada fase esté debidamente documentado a través de los formatos normalizados.
- Únicamente inician proceso de selección los aspirantes que cuenten con los siguientes registros, salvo los autorizados por la Gerencia de Talento Humano o por el cliente de manera escrita:
  - Curso VIGENTE del cargo a que aspiran.
  - Hoja de vida (1003 en el caso de aspirantes a cargos operativos).
  - Originales de los documentos de identificación, estudios y formación conforme el perfil del cargo al cual aspiran.
  - Originales de referencias laborales.
  - Certificación original y vigente de antecedentes judiciales de la PONAL y PROCURADURIA GENERAL DE LA NACIÓN.
  - Extracto de hoja de vida militar o de PONAL en el caso de personal retirado o con asignación de retiro, para quienes además se exigirá la resolución de retiro antes de la firma de contrato en caso de ser seleccionado.
- Si el aspirante está optando por un cargo cuyas funciones incluyan conducción, debe presentar la licencia de conducción vigente y el Departamento de Selección a través de su delegado debe llevar a cabo la verificación de multas y comparendos y estado de la licencia en los portales de SIMIT, RUNT y MOVILIDAD. En todos los casos debe presentar prueba de conducción y los exámenes médicos complementarios que se requieran.
- Según el cargo a desempeñar, los resultados obtenidos inicialmente por el aspirante y solicitudes expresas del cliente, se hará necesario profundizar en la verificación de confiabilidad del personal a través de otros sistemas complementarios como polígrafo, V.S.A. o estudio económico (centrales de riesgo).
- Los responsables del proceso de selección deben garantizar la ejecución de visitas domiciliarias y prueba de poligrafía pre empleo para el personal de cargos críticos, para el personal de sector aeroportuario y para el personal de otros sectores siempre si aplica.

Cualquier señal de alerta identificada que se vincule con comportamientos asociados al riesgo LA/FT debe ser canalizada al Oficial de Cumplimiento quien deberá gestionar al interior lo pertinente frente a las entidades de vigilancia, control y policía judicial, según sea el caso, bajo los parámetros de las normas colombianas y el código penal colombiano.

## **5.6. Movimientos de dinero**

VIGILANCIA ACOSTA LTDA., tiene establecido que los movimientos de dinero, tanto ingresos como egresos deben realizarse por medio de las entidades financieras, el uso de dinero en efectivo es una excepción, el cual debe encontrarse debidamente soportado y autorizado por la Gerencia Administrativa y Financiera y/o Gerencia General.

## **5.7. Procedimientos para el control del riesgo de LA/FT**

### **5.7.1. Herramientas para identificar Operaciones Inusuales o Sospechosas**

VIGILANCIA ACOSTA LTDA., ha establecido las siguientes actividades a seguir en la organización para realizar el control y manejo de las Operaciones Inusuales o Sospechosas, tanto para operaciones y procedimientos a nivel interno como externo.

#### **5.7.1.1. Identificación de Operaciones Sospechosas**

Cualquier empleado de VIGILANCIA ACOSTA LTDA., tiene la responsabilidad de reportar al Oficial de Cumplimiento operaciones sospechosas, para los cuales se pueden identificar señales de alerta frente al personal (clientes, empleados o proveedores) como las siguientes:

- Reportado en listas restrictivas o vinculantes.
- Presenta vínculos con delincuentes.
- Presenta incremento patrimonial injustificado.
- Presenta fraccionamientos frecuentes en sus operaciones financieras.
- Presenta altas operaciones en efectivo no acordes con su estructura financiera.
- Cambios repentinos en su forma de actuar.
- Cambios repentinos en su estilo de vida y adquisición de bienes por encima de los ingresos.
- Operaciones realizadas con monedas virtuales.
- Operaciones en las que se detecta que la persona que está solicitando el servicio de vigilancia está actuando a nombre de un tercero.
- Solicitud de servicio de vigilancia por parte de personas naturales o jurídicas con escaso capital o sin aparente capacidad económica para poder solicitar dicho servicio.
- Solicitud de servicios por personas con domicilio aparentemente falsos.

- Pagos de valor significativo mediante la utilización de recursos en efectivo no acordes con su estructura financiera.
- Contratos y acuerdos con proveedores y clientes sin la debida autorización.
- Intentos de soborno u ofrecimientos de dádivas con el fin de otorgar servicios.
- Presionar o amenazar a funcionarios para que no cumplan con la reglamentación en cuanto a la vinculación de clientes nuevos dentro de la organización.
- Proveedores que ofrezcan descuentos inusuales o fuera de las condiciones de mercado.

#### **5.7.1.2. Recolectar información y reportar la Operación Sospechosa**

Cuando se identifique alguna de estas conductas se debe proceder a recopilar la máxima información disponible que permita soportar la novedad. Posteriormente se debe remitir dicha información al Oficial de Cumplimiento quien deberá asegurar la confidencialidad, disponibilidad y completitud de la misma, así como la verificación y reporte a las unidades de control si así lo requiere.

La información mínima que debe relacionarse en el reporte es la siguiente:

- Fecha en la que se envía el reporte.
- Ciudad donde se elabora el reporte.
- Persona / Funcionario / Cliente según corresponda.
- Número de Identificación (Si se tiene).
- Redacción con el mayor detalle posible de los hechos o indicios que lo motivaron a reportar la operación como sospechosa. ¿Qué observó y que le causó curiosidad o inquietud?

El reporte se debe realizar a través de los correos electrónicos: [waponte@grupoaltum.com.co](mailto:waponte@grupoaltum.com.co) y [alara@grupoaltum.com.co](mailto:alara@grupoaltum.com.co)

#### **5.7.2. Reportes a la UIAF**

##### **5.7.2.1. Reportes de Operaciones Intentadas y Operaciones Sospechosas – ROS**

Si se llegara a tener conocimiento de una operación sospechosa o una operación intentada en la medida de lo posible debería reportarse como ROS directamente a la UIAF de manera inmediata a través de los medios establecidos.

Se debe entender por inmediato el momento a partir del cual la empresa toma la decisión de catalogar la operación como intentada o sospechosa. Para tal efecto no se necesita que la empresa tenga certeza de que se trata de una actividad delictiva ni de identificar el tipo penal o de verificar que los recursos tienen origen ilícito; tan solo se requiere que la operación sea sospechosa de acuerdo a lo definido en el presente documento.

Si no se presentan operaciones sospechosas en el trimestre de presentación del Reporte de Operaciones Sospechosas se generará un reporte de operaciones sospechosas negativas.

Los soportes de la operación reportada se deben organizar y conservar como mínimo por cinco (5) años, dado que pueden ser solicitados por las autoridades competentes.

#### **5.7.2.2. Reportes de transacciones en efectivo**

Las operaciones en efectivo de clientes externos con VIGILANCIA ACOSTA LTDA., son de giro ordinario de los negocios y son por montos menores. Las transacciones en efectivo frente a otros clientes usualmente se canalizan a través del sistema financiero por lo cual de conformidad con las normas vigentes no deben ser reportados.

Si excepcionalmente se llegaren a realizar transacciones en efecto que ameriten ser reportadas, se deben hacer los reportes que requieran las autoridades competentes.

#### **5.7.2.3. Otros reportes**

Los anteriores reportes y los demás que de acuerdo con su competencia exija la Unidad de Información y Análisis Financiero (UIAF) deberán ser remitidos a esa entidad en la forma y bajo las condiciones que ella establezca.

#### **5.7.2.4. Responsabilidad del reporte**

Será responsabilidad del Oficial de Cumplimiento todos los reportes que se envíen a los entes internos y externos de VIGILANCIA ACOSTA LTDA., asociados con el riesgo de LA/FT.

### **6. FUNCIÓN DE LOS ADMINISTRADORES DEL SIPLAFT**

Sin perjuicio de las funciones y responsabilidades consignadas en la ley y los administradores (Junta Directiva y Representante Legal) y los órganos de administración y control tienen las siguientes funciones específicas en relación con el Sistema Integral de Prevención y Control del Riesgo de Lavado de Activos y Financiación del Terrorismo (SIPLAFT):

- Junta Directiva:
  - Fijar las políticas, definir los mecanismos, instrumentos y los procedimientos que se aplicarán en la empresa y los demás elementos que integren el SIPLAFT.
  - Nombrar al Oficial de Cumplimiento y su respectivo Suplente.

- Pronunciarse sobre los informes presentados por el Oficial de Cumplimiento, Revisor Fiscal y la Auditoría Interna, realizando seguimiento a las observaciones o recomendaciones adoptadas, dejando constancia en actas.

- Representante Legal:

El Representante Legal, como ejecutor de las decisiones de la Asamblea General y de la Junta Directiva tiene a su cargo las siguientes funciones relacionadas con el SIPLAFT:

- Verificar que los procedimientos establecidos, desarrollan las políticas aprobadas por la Junta Directiva.
- Disponer de los recursos técnicos y humanos para implementar y mantener en funcionamiento el SIPLAFT, según la aprobación impartida por la Junta directiva.
- Brindar el apoyo que requiera el Oficial de Cumplimiento.
- Verificar la adopción y funcionamiento de los procedimientos definidos para el adecuado manejo, conservación y archivo de los documentos y reportes relacionados con el SIPLAFT y garantizar la confidencialidad de la dicha información.

- Revisor Fiscal:

- Cerciorarse de que las operaciones, objeto social y contratos que celebre o cumpla la empresa, se ajustan a las instrucciones y políticas aprobadas por el máximo órgano social.
- Deberá poner en conocimiento del Oficial de Cumplimiento, las inconsistencias y falencias que detecte respecto a la implementación del SIPLAFT o de los controles establecidos.

- Oficial de Cumplimiento:

La empresa tiene como obligación la designación de un Oficial de Cumplimiento y un suplente el cual debe cumplir con los siguientes requisitos:

- Pertener al segundo nivel jerárquico dentro de la estructura administrativa de la empresa.
- Ser nombrado por la Junta Directiva.
- Contar con el efectivo apoyo de los órganos de administración de la empresa.

El Oficial de Cumplimiento debe cumplir como mínimo con las siguientes funciones:

- Verificar el cumplimiento de las disposiciones legales para la prevención de lavado de activos y financiación del terrorismo.

- Diseñar e implementar los procedimientos y puntos de control para la adecuada prevención del blanqueo de capitales y financiación del terrorismo.
  - Realizar el seguimiento de la debida implementación de los mecanismos e instrumentos del Sistema Integral de Prevención de Lavado de Activos y Financiación del Terrorismo.
  - Contar con una evaluación periódica de las medidas adoptadas en el SIPLAFT, especialmente, sobre la información suministrada por los clientes activos en desarrollo de las actividades económicas.
  - Enviar los Reportes de Operaciones Sospechosas (ROS) a la Unidad de Información y Análisis Financiero (UIAF), una vez se haya realizado la respectiva valoración del ROS.
  - Informar a las directivas sobre fallas u omisiones en los controles del SIPLAFT que vincule responsabilidad de funcionarios de la sociedad.
  - Capacitar a todos los niveles de la organización para que los funcionarios tengan claridad sobre el papel que deben desempeñar en la gestión del riesgo de lavado de activos.
  - Atender y brindar respuesta oportuna a los requerimientos de las autoridades competentes en materia de prevención y control de lavado de activos y financiación del terrorismo.
  - Mantener actualizados los documentos que contengan las políticas y procedimientos del SIPLAFT.
  - Presentar semestralmente un informe de gestión a la Junta de Socios y Representante Legal.
- Empleados:

La designación del Oficial de Cumplimiento no exime a VIGILANCIA ACOSTA LTDA, ni a los demás empleados de la obligación de detectar y reportar inmediatamente las operaciones inusuales, determinar las sospechosas y reportarlas a la UIAF. Será responsabilidad de cada empleado, desde su puesto de trabajo, velar porque se dé el debido cumplimiento a los procedimientos y mecanismos de control establecidos en el presente documento.

## **7. ESTRUCTURA ORGANIZACIONAL**

El Oficial de Cumplimiento implementará el Sistema Integral para el Lavado de Activos y Financiamiento del Terrorismo de manera transversal en la Organización, con el respaldo de la Junta Directiva, Representante Legal, Gerencia General, Gerencias de Área y todos los empleados de VIGILANCIA ACOSTA LTDA.

## **8. SANCIONES**

Cualquier incumplimiento grave en relación con las políticas y/o procedimientos establecidos en el presente Manual, bien sea intencional o causado por descuido o negligencia de cualquier empleado, director o administrador de cualquier condición o nivel, será sancionado en la forma prevista por la

empresa, sin perjuicio de las sanciones administrativas y penales establecidas en las leyes y en las regulaciones internacionales, si afectan alguna jurisdicción extraterritorial.

Las sanciones laborales se aplicarán sin perjuicio de las demás sanciones civiles, administrativas y penales existentes en la normatividad vigente incluyendo de manera especial aquellas relacionadas con la prevención y control del Lavado de Activos y Financiación del Terrorismo y las contenidas en el Código Penal Colombiano y las normas que lo adicionen o modifiquen.

El incumplimiento del presente Manual será considerado como falta grave y dará a lugar a la terminación del contrato de trabajo por parte de la compañía.

Cuando se detecten incumplimientos de los procedimientos definidos en el presente Manual, se debe poner en conocimiento de manera inmediata del Oficial de Cumplimiento tal circunstancia para que realice el proceso investigativo correspondiente y se adopten las medidas pertinentes.

## **9. PROGRAMAS DE CAPACITACIÓN**

VIGILANCIA ACOSTA LTDA., tendrá como política brindar capacitación con una periodicidad anual a todos los empleados sobre los elementos que conforman el sistema de gestión. Fruto de esta capacitación los empleados deberán estar en la capacidad de identificar y reportar las señales de alerta, las cuales gestionará el Oficial de Cumplimiento de acuerdo a los lineamientos descritos en el presente documento.

Esta capacitación deberá ser formalizada a través de actas de asistencia o registro del sistema si esta es realizada a través de plataformas digitales.

## **10. DOCUMENTACIÓN**

Toda gestión desarrollada por el SIPLAFT deberá estar documentada garantizando integridad, oportunidad, confiabilidad, disponibilidad y un manejo adecuado de su custodia y conservación (5 años). Lo anterior se encuentra a cargo del Oficial de Cumplimiento.

La documentación a conservar contempla:

- Manual SIPLAFT
- Reportes a la UIAF
- Informes a la Junta Directiva – Representante Legal
- Soportes de capacitación
- Comunicados
- Requerimientos de los órganos de control

## 11. DOCUMENTOS RELACIONADOS

Complementan el presente Manual todos los documentos relacionados a continuación como son:

- GI-MN-02 – Manual de Administración de Riesgos de Vigilancia Acosta Ltda.
- Documento maestro gestión de riesgo.
- GAF-RG-09– Identificación de proveedores.
- GC-RG-03 – Registro información de clientes.
- GC-RG-02 - Avisó y autorización de recolección y tratamiento de datos