

# MANUAL DE PROCEDIMIENTOS DE PREVENCIÓN DEL LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO

## Tabla de contenido

<b>INTRODUCCIÓN Y ÁMBITO DE APLICACIÓN.....</b>	<b>3</b>
1.1 · CONCEPTO DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO .....	3
1.2 A MBITO DE APLICACIÓN .....	3
1.3 LEGISLACIÓN APLICABLE .....	4
<b>ÓRGANOS DE CONTROL INTERNO .....</b>	<b>4</b>
2.1 OFICIAL DE CUMPLIMIENTO.....	4
2.2 DEPENDENCIA ORGANIZACIONAL .....	4
2.3 FUNCIONES.....	4
2.4 APOYO EN MATERIA DE PREVENCIÓN DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO .....	5
2.5 COMITÉ DE CUMPLIMIENTO.....	6
2.6 COMPOSICIÓN Y RÉGIMEN DE FUNCIONAMIENTO .....	6
2.7 FUNCIONES.....	7
<b>ADMINISTRACIÓN DEL RIESGO DE LA/FT .....</b>	<b>7</b>
<b>POLÍTICA DE DEBIDA DILIGENCIA - EN EL CONOCIMIENTO DE CLIENTE, PROVEEDOR Y COLABORADOR .....</b>	<b>7</b>
4.1 CLIENTES Y PROVEEDORES NO ADMITIDOS: .....	9
4.2 POLÍTICA DE IDENTIFICACIÓN Y CONOCIMIENTO DE LOS CLIENTES Y PROVEEDORES.....	9
4.3 PROCEDIMIENTOS DE IDENTIFICACIÓN Y CONOCIMIENTO DE LOS CLIENTES Y PROVEEDORES .....	10
4.4 INFORMACIÓN A SOLICITAR .....	10
4.5 INFORMACIÓN ADICIONAL PARA CLIENTES O PROVEEDORES DE RIESGO SUPERIOR AL PROMEDIO .....	11
4.6 FORMULARIOS .....	11
4.7 VERIFICACIÓN DE LA INFORMACIÓN FACILITADA .....	12
4.8 · PROCEDIMIENTOS DE IDENTIFICACIÓN Y CONOCIMIENTO COLABORADORES .....	12
4.9 CONOCIMIENTO DEL MERCADO .....	13
4.10 PROCEDIMIENTO DE ACTUALIZACIÓN DE DOCUMENTACIÓN .....	13
<b>V. POLÍTICA DE CONSERVACIÓN DE DOCUMENTACIÓN .....</b>	<b>13</b>
5.1 PROCEDIMIENTO DE CONSERVACIÓN DOCUMENTAL .....	13
<b>VI. POLÍTICA DE DETECCIÓN, ANÁLISIS Y COMUNICACIÓN DE OPERACIONES SUSCEPTIBLES DE ESTAR VINCULADAS CON EL LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO.....</b>	<b>14</b>
6.1 DETECCIÓN Y COMUNICACIÓN INTERNA DE OPERACIONES INUSUALES SUSCEPTIBLES DE SER SOSPECHOSAS .....	14
6.2 · ANÁLISIS DE OPERACIONES .....	15
6.3 COMUNICACIÓN O ARCHIVO DE OPERACIONES ANALIZADAS .....	16
<b>VII. DECLARACIÓN MENSUAL DE OPERACIONES .....</b>	<b>17</b>

7.1 · OBLIGACIÓN DE REALIZAR COMUNICACIONES.....	17
7.2 · PROCEDIMIENTO DE COMUNICACIÓN.....	17
<b>VIII. REQUERIMIENTOS DE LAS AUTORIDADES.....</b>	<b>17</b>
8.1 · PROCEDIMIENTOS A SEGUIR.....	18
<b>IX. CAPACITACIÓN.....</b>	<b>18</b>
<b>X. AUDITORÍA INTERNA.....</b>	<b>19</b>
<b>XI. REVISORÍA FISCAL.....</b>	<b>19</b>
<b>XII. SUCURSALES.....</b>	<b>19</b>
<b>XIII. SANCIONES.....</b>	<b>20</b>
13.1 SANCIONES ADMINISTRATIVAS.....	20
13.2 · SANCIONES PENALES.....	21
13.3 SANCIONES A EMPLEADOS.....	21

## Introducción y ámbito de aplicación

El presente Manual de Procedimientos (en adelante el Manual) está aprobado por la Junta Directiva de la organización GURUSOFT. En este documento también se mencionan las directrices en cuanto a debida diligencia respecto al conocimiento de los clientes, proveedores, empleados así como potenciales inversionistas en las operaciones locales. El propósito del presente Manual es establecer los procedimientos de Prevención de Lavado de Activos y Financiación del Terrorismo implantados por la Organización GURUSOFT.

### 1.1 · Concepto de Lavado de Activos y Financiación del Terrorismo

Se entiende por Lavado de Activos y Financiación del Terrorismo, conforme la legislación colombiana, “la adquisición, resguardo, inversión, transporte, transformación, custodia o administración de bienes que tengan su origen mediano o inmediato en actividades de tráfico de migrantes, trata de personas, extorsión, enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, financiamiento del terrorismo y administración de recursos provenientes de actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias psicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, o vinculados con el producto de los delitos ejecutados bajo concierto para delinquir, o dar a los bienes provenientes de dichas actividades apariencia de legalidad o legalizarlos, ocultar o encubrir la verdadera naturaleza, origen, ubicación, destino, movimiento o derechos sobre tales bienes, o realizar cualquier otro acto para ocultar o encubrir su origen ilícito”.

El proceso de Lavado de Activos y Financiación del Terrorismo, a escala general, consta de las siguientes fases:

**Colocación:** Ingreso del dinero en los circuitos legales del mercado.

**Estratificación:** Realización de operaciones sucesivas con el fin de fraccionar, acumular, ocultar y borrar el origen del dinero.

**Integración:** Conversión o inversión en activos de origen aparentemente legítimo.

El presente Manual recoge e incorpora los principales requerimientos establecidos en la legislación, normas y publicaciones colombiana e internacional en relación con la prevención del Lavado de Activos y Financiación del Terrorismo. Este Manual recoge también los aspectos operativos y procedimientos a realizar para su correcto cumplimiento. Por tanto, todos los colaboradores de las empresas sujetas al cumplimiento de la normatividad y específicamente aquellos cuyas actividades están especialmente relacionadas con la aceptación y vinculación de clientes, proveedores, empleados e inversionistas deben conocer y cumplir las normas vigentes.

Todas las Empresas de La Organización GURUSOFT serán responsables del correcto cumplimiento de la legislación local y de las políticas publicadas en relación al Lavado de Activos y Financiación del Terrorismo y deben incorporar dichas políticas y normas en sus procedimientos de trabajo. En caso de conflicto entre las normas internas y externas siempre prevalecerán aquellas que establezcan los requisitos más estrictos.

### 1.2 Ámbito de aplicación

El presente Manual recoge e incorpora los principales requerimientos establecidos en la legislación, normas y publicaciones colombiana e internacional en relación con la prevención del Lavado de Activos y Financiación del Terrorismo. Este Manual recoge también los aspectos operativos y procedimientos a realizar para su correcto cumplimiento. Por tanto, todos los colaboradores de las empresas sujetas al cumplimiento de la normatividad y específicamente aquellos cuyas actividades están especialmente relacionadas con la aceptación y vinculación de clientes, proveedores, empleados e inversionistas deben conocer y cumplir las normas vigentes.

Todas las Empresas de La Organización Carvajal serán responsables del correcto cumplimiento de la legislación local y de las políticas publicadas en relación al Lavado de Activos y Financiación del Terrorismo y deben incorporar dichas políticas y normas en sus procedimientos de trabajo. En caso de conflicto entre las normas internas y externas siempre prevalecerán aquellas que establezcan los requisitos más estrictos.

### 1.3 Legislación aplicable

El presente Manual viene a dar cumplimiento a la legislación colombiana vigente en materia de prevención del Lavado de Activos y Financiación del Terrorismo. Así, el presente procedimiento se deriva de:

- Ley 599 de 2000
- Ley 1121 de 1996 la Financiación del Terrorismo Decreto Ley 663 de 1993
- Ley 190 de 1995
- Ley 526 de 1999

En materia de prevención del Lavado de Activos y Financiación del Terrorismo, respecto de la actividad desarrollada por las empresas de la Organización GURUSOFT, aparte de la legislación mencionada en el apartado anterior, resultan de aplicación:

- Circular Externa de la Dirección de Impuestos y Aduanas Nacionales: 170 de 2002
- Circular 100-5, de 2014
- Resolución UIAF 285, de 2007
- Recomendaciones del GAFI.
- Resolución UIAF 212, de 2009
- Ley 222 de 1995

Este Manual, se encontrará a disposición de los colaboradores que deseen consultarlo en la Intranet y para proveedores y contratistas en la página web de la Organización.

## Órganos de Control Interno

### 2.1 Oficial de Cumplimiento

Será designado por la Junta Directiva de la Organización GURUSOFT y su nombramiento será ratificado por la junta directiva de GURUSOFT S.A. quien será responsable interno en materia de Prevención del Lavado de Activos y Financiación del Terrorismo.

Este cargo desempeñado por el Oficial de Cumplimiento, quien posee el comportamiento profesional y la experiencia y conocimiento adecuados para ejercer las funciones propias del cargo. El empleado de cumplimiento, será el enlace con la Subdirección de Fiscalización Aduanera para atender temas relacionados con el Lavado de Activos y Financiación del Terrorismo y con la Unidad de Análisis Financiero – UIAF.

### 2.2 Dependencia Organizacional

El Oficial de cumplimiento depende del CFO, reportando a éste y a la Junta Directiva cuanto él lo estime conveniente.

El Oficial de cumplimiento tiene como funciones principales las establecidas en el punto siguiente, las cuales serán desempeñadas según se describe en el punto 2.1.2 de este Manual.

### 2.3 Funciones

Las funciones a realizar por el Oficial de Cumplimiento son las siguientes:

- Establecer, para posterior aprobación del Comité de Cumplimiento políticas, normas y procedimientos internos, de actuación en La Organización en materia de Prevención de Lavado de Activos y Financiación del Terrorismo.

- Actualizar el manual de Prevención del Lavado de Activos y Financiación del Terrorismo de acuerdo con la normatividad vigente o de acuerdo a las políticas de la Organización.
- Informar a las directivas de la empresa acerca de las posibles fallas u omisiones en los controles para la prevención de actividades delictivas, que comprometan la responsabilidad de los colaboradores y de la empresa;
- Presentar al Vicepresidente Financiero un informe semestral detallado a cerca del cumplimiento de las labores a su cargo. Atender y coordinar cualquier requerimiento, solicitud o diligencia de autoridad judicial o administrativa en materia de prevención y control de actividades delictivas.
- Presentar al Representante Legal de las empresas el informe anual de la gestión a su cargo, con el fin de que este sea base para la presentación de gestión respecto al riesgo LA/FT por parte del Presidente de cada empresa a los miembros de la Junta Directiva.
- Realizar los reportes mensuales a la UIAF de operaciones en efectivo, así como de las operaciones sospechosas.
- Participar en las reuniones que competan a la prevención del Lavado de Activos y Financiación del Terrorismo que convoquen las autoridades competentes, con finalidad consultiva o informativa, bien sea con La Organización GURUSOFT o con los sujetos obligados en general.
- Mantener permanentemente informados al Comité de Cumplimiento y a la Junta Directiva de la Organización GURUSOFT sobre cualquier circunstancia que pudiera o debiera alterar o modificar la política de Prevención de Lavado de Activos y Financiación del Terrorismo que realiza la Organización.
- Seguimiento de las decisiones tomadas en materia de Prevención de Lavado de Activos y Financiación del Terrorismo y del cumplimiento de las normas y procedimientos instaurados.
- Promover el desarrollo de la Prevención de Lavado de Activos y Financiación del Terrorismo en las diferentes empresas o sociedades que pudieran adherirse a la Organización GURUSOFT.
- Analizar las operaciones susceptibles de estar vinculadas con el Lavado de Activos y Financiación del Terrorismo en las operaciones de la Organización, detectadas por la herramienta informática utilizada al efecto o comunicada internamente por algún colaborador de la Organización, recopilando la información precisa y realizando gestiones adicionales de verificación.
- Determinar los asuntos a tratar en las reuniones del Comité de Cumplimiento y levantar acta de las sesiones.
- En caso de presentarse operaciones inusuales sujetas a validación y estudio, convocar al Comité de Cumplimiento para el inmediato análisis pormenorizado de la operación, una vez recopilada la información y realizadas las gestiones adicionales necesarias.
- Informar fehacientemente al colaborador o directivo comunicante del curso dado a la operación inusual comunicada.
- Promover y supervisar el desarrollo de los planes de capacitación establecidos por las empresas para los colaboradores de áreas críticas de la Organización GURUSOFT en materia de Prevención del Lavado de Activos y Financiación del Terrorismo.
- Controlar y verificar periódicamente la ejecución de las medidas adoptadas en este campo, así como la información suministrada por los clientes y proveedores activos de la Organización GURUSOFT.

#### 2.4 Apoyo en materia de prevención de Lavado de Activos y Financiación del Terrorismo

Para la realización y desarrollo de las tareas administrativas del Oficial de Cumplimiento, descritas en el punto anterior, éste deberá contar con el apoyo personal y técnico suficiente, conforme al volumen de operación de la entidad.

En este sentido, la necesidad de apoyo técnico consistirá en la implantación o configuración de herramientas informáticas adecuadas para detectar operaciones susceptibles de estar vinculadas con el Lavado de Activos y Financiación del Terrorismo y para su correspondiente tratamiento y análisis.

Así mismo, teniendo en cuenta las funciones a realizar, deberá contar con personal de apoyo suficiente para el desarrollo de las mismas. En este sentido, deberá ponerse a su disposición personal que colabore directamente en el cumplimiento diario de las funciones.

Adicionalmente como persona responsable de informar cualquier irregularidad a la UIAF, deberá contar con apoyo gerencial de la compañía, en especial de la Vicepresidencia Financiera, Presidencia y Junta Directiva de la Organización.

El Oficial de cumplimiento se apoyará en las áreas críticas que tienen una participación significativa en las operaciones de la Organización GURUSOFT frente a la prevención del Lavado de Activos y Financiación del Terrorismo que radica en:

#### Área de Servicios Logísticos

Concentrarse en la búsqueda cuidadosa y sistemática de los proveedores que aspiran a ser beneficiarios de las compras que realicen la empresas de la Organización GURUSOFT.

#### Áreas Comerciales y de Crédito

Encargadas de velar por que los clientes de la Organización GURUSOFT sean cuidadosamente seleccionados dando cumplimiento a las directrices impartidas en este manual.

#### Área de Tesorería (Corporativa y de GURUSOFT Servicios)

Velará porque sus operaciones de pagos realizados y recibidos por La Organización GURUSOFT se encuentren registradas con los respectivos documentos soportes que le competen de acuerdo con normatividad aplicable, adicionalmente deberá cumplir con las normas y procedimiento internos para manejo de recursos en cuanto a pagos y recaudos.

Toda transacción que implique manejo de divisas deben realizarse a través del Sector Financiero, en la Organización GURUSOFT todas las operaciones de pago y recaudo se canalizaran a través de entidades vigiladas por la Superintendencia Financiera, cualquier excepción deberá ser aprobada por el CFO.

### 2.5 Comité de Cumplimiento

En aras de mejorar y establecer mecanismos internos de trabajo con una metodología clara de acciones a seguir, se conformará un Comité de Cumplimiento quien supervisará la adopción y eficacia de los mecanismos de Prevención de Lavado de Activos y Financiación del Terrorismo, adicionalmente tendrá como misión analizar, controlar y comunicar a la UIAF, a través del Oficial de Cumplimiento toda la información relativa a las operaciones o hechos susceptible de estar relacionados con el Lavado de Activos y Financiación del Terrorismo, según el procedimiento establecido en el presente manual y en la legislación aplicable.

Al frente del Comité y cumpliendo las funciones de Presidente del mismo, se encuentra el Vicepresidente Financiero. Así, el Comité de Cumplimiento de La Organización GURUSOFT está formado por:

- Vicepresidente Financiero (realizando funciones de Presidente).
- Representante de GURUSOFT Soluciones de Comunicación (Jefatura del área comercial).
- Representante de GURUSOFT Tecnología y Servicios (Jefatura del área Técnica).
- Representante de GURUSOFT Administración (Jefatura del área Administrativa).
- Oficial de Cumplimiento (realizando funciones de Secretario).
- Asimismo, el Comité podrá invitar a cada reunión a quien estime conveniente por los temas a tratar en las mismas.

### 2.6 Composición y régimen de funcionamiento

La participación en el comité no podrá delegarse a ninguna otra persona.

El funcionamiento del Comité se regirá por los principios de rapidez, seguridad, eficacia y coordinación tanto en la transmisión interna como en el análisis y comunicación a la UIAF de toda la información relevante a efectos de Lavado de Activos y Financiación del Terrorismo.

El Comité se reunirá con carácter semestral, de forma ordinaria y de forma extraordinaria siempre y cuando sea convocado por el Oficial de cumplimiento, dejando constancia de cada reunión en la correspondiente acta. Las reuniones del Comité quedarán válidamente constituidas cuando concurren, al menos, la mitad más uno de los miembros y el Oficial de cumplimiento.

Los acuerdos y temas tratados serán adoptados por la unanimidad de los miembros presentes y se recogerán en las correspondientes actas que serán conservadas por el Oficial de Cumplimiento, en el archivo de actas del Comité de Cumplimiento de la Organización GURUSOFT.

## 2.7 Funciones

Adicionalmente, el Comité de Cumplimiento deberá analizar o comprobar los hechos u operaciones comunicadas por los colaboradores, decidiendo si hay indicio o certeza de que existe Lavado de Activos y Financiación del Terrorismo y actuando en consecuencia según lo dispuesto en el presente Manual. En este sentido, las funciones son las siguientes:

- Establecer políticas, normas, procedimientos y controles de actuación en La Organización GURUSOFT en materia de Prevención de Lavado de Activos y Financiación del Terrorismo.
- Decidir acerca de las operaciones inusuales susceptibles de ser reportadas a la UIAF como operaciones sospechosas.
- Conocer los resultados del informe de revisoría fiscal al cierre del periodo y de auditoría interna, estableciendo un plan de acción para subsanar las posibles deficiencias que impacten las áreas críticas o los posibles riesgos en las deficiencias detectadas asociadas al Lavado de Activos y Financiación del Terrorismo que se hayan puesto de manifiesto y haciendo el correspondiente seguimiento para resolverlas todas ellas.
- Adoptar medidas cautelares, tales como la decisión de condicionar a seguimiento una determinada operación o cliente o, en su caso, decisiones sobre clientes concretos o sectores de riesgo
- Recibir anualmente sesiones de capacitación, de manera que estén al corriente de las obligaciones legales de La Organización GURUSOFT.

## Administración del Riesgo de LA/FT

La Organización GURUSOFT para efectos de la administración del riesgo LA/FT, contará con una matriz de riesgos que le permitirá identificar por cada factor, el nivel de riesgo al cual se encuentra expuesta la Organización.

La revisión y ajuste en la calificación de la matriz debe efectuarse anualmente, dicha actividad estará bajo la responsabilidad y seguimiento del Gerente Financiero de la empresa, quien en conjunto con el Oficial de Cumplimiento, establecerán los controles necesarios que mitiguen los riesgos identificados.

El oficial de cumplimiento es el responsable de establecer el modelo de matriz a calificar, así como los factores de riesgo a evaluar.

## Política de debida Diligencia - en el conocimiento de cliente, proveedor y colaborador

Los procedimientos recogidos en esta sección tienen como objeto regular internamente la aceptación y conocimiento de la contraparte. Las políticas de conocimiento ayudan a proteger la reputación de las entidades, al reducir la posibilidad de que se conviertan en vehículo o víctima del crimen financiero. Los aspectos fundamentales de dichas políticas son la identificación, verificación y aceptación de clientes y proveedores.

El conocimiento de la contraparte no termina con la identificación formal de los mismos, sino que exige el conocimiento del marco en el que se desenvuelven y el detenido seguimiento de la evolución de sus actividades. Por lo tanto, y con carácter general, en el momento de establecer relaciones de negocio deberá recopilar y analizar de terceros la información necesaria a fin de conocer la naturaleza de su actividad profesional y empresarial.

Se deben aplicar las medidas contenidas en las políticas, debida diligencia emitidas por la Organización GURUSOFT, para comprobar razonablemente la veracidad de la información recolectada que están orientadas a la verificación de las actividades declaradas por los mismos, basadas adicionalmente en la obtención de documentos que guarden relación con la actividad declarada o en la obtención de la información ajena al propio cliente, en aras de establecer la coherencia entre éstas y las operaciones de comercio que realizan. Los aspectos más relevantes de la información recopilada y analizada en el estudio de los clientes y los proveedores que debe ser registrada en los formularios de “Cumplimiento circular 0170 de la DIAN identificación y actualización de clientes y/o proveedores”, para operaciones de comercio exterior y formulario de conocimiento del cliente/proveedor para operaciones locales.

Cada Empresa será responsable de realizar las medidas descritas en éste Manual (de aceptación y conocimiento del cliente, así como la evaluación del riesgo del potencial cliente, previo a su aceptación).

En el caso de proveedores, a pesar de que la selección y negociación inicial de proveedores de compras estratégicas corresponde a cada Empresa, dicha responsabilidad corresponderá a GURUSOFT Servicios, por ser quien se encarga de la vinculación y formalización de la relación de los mismos con la Organización.

Como parte de la evaluación del riesgo, las comprobaciones principales que deben efectuarse por la Organización GURUSOFT son las siguientes:

- **Comprobación de listas internacionales:** Se harán las siguientes comprobaciones del cliente persona Jurídica y natural así como de los representantes legales No inclusión en la lista de “Nacionales Especialmente Designados y Personas Bloqueadas” publicada por OFAC.
- No inclusión en la lista de individuos y/u organizaciones terroristas publicada por la Organización de Naciones Unidas.

Si alguna de las comprobaciones referidas anteriormente resultan en una identificación en las listas o bases de datos indicados, el cliente o el proveedor será catalogado como **inaceptable** y se dejará documentado tal situación en la herramienta tecnológica establecida para tal fin.

Si la identificación resultara en la lista de “Nacionales Especialmente Designados y Personas Bloqueadas” publicada por OFAC, y la Empresa hubiera obtenido una licencia de OFAC para ser gestionada por el Estado, podrá autorizarse su vinculación, previa autorización del Oficial de cumplimiento.

Esta comprobación se realiza al momento de efectuar cualquier tipo de cotización o acercamiento a terceros. Para los clientes y proveedores ya vinculados, mensualmente se realizará una nueva comprobación de toda la base de datos de clientes y proveedores activos, a efectos de detectar si alguno de ellos ha sido posteriormente incluido, adicionalmente se verificará semanalmente los nuevos clientes y proveedores vinculados en la semana inmediatamente anterior.

- **Comprobación de las actividades declaradas:** La Organización GURUSOFT adoptará las medidas necesarias para comprobar razonablemente la veracidad de la información proporcionada por los terceros, referida a su actividad profesional o empresarial. Tales medidas consistirán en el establecimiento de procedimientos de verificación de las actividades declaradas por los clientes. Dichos procedimientos tendrán en cuenta el diferente nivel de riesgo y se basarán en la obtención de los documentos de los clientes que guarden relación con la actividad.
- **Identificación en caso de no actuación por cuenta propia y composición accionaria:** Cuando existan indicios o certeza de que los clientes o proveedores cuya identificación fuera preceptiva, no actúan por cuenta propia, la Organización GURUSOFT recopilará la información precisa a fin de conocer tanto la identidad de los clientes como de las personas por cuenta de las cuales actúan. En el caso de personas jurídicas, se adoptarán medidas razonables a efecto de conocer tanto los representantes legales cómo la composición accionaria de la empresa, es decir, la identidad de los accionistas o asociados que tengan participación directa en más del 5% de su capital social, aporte o participación en la entidad.



- **Identificación de Titular real:** Se define como toda persona natural o jurídica que, sin tener la condición de cliente, es la propietaria o destinataria de los recursos o bienes objeto del contrato.
- **Identificación de personas públicamente expuestas:** Se define como “personas públicamente expuestas” aquellas personas nacionales o extranjeras que, por razón de su cargo, manejan recursos públicos, ejercen algún grado de poder público o gozan de reconocimiento público. Con esta información recopilada, se clasificarán los clientes y los proveedores en las siguientes categorías:
- **Clientes/proveedores de riesgo superior al promedio:**
  - Clientes/proveedores con nacionalidad o residencia en algún ‘País de alto riesgo’. La lista de países de alto riesgo que la Entidad ha establecido es la publicada por la OCDE y el GAFI.
  - Clientes/proveedores que, estando en la lista de “Nacionales Especialmente Designados y Personas Bloqueadas” publicada por OFAC, hubieran obtenido una licencia de OFAC para ser gestionada por el Estado.
  - **Personas expuestas públicamente (PEP).** Se consideran PEP en base a las siguientes funciones:
    - Jefes de Estado, jefes de Gobierno, ministros, subsecretarios o secretarios de Estado
    - Parlamentarios
    - Miembros de tribunales supremos, tribunales constitucionales u otras instancias judiciales cuyas decisiones no admitan normalmente recurso
    - Miembros de tribunales de cuentas o de los consejos de los bancos centrales
    - Embajadores, encargados de negocio y altos funcionarios de las fuerzas armadas.
    - Miembros de los órganos administrativos, de gestión o de supervisión de empresas de propiedad estatal.
    - Otras Figuras Públicas de Gran Reconocimiento (por ejemplo: Cantantes, Futbolistas, Actores).

Los clientes y proveedores catalogados como de alto riesgo se identificarán de manera automática en la herramienta tecnológica, la cual generará alertas, con el fin de monitorear las operaciones efectuadas por terceros que presenten este perfil.

#### 4.1 Clientes y proveedores no admitidos:

En cualquier caso, la Organización GURUSOFT no admitirá como clientes ni proveedores a personas jurídicas o naturales vinculadas con:

- Actividades relacionadas con la prostitución o pornografía.
- Actividades relacionadas con el tráfico de drogas.
- Personas de dudosa integridad u honestidad, particularmente aquellas de las que se tenga conocimiento de que están vinculadas a cualquier tipo de delincuencia.
- Personas que estén incluidos en las listas de OFAC y Naciones Unidas indicadas anteriormente.
- Personas con negocios cuya naturaleza haga imposible la verificación de la legitimidad de sus actividades o la procedencia de los fondos.
- Personas que rehúsan facilitar la información o documentación requerida.

#### 4.2 Política de identificación y conocimiento de los clientes y proveedores

La identificación del cliente y el proveedor cumple con una doble finalidad: cumplir con la normativa legal e interna y poder identificar si el cliente o proveedor pertenece a alguno de los grupos de riesgo identificados en la política de aceptación de clientes y proveedores.

La obtención de las informaciones básicas indispensables para la identificación y conocimiento del cliente y el proveedor es responsabilidad de cada una de las empresas de la Organización GURUSOFT en cabeza de las áreas críticas.

Se deben aplicar medidas de identificación del cliente y el proveedor para comprobar razonablemente la veracidad de la información recopilada de los mismos. A tales efectos, podrá solicitarse la colaboración de empresas que realicen estas comprobaciones.

Cuando existan indicios o certeza de que los clientes o proveedores no actúan por cuenta propia, se recopilará y analizará la información precisa a fin de conocer la identidad de las personas por cuenta de las cuales actúan los mismos. Si se trata de personas jurídicas se adoptarán las medidas necesarias y razonables para determinar la composición accionaria o de control de los clientes y proveedores.

#### 4.3 Procedimientos de identificación y conocimiento de los clientes y proveedores

La normatividad aplicable respecto a Lavado de Activos y Financiación del Terrorismo, establece la necesidad de exigir la correcta identificación del cliente y el proveedor, tanto persona natural como jurídica, para salvaguardar a las entidades de prácticas destinadas a cometer delitos relacionados con el Lavado de Activos y Financiación del Terrorismo.

Para poder cumplir dichos objetivos, se impone a los sujetos precisados la obligatoriedad de desarrollar procedimientos de verificación de las actividades declaradas por los clientes y los proveedores. Dichos procedimientos tendrán en cuenta el diferente nivel de riesgo y se basarán en la obtención de documentos de los clientes y proveedores que guarden relación con la actividad declarada o en la obtención de información sobre ella, ajena al propio cliente o proveedor.

Así mismo, los sujetos obligados deberán aplicar medidas adicionales de identificación y conocimiento del cliente y el proveedor para controlar el riesgo de Lavado de Activos y Financiación del Terrorismo en las áreas de negocio.

#### 4.4 Información a solicitar

A continuación se exponen los niveles mínimos de información requerida para la identificación de clientes y proveedores y verificación de sus actividades.

##### a. Identificación de persona natural

Se solicitará del cliente y del proveedor la siguiente información:

- Nombre y apellido completos
- Número de identificación: Copia del RUT, cédula de ciudadanía nacionales) o cédula de extranjería (extranjero) o documento que acredite el número de identificación fiscal o personal.
- Nombre y apellidos completos del representante, apoderado y número de identificación (de aplicar) Dirección de residencia.
- Descripción actividad: Actividad económica principal: comercial, industrial, transporte, construcción, agroindustria, servicios financieros, etc., acorde con lo establecido en el código internacional CIU.
- Declaración de origen de los bienes y/o fondos. Identificación de la(s) cuenta(s) bancaria(s) mediante la cual operará y certificación bancaria de la cuenta para países en los cuales aplique esta figura, de lo contrario, carta firmada por el representante legal indicando los datos financieros de las cuentas que se registran.
- Ingresos y egresos mensuales.
- Patrimonio.
- Detalle de otros ingresos o ingresos no operativos o los originados en actividades diferentes a la principal.
- Autorización para consulta y verificación de la información suministrada.
- Firma y fecha de diligenciamiento.

##### b. Identificación de personas jurídicas

Las personas jurídicas deberán presentar documento que acredite su denominación, razón social, domicilio y objeto social. Así como los respectivos certificados de existencia y representación legal o poderes donde se validen las personas que actúan en su nombre.

Se ha de conocer la composición accionaria o de control de la empresa, identificando al verdadero propietario de los fondos, así como a los que ejercen el verdadero control sobre ellos, se excluyen del cumplimiento de este requisito las empresas que cotizan en bolsa y las entidades financieras.

El no suministro de esta información podrá ser autorizado siempre y cuando se observe evidencia de debida diligencia por parte de la Organización para la obtención de estos documentos y teniendo en cuenta que se trate de una empresa con trayectoria y legalmente constituida.

Así, se solicitará a las personas jurídicas la siguiente información:

- Razón social
- Número de identificación: Copia del NIT, cédula de ciudadanía (nacionales) o cédula de extranjería (extranjero)\*\*
- Nombre y apellidos completos del representante, apoderado y número de identificación, Dirección y teléfono del representante.
- Descripción actividad: Actividad económica principal: comercial, industrial, transporte, construcción, agroindustria, servicios financieros, etc., acorde con lo establecido en el código internacional CIIU.
- Dirección, teléfono, y ciudad de la oficina principal.
- Escrituras de apoderamiento de las personas que actúan en su nombre, sin perjuicio de la obligación que proceda de comunicar el DNI de las mismas.
- Composición accionaria e Identificación de los accionistas o socios que tengan directa o indirectamente más del 5% del capital social, aporte o participación.
- Tipo de empresa: privada, pública, mixta.
- Declaración de origen de los bienes y/o fondos.
- Identificación de la(s) cuenta(s) bancaria(s) mediante la cual operará y certificación bancaria o carta firmada por el representante legal indicando información de la cuenta, registrando la ciudad en la que se encuentra radicada.
- Ingresos y egresos mensuales.\*
- Patrimonio. \*
- Detalle de otros ingresos o ingresos no operativos o los originados en actividades diferentes a la principal.
- Firma del solicitante (representante legal de la entidad )
- Fecha de diligenciamiento.

Si el cliente o proveedor fuera del exterior, se recopilará y analizará la documentación equivalente o información necesaria que permita validar los datos anteriormente descritos.

\*Respecto a la información financiera, se podrá autorizar la vinculación sin el suministro de esta información siempre que se evidencie debida diligencia por parte de la empresa en la consecución de esta información y que se trate de una empresa legalmente constituida y con trayectoria.

\*\* El documento de identificación del representante legal, será exigible solo para validaciones de coincidencia en listas vinculantes para descartar falsos positivos.

#### 4.5 Información adicional para clientes o proveedores de riesgo superior al promedio

Adicionalmente, aquellos clientes o proveedores que, a partir de la evaluación inicial, presenten un riesgo superior al promedio (persona natural que ostente la categoría de PEP, persona jurídica con un PEP en su composición accionaria y personas naturales y/o jurídicas con residencia/nacionalidad de un país de riesgo) se identificarán de manera automática en la herramienta tecnológica, la cual generará alertas, con el fin de monitorear las operaciones efectuadas por terceros que presenten este perfil, de esta manera serán vigiladas las operaciones efectuadas por estos clientes o proveedores mediante la gestión oportuna de las alertas.

#### 4.6 Formularios

Según establece la legislación vigente, es necesario que la Organización GURUSOFT no sólo identifique a sus clientes y a sus proveedores al inicio de una relación de negocio sino que también debe establecer medidas adicionales de conocimiento del cliente y del proveedor y de la actividad desarrollada por los mismos.

Para el mejor conocimiento de los clientes y proveedores se diligenciarán los formularios establecidos para tal fin, desarrollados por la Organización GURUSOFT; para proveedores se encuentran disponibles en la intranet corporativa, para clientes estarán disponibles en cada empresa en cabeza del área de crédito y cartera.

El formulario se diligenciará al momento de entablar relaciones de negocio con los clientes y/o proveedores. El proceso aplicado por la Organización GURUSOFT consta de los siguientes procedimientos:

- Confirmar la verdadera identidad de los clientes y proveedores, y su actividad económica .
- Monitorear operaciones realizadas con los clientes y proveedores para detectar posibles operaciones inusuales que puedan estar relacionadas con el Lavado de Activos y Financiación del Terrorismo.

Documentar y custodiar toda la información relativa a la identificación del cliente y el proveedor, y las operaciones por ellos realizadas.

Actualizar los datos del cliente y el proveedor contenidos en bases de datos.

Comprobar la no pertenencia de ningún cliente o proveedor en los listados de personas, grupos y entidades terroristas recogidas en las Listas de Naciones Unidas y la no inclusión en la lista de Nacionales Especialmente Designados y Personas Bloqueadas publicada por OFAC, de acuerdo a lo previsto como parte de la evaluación del riesgo.

La información registrada y analizada en el formulario se incorporará a la base de datos de clientes y Proveedores, que servirá de fuente de información y nos permitirá elaborar un “perfil del tercero” que servirá como base para detectar operaciones susceptibles de estar vinculadas con el Lavado de Activos y Financiación del Terrorismo.

Se encuentran exentos del diligenciamiento del formato, aquellos proveedores creados bajo la categoría de tercero de caja menor, se entenderá como tercero de caja menor aquellos proveedores creados como resultado de una legalización correspondiente a un informe de viajes o pago efectuado con una tarjeta de crédito para compras por internet o tarjetas corporativas para viajes, así como los clientes creados en plataformas de ventas por internet.

#### 4.7. Verificación de la información facilitada

Se realizarán procedimientos de comprobación de la información registrada por el cliente versus los documentos soportes solicitados, los procedimientos de verificación de las actividades declaradas tendrán en cuenta el diferente nivel de riesgo y se basarán en la obtención de documentación de los clientes y proveedores que guarden relación con la actividad declarada o en la obtención de información sobre la misma ajena al propio tercero. Desde el momento de inicio de la relación de negocios debe quedar claramente entendido el origen de los recursos del futuro cliente y proveedor.

En el caso de clientes personas jurídicas, se verificará que la actividad real de la empresa si corresponde con su objeto social y se muestra en concordancia con sus principales datos financieros: patrimonio, ingresos y cifra de ventas.

#### 4.8 · Procedimientos de identificación y conocimiento colaboradores

Con el fin de analizar el riesgo y criticidad de los cargos, la Organización GURUSOFT cuenta con un modelo de matriz de riesgo que evalúa los cargos, de acuerdo a las funciones desarrolladas, estableciendo niveles de criticidad.

Cada nivel de criticidad, cuenta con un protocolo de seguridad que debe ser aplicado previo a la vinculación del candidato, la exigencia de aplicación de dicho control, estará en cabeza del área de Gestión Humana de cada empresa, siendo el responsable de la operación del control Seguridad Corporativa, quien es el garante de la custodia y evidencia de dicho proceso.

#### 4.9 Conocimiento del Mercado

Se deberá obtener información sobre las características usuales del mercado de los potenciales clientes y proveedores, con el fin de poder compararlos con las operaciones que realiza, lo que permitirá establecer su normalidad o posible anormalidad, o calificación de operación inusual, al compararla con otras operaciones de naturaleza similar efectuadas por clientes que se desempeñan en el mismo ramo de negocio. Para ello, podrá recurrirse a estudios de mercado del sector en que opere el cliente, a efectos de conocer las características generales de los mismos.

#### 4.10 Procedimiento de actualización de documentación

La Organización GURUSOFT deberá mantener actualizada la documentación de identificación de clientes y de proveedores durante toda la vigencia de la relación de negocio.

Para asegurar que los registros se mantienen actualizados se deberán realizar revisiones de la documentación atendiendo al riesgo asignado al cliente y al proveedor. De esta forma, en clientes de riesgo superior al promedio la documentación se actualizará en el mes de junio de cada año, en clientes de riesgo normal la actualización se realizará cada dos años.

Sin perjuicio de lo expuesto, de producirse cambios significativos en los datos del cliente o proveedor o en su actividad, la actualización se realizará de manera inmediata.

En cuanto a colaboradores, la Organización GURUSOFT fomentará y exigirá a sus colaboradores la actualización de la información correspondiente a sus datos, tan pronto se presente una novedad, o por lo menos una vez en el año; esta actualización estará a cargo del área de Gestión Humana de la empresa y se efectuará en el medio establecido para tal fin.

## V. Política de conservación de documentación

La Organización GURUSOFT conservará durante cinco años los documentos que soportan el conocimiento del cliente y proveedores, así como los registros correspondientes que acrediten adecuadamente la realización de las operaciones.

El plazo anteriormente indicado se contará a partir del día en que finalicen las relaciones con un cliente para los documentos relativos a su identificación y a partir de la ejecución de cada operación para la conservación de los documentos o registros que la acreditan.

#### 5.1 Procedimiento de conservación documental

Los documentos acreditativos de la identidad de los clientes y proveedores así como los documentos relativos a las operaciones con ellos realizadas por la Organización GURUSOFT se conservarán de forma electrónica o forma física de acuerdo a las herramientas establecidas para tal fin.

Para cada nuevo cliente se abrirá un expediente en el cual se recogerá toda la documentación física recopilada, copia de los documentos acreditativos de la identidad, formulario de creación y actualización de clientes.

Para nuevos proveedores toda la documentación referente al conocimiento de este, se registrará de manera electrónica en la herramienta definida por la Organización para tal fin. Cada Empresa será responsable de recopilar y analizar la información y documentación de los clientes que pretenda vincular y GURUSOFT Servicios será responsable de realizar dicha actividad en el caso de proveedores.

## VI. Política de detección, análisis y comunicación de operaciones susceptibles de estar vinculadas con el Lavado de Activos y Financiación del Terrorismo.

### 6.1 Detección y comunicación interna de operaciones inusuales susceptibles de ser sospechosas

La normatividad establece como requerimiento el examen especial de determinadas operaciones. La Organización GURUSOFT debe examinar con cuidadosa atención toda operación realizada por una persona natural o jurídica que, por su número, cantidad o características, no se enmarca dentro de los sistemas y prácticas 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 ha podido ser razonablemente justificada. Estas operaciones deberán ser comunicadas a la UIAF por ser susceptible de relación con actividades de Lavado de Activos y Financiación del Terrorismo.

El colaborador de la Organización GURUSOFT que detecte una operación con estas características, se abstendrá de ejecutar la operación y diligenciará el Formulario Interno de Comunicación (Anexo I), e inmediatamente lo enviará por correo interno o correo electrónico de la empresa del Oficial de Cumplimiento, quien remitirá el correspondiente acuse de recibo al colaborador comunicante.

Se deberá comunicar, en todo caso:

Cualquier operación realizada por una persona natural o jurídica que, por su número, cantidad o características, no se enmarca dentro de los sistemas y prácticas 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 ha podido ser razonablemente justificada,

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 y proveedores, o sobre transacciones de sus usuarios que por su número, por las cantidades transadas o por las características particulares de las mismas puedan conducir razonablemente a sospechar que los mismos están usando a la entidad para transferir, manejar, aprovechar o invertir dineros o recursos provenientes de actividades delictivas o destinados a su financiación.

Cuando se detecte que la naturaleza o el volumen de las operaciones activas o pasivas de algún cliente no corresponde con su actividad o antecedentes operativos, conforme al perfil del cliente establecido al momento de iniciar la relación de negocio.

Cualquier cambio en el comportamiento del cliente o proveedor, tales como:

- Cambios en la cuenta bancaria desde la que opera o a la que solicita que se efectúen los pagos correspondientes, sin comunicación previa y sin envío de la certificación bancaria o carta de autorización cuando aplique, requerida al efecto;
- Envío del pago o solicitud del mismo desde o hacia un paraíso fiscal;
- Envío del pago o solicitud del mismo desde o hacia un país distinto al de origen o destino de la mercancía sin que exista una relación de causalidad que lo explique;
- Que el instrumento o la orden de pago, el giro o la remesa que cancele la importación o exportación se expida o se halle a la orden o a favor de persona diferente del cliente o proveedor del exterior, sin que exista una relación de causalidad que lo explique.
- Clientes o proveedores que, de forma reiterada, comuniquen pérdida o hurto de mercancías entre el trayecto del lugar de arribo al depósito.
- Clientes que pretendan adquirir productos de la Organización, cuando su actividad económica no tenga relación directa con los mismos.
- Clientes o proveedores que presenten documentos presuntamente falsos entre los documentos exigidos para su identificación y conocimiento.
- Clientes o proveedores que hubieren sido sancionados por infracciones al régimen cambiario o al régimen aduanero.
- Inconsistencias en la información relacionada con la existencia, identificación, dirección del domicilio o ubicación del cliente o proveedor;
- Inconsistencias en la información que suministra el cliente o proveedor frente a la que suministran otras fuentes.

Las operaciones mencionadas son enunciativas y podrán modificarse de acuerdo a las nuevas tipologías que se detecten a futuro, las señales de alerta que emita la autoridad Competente, o la propia experiencia de la Organización.

El Comité de Cumplimiento adoptará las medidas adecuadas para mantener la confidencialidad sobre la identidad de los colaboradores y directivos que hayan realizado una comunicación. Para ello, la dirección de correo electrónico a la que se deben remitir las comunicaciones será de uso exclusivo del Oficial de Cumplimiento y, en caso de que la comunicación se realice por correo interno, deberá remitirse en sobre cerrado. Así mismo, el expediente analizado no contendrá, en ningún caso, copia del formulario remitido por el colaborador.

No se debe revelar al cliente ni a terceros las actuaciones que se pudieran estar llevando con motivo de las investigaciones iniciadas por una sospecha acerca de posibles actividades que pudieran estar relacionadas con el Lavado de Activos y Financiación del Terrorismo. El incumplimiento de este deber de confidencialidad puede acarrear sanciones tal y como se especifica en el código penal colombiano y el código de Principios y Políticas de la Organización GURUSOFT.

La comunicación de buena fé de informaciones relativa a actividades relacionadas con el Lavado de Activos y Financiación del Terrorismo no constituye violación de las restricciones sobre revelación de información impuestas por vía contractual o por cualquier disposición legal o reglamentaria, y no implica ningún tipo de responsabilidad para la persona comunicante.

Adicionalmente a los análisis mencionados, la Organización GURUSOFT dispone de un aplicativo informático que analiza operaciones detectando operaciones inusuales que de acuerdo con el análisis y determinados criterios establecidos, puedan resultar sospechosas de estar involucradas en un proceso de Lavado de Activos y Financiación del Terrorismo.

## 6.2 · Análisis de operaciones

Una vez recibida comunicación de operación inusual o sospechosa, tanto por parte de un colaborador de la Organización GURUSOFT como por resultado del análisis de la aplicación informática, el Oficial de Cumplimiento procederá de la siguiente manera:

Como norma general, realizará un primer contacto con el comunicante a fin de obtener la máxima cantidad de información acerca del perfil del cliente o proveedor tanto en lo que respecta a la información personal, como en la relación de negocios con la Organización.

Solicitará al comunicante fotocopias de la documentación que justifica la operación específica que ha motivado la comunicación.

Procederá a registrar la comunicación y a asignarle un número de referencia del expediente, compuesto por un código de dos cifras seguido del año de producción.

Aplicará aquellos procedimientos que permitan mantener la confidencialidad del comunicante y del hecho comunicado.

Igualmente, y en todo caso, se realizarán gestiones e investigaciones adicionales utilizando todos los medios disponibles.

Una vez se obtenga la información, se efectuará un pre-análisis detallado por el Oficial de Cumplimiento con el apoyo de las áreas involucradas que básicamente persigue la detección de:

- Coincidencias con los perfiles sospechosos.
- Incoherencias y/o desproporción respecto a la naturaleza y/o el volumen de la operación actual investigada, en relación a la actividad comercial y/o antecedentes operativos del cliente.
- Operaciones inusuales que puedan obedecer a nuevos canales utilizados para el Lavado de Activos y Financiación del Terrorismo.

Una vez realizado el análisis y con base en las conclusiones extraídas del mismo, el Oficial de Cumplimiento, convocará al Comité de Cumplimiento y presentará el expediente, debiendo éste tomar la decisión que se considere adecuada, o bien informará mediante un correo electrónico a los miembros del Comité de los hechos y de sus conclusiones si aprecia que no existen indicios de lavado ni operativas inusuales por parte del cliente o proveedor. Si cualquier miembro del Comité considerara necesario someter el expediente a revisión lo comunicará al Oficial de Cumplimiento, quien convocará una reunión a la mayor brevedad.

Tan pronto como el Oficial de Cumplimiento concluya sobre el resultado del análisis de la operación, procederá a informar al colaborador o directivo comunicante sobre el resultado del análisis efectuado.

### 6.3 Comunicación o archivo de operaciones analizadas

Una vez realizado el análisis, el Comité de Cumplimiento tomará la decisión del tratamiento a dar al expediente, asignándole una de las siguientes consideraciones:

**Expediente en seguimiento:** No se observan indicios pero se trata de una operación inusual. Con una periodicidad mensual el Oficial de Cumplimiento, atendiendo a la naturaleza del cliente y la operación, emitirá un informe de evolución de la operación en seguimiento, basado en la información suministrada por el área crítica y obtención de datos complementarios que resulten oportunos tales como:

- Recortes de prensa
- Consultas de información realizadas en internet — Información reportada en la página de UIAF
- En caso de observarse indicios o certeza de Lavado de Activos y Financiación del Terrorismo, se procederá a comunicar de inmediato a la UIAF por el Oficial de Cumplimiento. Debe limitarse al mínimo el número de expedientes en este estado, y el tiempo de vigilancia no excederá de los cuatro meses.

**Expediente a reportar:** Se observan indicios o certezas de su relación con el Lavado de Activos y Financiación del Terrorismo. De no haberse obtenido aún, se solicitará al jefe del área comercial, crédito o servicios logísticos según aplique de la respectiva empresa:

- Fotocopia de los Contratos relacionados con la operación a comunicar
- Documentos de identificación de los titulares, ordenantes o terceros implicados.
- RUT y poderes, certificado de existencia y representación legal si se trata de personas jurídicas.
- Cuanta información histórica se disponga de la actividad del cliente con el fin de contextualizar el perfil operativo global del mismo.
- En caso de que el departamento o unidad no localizara esta documentación, nunca deberá solicitársela abiertamente al cliente, a fin de no alertarle. El departamento o unidad deberá tomar nota de ello, para solicitársela cuando resulte oportuno, a fin de no levantar sospechas.

Se trasladarán los datos de intervinientes y operaciones, indicios de sospecha y descripción de las gestiones realizadas al aplicativo SiRel (se adjunta formulario como Anexo III). En concreto, deberá facilitarse la siguiente información:

- Relación e identificación de las personas que participan en las operaciones y el concepto de su participación en las mismas.
- La actividad conocida de las personas que participan en las operaciones y la correspondencia entre la actividad de los clientes y las operaciones realizadas.
- Relación de las operaciones y fechas a que se refieran con indicación de su naturaleza, monedas en que se realizan, cuantía, finalidad e instrumentos de pago o cobro utilizados.
- Gestiones realizadas para investigar las operaciones comunicadas.
- Exposición de las circunstancias de toda índole de las que pueda inferirse el indicio o certeza de vinculación al Lavado de Activos y Financiación del Terrorismo o que pongan de manifiesto la falta de justificación económica, profesional o de negocio para la realización de las operaciones.

La comunicación a la UIAF se efectuará por el Oficial de Cumplimiento, en la forma y a través de los medios electrónicos habilitados por la UIAF (SiRel) o en su defecto por correo. Una vez acuse de recibo la UIAF, donde se indica el número asignado a la comunicación, se procederá a registrar el número en el expediente, a archivarlo y a informar al Comité de Cumplimiento de la comunicación. Del mismo modo, el Oficial de Cumplimiento, dará traslado al colaborador o directivo comunicante, mediante el envío de un e-mail, del curso dado a su comunicación.

**Expediente para No reportar:** no se observan indicios v no se trata de una operación inusual en el sector del cliente, ni en la operaciones habituales del mismo. El Oficial de Cumplimiento dejará constancia por escrito de la información conseguida respecto al conocimiento del cliente y de la operación, el análisis efectuado y los criterios por los que se decide NO comunicar. Posteriormente, se enviará un correo electrónico confidencial al comunicante, informándole del curso dado a su comunicación, y por último se complementará la fecha de cierre del expediente, procediendo a su archivo durante un período mínimo de cinco años.



Una vez el comité haya tomado la decisión de comunicar o de no comunicar se dejará evidencia en el acta correspondiente.

## VII. Declaración Mensual de Operaciones

### 7.1 · Obligación de realizar comunicaciones

Con carácter mensual, en virtud de lo dispuesto en la resolución 212 de 2009 de la UIAF, la Organización GURUSOFT deberá comunicar a la UIAF:

Todas las operaciones que en desarrollo del giro ordinario de sus negocios realice, y que involucren pagos mediante entrega o recibo de dinero en efectivo (billetes o monedas) por un monto igual o superior a la suma de diez millones de pesos (\$10.000.000) m/cte o su equivalente en otras monedas.

La detección de aquellas operaciones objeto de reporte obligatorio, se realizará mediante la herramienta informática implementada para tales efectos por la Organización GURUSOFT. Así mismo, cada Empresa comunicará al Oficial de Cumplimiento, con carácter inmediato, las operaciones realizadas que reúnan las características antes descritas.

El Oficial de Cumplimiento recibirá el listado de operaciones identificadas y procederá a su comunicación, según los procedimientos establecidos.

### 7.2 · Procedimiento de comunicación

En aquellos casos en los que existan operaciones susceptibles de comunicación mensual a la UIAF, el Oficial de Cumplimiento procederá a la inserción en el aplicativo SiRel (Sistema de Reporte en Línea), indicado por la UIAF Servicio Ejecutivo, los datos relativos a dichas operaciones, a fin de generar y comunicar el correspondiente reporte.

De no haber existido operaciones susceptibles de declaración obligatoria u operaciones sospechosas en el mes, el Oficial de Cumplimiento, utilizando el sistema SiRel deberá remitir a la UIAF el correspondiente reporte de ausencia de operaciones sospechosas y transacciones individuales en efectivo.

Para ello, los Gerentes Financieros de las Empresas deberán enviar al Oficial de Cumplimiento certificaciones mensuales donde indiquen que no se recibieron operaciones en efectivo superiores a \$10.000.000; para las operaciones sospechosas las áreas críticas enviarán la certificación pertinente.

El Oficial de Cumplimiento procederá, dentro de los 10 primeros días calendarios del mes siguiente al mes calendario correspondiente, al envío por e-mail de la declaración correspondiente anexando el archivo generado por SiRel. A estos efectos, serán de aplicación las previsiones contenidas en la Resolución 212/2009 de la UIAF.

## VIII. Requerimientos de las Autoridades

De acuerdo a la normatividad aplicable, la reserva comercial no es oponible a las solicitudes de información formuladas de manera específica por las autoridades judiciales, de supervisión tributaria, aduanera o cambiaria y a la UIAF dentro de las investigaciones de su competencia, conforme a lo dispuesto en el artículo 15 de la Constitución Nacional y en los artículos 63 del Código de Comercio, 275 del Código de Procedimiento Penal y 288 del Código de Procedimiento Civil.

## 8.1 · Procedimientos a seguir

Los requerimientos que realicen las autoridades mencionadas en materia de Lavado de Activos y Financiación del Terrorismo a la Organización GURUSOFT, recibidos en el domicilio social o en cualquiera de las empresas de la organización, serán remitidos de manera inmediata al Oficial de Cumplimiento el cual deberá responder a tales requerimientos en los tiempos que interpone la ley.

El procedimiento establecido por la Organización GURUSOFT para dar respuesta a las solicitudes de información recibidas es el siguiente:

- Consulta en el archivo de expedientes existentes, por si se trata de un requerimiento nuevo o bien es la continuación de un requerimiento o comunicación anterior. En este último caso, se revisará el expediente.
- Se procede a registrarlo y a asignarle un número de referencia, compuesto por un código seguido del año de producción.
- Con carácter urgente se solicitará al área correspondiente, la documentación e información precisa para dar repuesta al requerimiento. La respuesta demandada por el Oficial de cumplimiento se deberá enviar en el mismo día salvo que dada su complejidad ello no sea posible en cuyo caso el plazo máximo de respuesta serán dos días.
- Se remite un correo electrónico informando del requerimiento y el sentido de la respuesta que procede, a los miembros del Comité de Cumplimiento.
- El Oficial de Cumplimiento efectuará la respuesta a la autoridad solicitante a través de los medios que hubiese indicado la misma, dentro del plazo establecido en el requerimiento y procederá a cerrar y archivar el expediente.

## IX. Capacitación

La Organización GURUSOFT ha diseñado un plan de capacitación anual, que podrá cumplirse a través de sesiones presenciales y capacitación “on line”, consistente en:

- Sesión anual para colaboradores de las áreas críticas.
- Sesiones formativas específicas dirigidas a los nuevos colaboradores de las áreas críticas, con ocasión de su incorporación.
- Capacitación anual a los colaboradores con cargos críticos.

Al momento de determinar el plan de formación anual y los contenidos de los cursos, se determinará quién es la persona encargada de dictar los mismos, dependiendo de los contenidos previstos.

El Oficial de Cumplimiento velará porque se cuente con un registro de los colaboradores asistentes.

Las acciones de capacitación se desarrollarán bajo la coordinación del Oficial de Cumplimiento y la documentación soporte estará a disposición de todos los colaboradores de acuerdo al medio establecido para tal fin.

Con carácter general, la capacitación se centrará en los siguientes aspectos:

- Políticas de aceptación de clientes y proveedores y de prevención del Lavado de Activos y Financiación del Terrorismo, así como los procedimientos establecidos para prevenir la utilización de la Organización para la financiación de actividades delictivas.
- Requerimientos legales actuales o futuros.
- Identificación de las personas o departamentos a cargo de la prevención del Lavado de Activos y Financiación del Terrorismo.
- Procedimientos de comunicación de cualquier sospecha o conocimiento acerca de actividades relacionadas con el Lavado de Activos y Financiación del Terrorismo al Oficial de cumplimiento.

- Posibles vulnerabilidades o debilidades de su línea de negocio o productos frente a actividades de Lavado de Activos y Financiación del Terrorismo.

Así mismo, la capacitación se adaptará cada año al conocimiento de las nuevas tipologías de Lavado de Activos y Financiación del Terrorismo según se vayan conociendo a través de las publicaciones emitidas por la UIAF, u otros órganos nacionales e internacionales relacionados con la lucha contra el Lavado de Activos y Financiación del Terrorismo, así como por la propia experiencia adquirida por la Organización.

## X. Auditoría interna

El Departamento de Auditoría Interna tiene bajo su responsabilidad supervisar el sistema de Prevención del Lavado de Activos y Financiación del Terrorismo, que está integrado por las políticas, normas y procedimientos de obligado cumplimiento, asegurando que las operaciones de la Organización GURUSOFT se realizan de acuerdo con la legislación vigente contra el Lavado de Activos y Financiación del Terrorismo. Con esta finalidad, Auditoría Interna realizará las revisiones necesarias conforme a lo establecido en normatividad aplicable. Como mínimo, dichas revisiones se realizarán con carácter anual. Los resultados de las verificaciones realizadas junto con su correspondiente informe deberán ser entregados al Oficial de cumplimiento quien lo discutirá y analizará con el fin de presentarlo al Comité de Cumplimiento y posteriormente a la Junta Directiva.

Las referidas revisiones incluyen a todas las áreas críticas en materia de Prevención del Lavado de Activos y Financiación del Terrorismo, en especial al Comité de Cumplimiento y al Oficial de Cumplimiento y se centrarán en la verificación de su supervisión y coordinación necesaria sobre los procedimientos implantados, que aseguren a la Organización el cumplimiento de la normas vigentes internas y externas aplicables en materia de Prevención del Lavado de Activos y Financiación del Terrorismo.

En particular, la auditoría se centrará en la revisión de aspectos concretos tales como el cumplimiento de los procedimientos de identificación y conocimiento del cliente y proveedor, conservación de la documentación requerida, detección, análisis y comunicación de operaciones susceptibles de estar vinculadas con el Lavado de Activos y Financiación del Terrorismo, respuesta a los requerimientos de las autoridades competentes, así como los correspondientes reportes mensual exigidos por la normativa colombiana y la capacitación interna de empleados, entre otros.

## XI. Revisoría Fiscal

De conformidad con lo requerido en la legislación colombiana, las medidas de prevención del Lavado de Activos y Financiación del Terrorismo implantadas por la Organización GURUSOFT podrán ser revisadas durante el proceso de revisoría fiscal de la Organización.

Dicha revisión deberá realizarse de conformidad con la obligación de fiscalización del cumplimiento normativo de las Entidades.

Los resultados de la revisión efectuada deberán quedar plasmados por escrito, en un informe anual que tendrá que ser presentado al Oficial de Cumplimiento.

## XII. Sucursales

El presente manual, aprobado por la Junta Directiva de la Organización, establece los estándares mínimos que las Empresas de la Organización deben observar.

Está dirigido a todos los colaboradores de las áreas críticas de la Organización y aquellas personas que, en nombre de cualquier empresa, establezcan relaciones con terceros.

Esta política y las normas que la desarrollan son de obligatorio cumplimiento en todas las sucursales de la Organización a nivel Colombia.

## XIII. Sanciones

### 13.1 Sanciones administrativas

El artículo 43 de la Ley 190/1995, modificado por la Ley 1121/2006 indica que “las obligaciones establecidas en los artículos 102 a 107 del Estatuto Orgánico del Sistema Financiero (Decreto 663 de 1993) y demás normas concordantes serán aplicables en lo pertinente a las personas que se dediquen profesionalmente a actividades de comercio exterior, operaciones de cambio y del mercado libre de divisas, casinos o juegos de azar, así como aquellas que determine el Gobierno Nacional”.

Así mismo, el artículo 10 de la Ley 1121/2006 indica que “el régimen previsto para las instituciones sometidas al control y vigilancia de la Superintendencia Financiera, o de la entidad que haga sus veces..., salvo norma especial, se aplicará a las entidades o personas obligadas a cumplir con las normas y principios contenidos en los artículos 102 a 107 del Estatuto Orgánico del Sistema Financiero” y establece que “la aplicación del procedimiento e imposición de las sanciones será realizada por la respectiva autoridad que ejerza las funciones de inspección, control o vigilancia, para lo cual dará cumplimiento a las normas administrativas de carácter especial que le sean aplicables o en su defecto dará aplicación al procedimiento contemplado en el Código Contencioso Administrativo.

Conforme al art. 107 del Estatuto Orgánico del Sistema Financiero (Sanciones), el incumplimiento de lo dispuesto en los artículos 102 a 106 por la no adopción o aplicación de los mecanismos de control dará lugar a la imposición de las sanciones administrativas correspondientes, sin perjuicio de las consecuencias penales a que hubiere lugar.

Las siguientes son las sanciones de carácter administrativo que la SFC puede imponer:

- a) Amonestación o llamado de atención.
- b) Multa pecuniaria a favor del Tesoro Nacional.
- c) Suspensión o inhabilitación hasta por cinco (5) años para el ejercicio de aquellos cargos en entidades vigiladas por la Superintendencia que requieran para su desempeño la posesión ante dicho organismo.
- d) Remoción de los administradores, directores, representantes legales o de los revisores fiscales de las personas vigiladas por la Superintendencia. Esta sanción se aplica sin perjuicio de las que establezcan normas especiales.
- e) Clausura de las oficinas de representación de instituciones financieras y de reaseguros del exterior.

Las multas pecuniarias previstas podrán ser sucesivas mientras subsista el incumplimiento que las originó.

El numeral 3º del artículo 211 del Decreto 663 de 1993, señala que cuando la violación recaiga sobre las disposiciones contenidas en el Capítulo XVI del Estatuto Orgánico del Sistema Financiero (PREVENCIÓN DE ACTIVIDADES DELICTIVAS), la multa que podrá imponerse será hasta de mil setecientos cuarenta y dos millones de pesos (\$1.742.000.000.00) de 2002. Establece el artículo 208 del Estatuto Orgánico del Sistema Financiero, que las sumas indicadas se ajustarán anualmente, en el mismo sentido y porcentaje en que varía el índice de precios al consumidor suministrado por el Departamento Administrativo Nacional de Estadística (DANE).

Adicionalmente, el Superintendente Bancario (hoy Superintendente Financiero) podrá ordenar al establecimiento multado que destine una suma hasta de mil setecientos cuarenta y dos millones de pesos (\$1.742.000.000.00) de 2002 a la implementación de mecanismos correctivos de carácter interno que deberá acordar con el mismo organismo de control.

Sumado a ello, la Resolución 285 de 2007, de la Unidad de Información y Análisis Financiero, modificada por la Resolución 212 de 2009, dirigida a los depósitos públicos y privados, sociedades de intermediación aduanera, sociedades portuarias, usuarios de zona franca, empresas transportadoras, agentes de carga internacional, usuarios aduaneros permanentes y usuarios altamente exportadores, establece que “el incumplimiento de la obligación de reportar operaciones sospechosas y operaciones individuales en efectivo por un monto igual o superior a 10.000.000 de pesos, dará lugar a la imposición de las respectivas sanciones por parte de

la Dirección de Impuestos y Aduanas Nacionales (DIAN) o la respectiva entidad competente, sin perjuicio de las acciones disciplinarias o penales a que haya lugar”.

### 13.2 · Sanciones penales

En materia penal, además del tipo base de lavado de activos se han tipificado igualmente otras conductas, relacionadas con el no cumplimiento de medidas al Lavado de Activos y Financiación del Terrorismo:

- El artículo 323 del Código Penal define el **lavado de activos** como: "El que adquiera, resguarde, invierta, transporte, transforme, custodie o administre bienes que tengan su origen mediato o inmediato en actividades de tráfico de migrantes, trata de personas, 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 psicotrópicas, o le de 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 se 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.
- Las penas privativas de la libertad previstas se aumentarán de una tercera parte a la mitad cuando para la realización de las conductas se efectuaren operaciones de cambio o de comercio exterior, o se introdujeran mercancías al territorio nacional.
- La responsabilidad penal se extiende en grado de coparticipación, autor o cómplice, a los partícipes en la operación sean estos exportadores, importadores o auxiliares de la función aduanera o cambiaria.
- La responsabilidad penal recae sobre la persona natural, ya sea como autor, coautor, determinante, cómplice, interviniente y quien actúe a nombre de otro ya sea como miembro u órgano de representación autorizado o de hecho de una persona jurídica, de un ente colectivo sin tal atributo, o de una persona natural cuya representación voluntaria se detecte, y realice la conducta punible, aunque los elementos especiales que fundamentan el tipo penal respectivo no concurren en él, pero sí en la persona o ente colectivo representada.

### 13.3 Sanciones a empleados

Los empleados de las empresas de la Organización GURUSOFT sujetas a la aplicación de las medidas y procedimientos previstos en el presente Manual, podrán ser objeto de sanciones por el incumplimiento del mismo.

Dichas sanciones serán determinadas por el Comité de Auditoría y el Comité de Cumplimiento, en el ejercicio de sus funciones de prevención del Lavado de Activos y Financiación del Terrorismo en la Organización.