TABLA DE CONTENIDO

1. OBJETIVO

1.1 OBJETIVO GENERAL

Establecer los lineamientos metodológicos, roles y responsabilidades de los actores claves para la Gestión del Riesgo de Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (en adelante LAFT/FPADM).

1.2 OBJETIVOS ESPECÍFICOS

- Orientar a las entidades en la definición y posible estandarización de los criterios de calificación y metodologías que permitan consolidar homogéneamente la información de éstas por parte de Grupo Aval.

- Empoderar a las unidades de cumplimiento de las entidades para que lideren el proceso de estandarización de la gestión de riesgo de LAFT/FPADM.

- Definir, compartir y adoptar las mejores prácticas a ser implementadas por las entidades, de manera que sean consistentes con recomendaciones internacionales tales como la "Adecuada gestión de los riesgos relacionados con el blanqueo de capitales, la proliferación de armas de destrucción masiva y la financiación del terrorismo" propuesta por el Comité de Basilea (Banco de Pagos internacionales – BPI), y las de otros organismos internacionales.

- Seguir los lineamientos y mejores prácticas internacionales, Grupo Aval orienta a sus entidades obligadas y no obligadas para que dentro de sus políticas, normas, procesos y controles asociados al riesgo del lavado de activos y de la financiación del terrorismo, apliquen las recomendaciones expedidas por el Grupo de Acción Financiera Internacional (GAFI).

2. ALCANCE

Velar por la aplicación de la presente política es responsabilidad de la Vicepresidencia Corporativa de Riesgos y Cumplimiento de Grupo Aval, no obstante, por tratarse de un proceso inherente al funcionamiento de las diferentes unidades del negocio de la organización, es responsabilidad de Grupo Aval y sus subordinadas conocer, acatar y aplicar las directrices establecidas en este documento, de acuerdo con las características particulares y normatividad aplicable a cada una de ellas.

3. LINEAMIENTOS GENERALES

3.1 POLÍTICAS

Grupo Aval acoge las siguientes políticas sobre los cuales fundamenta y estructura el Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo y de Proliferación de Armas de Destrucción Masiva (LAFT/FPADM) de Grupo Aval y sus entidades subordinadas. Tales políticas son expresiones de la gerencia para una presentación y valoración justa y transparente de dichos riesgos en los estados financieros y demás revelaciones de las Administraciones de Grupo Aval y las entidades subordinas. Lo anterior permite hacer una adecuada identificación de los controles que mitigan razonablemente los riesgos identificados.

3.1.1 Generales

- **Adoptar y mantener una sólida cultura del riesgo LAFT/FPADM.**
  La Administración de Grupo Aval y sus subordinadas deben tomar la iniciativa en el establecimiento de una sólida cultura de administración de riesgos Lavado de Activos y Financiación del Terrorismo y de Proliferación de Armas de Destrucción Masiva. La misma debe guiarse y apoyarse en directrices e incentivos apropiados para el comportamiento profesional y responsable de todos los miembros de las entidades. En este sentido, es responsabilidad de cada administración asegurarse de que exista una fuerte cultura de gestión del riesgo LAFT/FPADM en toda la organización.

- **Implementar y mantener un "Marco de Gestión del Riesgo – LAFT/FPADM".**
  Grupo Aval y sus subordinadas deben desarrollar, implementar y mantener un marco que esté totalmente integrado con los procesos de gestión de sus riesgos generales. Dentro de los marcos establecidos para la gestión del riesgo se encuentran: Norma NTC ISO 31000:2018, Análisis DOFA y Perfil de Capacidad Interna PCI, seleccionadas por una variedad de factores, incluyendo su naturaleza, magnitud, general aceptación por parte de los órganos de regulación tanto nacionales como del exterior.

- **Asegurar la Administración y Gestión del Sistema de Gestión del Riesgo LAFT/FPADM.**
  Las juntas directivas y/o comités de auditoría deben establecer, aprobar y revisar periódicamente el "Marco de Gestión del Riesgo Lavado de Activos y Financiación del Terrorismo". Así mismo, debe supervisar a la administración para asegurarse de que las políticas, procesos y sistemas se aplican eficazmente en todos los niveles de decisión.

- **Cero tolerancia al delito de Lavado de Activos y de la Financiación al Terrorismo y de la Proliferación de Armas de Destrucción Masiva.**
  Las entidades deben estar comprometidas con una política de "cero tolerancia" frente al delito de Lavado de Activos y de la Financiación al Terrorismo y de Proliferación de Armas de Destrucción Masiva, que promueva una cultura de lucha contra el mismo y que permita conducir sus negocios y operaciones con altos estándares éticos, en cumplimiento de las leyes y regulaciones vigentes.

- **Compromisos de la Administración**
  La administración de las entidades debe desarrollar para la aprobación por parte de sus juntas directivas, una estructura de gestión clara, eficaz y robusta con líneas de responsabilidad bien definidas, transparentes y coherentes. Las administraciones de todas las entidades son responsables por su implementación de forma consistente y de mantener en toda la organización políticas, productos, actividades, procesos y sistemas para la adecuada gestión del riesgo de LAFT/FPADM.

- **Modelo de las tres líneas**
  Las entidades deben estructurar las funciones y responsabilidades frente al LAFT/FPADM, y en general frente a todos los riesgos, siguiendo la metodología de las tres líneas, esto es, considerando (i) la gestión por la línea de negocio, (ii) una función de gestión del riesgo LAFT/FPADM independiente, y (iii) una revisión independiente, tal y como lo establece el Marco para la Gestión Integral del Riesgo.

  - **Primera Línea**
    La primera línea la constituyen las áreas operativas que gestionan el negocio (p.ej. las actividades de cara al público y en contacto directo con los clientes). Esto significa que el gobierno del riesgo LAFT/FPADM reconoce que la gestión de la primera línea de negocio es responsable de identificar, evaluar, gestionar y controlar los riesgos

inherentes a los productos, actividades, procesos y sistemas de los que es responsable. Esta línea debe conocer y aplicar las políticas y procedimientos, así como disponer de los recursos suficientes para realizar eficazmente estas tareas.

- **Segunda Línea**
  La segunda línea asigna responsabilidades a la unidad que lidera el Oficial de Cumplimiento en las entidades obligadas y el líder SARLAFT (o quien haga sus veces) en las entidades no obligadas, la cual debe hacer un seguimiento continuo del cumplimiento de todas las obligaciones en materia de Riesgo LAFT/FPADM por parte de su entidad. Esto implica hacer una validación del cumplimiento de la normatividad y un análisis de los informes de anomalías de manera que pueda comunicarlas a la alta dirección o a la junta directiva y/o al comité de auditoría de las entidades. Para el efecto, debe cuestionar a las áreas de negocio utilizando adecuadas herramientas de gestión del riesgo LAFT/FPADM, realizando actividades de medición del riesgo y utilizando los sistemas de información de riesgo LAFT/FPADM. El Oficial de Cumplimiento en las entidades obligadas o el Líder SARLAFT (o quien haga sus veces) en las entidades no obligadas debe ser el contacto para todas las cuestiones en esa materia de las autoridades internas y externas, incluidas las autoridades supervisoras o las unidades de inteligencia financiera (UIAF) o las autoridades jurisdiccionales.

- **Tercera Línea**
  La tercera línea juega un papel importante al evaluar de forma independiente la gestión y los controles del riesgo LAFT/FPADM, así como los procesos y sistemas de la entidad, rindiendo cuentas al comité de auditoría o a un órgano de vigilancia similar mediante evaluaciones periódicas de la eficacia del cumplimiento de las políticas y procedimientos para la gestión del Riesgo LAFT/FPAMD. Aquellas áreas (por lo general las auditorías internas) que deben realizar estas revisiones, deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura riesgo/control. Esta revisión puede ser realizada por la auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados.

3.1.2 Identificación y medición de riesgos

Las administraciones deben asegurar la identificación y evaluación del riesgo LAFT/FPADM que se encuentran en todos los procesos, productos, actividades y sistemas, considerando la actividad principal de la entidad, su estructura y su alcance regulatorio (sujeto obligado o no obligado), para la identificación de los riesgos inherentes.

3.1.3 Control y mitigación

En la gestión y administración del SARLAFT/SAGRILAFT adoptada por las entidades, se deberán aplicar medidas de prevención y control para prevenir ser utilizados como instrumentos para el ocultamiento, manejo, inversión o aprovechamiento en cualquier forma de dinero u otros bienes, provenientes de actividades delictivas o destinadas para su financiación, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos vinculados, de esta manera asegurar u adecuado ambiente de control, estructurado mediante, políticas, procesos, sistemas, controles internos y adecuado monitoreo de la efectividad de las medidas de control en materia de riesgo LAFT/FPADM.

3.1.4 Monitoreo

La administración de las entidades debe implementar un proceso para monitorear regularmente los perfiles de riesgo de LAFT/FPADM y las exposiciones a pérdidas

importantes asociadas a multas o sanciones. Se deben establecer adecuados flujos de información que apoyen la gestión proactiva del riesgo LAFT/FPADM por parte de los diferentes actores del modelo.

3.1.5 Flexibilidad empresarial y continuidad

Las entidades deben tener la capacidad de adaptación empresarial y planes de continuidad para asegurar la capacidad de operar ante impactos materiales y/o reputacionales y, ante eventos que pongan en entredicho el giro ordinario del negocio.

3.1.6 Reporte

- **Divulgación**
  La información pública de las entidades debe permitir a los interesados evaluar su enfoque de la gestión del riesgo LAFT/FPADM.

- **Nuevos productos o modificación**
  Las entidades deben garantizar previo al lanzamiento o uso de cualquier producto, al uso de nuevas prácticas comerciales, incluyendo nuevos canales de prestación de servicios y el uso de nuevas tecnologías o tecnologías en desarrollo para productos nuevos o existentes, la modificación de las características del producto, la incursión en un nuevo mercado, apertura de operaciones en nuestras jurisdicciones y al lanzamiento o modificación de los canales de distribución.

- **Actualización de la información del cliente**
  Las entidades realizarán las diligencias necesarias para actualizar de forma periódica en función del nivel de riesgo, la información suministrada por los clientes, que por su naturaleza pueda variar (dirección, teléfono, actividad, ingresos, origen de los recursos, accionistas y/o beneficiarios finales, etc.), o cuando se requiera aclarar cualquier concepto por parte de la entidad o por las autoridades competentes, de esta manera la entidad debe mantener un indicador de actualización, y realizar monitoreo del cumplimiento de forma constante.

  En el caso de las personas pertenecientes a los segmentos más riesgosos, dicha verificación deberá realizarse al menos anualmente.

  En jurisdicciones diferentes a Colombia prima la reglamentación más conservadora entre la local y la colombiana.

3.1.7 Capacitación

Las políticas, normas y procedimientos establecidos por las entidades para prevenir y controlar el lavado de activos y la financiación del terrorismo, enmarcan sus directrices de cumplimiento en la presente política, por tanto, es responsabilidad de las unidades de cumplimiento o quien haga sus veces asegurar el debido proceso de capacitación de los colaboradores, así mismo asegurar que estén dentro de los procesos de inducción a los nuevos colaboradores. La capacitación se podrá impartir de manera presencial o virtual.

3.2 MODELO DE RIESGO LAFT/FPADM CORPORATIVO

Este modelo corporativo orienta a las entidades del grupo en la estandarización de las metodologías para la administración del Riesgo LAFT/FPADM, asegurando que las

entidades atiendan los principios y normatividad dispuestos por los órganos de control de cada país y mitiguen el riesgo LAFT/FPADM.

Con este modelo las entidades de Grupo Aval cuentan con los elementos para realizar la gestión de los riesgos de LAFT/FPADM alineado a las buenas prácticas, dando cumplimiento el marco normativo.

Este requisito debe considerarse una parte concreta de la obligación general de las entidades de contar con sólidos programas de Gestión del Riesgo para tratar toda clase de riesgos, incluidos los riesgos LAFT/FPADM. En este contexto, disponer de políticas y procesos adecuados exige la aplicación de otras medidas adicionales eficaces. Estas medidas también deben ser proporcionadas y estar en función del riesgo, e informadas por la propia evaluación que las entidades hacen de los riesgos LAFT/FPADM (considerando su actividad principal y estructura). LAFT/FPADM[1].

3.2.1 Sistema integral e integración de los componentes del Programa

El programa de cumplimiento para la prevención de LAFT/FPADM debe permitir que sus componentes se encuentren relacionados y sean coherentes entre sí. El eje que permite articular el sistema es la matriz de riesgos en la cual se debe identificar claramente los riesgos / eventos de riesgo / causas, derivados de los análisis de contextos externo e interno de cada entidad, su relación con la segmentación, controles y, finalmente, señales de alerta.

Una vez analizados sus contextos, cada entidad deberá preparar la segmentación e identificar los riesgos / eventos / causas que deben ser insumo para la matriz de riesgo. Además, debe comprender las causas por las que un segmento representa mayor exposición que otro. La identificación de riesgos desde el contexto y la definición de segmentaciones llevan de la mano a la entidad a resumirlos en lo que se denomina matriz de riesgos, en donde se cuantifica la exposición por riesgo residual, en cada segmento, aplicando metodologías definidas de calificación de probabilidades e impactos, y el efecto de contar con controles efectivos que los mitiguen el riesgo inherente.

Finalmente, los resultados de la evaluación de riesgos registrados en la matriz ayudan en la definición de los parámetros a ser calibrados en las herramientas de monitoreo transaccional, siempre enfocados en las exposiciones de mayor riesgo que se observan en cada segmento definido.

El siguiente diagrama describe la interrelación entre los componentes principales del sistema, que permiten visualizar la coherencia entre sí:

[1] Autor: Comité de Supervisión Bancaria de Basilea -Fuente: “Adecuada gestión de los riesgos relacionados con el blanqueo

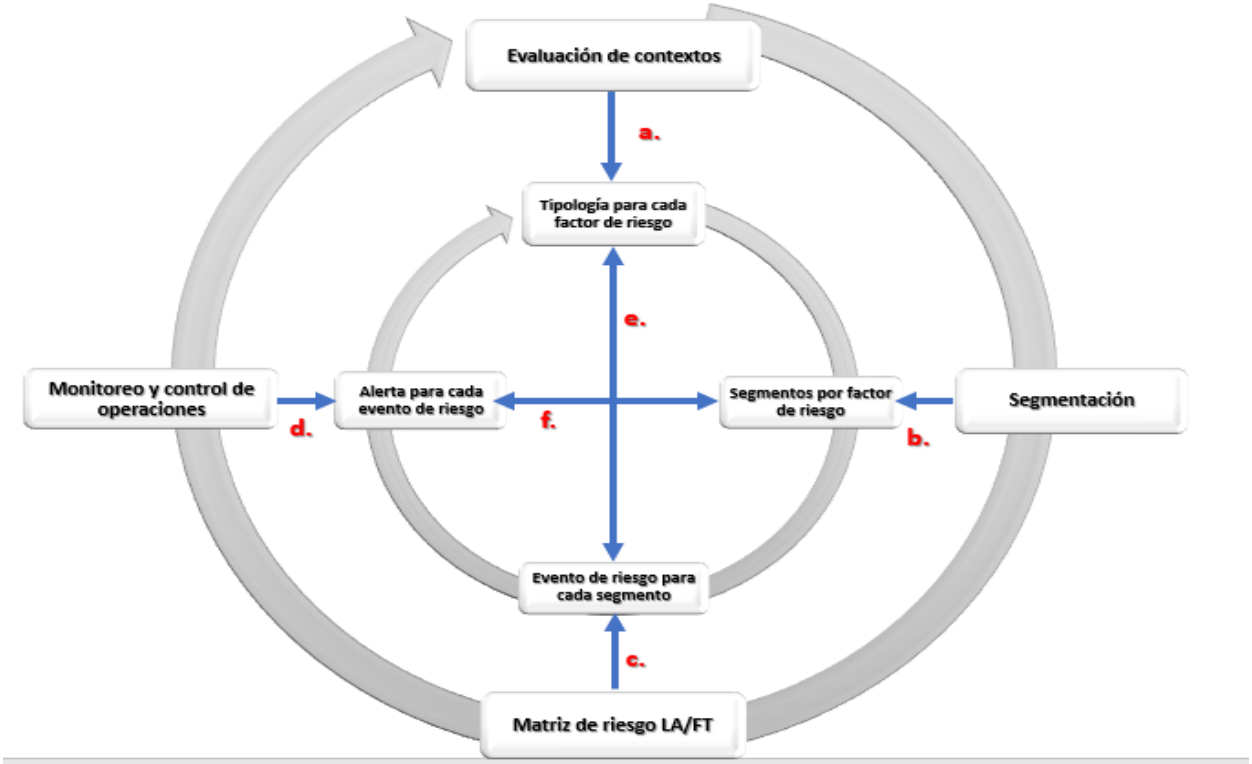


Ilustración. Modelo de integración de componentes

Una ampliación de cómo procede la integración de los componentes del sistema se detalla en documento independiente.

3.2.2 Evaluación y comprensión de los riesgos

3.2.2.1 Gestión del Riesgo[2]

Una sólida gestión del riesgo exige la identificación y el análisis de los riesgos LAFT/FPADM presentes en las entidades, y el diseño y la eficaz aplicación de políticas y procedimientos acordes con los riesgos identificados.

Al realizar un análisis integral del riesgo para evaluar los riesgos LAFT/FPADM, las entidades deben considerar todos los factores de riesgo relevantes, a escala nacional y supranacional cuando sea el caso, sectorial, bancaria y de relación comercial, entre otras líneas de negocio, para determinar su perfil de riesgo y el adecuado nivel de mitigación que se aplicará.

Así pues, las políticas y procedimientos en materia de conocimiento del cliente, aceptación de clientes, identificación de clientes y seguimiento de relaciones comerciales y operaciones (productos y servicios ofrecidos) deben tener en cuenta la evaluación del riesgo y el resultante perfil de riesgo de las entidades.

3.2.2.2 Conocimiento del cliente vinculado por canales presenciales y no presenciales

Las entidades deben diseñar, desarrollar e implementar medidas de debida diligencia para el conocimiento de las personas con quienes tienen relaciones de naturaleza civil, comercial o laboral en función de la calificación del perfil del riesgo.

[2] Principio 15 de los Principios básicos para una supervisión bancaria eficaz, septiembre de 2012. Así como el Principio 6 de los Principles for enhancing corporate governance, octubre de 2010.

El conocimiento debe basarse en datos concretos de operaciones y transacciones y en otra información interna recogida por las entidades, así como en fuentes de información externa independiente, como evaluaciones del riesgo de ámbito nacional e informes sobre países elaborados por organismos internacionales, de acuerdo con lo indicado en el Instructivo – Directiva de Debida Diligencia SARLAFT 4.0 y conceptos que lo aclaren. Las políticas y procedimientos en materia de aceptación de clientes diligencia debida y seguimiento continuo deben diseñarse y aplicarse a clientes nuevos y antiguos vinculados por canales presenciales y no presenciales, para controlar adecuadamente esos riesgos inherentes identificados. Cualquier riesgo residual resultante debe gestionarse en consonancia con el perfil de riesgo de las entidades establecido a partir de su evaluación del riesgo3.

Al evaluar el riesgo, las entidades además de las directrices que imparten los entes de control tanto nacionales como internacionales sobre el conocimiento del cliente4 vinculado por canales presenciales y no presenciales, deben tener en cuenta los siguientes factores, atendiendo las características y naturaleza de cada negocio:

- Los antecedentes del cliente, su ocupación (incluido si ocupa un puesto relevante en el sector público o privado), para debida diligencia ampliada,
- Sus fuentes de renta y riqueza,
- Su país de origen y de residencia (cuando difieran),
- Los productos utilizados,
- La naturaleza y finalidad de sus cuentas,
- Las cuentas vinculadas, en casos de debida diligencia ampliada
- Las actividades comerciales, y
- otros indicadores de riesgo relacionados con el cliente, para determinar cuál es el nivel de riesgo total y las oportunas medidas a adoptar para gestionar esos riesgos.

Esas políticas y procedimientos de conocimiento del cliente vinculado por canales presenciales y no presenciales deben exigir una debida diligencia básica con todos los clientes y una debida diligencia ampliada o intensificada conforme varíe el nivel de riesgo asociado al cliente. El posible cliente desde el momento de su vinculación debe tener determinado el nivel de riesgo de acuerdo con sus características y conforme a este se le deberá aplicar la debida diligencia que corresponda. De manera recurrente las entidades deberán monitorear al cliente para determinar el cambio en su perfil y de presentarse un cambio a un alto riesgo deberán contar con un mes para su actualización de datos aplicando la debida diligencia que corresponda. En caso de situaciones probadas de bajo riesgo, pueden aceptarse medidas simplificadas, siempre que la legislación lo permita.

En el desarrollo de los procedimientos de conocimiento del cliente vinculado por canales presenciales y no presenciales, las entidades obligadas, a medida que cuenten con información adicional, deben dar cumplimiento a los lineamientos corporativos de acuerdo con lo indicado en el Instructivo para debida diligencia y conceptos que lo aclaren, en especial en lo relativo con la debida diligencia simplificada en la cual como mínimo deberá realizarse la verificación de identidad al momento de la vinculación con la siguiente información: el tipo de documento de identificación, el nombre, el número y la fecha de expedición del documento de identificación y solicitar cualquier otra información que estimen pertinente. Estas excepciones legales y las que la ley podría llegar a implementar no eximen a las entidades obligadas de llevar a cabo el conocimiento de sus clientes de acuerdo con los parámetros

[3] Autor: Comité de Supervisión Bancaria de Basilea -Fuente: “Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo” -Enero de 2014.- Sección II - capítulo 1-a).
[4] Circular Externa 055 de 2016 Superintendencia Financiera de Colombia Título I capitulo XI Instrucciones relativas a la administración del riesgo de lavado de activos y de la financiación del terrorismo - Parámetros de los procedimientos de conocimiento del cliente.

establecidos en el Instructivo – Directiva de Debida Diligencia SARLAFT 4.0 destacándose de entre la amplia tipología relacionada, las siguientes (para su detalle dirigirse a la norma):

- Operaciones realizadas con organismos multilaterales.
- La constitución de fiducias de administración para el pago de obligaciones pensionales.
- En los títulos de capitalización colocados mediante mercadeo masivo o contratos de red, siempre que el pago de las cuotas se haga mediante descuento directo de cuenta de ahorros, cuenta corriente o tarjeta de crédito, y que el cliente haya autorizado expresamente el traslado.
- Varios tipos de seguros, como por ejemplo los tomados por entidades financieras, aseguradoras o sociedades administradoras de fondos de pensiones por cuenta de sus clientes; Los relativos a la seguridad social; Los contratos de reaseguro; los seguros otorgados mediante procesos de licitación pública; Los tomados mediante mercadeo masivo o banca seguros siempre que el pago de las primas se haga mediante descuento directo de cuenta de ahorros, cuenta corriente o tarjeta de crédito, y que el cliente haya autorizado expresamente el traslado; Pólizas judiciales; De salud; Exequiales.
- Cuentas de ahorro abiertas exclusivamente para el manejo y pago de pasivos pensionales.
- En los créditos que se instrumentan a través de libranza siempre que estas no excedan de 6 SMMLV y sean otorgadas a empleados de empresas que se encuentren previamente vinculadas en calidad de cliente con la entidad vigilada otorgante del crédito.
- La vinculación a entidades administradoras del sistema general de pensiones en cuanto a los aportes obligatorios. y cesantías.
- La vinculación a entidades administradoras de cesantías en lo relacionado con los recursos provenientes de dicha prestación.
- Cuentas de ahorro abiertas exclusivamente para el pago de nómina. Cuando se manejen otros recursos en tales cuentas, no se aplica dicha excepción.
- Cuentas de ahorro electrónicas de que trata el art. 2.25.1.1.1 del Decreto 2555 de 2010.

Cuando los riesgos sean más elevados, las entidades deben reforzar sus medidas para mitigar y gestionar esos riesgos.

Las decisiones de establecer o proseguir relaciones comerciales con clientes de mayor riesgo (alto o extremo) exigen la aplicación de medidas reforzadas de debida diligencia. La política de aceptación de clientes también debe definir las circunstancias en las cuales la entidad no acepta una nueva relación comercial o cancela una relación ya existente.

Las entidades tendrán un procedimiento para identificar y verificar a sus clientes y, cuando proceda, a cualquier persona que actúe en nombre de aquéllos y de cualquier beneficiario final, siempre y cuando ello sea factible. En general, las entidades no deben establecer una relación comercial, ni realizar transacción alguna, hasta que la identidad del cliente haya sido satisfactoriamente establecida y verificada conforme a la Recomendación 10 del GAFI. En consonancia con el Principio Básico 29 de Basilea y las normas GAFI, los procedimientos también deben incluir la adopción de medidas razonables para verificar la identidad del beneficiario final. La entidad también debe verificar que cualquier persona que actúe en nombre del cliente está autorizada para hacerlo, y debe verificar la identidad de esa persona.

La identidad de clientes y beneficiarios finales, así como de las personas que actúen en nombre de aquéllos, debe verificarse mediante documentos, datos o informaciones fiables e independientes. Cuando se recurra a documentos, la entidad debe tener presente que los mejores documentos para verificar la identidad son aquéllos más difíciles de obtener ilícitamente o falsificar. Cuando se recurra a otras fuentes de información distintas de documentos, la entidad debe cerciorarse de que los métodos (que pueden incluir la

comprobación de referencias con otras instituciones financieras y la obtención de estados financieros) y las fuentes de información son adecuados y están en consonancia con las políticas y procedimientos de la entidad y con el perfil de riesgo del cliente.

La entidad puede exigir a los clientes que diligencien una declaración sobre la identidad y los detalles del beneficiario final, aunque no debe recurrir únicamente a esas declaraciones. Al igual que en todos los elementos del proceso de conocimiento del cliente, la entidad también debe considerar la naturaleza y nivel del riesgo planteado por un cliente cuando determine el alcance de las medidas aplicables de debida diligencia.

En ningún caso debe la entidad evitar sus procedimientos de identificación y verificación de clientes solo porque el cliente no pueda presentarse a una entrevista (clientes no presentes); la entidad también debe tener en cuenta factores de riesgo como el motivo por el cual el cliente ha decidido abrir una cuenta lejos de su sede u oficina, especialmente en otra jurisdicción, cuando se tenga acceso a esta información.

Es importante tener en cuenta los riesgos relevantes asociados a clientes procedentes de jurisdicciones conocidas por sus deficiencias estratégicas en materia de LAFT/FPADM y practicar una diligencia debida reforzada cuando así lo exijan el GAFI, otros organismos internacionales o las autoridades nacionales.

La primera línea de la entidad debe obtener toda la información necesaria para establecer a su entera satisfacción la identidad del cliente y la de cualquier persona que actúe en nombre de aquél y de los beneficiarios finales, en armonía con la legislación vigente (p.ej. Hábeas Data). Si bien la entidad está obligada tanto a identificar a sus clientes como a verificar su identidad, la naturaleza y el alcance de la información requerida para la verificación depende de la evaluación del riesgo, incluidos el tipo de solicitante (persona física, jurídica, etc.) y el volumen y uso previsto del producto y/o servicio solicitado (CDTs, cuentas de ahorro, créditos, giros, etc.). Los requisitos específicos necesarios para comprobar la identidad de las personas físicas suelen establecerse en la legislación nacional o reglamentaria de los supervisores o UIAF. Si el importe de la cuenta es sustancial es aconsejable medidas de identificación adicionales, que deben determinarse en función del nivel de riesgo total.

No obstante, existen circunstancias en las que sería admisible completar la verificación tras establecer la relación comercial, porque resultaría esencial no interrumpir el curso normal de los negocios. En tales circunstancias, la entidad debe adoptar procedimientos adecuados de gestión del riesgo con respecto a las condiciones y limitaciones bajo las cuales el cliente puede utilizar la relación comercial o contractual antes de la verificación, así como consagrar la exigencia de que los funcionarios antepongan el cumplimiento de las normas en materia de administración de riesgo de LA/FT al logro de las metas comerciales.

En situaciones en que la cuenta haya sido abierta, pero surjan problemas de verificación en el transcurso del establecimiento de la relación comercial o contractual que no puedan ser resueltos, las entidades deben bloquear el acceso al producto. En cualquier caso, la entidad obligada debe evaluar si procede a elaborar un reporte de operación sospechosa (ROS) en los casos en que existan problemas para completar las medidas de conocimiento del cliente (con sujeción a la legislación nacional sobre tratamiento de operaciones sospechosas, adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo). Además, cuando las comprobaciones levanten sospechas u ofrezcan motivos razonables para sospechar que los activos o fondos del futuro cliente proceden de infracciones y delitos incluidos en supuestos de LAFT/FPADM, las entidades no deben aceptar voluntariamente la apertura de cuentas a esos clientes. En dichas situaciones, las entidades deben elaborar un ROS, notificándolo a las autoridades competentes (UIAF), y

asegurarse de que el cliente no está informado, ni siquiera de forma indirecta, de que un ROS ha sido, está siendo o será elaborado.

Si una entidad tiene motivos para pensar que otra entidad ha negado servicios a un solicitante por sospechar actividades ilícitas del cliente, debe considerar la clasificación de ese solicitante como de alto riesgo y aplicar procedimientos reforzados de diligencia debida al cliente y a la relación, la entidad, en el caso de tratarse de una entidad obligada, debe evaluar si procede a elaborar un reporte de operación sospechosa (ROS) y/o no aceptar al cliente con arreglo a sus propios procedimientos y evaluaciones del riesgo.

La entidad no debe abrir un producto ni realizar negocios con un cliente que insista en el anonimato o que proporcione un nombre a todas luces ficticio, así como tampoco cuentas confidenciales numeradas, aunque una cuenta numerada puede ofrecer mayor confidencialidad al titular, la identidad de éste debe ser verificada por la entidad y conocida por un número suficiente de empleados para facilitar la práctica de una eficaz diligencia debida, especialmente si otros factores de riesgo indican que el cliente es de mayor riesgo. La entidad debe garantizar que sus unidades internas de control, cumplimiento, auditoría y otras funciones de vigilancia, en particular el Oficial de Cumplimiento en caso de entidad Obligada o Líder SARLAFT (o quien haga sus veces) en entidades no obligadas, así como los supervisores de la entidad, tienen pleno acceso a esta información si fuera necesario[5]

Finalmente, cada entidad debe asegurar la efectiva identidad de los potenciales clientes por canales presenciales y no presenciales, al momento de la vinculación utilizando información de fuentes confiables e independientes como certificados de firma digital, sistemas biométricos, mecanismos fuertes de autenticación, entre otros.

- **Países de mayor riesgo**

Se deberán establecer procedimientos más estrictos e intensificados respecto de las operaciones que se celebren con personas naturales y/o jurídicas, o asimiladas a personas jurídicas, que procesan o tengan destinación, se encuentren relacionadas o vinculadas con países en donde no exista cooperación o no se apliquen las recomendaciones del Grupo de Acción Financiera – GAFI.

3.2.2.3 Perfil del cliente

Si bien el proceso de identificación y verificación del cliente tiene lugar al comienzo de la relación o antes de realizarse una transacción bancaria o financiera, la entidad debe utilizar esa información para individualizar al potencial cliente y determinar su perfil de riesgo y el nivel de debida diligencia a aplicar. La finalidad de la relación o de la transacción bancaria o financiera, el volumen de activos y el de operaciones del cliente, así como la regularidad o duración de la relación, son ejemplos de información habitualmente recabada. Así pues, la entidad debe contar con políticas y procedimientos de debida diligencia con sus clientes que sean suficientes para elaborar perfiles de riesgo de clientes concretos o de determinadas categorías de clientes. La información obtenida a estos efectos debe venir determinada por el nivel de riesgo asociado al modelo de negocio y actividades del cliente, así como a los productos o servicios financieros demandados por éste.

Estos perfiles de riesgo facilitan el nivel de debida diligencia a aplicar a los potenciales clientes, establecer reglas especiales de monitoreo y determinar el plazo de actualización de datos. Los perfiles de riesgo de los clientes facilitan a la entidad determinar posteriormente

[5] **Fuente:** Para el factor cliente se han seguido las directrices planteadas en el documento “Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo” propuesta por el Comité de Basilea (Banco de Pagos internacionales – BPI (Enero de 2014).

si el cliente o categoría de clientes plantea un alto riesgo y exige la aplicación de medidas y controles en la administración del riesgo LAFT/FPADM reforzados.

Los perfiles también deben reflejar el conocimiento que la entidad tiene de la finalidad y naturaleza de la relación comercial o transacción bancaria o financiera ocasional, del volumen de actividad previsto, del tipo de operaciones y de las fuentes de fondos, renta o riqueza del cliente, así como de otras consideraciones análogas. Cualquier información significativa obtenida sobre la actividad o conducta del cliente debe utilizarse para actualizar la evaluación que realiza la entidad del riesgo que presenta el cliente.

La primera línea en la entidad debe verificar la identificación del cliente, así como cualquier otra información y documentación recabada como resultado de la actividad de conocimiento del cliente (CMR - Customer Relationship Management). Esa información puede incluir copias o expedientes de documentos oficiales (como pasaportes, tarjetas de identidad, permisos de conducir), archivos de cuentas (por ejemplo, registros de operaciones financieras) y correspondencia comercial, incluidos los resultados de cualquier análisis realizado, como la evaluación del riesgo y las indagaciones efectuadas para averiguar los antecedentes y la finalidad de las relaciones y actividades comerciales o contractuales y FPADM.

Políticas generales de conocimiento del cliente para las Personas Expuestas Políticamente PEPs

Esta categoría de clientes para las entidades de Grupo Aval requiere la implementación de controles particulares tanto en el momento de la vinculación, como durante el desarrollo de la relación comercial o de negocios, lo anterior considerando que la connotación de PEP sugiere algunos riesgos más notables y sensibles que los de clientes sin este atributo. Dichos riesgos están enmarcados principalmente en la posibilidad o facilidad para apropiarse de recursos del Estado, malversar y desviar fondos públicos con destino a intereses particulares o a la financiación de campañas políticas, grupos al margen de la Ley u otras estructuras o formas de asociación como fundaciones, organizaciones sin fines de lucro que hayan sido creadas con la intención de ocultar o dar apariencia de legalidad a operaciones de LAFT/FPADM.

Lo anterior exige en consecuencia que las entidades implementen medidas de debida diligencia mejorada o intensificada al establecer y mantener relaciones comerciales con esta categoría de clientes.

Para este efecto, es importante determinar el alcance de la denominación de PEPs en el Grupo Aval, considerando como tal a las personas naturales que se cataloguen como: PEPs locales y PEPs extranjeros**.**

Igualmente se catalogan como PEPs, las personas que tengan una sociedad conyugal, de hecho, o derecho con las personas políticamente expuestas nacionales o extranjeras, así como a sus familiares hasta el segundo grado de consanguinidad, primero de afinidad y primero civil.

El tiempo mínimo para mantener la condición de PEPs estará atado al periodo en el que ese tercero ocupe su cargo y el tiempo posterior a la dejación, renuncia, despido, o cualquier otra forma de desvinculación establecido en las diferentes normativas que deben cumplir las compañías de Grupo Aval.

Para la vinculación de un potencial cliente que tenga la calidad de PEP o persona jurídica cuyos beneficiarios finales tengan la calidad de PEP, las entidades deberán llevar a cabo las

siguientes gestiones de debida diligencia:

- Contar con mecanismos para identificarlos, tales como: Inclusión de esta información en los formularios de conocimiento del cliente y contrapartes, a través del uso de preguntas y autodeclaraciones del potencial cliente sobre su posible condición de PEP, la compra de información a proveedores de bases de datos, o el establecimiento de listas internas a través de la recolección de información de uso público, entre otras.

- La verificación de la calidad de PEP debe realizarse previo al inicio de la relación comercial, con el fin de prever procedimientos más exigentes. No se deben admitir excepciones en la entrega de información y/o documentación por parte del solicitante.

- Será fundamental en el proceso de vinculación centrar la atención del equipo comercial en el origen de la riqueza y el origen de los fondos del PEP, para ello cada entidad debe dejar constancia a través de medio verificable de la actividad, profesión u oficio del que provienen los recursos y obtener copia de la declaración de renta, activos o ingresos ante la autoridad tributaria del país donde él mismo reside.

- En el momento de vinculación de un potencial cliente con calidad PEP se deberá efectuar una entrevista presencial o por medios digitales, dejando constancia de ello. Para entidades obligadas por la Superintendencia de Sociedades no es requerido.

Además de aplicar las medidas normales de procedimiento de conocimiento del cliente, se debe obtener la aprobación de la alta gerencia para la vinculación del cliente o para continuar con la relación comercial, adoptar medidas para establecer el origen de los recursos; prever procedimientos más exigentes de vinculación; y realizar un monitoreo continúo e intensificado de la relación comercial. Cabe resaltar que el concepto de alta gerencia no incluye al Oficial de Cumplimiento.

Cuando se conozca que un cliente o beneficiario final adquiere las condiciones para ser PEP, en los términos señalados en la presente política, deberán marcarse como tal en los sistemas, solicitar la actualización de datos toda vez que incrementa su nivel de riesgos, y recabar los documentos que correspondan a esta nueva condición.

Los colaboradores responsables de administrar la relación comercial con estas personas deben propender porque su información se encuentre actualizada, por lo anterior, la periodicidad establecida para la actualización de clientes con esta condición será cómo mínimo anual o antes si existen circunstancias que sí lo ameriten.

Durante la vigencia de la relación comercial con una Persona Expuesta Políticamente, el dueño de la relación comercial debe monitorearla transaccionalidad del cliente para detectar señales de alerta y gestionarlas, especialmente deben tomar medidas para determinar cuál es el origen de los fondos de dichas transacciones.

Por su parte, el equipo de cumplimiento de cada entidad deberá establecer el perfil transaccional del cliente PEP, realizar monitoreos y/o evaluaciones centralizadas especiales a las operaciones realizadas por esta clase de clientes, así como de las personas jurídicas que sean sociedades comerciales, fondos fiduciarios, fundaciones u otras estructuras donde se encuentren vinculados PEPs en calidad de beneficiarios finales o controlantes.

3.2.2.4 Conocimiento de los beneficiarios finales de estructuras sin personería jurídica y de las personas jurídicas, accionistas y/o asociados.

El conocimiento del cliente actual y potencial en cada una de las entidades implica conocer su identidad, para ello se deben obtener los datos que permitan individualizar a cada uno de los clientes actuales o potenciales, determinar la actividad económica que desarrolla el cliente y que constituye el origen de sus recursos, así como establecer el origen y el volumen de los recursos de los cuales el cliente es el titular.

La identificación del beneficiario final que tenga directamente más del 5% del capital social, aporte o participación del potencial cliente en las estructuras sin personería jurídica y de personas jurídicas, así como de los accionistas y/o asociados de personas jurídicas u otras estructuras de naturaleza similar, debe realizarse hasta donde la debida diligencia lo permita, de modo que la entidad esté convencida de que se conoce quién es el beneficiario final y que éste reúne las características incluidas en la definición.

El conocimiento de los beneficiarios finales de estructuras sin personería jurídica y de personas jurídicas, así como de los accionistas y/o asociados de personas jurídicas, se deberá obtener en los procedimientos de vinculación y actualización de clientes o en aquellos casos que, en razón al monitoreo por riesgo, se detecte la necesidad de la actualización de dicha información como parte de las acciones de debida diligencia intensificada.

Las entidades podrán contar con las herramientas, formularios o cuestionarios que consideren necesarios para identificar al beneficiario final de sus clientes personas jurídicas o estructuras similares. Para los casos de compañías en Colombia con las siguientes estructuras: Comandita Simple, Comandita por Acciones, Sociedades Unipersonales y Sociedades Limitadas, se podrá obtener la información de los beneficiarios finales a partir del certificado de existencia y representación legal vigente para la sociedad. Para aquellos tipos societarios donde dicha información no esté disponible, la misma se podrá solicitar al cliente u obtenerse a través de fuentes públicas o privadas previo análisis de riesgo sobre la integridad y confiabilidad de dicha fuente.

Si las entidades tienen duda de la veracidad de la información declarada en los formatos podrán aplicar medidas razonables para dicha identificación que permitan obtener más información. Asimismo, deberá establecer medidas de acuerdo con la información obtenida que determinen si el beneficiario final es una Persona Expuesta Políticamente, en cuyo caso deberán adoptar medidas para establecer el origen de la riqueza y el origen de los fondos de este y así, aplicar necesariamente un monitoreo continúo intensificado y de acuerdo con la exposición al riesgo realizar la debida diligencia.

Para el caso de Personas Jurídicas como Fideicomisos, Fundaciones Privadas, Instituciones sin ánimo de lucro, cuyos beneficiarios finales no pueden ser identificados por participación societaria, se deberá obtener un acta o declaración suscrita por los representantes del cliente, donde se detalle el o los beneficiarios finales.

Para la vinculación de entidades con estructuras societarias complejas, es decir, aquellas que tienen múltiples estructuras jurídicas en sus composición directa e indirecta, y generan opacidad o dificultad para obtener la información de las personas naturales que ostentan la titularidad o control de la compañía, será necesaria la obtención de pruebas satisfactorias sobre la identidad de los beneficiarios finales de dichas sociedades, entendiendo por dichas pruebas aquellos documentos públicos o privados de constitución donde sus nombres y números de identificación sean visibles o en su defecto, la entrega de una certificación escrita del beneficiario real sobre su propiedad en la entidad y de sus controlantes.

En aquellos casos en que no se pueda obtener la información por un documento público o privado, porque el cliente se reserve dicha información aduciendo razones objetivas y el dueño de la relación comercial dé cuenta de situaciones muy particulares del cliente (v.gr. motivos de seguridad personal, etc.), esta información deberá quedar documentada y obtenerse por cualquier otro medio verificable. En este último caso, se debe obtener la aprobación por parte de un colaborador de jerarquía superior definido por cada entidad, quien tomará la decisión sobre la vinculación del potencial cliente previa consulta de su perfil de riesgo.

Para el caso de personas jurídicas o estructuras similares donde definitivamente no pueda individualizarse al beneficiario final o controlante a través de otros medios; y solo cuando no se identifique a una persona natural, las entidades podrán considerar obtener la información de la persona natural que ostente la representación legal y tenga labor de dirección de la compañía. No obstante, no serán susceptibles de exceptuarse de la información sobre el beneficiario final y dejar en su reemplazo la información del funcionario que ostenta la representación legal, aquellos potenciales clientes jurídicos que:

- Aspiran a hacer parte de bancas o segmentos masivos o minoristas, es decir, cuando no tengan calidad de clientes corporativos, o empresariales.
- Pretendan adquirir productos en moneda extranjera u otros catalogados cómo alto riesgo por la entidad.
- Hayan quedado catalogados en el proceso de vinculación como clientes con perfil de riesgo LAFT/FPADM Alto.
- Se trate de compañías o vehículos corporativos que involucren sociedades beneficiarias en diferentes países, generando dificultad para seguir la trazabilidad del dinero y la disponibilidad de la información.
- Tengan un tiempo de constitución menor a un (1) año.

Si el potencial cliente o propietario de la participación mayoritaria es una compañía que cotiza en la Bolsa de Valores de Colombia y/o otras bolsas de valores que no correspondan a jurisdicciones de Alto Riesgo, y está sujeta a requisitos de disponibilidad de información y divulgación, que conducen asegurar la transparencia adecuada del beneficiario final o se trata de una filial propiedad mayoritaria de una compañía, podrán exceptuarse de la entrega de la información del beneficiario final, y en consecuencia no será necesario identificar y verificar la identidad de sus beneficiarios finales, ya que los datos relevantes de identificación si se llegaren a requerir durante la relación comercial pueden ser obtenidos de un registro público del cliente o de otras fuentes confiables. En otras palabras, ello no significa que las sociedades mercantiles que cotizan en bolsa no tengan que identificar a sus beneficiarios finales, sino que se supone que ya lo hacen y que la información sobre ellos ya está disponible en otro sitio.

En ningún caso, se aceptarán como clientes sociedades con acciones al portador o en cuya composición accionaria existan asociados que emitan acciones al portador o con posibilidad de emitir certificados de acciones al portador, así como sociedades que permitan accionistas o directores nominales. En ese caso será necesario requerir que revelen que ellos son nominales, y la identidad de la persona que los nominó, conservando ese registro. Tampoco son susceptible de vincular como clientes a los Bancos Pantalla.

En los casos de estructuras jurídicas, como cooperativas; fondos de empleados; fundaciones; ONGs y similares, se debe identificar a las personas que ocupan una posición en la alta gerencia, sin perjuicio de identificar a los fundadores o gestores y a los principales donantes o aportantes.

Respecto a fideicomisos, es necesario comprender la estructura del negocio fiduciario, quién ostenta la calidad de fideicomitente, quién es el aportante y el beneficiario de los fondos del negocio fiduciario.

Para la identificación del beneficiario final de estructuras sin personería jurídica, el procedimiento de conocimiento del cliente supone identificar y tomar medidas razonables para verificar la identidad de los beneficiarios finales.

3.2.2.5 Contexto interno y externo de las entidades

Las entidades del grupo deben establecer su contexto interno de acuerdo con el marco teórico establecido por Grupo Aval en cuanto a la Norma ISO 31000:2018, Análisis DOFA y la evaluación del Perfil de Capacidad Interna – PCI, la que más valor genere a la Entidad a su criterio experto; de igual forma, la evaluación del contexto externo es realizada desde Grupo Aval de forma transversal para todas las entidades que hacen parte del grupo. Las entidades deben complementar la evaluación de los contextos anteriores considerando las particularidades de su operación.

El contexto interno y externo es opcional para las entidades obligadas y las no obligadas por la Superintendencia de Sociedades, dado que por norma no es exigible.

3.2.2.6 Gestión de la información

3.2.2.6.1 Mantenimiento de registros

- La entidad debe garantizar el registro de toda la información requerida en el contexto del sistema de conocimiento del cliente y debe incluir:
  - El registro de los documentos facilitados al banco al verificar la identidad del cliente o del beneficiario final y
  - la transcripción en los propios sistemas TI de la entidad de la información de Debida Diligencia con el Cliente (DDC) relevante contenida en dichos documentos u obtenida por otros medios.

- La entidad debe desarrollar y aplicar reglas claras sobre los registros que deben mantenerse para documentar la debida diligencia practicada a los clientes y a las transacciones individuales. Estas reglas deben tener en cuenta cualquier medida reglamentada en materia de privacidad.

- Deben incluir una definición de los tipos de información y documentación en los registros, así como el periodo de conservación de estos registros físicos, el cual debe ser acorde con los requerimientos legales y regulatorios, desde el cese de la relación comercial o contractual. Posterior a este tiempo se debe garantizar su reproducción electrónica.

- Aun cuando las cuentas estén canceladas, en caso de una investigación o litigio en curso, todos los registros deben conservarse hasta el cierre del procedimiento o acorde con los requerimientos legales y regulatorios. El mantenimiento de registros completos y actualizados resulta esencial para permitir a la entidad vigilar la relación con su cliente, comprender el negocio y actividades recurrentes del cliente y, si fuera necesario, para aportar un registro de auditoría en caso de controversias, acciones legales o indagaciones o investigaciones que pudieran acarrear medidas reglamentarias o un proceso penal.

- Deben mantenerse registros adecuados que documenten el proceso de evaluación relacionado con el análisis y seguimiento continuo y con las conclusiones extraídas, de

forma que permitan demostrar el cumplimiento de los requisitos de conocimiento del cliente por parte de la entidad y su capacidad para gestionar el riesgo LAFT/FPADM.

3.2.2.6.2 Actualización de la información

Las entidades deben garantizar que los registros mantienen su fiabilidad, vigencia y relevancia periódica y de la actualización de la información con la Debida Diligencia del Cliente. Otras autoridades competentes, agencias policiales o unidades de inteligencia financiera podrán hacer un uso eficaz de esa información para desarrollar sus propias funciones en el contexto de LAFT/FPADM. Además, mantener la información actualizada contribuye a que la entidad vigile eficazmente las actividades anómalas o sospechosas en los productos.

3.2.2.6.3 Suministro de información a los Entes de Control

La entidad debe ser capaz de demostrar a los entes de control, a requerimiento de éstos, la adecuación de sus sistemas de evaluación, gestión y mitigación de riesgos LAFT/FPADM; de su política de aceptación de clientes; de sus procedimientos y políticas sobre identificación y verificación de clientes; de sus procesos de seguimiento continuo y de sus procedimientos para notificar operaciones sospechosas, así como de todas las medidas adoptadas en el contexto de prevención de LAFT/FPADM.

3.2.2.6.4 Notificación de operaciones sospechosas de entidades obligadas

- El proceso para identificar, investigar y notificar operaciones sospechosas a la UIAF debe especificarse claramente en las políticas y procedimientos de las entidades y comunicarse a todo el personal a través de programas periódicos de formación. Estas políticas y procedimientos deben ofrecer a los empleados una descripción clara de sus obligaciones, así como instrucciones para el análisis, investigación y notificación de dichas actividades dentro de la entidad, al igual que directrices sobre la forma de efectuar esos informes.

- Deben existir procedimientos establecidos para evaluar si las obligaciones reglamentarias de la entidad con arreglo a los regímenes de notificación de actividades sospechosas detectadas exigen notificar la transacción a la UIAF y/o a las autoridades supervisoras competentes, si procede. Estos procedimientos deben reflejar el principio de confidencialidad (como mínimo la reserva legal), garantizando que la investigación se desarrolla con rapidez y que los informes se elaboran y notifican oportunamente, incorporando la información. El Oficial de Cumplimiento debe propender por una notificación rápida cuando se sospeche que los fondos u otros activos puedan proceder de actividades delictivas.

- Una vez que se sospecha de una cuenta o relación, además de notificar la actividad sospechosa, la entidad debe garantizar la adopción de medidas oportunas para mitigar adecuadamente el riesgo de que la entidad sea utilizada en actividades delictivas. Estas medidas pueden incluir la revisión de la clasificación de riesgo del cliente o cuenta o de la relación en su totalidad. La adopción de medidas oportunas puede exigir trasladar el asunto en cuestión al nivel decisorio apropiado para determinar la forma de gestionar la relación, teniendo en cuenta cualquier otro factor relevante, como la cooperación con las autoridades.

3.2.2.7 Bloqueo de activos

- La financiación del terrorismo presenta similitudes con el blanqueo de capitales, pero también muestra singularidades que las entidades deben tener en cuenta: los fondos utilizados para financiar actividades terroristas pueden proceder de actividades delictivas o de fuentes lícitas y la naturaleza de las fuentes de financiación puede variar según el tipo de organización terrorista. Además, cabe señalar que los importes de las transacciones asociadas a la financiación de terroristas pueden ser muy reducidos.

- La entidad debe ser capaz de identificar y cumplir las decisiones de bloqueo de fondos adoptadas por la autoridad competente y bajo ningún motivo debe mantener relaciones con entidades o individuos designados (por ejemplo, terroristas, organizaciones terroristas), en consonancia con las pertinentes legislaciones nacionales (colombiana y de países donde se tienen entidades subordinadas) y la legislación americana aplicable relacionada con lavado de activos y financiación del terrorismo.

- El Manejo de Relaciones con Clientes (MRC-CRM) debe permitir a la entidad detectar e identificar posibles transacciones de financiación al terrorismo, propiciando un conocimiento más preciso de sus clientes y de las transacciones que realizan. Al desarrollar sus políticas y procedimientos de aceptación de clientes, la entidad debe abstenerse de relaciones comerciales con entidades o individuos vinculados a grupos terroristas. Antes de establecer una relación comercial o realizar una transacción ocasional con nuevos clientes, la entidad debe comprobar si éstos figuran en listados de terroristas conocidos o presuntos publicados por las autoridades competentes (nacionales e internacionales). Del mismo modo, el seguimiento continuo debe verificar que los actuales clientes no figuran en esos mismos listados.

- Todas las entidades deben contar con sistemas para detectar transacciones prohibidas (como transacciones con entidades designadas en las pertinentes Resoluciones del Consejo de Seguridad de las Naciones Unidas RCSNU o en los listados de sanciones nacionales). La detección de terroristas no es una medida de diligencia debida sensible al riesgo, por lo que debe realizarse independientemente del perfil de riesgo atribuido al cliente. Con el fin de detectar terroristas, la entidad puede adoptar sistemas de detección automática, pero debe asegurarse de que esos sistemas son adecuados a sus fines[6].

3.2.2.8 Utilización de otro banco, institución financiera subordinada del Grupo Aval Para practicar la Debida Diligencia a Clientes

En algunos países, se permite a las entidades utilizar otros bancos, instituciones financieras u otras entidades para practicar la debida diligencia a clientes sin que esto exima la responsabilidad a las entidades. Estos mecanismos pueden adoptar diversas formas, pero, en esencia, suelen conllevar alguna de las situaciones siguientes:

Recurso a terceros:

a. Identificar al cliente y verificar su identidad utilizando documentos, datos o informaciones fiables e independientes.

b. Identificar al beneficiario final en la medida que ello fuera posible y adoptar medidas razonables para verificar su identidad, de forma que la institución financiera quede satisfecha de que conoce quién es el beneficiario final. En el caso de personas y

[6] Autor: Comité de Supervisión Bancaria de Basilea Documento: Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo- Capítulo 5 y 6-Enero 2014.

estructuras jurídicas, las instituciones financieras deben entender la estructura de propiedad y control del cliente.

.

Cuando dependan de otro banco o institución financiera para practicar ciertos aspectos de la DDC, las entidades deberán evaluar la razonabilidad de ese recurso. Además de garantizar la existencia de capacidad legal para formalizar el recurso, los criterios relevantes para su evaluación incluyen:

a. La entidad bancaria, institución financiera u otra entidad (según permita la legislación nacional) a la que se recurra debe estar sometida a una regulación y supervisión tan exhaustiva como el banco, utilizar requisitos comparables para la identificación de consumidores durante la apertura de cuentas y tener una relación previa con el cliente que abre una cuenta en el banco.

b. El banco-entidad y la otra entidad deben formalizar por escrito un convenio o acuerdo reconociendo el recurso del banco-entidad a los procesos con la Debida Diligencia con el Cliente de la otra institución financiera.

c. Los procedimientos y políticas de la entidad deben documentar ese recurso y establecer adecuados controles y procedimientos de evaluación de dicha relación.

d. Podrá exigirse a un tercero que certifique a la entidad que ha aplicado su programa de gestión del riesgo LAFT/FPADM y que practica una Debida Diligencia con el Cliente sustancialmente equivalente a la del banco o coherente con las obligaciones de éste.

e. El banco-entidad debe tener debidamente en cuenta informaciones públicas desfavorables sobre el tercero, como estar sometido a medidas coercitivas por causa de deficiencias o violaciones en materia de LAFT/FPADM.

f. La entidad debe identificar y mitigar cualquier riesgo adicional que plantee recurrir a una multitud de terceros (una cadena de recursos) en vez de mantener una relación directa con una sola entidad.

g. La evaluación de riesgos de la entidad debe considerar la entrega de recursos a terceros como un factor potencial de riesgo.

h. La entidad debe examinar periódicamente a la otra entidad para cerciorarse de que ésta continúa practicando la Debida Diligencia con el Cliente de una forma tan exhaustiva como la entidad. A estos efectos, la entidad debe obtener toda la información y documentación de la Debida Diligencia con el Cliente del banco, institución financiera o entidad a la que recurra y evaluar la diligencia debida practicada, incluido su cotejo con bases de datos locales para garantizar el cumplimiento de los requisitos reglamentarios locales.

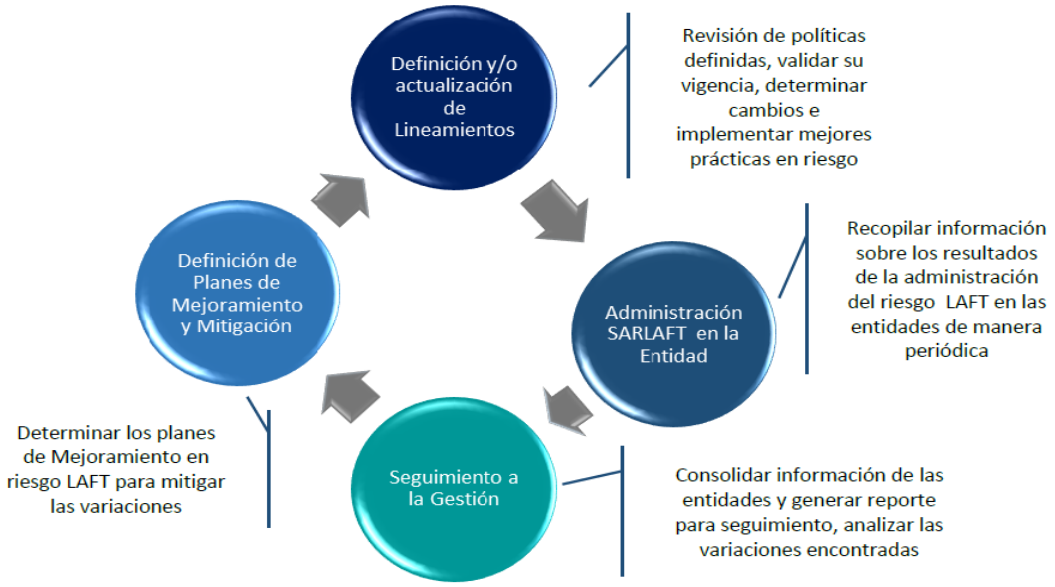
i. Las entidades deben contemplar el cese de su recurso a entidades que no practiquen una adecuada Debida Diligencia con el Cliente a sus clientes o incumplan requisitos y expectativas.

Los bancos con filiales o sucursales fuera de la jurisdicción de origen pueden utilizar el grupo financiero para presentar sus clientes a otras partes del grupo. En países que permiten este recurso transfronterizo a filiales, las entidades que confíen la identificación de clientes a otras partes del grupo deben cerciorarse de la vigencia de los criterios de evaluación precedentes. Se precisa que las normas GAFI40 permiten a los países excluir el riesgo país de esta

evaluación si la institución financiera está sujeta a las normas de LAFT/FPADM de todo el grupo y supervisada a escala del grupo por su supervisor financiero[7].

3.2.3 Etapas del Modelo

El "Modelo de Administración del Riesgo LAFT/FPADM Corporativo" consta de cuatro etapas, las cuales están definidas para direccionar y unificar los criterios de administración del Riesgo de LAFT/FPADM en Grupo Aval y sus entidades subordinadas, etapas que se relacionan de manera cíclica y continua, de acuerdo con el siguiente diagrama:



3.2.3.1 Definición y/o actualización de lineamientos

Desde la Vicepresidencia Corporativa de Riesgos y Cumplimiento de Grupo Aval se proponen los lineamientos corporativos encaminados al cumplimiento de la normatividad aplicable, considerando las diferentes jurisdicciones y tipo de entidades que conforman el Grupo. A través del Comité Corporativo LAFT/FPADM se analiza la viabilidad de dichos lineamientos y se identifican conjuntamente mejores prácticas para robustecer el sistema.

3.2.3.2 Administración del Riesgo LAFT/FPADM en la entidad

Cada entidad adapta el modelo de Gestión de Riesgo LAFT/FPADM atendiendo la normativa propia de su industria y jurisdicción, así como los lineamientos corporativos. Cuando hay cambios en los lineamientos Corporativos, el Oficial de Cumplimiento en el caso de entidades obligadas o el Líder SARLAFT (o quien haga sus veces) en entidades no obligadas, orienta y ejecuta su implementación en el interior de su entidad.

3.2.3.3 Seguimiento a la gestión

Cada entidad debe diligenciar los Reportes de Seguimiento SARLAFT según aplique, con la información de su gestión del riesgo LAFT/FPADM; estos reportes son el insumo para valorar de manera consolidada los riesgos a los cuales están expuestos las entidades.

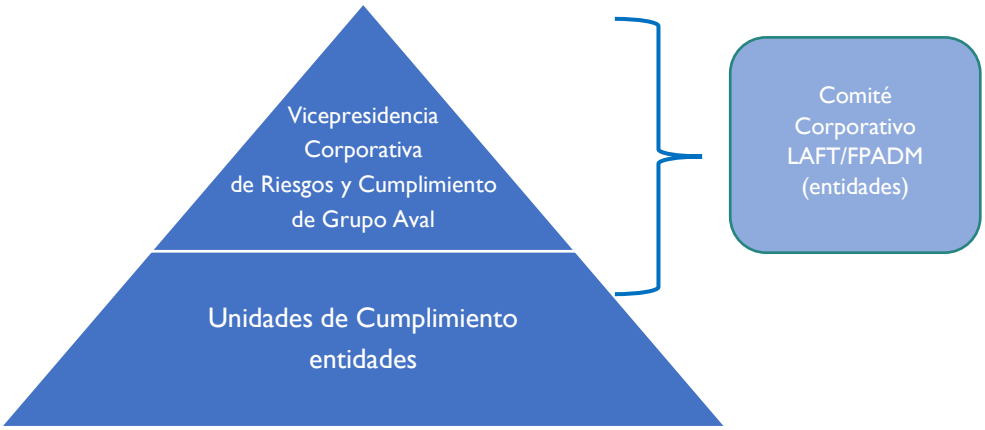
[7] Autor: Comité de Supervisión Bancaria de Basilea Documento: Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo- Anexo 1.

3.2.3.4 Definición de planes de mejoramiento y mitigación

Cada entidad debe velar por mantener un proceso de mejora continua al Sistema. Grupo Aval, en conjunto con las entidades a través de las sesiones del Comité Corporativo LAFT / FPADM identifican cambios normativos o componentes del sistema que requieran ser mejorados/ modificados, para dar cumplimiento a requerimientos legales y para propender por una adecuada y eficiente gestión de los riesgos.

3.2.4 Mecanismos de gobierno adecuado

El modelo define los siguientes actores que participan en las etapas del modelo y tienen funciones específicas.



La participación de los actores en el modelo tiene dos frentes: en la ejecución y en la supervisión, de acuerdo con el detalle del siguiente cuadro de actores y responsabilidades:

Actor	Responsabilidades	
	De Ejecución	De Supervisión
Comité Corporativo LAFT/FPADM Grupo Aval	• Definir las directrices que crean convenientes, tanto para Grupo Aval como para las entidades subordinadas, para el mejoramiento del SGR. Validar la Gestión del SGR por medio de los reportes consolidados que se le presentan periódicamente. Como resultado de esta revisión propone la generación o modificación de lineamientos corporativos que pueden afectar a una o a todas las entidades del Conglomerado, según se requiera.	• Conocer la Gestión de Riesgos realizada por parte de las entidades. • Conocer los eventos de riesgo en las entidades que conforman el grupo y los planes de acción llevados a cabo para la mitigación de estos.
Comité Ejecutivo Riesgo LAFT/FPADM entidades	• Definir el cronograma de reuniones a realizar durante el año vigente. • Realizar reuniones mensuales, para informar de las novedades de los procesos de riesgo LAFT/FPADM en cada entidad. • Determinar y revisar, cuando se requiera, las políticas generales del modelo. • Revisar temas regulatorios que puedan afectar al riesgo LAFT/FPADM y darlos a conocer para tomar medidas de aplicación. • Establecer lineamientos de mejora en los procesos de riesgo LAFT/FPADM. • Compartir las buenas prácticas utilizadas en el mercado	• Conocer el estado de la gestión de riesgo por cada una de las entidades. • Revisar la metodología de riesgo LAFT/FPAMD establecida a nivel corporativo.

Actor	Responsabilidades	
	De Ejecución	De Supervisión
Vicepresidencia Corporativa de Riesgos y Cumplimiento Grupo Aval.	• Diseñar y mantener los formatos de reportes de seguimiento de riesgo LAFT/FPADM. • Reportar el estado actual de la Gestión de Riesgo LAFT/FPADM en las entidades, al Comité de auditoría de Grupo Aval. • Establecer directrices de acuerdo con las mejores prácticas definidas en el Comité. • Mantener actualizadas las políticas de los SGR de acuerdo con las directrices impartidas por Grupo Aval.	• Recibir y consolidar información de los diferentes riesgos de las entidades para generar reportes de monitoreo periódicos. • Establecer desviaciones a los principios y convocar cuando lo considere necesario para efectuarse ajustes.
Áreas de cumplimiento de las entidades	• Presentar Informe de Gestión conforme a la aplicabilidad de los requerimientos, atendiendo la actividad principal de la entidad, su estructura y enfoque regulatorio (entidad obligada trimestralmente y no obligada semestralmente). • Participar mensualmente en el Comité Ejecutivo de Riesgo LAFT/FPADM entidades • Adoptar y socializar las mejores prácticas recibidas de Grupo Aval.	• Analizar y monitorear las operaciones diarias de la entidad garantizando la aplicación del riesgo LAFT/FPADM.

3.2.5 Actores del Modelo

3.2.5.1 Responsabilidades de Grupo Aval Acciones y Valores S.A.

Velar por la gestión eficiente del Riesgo del Lavado de Activos, Financiación del Terrorismo y Proliferación de Armas de Destrucción Masiva por parte de sus subsidiarias.

3.2.5.2 Responsabilidades de las entidades de Grupo Aval

- Gestionar el riesgo LAFT/FPADM bajo su entera responsabilidad conforme a las políticas internas definidas y la normatividad vigente aplicable.

- La entidad debe realizar un seguimiento continuo de todas las relaciones comerciales y transacciones, ya que este constituye un aspecto esencial de una sólida y eficaz gestión del riesgo LAFT/FPADM. El alcance de este seguimiento debe estar en función del riesgo identificado en la evaluación de riesgos realizada por la entidad en sus labores de conocimiento del cliente. Debe reforzar el seguimiento de los clientes o transacciones de alto riesgo y mantener una vigilancia transversal de los productos o servicios con el fin de identificar y mitigar los patrones de riesgo emergentes.

- Todas las entidades deben disponer de sistemas para detectar transacciones o patrones de actividad inusual o sospechosos (acorde a su tipo y tamaño considerando las características de su negocio). Al diseñar escenarios para identificar dichas actividades, la entidad debe considerar el perfil de riesgo del cliente elaborado de acuerdo con la Directiva para la Debida diligencia.

- La entidad debe aplicar políticas y procedimientos robustos de debida diligencia para los clientes que sean identificados como de alto riesgo detallados en esta Política.

- La entidad debe asegurar que dispone de sistemas integrados de gestión de la información, proporcionados a su tamaño, estructura organizativa o complejidad,

basados en criterios de importancia relativa y en los riesgos, que ofrezcan a las unidades de negocio (por ejemplo, los gerentes de relaciones) y a los responsables de riesgos y cumplimiento (incluido el personal de investigación) la oportuna información necesaria para identificar, analizar y realizar un seguimiento eficaz de las cuentas de clientes.

Los sistemas utilizados y la información disponible deben facilitar el seguimiento de esas relaciones con clientes por líneas de negocio e incluir toda la información disponible sobre esa relación con el cliente, incluyendo el historial de transacciones, documentación omitida en la apertura de cuentas y cambios significativos en la conducta o el perfil de negocio del cliente, así como transacciones anómalas efectuadas a través de una cuenta de cliente.

- La entidad debe cotejar su(s) base(s) de datos de clientes cuando haya modificaciones en los listados de sanciones. La entidad también debe cotejar periódicamente su(s) base(s) de datos de clientes para detectar PEPs y otras cuentas de alto riesgo y practicarles una debida diligencia.

- Realizar el reporte de seguimiento del estado actual del Riesgo LAFT/FPADM bajo el formato diseñado por Grupo Aval, y entregarlo un mes subsiguiente al corte.

- Las entidades financieras deben remitir a Grupo Aval, en formato Excel, el reporte de identificación y gestión de operaciones alertadas, inusuales y sospechosas enviado a la Superintendencia Financiera, con la periodicidad indicada en la Circular Externa 018 de 2022.

- Manejar para efectos de reporte consolidado a Grupo Aval la matriz de consolidación de 5 x 5, con los niveles de riesgo según la metodología establecida por Grupo Aval.

- Seguir los lineamientos establecidos por el Comité de Corporativo LAFT/FPADM.

- Fomentar la confianza del público y de los inversionistas; evitando ser utilizadas para LAFT/FPADM velando por mantener la reputación, seriedad y transparencia del negocio.

- Propender por abstenerse de hacer negocios con personas (naturales o jurídicas) cuya ética es o ha sido cuestionable, ya que su vinculación puede afectar la buena imagen de la entidad en el mercado, exponiendo la marca y activos.

- Aplicar las normas contra el LAFT/FPADM y adoptar los controles adecuados para evitar sanciones que puedan imponer las autoridades de supervisión y control a las entidades financieras o a los empleados bancarios.

- Respecto de las relaciones comerciales y transacciones con personas naturales y jurídicas e instituciones financieras de países listados de mayor riesgo por el GAFI, jurisdicciones bajo mayor vigilancia, los procedimientos especiales que establezcan las entidades vigiladas deben contemplar, entre otras medidas, la aplicación de medidas intensificadas de conocimiento del cliente y de monitoreo de aquellas relaciones comerciales y transaccionales con personas naturales y jurídicas.

- Para los países listados por el GAFI como jurisdicciones (países) de alto riesgo, se debe propender por no se tener relaciones comerciales.

- Cumplir con las demás obligaciones que les establezca la ley de acuerdo con su industria, jurisdicción y ente de vigilancia.

3.2.5.3 Responsabilidades AVC

AVC es el apoyo tecnológico de los canales electrónicos de los bancos de Grupo Aval, ya que cuenta con un sistema central de procesamiento de datos, que permite dar soporte a las operaciones financieras que se realizan por medio de éstos y puede analizar las transacciones realizadas por los usuarios, siendo el proveedor de información hacia los bancos y hacia la UIAF en el momento que se requiera.

Por esta razón, AVC en su modelo de riesgo LAFT/FPADM debe:

- Realizar seguimiento de las transacciones de tarjetas internacionales por medio de este canal, identificando comportamientos inusuales de acuerdo con el nivel transaccional de los usuarios de los bancos.

- El Oficial de Cumplimiento de AVC debe reportar las operaciones sospechosas a los oficiales de cumplimiento de las correspondientes entidades (según sea necesario) y a la UIAF, según sea el caso, con el fin de que estos tomen las medidas que consideren necesarias.

- Reportar a los entes de control (comités, junta directiva, etc.) las estadísticas de los ROS reportados a la UIAF.

3.2.5.4 Roles y responsabilidades de la Junta Directiva y/o Alta Gerencia

- Una eficaz gestión del riesgo LAFT/FPADM exige unos mecanismos de gobierno adecuados. En particular, el requisito de que la Junta Directiva y/o Comité de Auditoría apruebe y supervise las políticas en materia de riesgos, gestión del riesgo y cumplimiento es totalmente relevante en el contexto del riesgo LAFT/FPADM. La Junta Directiva y/o el Comité de Auditoría deben comprender claramente los riesgos LAFT/FPADM. La información sobre la evaluación del riesgo LAFT/FPADM debe comunicarse a la Junta Directiva y/o Comité de Auditoría de forma puntual y oportuna, completa, comprensible y precisa, a fin de capacitarlo para adoptar decisiones informadas.

- La Junta Directiva debe asignar las competencias explícitas teniendo realmente en cuenta la estructura de gobierno de la entidad para garantizar la gestión eficaz de las políticas y procedimientos. La Junta y/o la alta dirección deberán nombrar un Oficial de Cumplimiento para entidades obligadas o un Líder SARLAFT (o quien haga sus veces) para entidades no obligadas LAFT/FPADM con la preparación adecuada para asumir las competencias generales de esa función y con la categoría y autoridad necesarias dentro de la entidad para que las cuestiones planteadas en esta política reciban la necesaria atención de la Junta, la alta dirección y las líneas de negocio[8].

3.2.6 Riesgo LAFT/FPADM a escala de Grupo y en un contexto transfronterizo

Cuando un grupo financiero como Grupo AVAL opera en otras jurisdicciones, se requiere de una sólida gestión del riesgo LAFT/FPADM, lo cual implica tener en cuenta los requisitos legales de los países de acogida. Dados los riesgos, Grupo AVAL debe aplicar las políticas y procedimientos de riesgo LAFT/FPADM vigentes de acuerdo con la legislación colombiana a escala del Grupo, con una aplicación y supervisión coherentes.

[8] Autor: Comité de Supervisión Bancaria de Basilea -Fuente: “Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo” -Enero de 2014.- Sección II - capítulo 1-b)

A su vez, las políticas y procedimientos en sucursales y filiales, aun cuando tengan en cuenta los patrones de negocio locales y los requisitos de la jurisdicción de acogida, deben secundar y ser coherentes con las políticas y procedimientos generales para todo el Grupo. En los casos en que los requisitos de la jurisdicción de acogida sean más estrictos que los de Grupo AVAL, la política del Grupo debe permitir a la sucursal o filial su adaptación y aplicación de los requisitos locales de la jurisdicción de acogida.

A nivel de Grupo y subsidiarias se deben seguir las pautas mínimas establecidas por la Superintendencia Financiera de Colombia[9]:

Las entidades obligadas en Colombia que se encuentren en las situaciones previstas en los arts. 260 del Código de Comercio y el art. 28 de la Ley 222 de 1995 pueden llevar a cabo la vinculación de clientes a través de la entidad del Grupo que establezca una relación contractual y lo vincule por primera vez, siempre y cuando se dé cumplimiento a las siguientes reglas:

- La responsabilidad de adelantar todas las gestiones necesarias tendientes a confirmar y actualizar, como mínimo, en forma anual la información corresponderá a la entidad obligada que el Grupo designe para el efecto o, en su defecto, a la matriz.

- El Grupo puede mantener el diseño del formato único de vinculación de cliente en físico o en digital, que contenga, cuando menos, la totalidad de los requisitos de información exigidos en el Instructivo – Directiva de Debida Diligencia SARLAFT 4.0, así como la información requerida respecto de todos los productos que ofrezcan las entidades del Grupo. Así mismo, el formato debe contener una estipulación en la que el cliente autorice de manera expresa e inequívoca su remisión a las demás entidades del mismo Grupo a las que sucesivamente se vincule. En todo caso corresponderá a la entidad con la cual se pretende vincular el potencial cliente determinar cuál información, además de la mínima exigida en el Instructivo – Directiva de Debida Diligencia SARLAFT 4.0, debe suministrarle para llevar a cabo su vinculación.

- La responsabilidad de actualizar la información adicional a la mínima estará en cabeza de cada una de las entidades con las cuales el cliente mantenga una relación contractual, sin perjuicio de dar cumplimiento a las demás normas del riesgo LAFT/FPADM.

- Es obligación permanente de cada una de las entidades obligadas que conforman el Grupo incluir las modificaciones y solicitar la información adicional que como resultado de la evaluación y seguimiento de los factores de riesgo haya determinado cada una de ellas como relevante y necesaria para controlar el riesgo de LAFT/FPADM.

3.2.6.1 Proceso global para la gestión del riesgo de clientes

La gestión consolidada del riesgo LAFT/FPADM implica establecer y administrar un proceso de coordinación y aplicación de políticas y procedimientos para todo el grupo, que establezca un punto de referencia sistemático e integral para gestionar los riesgos de las diferentes operaciones nacionales e internacionales de las entidades. En este contexto, el diseño de las políticas y procedimientos indicados en esta política no persiguen únicamente el estricto cumplimiento de toda la legislación y regulación pertinentes, sino el objetivo más general de identificar, vigilar y mitigar los riesgos en todo el grupo.

[9] Circular Externa 027 de 2020 Parte I Título IV Capítulo IV - numeral 4.2.2.2.1.3 Conocimiento del cliente en conglomerados financieros

- Debe hacerse todo lo posible por garantizar que la capacidad del Grupo para obtener y analizar información conforme a esta política y procedimientos globales no sufra menoscabo como resultado de modificaciones de las políticas o procedimientos locales que viniesen exigidas por requisitos legales locales. A este respecto, la entidad debe disponer de un robusto sistema de intercambio de información entre la matriz y todas sus sucursales y filiales. Finalmente, cuando los requisitos reglamentarios o legales mínimos de los países de origen y acogida difieran, las oficinas o filiales ubicadas en las jurisdicciones de acogida aplicarán las normas más estrictas.

- En el desarrollo de los procedimientos de conocimiento del cliente, las entidades no están obligadas a exigir el formulario de solicitud de vinculación ni realizar entrevista al potencial cliente cuando quiera que se trate de alguna de las operaciones, productos o servicios que se encuentran en el numeral Evaluación y Comprensión de los Riesgos - Conocimiento del Cliente. En todo caso, las entidades, a medida que cuenten con información adicional, deben dar cumplimiento a las instrucciones impartidas por Grupo Aval. Estas excepciones no eximen a las entidades obligadas de llevar a cabo el conocimiento de sus clientes de acuerdo con los parámetros establecidos en el en el Instructivo – Directiva de Debida Diligencia SARLAFT 4.0.

- Asimismo, se entiende que conforme a las normas GAFI, si el país de acogida no permitiera la adecuada aplicación de esas normas, el Oficial de Cumplimiento debe informar a los supervisores de origen (SFC).

- Se reconoce que la aplicación de procedimientos LAFT/FPADM en todo el Grupo resulta más difícil que la de muchos otros procesos de gestión del riesgo, dadas las particularidades entre jurisdicciones en las que se opera. Para un seguimiento eficaz en todo el grupo y a efectos de la gestión del riesgo LAFT/FPADM, resulta fundamental que, sin perjuicio de las debidas salvaguardas jurídicas, las entidades estén autorizados a intercambiar información sobre sus clientes con sus matrices. Esto es aplicable tanto a sucursales como a filiales.

3.2.6.2 Evaluación y Gestión del Riesgo

La entidad debe tener un conocimiento exhaustivo de todos los riesgos asociados a sus clientes en todo el grupo, individualmente o por categorías, y debe documentar y actualizar periódicamente esa información, en consonancia con el nivel y naturaleza del riesgo en el grupo.

Al evaluar el riesgo asociado a un cliente, la entidad debe identificar todos los factores de riesgo relevantes, como clientes y usuarios, productos, canales de distribución y jurisdicciones, la utilización de productos y servicios, y establecer criterios para identificar a los clientes de alto riesgo. Estos criterios deben aplicarse en todo el banco - entidad, sus filiales y sucursales y en las actividades subcontratadas. Los clientes que planteen un alto riesgo de LAFT/FPADM para la entidad deben identificarse utilizando estos mismos criterios en todo el grupo. Las evaluaciones del riesgo asociado a los clientes deben aplicarse del mismo modo en todo el grupo o, al menos, ser congruentes con la evaluación del riesgo a escala del grupo.

Teniendo en cuenta las diferencias en los riesgos asociados a diferentes categorías de clientes, la política del Grupo debe reconocer que clientes incluidos en la misma categoría podrían plantear diferentes riesgos en distintas jurisdicciones. La información obtenida en el proceso de evaluación debe utilizarse posteriormente para determinar el nivel y naturaleza del riesgo total del Grupo y facilitar el diseño de controles adecuados en el grupo para mitigar esos riesgos. Los factores mitigadores pueden incluir información adicional del cliente,

seguimientos más estrechos, actualizaciones más frecuentes de datos personales y visitas de personal de la entidad al domicilio del cliente.

El personal encargado del cumplimiento y la auditoría interna de las entidades, en particular el Oficial de Cumplimiento para entidades obligadas o un Líder SARLAFT (o quien haga sus veces) para entidades no obligadas, deben evaluar el cumplimiento de todos los aspectos de las políticas y procedimientos de su grupo, incluida la eficacia de las políticas DDC centralizadas y los requisitos para intercambiar información con otros miembros del grupo y responder a consultas de la matriz.

3.2.6.3 Políticas y procedimientos del Riesgo LAFT/FPADM a escala consolidada

- La entidad debe garantizar que entiende el grado en que la legislación de riesgo LAFT/FPADM le permite recurrir a los procedimientos aplicados por otros bancos-entidades (por ejemplo, dentro del mismo grupo) cuando se está recomendando un negocio. El banco-entidad no debe recurrir a presentadores que estén sujetos a normas menos estrictas que las que rigen sus propios procedimientos de riesgo LAFT/FPADM. En consecuencia, las entidades deben vigilar y evaluar las normas de riesgo LAFT/FPADM vigentes en la jurisdicción del banco-entidad que realiza la recomendación.

- La entidad puede recurrir a un presentador que forme parte del mismo grupo financiero y puede sopesar conceder un mayor grado de fiabilidad a la información suministrada por éste, siempre que éste se encuentre sujeto a las mismas normas que la entidad y que la aplicación de estos requisitos se supervise a escala del grupo. No obstante, el banco-entidad que adopte este enfoque debe cerciorarse de que obtiene la información de la cliente suministrada por la entidad que lo recomienda, ya que podría exigirse remitir esta información a la UIAF si se determinara que una transacción en la que participa el cliente recomendado es sospechosa.

- La matriz del Grupo debe tener acceso a la información relevante con el fin de hacer cumplir las políticas y procedimientos de riesgo LAFT/FPADM del grupo. Cada oficina y filial del grupo debe estar en disposición de cumplir las políticas y procedimientos de riesgo LAFT/FPADM y de accesibilidad mínimos aplicados por la matriz y definidos con arreglo a las directrices del Comité.

- Las políticas de aceptación de clientes, la Debida Diligencia con el Cliente y el mantenimiento de registros deben implementarse mediante la aplicación coherente de políticas y procedimientos en toda la organización, con los ajustes precisos para tener en cuenta las diferencias de riesgo por líneas de negocio o áreas geográficas de actividad. Además, se reconoce que puede ser necesario utilizar diferentes métodos de recopilación y conservación de la información en distintas jurisdicciones para adecuarse a los requisitos reglamentarios locales o a factores de riesgo relativo. No obstante, estos métodos deben ser coherentes con las normas para todo el grupo anteriormente expuestas.

- Independientemente de su ubicación, cada oficina y filial debe establecer y mantener políticas y procedimientos eficaces acordes con los riesgos presentes en la jurisdicción y en la entidad. Este seguimiento local debe complementarse con un robusto proceso de intercambio de información con la matriz y, si procede, con otras sucursales y filiales en relación con las cuentas y actividades que puedan plantear un mayor riesgo.

- A fin de gestionar eficazmente los riesgos LA FT/FPADM procedentes de tales cuentas, el banco - entidades debe integrar esa información en función no solo del cliente, sino también de su conocimiento de los beneficiarios finales) del cliente y de los fondos en

cuestión. La entidad debe vigilar a escala consolidada las relaciones, saldos y actividades de importancia con clientes, con independencia de si las cuentas se mantienen dentro del balance, fuera del balance, como activos en administración o en Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo y FPADM.

- Las entidades con actividad nacional e internacional deben nombrar un Oficial de Cumplimiento para entidades obligadas o un Líder SARLAFT (o quien haga sus veces) para entidades no obligadas. Este Oficial tiene la responsabilidad, como parte de la gestión global del riesgo, de crear, coordinar y evaluar a escala del grupo la aplicación de una única estrategia de riesgo LAFT/FPADM (que incluye políticas y procedimientos obligatorios y autorización para impartir órdenes a todas las sucursales, filiales y entidades subordinadas nacionales e internacionales).

- La función del Oficial de Cumplimiento para entidades obligadas o un Líder SARLAFT (o quien haga sus veces) para entidades no obligadas incluye el seguimiento continuo del cumplimiento de todos los requisitos de riesgo LAFT/FPADM, tanto nacional como internacional, en todo el grupo. Así pues, el responsable de riesgo LAFT/FPADM del grupo debe cerciorarse (incluso realizando visitas periódicas in situ) del cumplimiento de los requisitos de riesgo LAFT/FPADM en todo el grupo. En caso necesario, debe estar facultado para impartir órdenes o adoptar las medidas oportunas en todo el grupo.

3.2.6.4 Intercambio de información dentro del Grupo

- Las entidades deben vigilar la coordinación del intercambio de acuerdo con las normas legales de intercambio de información de cada jurisdicción. Las filiales y sucursales deben estar obligadas a suministrar de forma proactiva a la matriz información sobre clientes y actividades de alto riesgo que sea relevante a efectos de las normas globales de riesgo LAFT/FPADM y a responder de manera oportuna a las solicitudes de información sobre cuentas remitidas desde la matriz. Las normas de la entidad matriz para el conjunto del Grupo deben incluir una descripción del proceso a seguir en todos los establecimientos para identificar, vigilar e investigar posibles circunstancias anómalas y notificar actividades sospechosas.

- Las políticas y procedimientos de la entidad para todo el Grupo deben tener en cuenta las cuestiones y obligaciones relacionadas con la protección de datos a escala local y con la legislación y regulación en materia de privacidad. También deben tener en cuenta los diferentes tipos de información que podrán compartirse dentro del grupo y los requisitos de almacenamiento, recuperación, intercambio/distribución y eliminación de esa información.

- La función global de gestión del riesgo LAFT/FPADM del Grupo debe evaluar los posibles riesgos planteados por las actividades notificadas por sus sucursales y filiales y, cuando proceda, evaluar los riesgos en todo el Grupo planteados por un determinado cliente o categoría de clientes. También debe contar con políticas y procedimientos para comprobar si otras sucursales o filiales mantienen cuentas de un mismo cliente (incluidas las de partes vinculadas a ese cliente o pertenecientes a su mismo grupo). Asimismo, la entidad matriz debe disponer de políticas y procedimientos globales en materia de relaciones de cuenta consideradas de alto riesgo o que hayan estado asociadas a actividades potencialmente sospechosas, incluidos procedimientos de remisión a directivo de mayor jerarquía y directrices sobre restricciones a las actividades de las cuentas, incluido su cierre cuando proceda.

- Además, la matriz y sus sucursales y filiales deben, con arreglo a sus respectivas legislaciones nacionales y a requerimiento de agencias de inteligencia financiera, autoridades supervisoras u otras habilitadas, cooperar ante solicitudes de información sobre clientes que aquéllas precisen en sus labores de lucha contra LA FT/FPADM. La matriz bancaria ha de poder exigir a todas sus sucursales y filiales el cotejo de sus archivos con determinados listados o solicitudes a fin de comprobar la presencia de individuos u organizaciones sospechosos de colaborar e instigar Lavado de Activos y Financiación del Terrorismo y que notifiquen las coincidencias.

- La entidad matriz debe ser capaz de informar a sus supervisores, a requerimiento de éstos, sobre su proceso global de gestión del riesgo de clientes, su evaluación y gestión de los riesgos LAFT/FPADM, sus políticas y procedimientos de riesgo LAFT/FPADM a escala consolidada y sus sistemas de intercambio de información dentro del grupo.

- Tratándose de relaciones de corresponsalía trasnacional, las entidades obligadas deben establecer mecanismos que les permitan[10]:

    - Obtener la aprobación de los funcionarios de alto nivel jerárquico antes de establecer relaciones de corresponsalía trasnacional*;*
    - Reunir información suficiente sobre el establecimiento representado que les permita comprender cabalmente la naturaleza de sus negocios, incluyendo si ha sido objeto de sanción o intervención de la autoridad de control por lavado de activos o financiación del terrorismo, así como cualquier otra información que permita establecer una relación de corresponsalía trasnacional con transparencia para ambas partes.
    - Determinar que la entidad tenga controles para prevenir y controlar el lavado de activos y la financiación del terrorismo;
    - Documentar las respectivas responsabilidades de cada institución frente al LAFT/FPADM.
    - Aplicar procedimientos más estrictos para el seguimiento a tales relaciones.
    - Asegurarse de que el establecimiento representado cumpla con las medidas de conocimiento del cliente.
    - Las instrucciones contenidas en el presente numeral deben aplicarse igualmente respecto de las personas naturales o jurídicas que pretendan adquirir activos fijos de una entidad.
    - Cumplir con cualquier obligación, de acuerdo con la regulación aplicable.

- **Operaciones con valores y actividades de seguro:** La aplicación de controles de gestión del riesgo LAFT/FPADM en los grupos financieros mixtos plantea cuestiones adicionales que podrían ser ajenas a las propias de las operaciones de captación de depósitos y concesión de préstamos. Los grupos mixtos deberán ser capaces de vigilar e intercambiar información sobre la identidad de los clientes y sobre sus transacciones y cuentas en el conjunto del grupo, y estar atentos a los clientes que utilicen sus servicios en diferentes sectores.

  Las diferencias en la naturaleza de las actividades y en los patrones de relaciones entre bancos y clientes en cada sector podrán requerir o justificar variaciones de los requisitos de riesgo LAFT/FPADM exigidos a cada sector. Las entidades del sector financiero deben estar atentas a estas diferencias cuando se realicen ventas cruzadas de productos y

[10] Circular Externa 055 de 2016 Superintendencia Financiera de Colombia Título I capitulo XI Instrucciones relativas a la administración del riesgo de lavado de activos y de la financiación del terrorismo - Conocimiento del cliente por parte de grupos.

servicios a los clientes desde distintas unidades de negocio, debiéndose aplicar los oportunos requisitos de riesgo LAFT/FPADM a los correspondientes sectores[11].

3.3 ACUERDO SISTEMA DE MONITOREO DE TRANSACCIONES

3.3.1 Seguimiento a cargo de entidades

Las entidades deben disponer de un sistema de monitoreo acorde con su tamaño, sus actividades y complejidad, así como con los riesgos presentes en la entidad. Cuando se utilice un sistema donde se inicie, procese, reporte o almacene información para la administración del riesgo de LAFT/FPADM, este sistema debe permitir realizar un análisis de tendencias con los datos de transacciones con el fin de identificar operaciones inusuales.

En particular, este sistema debe ser capaz de ofrecer información fidedigna a la alta dirección sobre ciertos aspectos cruciales, incluidos cambios en el perfil de las transacciones realizadas por los clientes. Para elaborar el perfil del cliente, se debe incorporar la información de conocimiento del cliente actualizada, completa y fidedigna facilitada por el cliente. El sistema TI debe permitir a la entidad disponer de un repositorio centralizado de información (esto es, organizado por cliente, producto, entidades del grupo, transacciones realizadas durante un cierto intervalo de tiempo, etc.). Sin que se les exija disponer de un único archivo por cliente, las entidades deben calificar a sus clientes en función del riesgo y gestionar alertas con toda la información relevante a su disposición. Un sistema de seguimiento TI debe utilizar parámetros adecuados basados en la experiencia nacional e internacional sobre los métodos y la Administración del riesgo de LAFT/FPADM. Los parámetros utilizados deben reflejar y tener en cuenta la situación de riesgo específica de la entidad.

El sistema de monitoreo debe permitir determinar sus propios criterios para realizar seguimientos adicionales, y ser fuente para la elaboración de informes de Operaciones Sospechosas (ROS) o adoptar otras medidas para minimizar el riesgo. El Oficial de Cumplimiento para entidades obligadas o un Líder SARLAFT (o quien haga sus veces) para entidades no obligadas debe tener acceso al sistema de Monitoreo. Los parámetros del Sistema de Monitoreo deben permitir la generación de alertas sobre transacciones anómalas, en cuyo caso también deben someterse a posterior evaluación por parte del Oficial de Cumplimiento.

La auditoría interna también debe evaluar el Sistema de Monitoreo y el Sistema de Administración de Riesgo LAFT/FPADM para garantizar que es adecuado y que la primera y segunda línea de lo utilizan eficazmente, y remitir el resultado al Oficial de Cumplimiento[12].

3.3.2 Seguimiento Grupo Aval

Grupo AVAL cuenta con mecanismos de reporte incluyendo tablero de control que le permiten conocer de primera mano la gestión de riesgo a nivel de las entidades que lo conforman. Los análisis se adelantan desde el punto de vista de entidades sujetos obligados por la Superintendencia Financiera, la Superintendencia de Sociedades y los sujetos no obligados.

[11] "Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo" propuesta por el Comité de Basilea (Banco de Pagos internacionales – BPI (Enero de 2014).
[12] Fuente: "Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo" propuesta por el Comité de Basilea (Banco de Pagos internacionales – BPI (Enero de 2014).

3.4 MODELO DE GESTIÓN

El modelo de Gestión corporativa comprende de manera general las siguientes fases:

Identificación	Medición	Control	Monitoreo
• Las entidades aplicarán los tres riesgos enfocados a LA/FT/FPADM • Cada una de las enitidades realiza la identificación de causas y controles.	• Valoración de los riesgos • Generación del perfil de riesgo del Grupo	• Planes de mejoramiento y seguimiento a los mismos • Identificar controles y evaluar su diseño y efectividad	• Generación de reportes a las diferentes instancias • Compartir eventos relevantes y mejores prácticas • Revisión de la ejecución de controles

3.4.1 Identificación de riesgos

Las entidades identificarán los tres riesgos a ser utilizados para:
- Lavado de activos
- Financiación del terrorismo
- Financiación de la proliferación de armas de destrucción masiva

Se debe tener en cuenta que toda inclusión, modificación o eliminación a los riesgos anteriormente expuestos, que surja como resultado de la evolución natural del negocio y de la normatividad vigente, deberá informarse a la Gerencia Corporativa de Cumplimiento y SOX de Grupo Aval indicando: Referencia Riesgos / Riesgo / Referencia Causa / Causa / Tipo de cambio (Inclusión, modificación o eliminación) / Cambio sugerido / Justificación.

3.4.1.1 Segmentación de los factores de riesgo LAFT/FPADM

Las entidades que ostentan la calidad de sujetos obligado deben segmentar, como mínimo, cada uno de los factores de riesgo de acuerdo con las características particulares de cada uno de ellos asegurando que las variables de análisis definidas garanticen la consecución de las características de homogeneidad al interior de los segmentos y heterogeneidad entre ellos. La segmentación de los factores de riesgo será incluida en la matriz de riesgo control la cual incluye el factor de riesgo, segmentación de los modelos a priori, número de segmento y detalle del segmento de acuerdo con el alcance de la norma para las entidades obligadas de Grupo Aval.

3.4.1.2 Eventos de riesgo LAFT/FPADM

Tiene como objetivo capturar la información de los eventos de riesgo identificados, con base en juicio experto, en el contexto interno y externo, en información de tipologías y tendencias del mercado y en la evolución propia del negocio.

3.4.1.3 Análisis de riesgo

Son los atributos asociados a cada uno de los eventos de riesgo teniendo en cuenta las causas definidas, tipologías LAFT/FPADM asociadas al evento de riesgo, señales de alerta los cuales deben incluir como mínimo las opciones de contexto interno y externo para entidades obligadas por la SFC.

3.4.2 Medición de Riesgos

El modelo de medición se basa en la medición a través de mapas de Calor del Riesgo Inherente y Residual de las entidades y del Grupo. Los mapas de calor permiten establecer los riesgos más relevantes a los que están expuestas las entidades teniendo en cuenta los criterios de probabilidad e impacto. La colorimetría permite priorizar los riesgos que requieren atención inmediata, y sus escalas están acordes con la naturaleza, complejidad y volumen de las operaciones de las entidades de Grupo Aval. Remitirse al Instructivo Modelo de Gestión de Riesgos Corporativos LAFT/FPADM.

3.4.2.1 Riesgo Inherente

El Riesgo Inherente es el nivel de riesgo propio de la actividad, asumiendo que no existen controles para mitigarlo; es decir, la susceptibilidad de que eventos de LAFT/FPADM pudieran afectar considerablemente a Grupo Aval y sus entidades subordinadas, de manera individual o agregada, asumiendo que no hay controles internos.

Es importante indicar que el análisis y evaluación del Riesgo Inherente para cada uno de los riesgos LAFT/FPADM es responsabilidad del dueño del proceso en validación y acompañamiento por parte del Oficial de Cumplimiento, sino de los dueños de proceso. Para la evaluación del riesgo inherente se clasifican en categorías bajo, moderado, alto y extremo, de acuerdo con la Probabilidad de Ocurrencia (PO) y la Magnitud del Impacto (MI).

3.4.2.2 Probabilidad de ocurrencia

La evaluación de la Probabilidad de Ocurrencia de que el riesgo se materialice sin la consideración de los controles; se mide con la siguiente escala tanto en Ocurrencia como en Frecuencia, en donde se deberá seleccionar solo uno de los dos criterios para la evaluación de cada riesgo, aquel de mayor relevancia frente al riesgo evaluado. Así las cosas, cada uno de estos dos elementos se evalúa con un peso del 100%. Tanto la Ocurrencia como la Frecuencia se califica en cinco niveles entre 1, 2, 3, 4 o 5

3.4.2.3 Magnitud del impacto

La evaluación del riesgo y cada causa asociada sin la consideración de los controles se mide con una escala que incluye cuatro (4) factores (Legal, Reputacional, Operativo y Contagio) que deben calificarse entre 1, 2, 3, 4 o 5. Cada factor tiene un peso diferente dentro de la magnitud impacto.

3.4.2.4 Riesgo Residual

Identificación de controles clave

La administración (primera línea) de cada entidad debe evaluar si tiene controles en operación que estén diseñados para gestionar adecuadamente los riesgos de LAFT/FPADM. Aquellos controles que de forma efectiva y eficiente mitiguen los riesgos y causas, y sean identificados como relevantes para incluir en las matrices de riesgo serán denominados como “controles clave”. Los controles pueden ser de dos tipos: automatizados o manuales, y pueden tener dos funciones: prevenir o detectar.

En todo caso, para la identificación de los controles clave, se deberán tener en cuenta los siguientes aspectos:

- ✓ Se considerará un control preventivo aquel que tiene el propósito de prevenir errores, omisiones o irregularidades.
- ✓ Se considerará un control detectivo aquel que permite detectar los errores en el momento en que se presentan.
- ✓ Un control preventivo desplaza la probabilidad de ocurrencia toda vez que el foco de este tipo de controles es evitar que se materialice el riesgo.
- ✓ Los controles detectivos desplazarán la magnitud del impacto considerando que una vez materializado el riesgo se requiere enfocarse en disminuir su impacto.
- ✓ Un control no podrá mitigar a la vez tanto probabilidad como impacto.
- ✓ Para la calificación de los controles que son transversales, es decir, que están mitigando diferentes riesgos, se califica una sola vez, es decir, que su calificación de eficacia será la misma en todos los procesos y causas en donde se encuentre asociado.
- ✓ Se deben implementar controles que gestionen tanto la probabilidad como el impacto del riesgo inherente.
- ✓ Una vez calificada la eficacia del control, su calificación es promediada para disminuir el riesgo inherente por riesgo, arrojando como resultado el riesgo residual.
- ✓ Se debe realizar la adecuada identificación y documentación de controles logrando una adecuada coherencia entre Riesgo-Causa-Control.

Evaluación de Eficacia del Control

Desde Grupo Aval y en trabajo conjunto con las subordinadas que participan en el Comité Corporativo LAFT/FPADM se han definido diferentes factores para realizar la evaluación del control, cada uno con una ponderación diferente dependiendo de su efecto en la eficacia del control. Sus calificaciones cuentan con unos pesos definidos midiéndose a través de las escalas 1, 2 o 3.

Se ha definido que el grado de mitigación máxima de un control es del 85% sobre cada riesgo.

Resultado Riesgo Residual

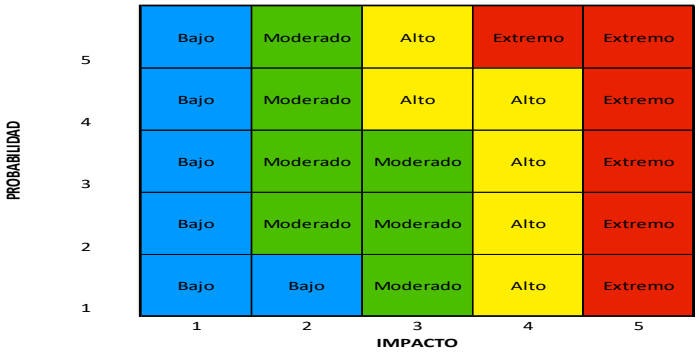
Basado en las calificaciones de “Riesgo Inherente” y en los factores que determinan la “Eficacia del Control”, y en la resta de estos dos criterios se deriva el Riesgo Residual. En consecuencia, el Riesgo Residual es determinado por:

RIPO: Calificación riesgo inherente de probabilidad ocurrencia
ECPO: Calificación eficacia control de probabilidad ocurrencia
RIMI: Calificación riesgo inherente de magnitud impacto
ECMI: Calificación eficacia control de magnitud impacto
RIPO – (RIPO*ECPO%)
RIMI – (RIMI*ECMI%)

Con el fin de obtener una calificación más ácida del riesgo residual derivado de la efectividad en conjunto de los controles asociados, se aplica la ponderación máxima de calificación de estos, dependiendo del resultado de los factores calificados.

Mapa de Calor

El modelo de medición se basa en la medición a través de mapas de calor del riesgo inherente y residual de las entidades y del Grupo. Los mapas de calor permiten establecer los riesgos más relevantes a los que están expuestas las entidades teniendo en cuenta los criterios de probabilidad e impacto. La colorimetría permite priorizar los riesgos que requieren atención inmediata, y sus escalas están acordes con la naturaleza, complejidad y volumen de las operaciones de las entidades de Grupo Aval.



	Nivel de Impacto
Extremo	5
Alto	4
Moderado	3
Bajo	1 y 2

3.5 TABLERO DE CONTROL

Un indicador es un instrumento que provee evidencia cuantitativa acerca de si una determinada condición existe o ciertos resultados han sido logrados o no. Si no han sido logrados permite evaluar el proceso realizado. Un indicador de desempeño, por ejemplo, nos entrega información cuantitativa respecto del logro de los objetivos de un programa puede cubrir aspectos cuantitativos o cualitativos.

Grupo Aval define unos indicadores de la gestión del riesgo de LAFT/FPADM, basados en las buenas prácticas realizadas por las entidades, los cuales son resumidos a través de tableros de control que deben ser reportados a Grupo Aval periódicamente.

3.6 DEFINICIÓN DE PLANES DE MEJORAMIENTO Y MITIGACIÓN

Los reportes de seguimiento son analizados por el Comité Corporativo LAFT/FPADM, con el fin de determinar los puntos de control a fortalecer, revisar los cambios relevantes y buscar planes de acción tendientes a mitigar dichos cambios. Estos planes de acción son acordados en el Comité para ser implementados en las entidades y en Grupo Aval, de acuerdo con los cronogramas proyectados, para cada caso.

Adicionalmente, los reportes permiten conocer el estado de gestión de riesgo de cada una de las entidades y las novedades que pueden presentarse en el periodo, lo que da herramientas al Comité para definir cambios en la metodología y/o adaptar prácticas de prevención para mitigar el riesgo.

4. GLOSARIO

- **Alta Gerencia:** Son las personas responsables de dirigir, ejecutar y supervisar las operaciones de la entidad bajo la dirección de la Junta Directiva.

- **Apetito de Riesgo:** Nivel de riesgo que la entidad está dispuesta a aceptar o asumir, con el fin de lograr sus objetivos estratégicos y plan de negocio.

- **Áreas Geográficas:** Lugar donde está ubicado el establecimiento de comercio autorizado de la persona natural o jurídica prestadora del servicio y la jurisdicción donde se encuentran ubicadas sus contrapartes (ciudades o países), donde se transan o registran las operaciones bien sea por su origen o destino.

- **Banco Pantalla:** Es una institución financiera que:
  - No tiene presencia física en el país en el que está constituido y recibe licencia.
  - No pertenece a un conglomerado financiero que esté sujeto a una supervisión comprensiva y consolidada por parte de la Superintendencia Financiera de Colombia (SFC).

- No es objeto de inspección, vigilancia y/o control o un grado de supervisión equivalente, por parte del supervisor de la jurisdicción donde se encuentre domiciliado o constituido.

- **Beneficiario Final:** Persona(s) natural(es) que finalmente posee(n) o controla(n), directa o indirectamente, a un cliente y/o la persona natural en cuyo nombre se realiza una transacción. Incluye también a la(s) persona(s) natural(es) que ejerzan el control efectivo y/o final, directa o indirectamente, sobre una persona jurídica u otra estructura sin personería jurídica**.**

- **Clientes:** Es toda persona natural o jurídica y estructuras sin personería jurídica con la cual la entidad establece y mantiene una relación contractual o legal para el suministro de cualquier producto propio de su actividad.

- **Colaboradores:** Personas naturales que se obligan a prestar un servicio a Grupo Aval o sus subordinadas, bajo una continuada dependencia o subordinación y mediante remuneración.

- **Comité de Basilea (Comité de Supervisión Bancaria de Basilea):** Es la organización mundial que reúne a las autoridades de supervisión bancaria, cuyo objetivo es fortalecer la solidez de los sistemas financieros y la regulación prudencial de las entidades con el propósito de mejorar la estabilidad financiera. Su función principal es actuar como un foro internacional para encontrar soluciones de política y promulgar estándares.

- **Comité Corporativo LAFT/FPADM**: Es el grupo asesor conformado por los Oficiales de Cumplimiento de las entidades (Grupo Aval, 4 Bancos, Corficolombiana y Porvenir), responsable de hacer seguimiento a la gestión estratégica de los riesgos y formular recomendaciones y buenas prácticas para el manejo de los riesgos que afecten la actividad de las entidades. Su modificación, ajuste o invitación estará a cargo del mismo comité.

- **Contexto Externo:** Es el ambiente externo en el cual la organización busca alcanzar sus objetivos, que puede incluir: (i) el ambiente cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo, bien sea internacional, nacional, regional o local; (ii) impulsores clave y tendencias que tienen impacto en los objetivos de la organización; y (iii) relaciones con personas y organizaciones que puede afectar, verse afectada, o percibirse a sí misma como afectada por una decisión o una actividad, y sus percepciones y valores.

- **Contexto Interno:** Es el ambiente interno en el cual la organización busca alcanzar sus objetivos, que puede incluir: (i) el gobierno, estructura organizacional, funciones y responsabilidades; (ii) políticas, objetivos y estrategias implementadas para lograrlos; (iii) las capacidades, entendidas en términos de recursos y conocimiento (vr.gr. capital, tiempo, personas, procesos, sistemas y tecnologías); (iv) sistemas de información, flujos de información y procesos para la toma de decisiones (tanto formales como informales); (v) la cultura de la organización; (vi) normas, directrices y modelos adoptados por la organización; y (vii) formas y extensión de las relaciones contractuales.

- **Corresponsalía Trasnacional:** Es la relación contractual entre dos instituciones financieras, el primero denominado "establecimiento corresponsal" y el segundo “establecimiento representado". Los establecimientos de crédito deben encontrarse en jurisdicciones diferentes. Son "establecimientos corresponsales" las entidades que le ofrecen/prestan determinados servicios a otras instituciones financieras y

"establecimiento representado" aquellos que utilizan/reciben los servicios contratados con el "establecimiento corresponsal".

- **Debida Diligencia:** Los principios de debida diligencia están basados en los riesgos, y describen lo que una institución debe considerar al iniciar una relación con el cliente, para determinar qué tipo de actividades debe llevar a cabo para conocer el cliente. La debida diligencia se profundiza en función de la calificación del perfil de riesgo y puede considerar niveles como la Debida Diligencia Simplificada, Debida Diligencia, Debida Diligencia Ampliada, y Debida Diligencia Intensificada.

- **Debida Diligencia Ampliada o Intensificada:** Contempla, además de lo anterior, profundizar en el conocimiento del cliente en determinados tipos de clientes o actividades, para lo cual la entidad solicitará información adicional, independiente de la política documental establecida para cada producto, lo que permitirá tener una adecuada razonabilidad acerca del origen y destino de los fondos, del cumplimiento de los marcos regulatorios o de la adopción de las buenas prácticas en materia de prevención de LAFT/FPADM. También se conoce como medidas intensificadas.

- **Entidad Beneficiaria:** Son aquellas entidades que reciben una transferencia electrónica de una entidad que hace la orden, directamente o a través de una entidad intermediaria y suministra los fondos al beneficiario.

- **Entidad Intermediaria:** Son aquellas entidades obligadas en una cadena en serie o de pago de cobertura, que reciben y transmiten una transferencia electrónica en nombre de la entidad financiera que hace la orden y la entidad beneficiaria u otra entidad intermediaria.

- **Entidad Matriz:** Es la entidad que controla o ejerce influencia dominante en sus entidades subordinadas. Ésta proporciona gestión, administración y/o controles sobre su estrategia y/u operación.

- **Entidades:** Para los efectos de esta Política, son los bancos, corporaciones, administradoras de Fondos de Pensiones (AFPs), Sociedades Fiduciarias, Almacenes Generales Deposito, Comisionistas, y demás, obligadas y no obligadas, subordinadas de Grupo Aval Acciones y Valores S.A., tanto en Colombia como en el exterior.

  Factores de Riesgo[13]**:** Son los agentes generadores del riesgo de LAFT/FPADM. Para efectos del SARLAFT se deben tener en cuenta como mínimo los siguientes:
  - Clientes/usuarios
  - Productos
  - Canales de distribución
  - Jurisdicciones

  Se pueden considerar otros factores de riesgo, los cuales serán identificados a partir del proceso de evolución del contexto interno y externo.

- **Financiación del Terrorismo:** es el conjunto de actividades encaminadas a canalizar recursos lícitos o ilícitos para promover, sufragar o patrocinar individuos, grupos o actividades terroristas.

[13] **Definición de cliente, usuario y producto** - Circular Básica jurídica Parte 1-Titulo 1- Capítulo 1 de la Superintendencia Financiera de Colombia -Instrucciones Relativas a la Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo - Punto 1 Definiciones.

- **Financiamiento de la Proliferación de Armas de Destrucción Masiva o FPADM:** Es todo acto que provea fondos o utilice servicios financieros, en todo o en parte, para la fabricación, adquisición, posesión, desarrollo, exportación, trasiego de material, fraccionamiento, transporte, trasferencia, deposito o uso dual para propósitos ilegítimos en contravención de las leyes nacionales u obligaciones internacionales, cuando esto último sea aplicable.

- **Grupo:** Hace referencia a uno o más entidades subordinadas por una o una organización, así como sus sucursales y filiales.

- **Grupo de Acción Financiera Internacional para la Prevención del Lavado de Activos (GAFI):** Es un organismo intergubernamental que desarrolla normas internacionales y promueve políticas para proteger al sistema financiero internacional contra el blanqueo de capitales, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva. Este grupo define el blanqueo de capitales como el reciclado de fondos procedentes de actividades delictivas para ocultar su origen ilícito y trabaja en estrecha colaboración con otras entidades involucradas en estos temas, en particular con sus miembros asociados y observadores. El Comité de Basilea tiene estatus de observador en el GAFI.

- **Jurisdicción:** Ámbito o territorio en el que se ejerce una autoridad o poder.

- **Lavado de Activos:** Es el conjunto de actividades encaminadas a ocultar el origen ilícito o a dar apariencia de legalidad a recursos obtenidos producto de la ejecución de actividades ilícitas.

- **Listas Internacionales Vinculantes para Colombia:** Son aquellas listas de personas y entidades asociadas con organizaciones terroristas que son vinculantes conforme al Derecho Internacional, incluyendo, pero sin limitarse a las Resoluciones 1267 de 1999, 1988 de 2011, 1373 de 2001, 1718 y 1737 de 2006 y 2178 de 2014 del Consejo de Seguridad de las Naciones Unidas, a todas aquellas que le sucedan, relacionen y complementen, y cualquiera otra lista que se adopte en los países en donde se encuentran las entidades del grupo.

- **Matriz de Riesgo:** Es una herramienta que facilita una evaluación de riesgos holística.

- **Monitoreo:** Etapa donde debe compararse y hacer seguimiento de la evolución del perfil de riesgo Inherente y residual y en general del SARLAFT.

- **Operaciones Inusuales:** Son aquellas operaciones que cumplen por lo menos con alguna de las siguientes características:
  - No guarda relación con la actividad económica del cliente y sobre la cual no se ha encontrado explicación que se considere razonable.
  - Se sale de los parámetros fijados por la entidad y de la cual no se ha encontrado explicación que se considere razonable.

  En el caso de identificación y análisis de las operaciones de usuarios (personas naturales o jurídicas a las que, sin ser clientes, la entidad les presta un servicio), las entidades deben determinar cuáles de éstas resultan relevantes, teniendo en cuenta el riesgo al que se ven expuestas y basados en los criterios previamente establecidos por las mismas.

Las alertas de operaciones generadas por el sistema de monitoreo pueden ser evaluadas por áreas de negocio (primera línea) o de cumplimiento (segunda línea), y facilitan la identificación de operaciones inusuales. De ellas pueden derivar operaciones inusuales, las cuales a su vez pueden concluir en operaciones sospechosas.

- **Operaciones Sospechosas:** Constituye una operación sospechosa sobre cualquier información relevante sobre manejo de activos, pasivos u otros recursos, cuya cuantía o características no guarden relación con la actividad económica de sus clientes, 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.

- **País de Acogida:** País en el cual se ubica una filial de una entidad domiciliada en el exterior. Las entidades que se clasifican de esta forma deben cumplir con la normatividad de LAFT/FPADM que aplique ese país, y en el caso que la normatividad colombiana sea más rigurosa, deberá cumplir la normatividad más completa.

- **País de Origen:** País en el que está domiciliada una casa matriz, de donde salen las mejores prácticas en administración de LAFT/FPADM-para las filiales que se encuentran bajo ésta.

- **Países de Mayor riesgo:** Se consideran países de mayor riesgo los contenidos en los listados del GAFI de países no cooperantes y jurisdicciones de alto riesgo.

- **Persona Expuesta Políticamente (PEPs)[14]:** Se considerarán como PEP los servidores públicos de cualquier sistema de nomenclatura y clasificación de empleos de la administración pública nacional y territorial, cuando tengan asignadas o delegadas funciones de: expedición de normas o regulaciones, dirección general, formulación de políticas institucionales y adopción de planes, programas y proyectos, manejo directo de bienes, dineros o valores del Estado, administración de justicia o facultades administrativo sancionatorias, y los particulares que tengan a su cargo la dirección o manejo de recursos en los movimientos o partidos políticos.

  La calidad de Personas Expuestas Políticamente (PEP) se mantendrá en el tiempo durante el ejercicio del cargo y por dos (2) años más desde la dejación, renuncia, despido o declaración de insubsistencia del nombramiento, o de cualquier otra forma de desvinculación, o terminación del contrato.

- **PEP extranjeros:** Son aquellas personas que desempeñan funciones prominentes en otro país. Se entienden por PEP extranjeros: (i) jefes de Estado, jefes de Gobierno, ministros, subsecretarios o secretarios de Estado; (ii) congresistas o parlamentarios; (iii) miembros de tribunales supremos, tribunales constitucionales u otras altas instancias judiciales cuyas decisiones no admitan normalmente recurso, salvo en circunstancias excepcionales; (iv) miembros de tribunales o de las juntas directivas de bancos centrales; (v) embajadores, encargados de negocios y altos funcionarios de las fuerzas armadas, (vi) miembros de los órganos administrativos, de gestión o de supervisión de empresas de propiedad estatal, y (vii) representantes legales, directores, subdirectores y/o miembros de las juntas directivas de organizaciones internacionales.

  En ningún caso, dichas categorías comprenden funcionarios de niveles intermedios o inferiores. Adicionalmente, se consideran PEP extranjeros durante el periodo en que

[14] Decreto 830 del 26 de julio de 2021

ocupen sus cargos y durante los dos (2) años siguientes a su dejación, renuncia, despido, o cualquier otra forma de desvinculación.

- **Producto**: Son las operaciones legalmente autorizadas que pueden adelantar las entidades vigiladas mediante la celebración de un contrato (vr.gr. cuenta corriente o de ahorros, seguros, inversiones, CDT, giros, emisión de deuda, compra venta de valores, negocios fiduciarios, etc.).

- **ROS**: Es el Reporte de Operación Sospechosa que todo oficial de cumplimiento o funcionario responsable de las personas naturales o jurídicas debe enviar a la Unidad de Análisis Financiero - UIAF cuando, en el ejercicio de su actividad o de sus funciones, detecte una operación sospechosa de lavado de activos o financiamiento del terrorismo, que corresponda ser informada.

- **Riesgos Asociados al Lavado de Activos y Financiación del Terrorismo (LAFT/FPADM)[15]:** Son los riesgos a través de los cuales se materializa el riesgo de LAFT/FPADM; estos son: reputacional, legal, operativo y de contagio.

  - **Riesgo Reputacional:** Es la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

  - **Riesgo Legal:** Es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales.

    El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

  - **Riesgo Operativo:** Es la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal.

  - **Riesgo de Contagio:** Es la posibilidad de pérdida que una entidad puede sufrir, directa o indirectamente, por una acción o experiencia de un vinculado. El vinculado es el relacionado o asociado e incluye personas naturales o jurídicas o estructuras sin personería jurídica que tienen posibilidad de ejercer influencia sobre la entidad.

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

- **Riesgo Residual**: Es el nivel resultante del riesgo después de aplicar los controles.

- **SAGRILAFT:** Es el sistema de autocontrol y gestión del riesgo integral de lavado de activos y financiación del terrorismo aplicable a las entidades obligadas por la Superintendencia de Sociedades.

[15] **Definiciones de Riesgos** - Circular Básica jurídica Parte 1-Titulo 1- Capítulo 1 de la Superintendencia Financiera de Colombia-: Instrucciones Relativas a la Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo - Punto 1 Definiciones

- **SARLAFT:** Sistema de Administración de Riesgo de Lavado de Activos y de la Financiación al Terrorismo es el conjunto integrado de políticas, procedimientos, infraestructura, controles, capacitación y divulgación que busca responder a las posibles amenazas que las entidades sean usadas para la práctica de conductas delictivas que buscan la canalización de recursos de actividades delictivas y en particular disminuir la exposición al riesgo de LAFT/FPADM.

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

- **Servicios:** Son todas aquellas interacciones de las entidades sometidas a inspección y vigilancia de la Superintendencia Financiera de Colombia con personas o estructuras sin personería jurídica diferentes a sus clientes.

- **Señales de Alerta o Alertas Temprana:** Son los 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 oportuna y/o prospectivamente la posible existencia de un hecho o situación que escapa a lo que la entidad, en el desarrollo del SARLAFT/SAGRILAFT, ha determinado como normal.

  Estas señales deben considerar cada uno de los factores de riesgo y las características de sus operaciones, así como cualquier otro criterio que a juicio de la entidad resulte adecuado.

- **Transferencia:** Es la transacción efectuada por una persona natural o jurídica denominada ordenante, a través de una entidad autorizada en la respectiva jurisdicción para realizar transferencias nacionales y/o internacionales, mediante movimientos electrónicos o contables, con el fin de que una suma de dinero se ponga a disposición de una persona natural o jurídica denominada beneficiaria, en una entidad autorizada para realizar este tipo de operaciones. El ordenante y el beneficiario pueden ser la misma persona.

- **Unidad de Información y Análisis Financiero (UIAF):** Es una entidad adscrita al Ministerio de Hacienda y Crédito Público de Colombia, su misión es proteger la seguridad nacional en el ámbito económico, basado en procesos de investigación e innovación mediante la prevención y detección de actividades criminales, relacionadas con los delitos de Lavado de Activos y la Financiación del Terrorismo.

- **Usuarios:** Son aquellas personas naturales o jurídicas o estructuras sin personería jurídica a las que, sin ser clientes, la entidad les presta un servicio.

- **Vinculados:** Son aquellos que cumplen alguno de los criterios previstos en el artículo 2.39.3.1.2 del Decreto 2555 de 2010.
  a) Control, subordinación y/o grupo empresarial: la persona natural, persona jurídica y vehículo de inversión que presenta situación de control o subordinación respecto de una entidad del conglomerado financiero de manera directa o indirecta, en los casos previstos en los artículos 260 y 261 del Código de Comercio, o pertenece al mismo grupo empresarial de acuerdo con la definición del artículo 28 de la Ley 222 de 1995, o las normas que los modifiquen, sustituyan o adicionen.

b) Participación significativa: tiene(n) una participación significativa quien o quienes cumplan alguna de las siguientes condiciones:
- El o los participantes de capital o beneficiarios finales del diez por ciento (10%) o más de la participación en alguna entidad del conglomerado financiero. Para tal efecto, no se computarán las acciones sin derecho a voto.
- Las personas jurídicas en las cuales alguna entidad del conglomerado financiero sea beneficiaria real del diez por ciento (10%) o más de la participación. Para tal efecto, no se computarán las acciones sin derecho a voto.
- Las personas jurídicas que presenten situación de subordinación respecto de aquellos definidos en el primer bullet del presente literal. Las situaciones de subordinación serán las previstas en los artículos 260 y 261 del Código de Comercio. Para tal efecto, no se computarán las acciones sin derecho a voto.

5. REGULACIÓN

Normatividad utilizada en el desarrollo de la Gestión de Riesgo de Lavado de Activos y Financiación al Terrorismo:

- **Colombia:**
  - Circular Básica Jurídica de la Superintendencia Financiera de Colombia, (Circular Externa 29 de 2014), Parte I Instrucciones Generales Aplicables a las Entidades Vigiladas Título IV Deberes y Responsabilidades Capítulo IV: Instrucciones Relativas a la Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo.
  - Circular Básica Jurídica de la Superintendencia de Sociedades (Circular Externa 100-000005 de 2017) en su Capitulo X Autocontrol y Gestión del Riesgo LA/FT y Reporte de Operaciones Sospechosas a la UIAF.
  - Decreto 830 de 2021 “por el cual se modifican y adicionan algunos artículos al Decreto 1081 de 2015, en lo relacionado con el régimen de las Personas Expuestas Políticamente (PEP)”.

- **Internacional:**
  - Normas en relación con la administración de Lavado de Activos y de la Financiación al Terrorismo que apliquen a las entidades que se encuentran en el exterior.
  - Comité de Basilea: Directriz para una “Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo”. Banco de Pagos internacionales – BPI (enero de 2014).
  - GAFI: Listado de recomendaciones relevantes.
  - Nuevas recomendaciones del GAFI (incluidas sus notas interpretativas), entre otras:
    - R. 1: Evaluación del riesgo y aplicación de un enfoque en función del riesgo
    - R. 2: Cooperación nacional y coordinación
    - R. 9: Legislación sobre el secreto profesional de las instituciones financieras
    - R. 10: Debida diligencia con clientes
    - R. 11: Mantenimiento de registros
    - R. 12: Personas Políticamente Expuestas (PEP)
    - R. 13: Corresponsalía bancaria
    - R. 15: Nuevas tecnologías
    - R. 16: Transferencias electrónicas
    - R. 17: Recurso a terceros
    - R. 18: Controles internos, y sucursales y filiales en el extranjero
    - R. 20: Notificación de operaciones sospechosas
    - R. 26: Regulación y supervisión de instituciones financieras
    - R. 40: Cooperación internacional