

1. OBJETIVO

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 (LA/FT/FPADM).

2. ALCANCE

Esta política está orientada a la gestión integral para garantizar el cumplimiento de la normatividad internacional y local aplicable a Grupo Aval Acciones y Valores y sus subsidiarias (Grupo), en materia de Prevención de LA/FT/FPADM. En ella se establecen los criterios que deben considerarse en la administración de los riesgos asociados a LA/FT/FPADM, de acuerdo con las características particulares y la normatividad vigente aplicable a cada entidad.

3. DECLARACIÓN DE COMPROMISO

Grupo Aval, está comprometido con una política de cero tolerancia frente a los delitos de LA/FT/FPADM en cualquiera de sus modalidades, y se compromete a:

- Anteponer el cumplimiento de las normas en materia de administración de riesgo de LA/FT/FPADM al logro de las metas comerciales.
- Gestionar de manera estructurada y estratégica, los riesgos LA/FT/FPADM asociados al negocio y su relacionamiento con contrapartes.
- Promover y mantener una cultura sólida y ética del riesgo como elemento indispensable para la prevención, detección, investigación y remediación de los riesgos LA/FT/FPADM.
- Prevenir los daños a la imagen y reputación a través de la adopción y cumplimiento de disposiciones que prohíben la realización de acciones asociadas con LA/FT/FPADM.
- Abstenerse de vincular o mantener relaciones comerciales con personas naturales o jurídicas cuando, como resultado de los procesos de debida diligencia, monitoreo y control, se identifiquen riesgos de LA/FT/FPADM no mitigables conforme al apetito de riesgo definido por el Grupo, o cuando existan causales objetivas derivadas de decisiones de autoridades competentes, listas vinculantes u otros criterios verificables establecidos en la normatividad y en los procedimientos internos.

4. LINEAMIENTOS GENERALES

- Cumplir con las pautas generales de comportamiento definidas en el Código de Ética y Conducta.
- Informar y/o denunciar potenciales casos de LA/FT/FPADM de los que pudiera llegar a tener conocimiento o conductas que ponga en riesgo la integridad y los intereses del Grupo, con el objetivo de fomentar la transparencia.
- Mantener un sistema de control interno adecuado y efectivo que garantice que todas las relaciones comerciales o laborales cuenten con las aprobaciones correspondientes, estén debidamente soportadas con la documentación exigida por la normativa vigente y las políticas internas del Grupo, y que se apliquen las medidas de debida diligencia ampliada o intensificada que resulten pertinentes, de acuerdo con el perfil de riesgo identificado.

- Propender por la protección frente a represalias en contra de una persona vinculada mediante contrato de trabajo, directivo o tercero que informe acerca de un incumplimiento o sospecha de LA/FT/FPADM y facilite información de buena fe sobre una conducta antiética o coopere con una investigación debidamente autorizada. Cualquier persona que sea objeto de represalias es responsable de comunicar toda la información y documentación al Comité de Ética.
- Identificar y gestionar todo conflicto de interés que pueda afectar la objetividad y juicio en el desarrollo del trabajo de cualquier persona vinculada mediante un contrato de trabajo y que pudiera llevar a contraponer los intereses personales sobre los del Grupo.
- Establecer y ejecutar periódicamente o cuando circunstancias especiales ocurran, un proceso para identificar, evaluar, documentar, gestionar y mitigar los riesgos de LA/FT/FPADM considerando de forma diferenciada los factores generadores de riesgo.
- Realizar inducción en materia de LA/FT/FPADM dirigido a las personas nuevas vinculadas, así como capacitar, al menos de manera anual, al personal antiguo y demás partes interesadas, según lo defina la normatividad vigente para promover y afianzar la cultura de la prevención de LA/FT/FPADM. Dichos procesos deberán guiarse y apoyarse en directrices claras que fomenten el comportamiento profesional, ético y responsable de todos los miembros de la entidad.
- Disponer de un repositorio de información que permita soportar los elementos del SARLAFT/SAGRILAFT/SIPLAFT/SIPLA, así como con herramientas que permitan hacer una gestión de los riesgos identificados y los controles implementados.
- Establecer estrategias de prevención, mitigación y control que permitan una adecuada gestión del riesgo LA/FT/FPADM en caso de materialización y enfocado a los delitos fuente.
- Reportar al Comité de Crisis o comité que haga sus veces de la entidad correspondiente, cualquier acto que pueda constituir una extorsión en contra del Grupo por el mero ejercicio de sus funciones, y del cual se tenga conocimiento, con el fin de ejecutar el procedimiento establecido para la atención del hecho, poner en conocimiento de las autoridades competentes e implementar las medidas que sean necesarias.
- Garantizar una estructura de gestión clara, eficaz y robusta con líneas de responsabilidad bien definidas, transparentes y coherentes, debidamente aprobadas por la Alta Gerencia correspondiente y asegurar la consistencia y mantenimiento de políticas, productos, actividades, procesos y sistemas para la adecuada gestión del riesgo de LA/FT/FPADM.
- Asegurar la evaluación y calificación del riesgo inherente de LA/FT/FPADM que se encuentra en todos los procesos, actividades, sistemas, canales, clientes, usuarios, productos y jurisdicciones, considerando la actividad principal, estructura y alcance regulatorio (sujeto obligado o no obligado).
- Identificar, evaluar y gestionar los riesgos de LA/FT/FPADM asociados a la implementación o utilización de nuevos productos, servicios, canales de distribución y tecnologías emergentes, incluyendo procesos de transformación digital, inteligencia artificial, automatización, ecosistemas abiertos, activos virtuales y demás innovaciones que puedan impactar el perfil de riesgo definido por la Entidad.

- Aplicar medidas de control en la gestión y administración del LA/FT/FPADM para evitar ser utilizado como instrumento 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 un 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 LA/FT/FPADM.
- Realizar la debida diligencia necesaria para la vinculación y actualización periódica de las contrapartes del negocio, operaciones, servicios y productos, teniendo como base los datos e información de fuentes confiables e independientes para verificar la identidad de la contraparte, beneficiarios finales, representante legal, revisores fiscales y demás relacionados.
- Implementar procedimientos de debida diligencia y monitoreo continuo respecto de proveedores, contratistas, corresponsales, aliados estratégicos, intermediarios y demás terceros con los que se mantengan relaciones, considerando la naturaleza de los servicios prestados, el nivel de acceso a información, el impacto sobre los procesos críticos y la exposición al riesgo de LA/FT/FPADM, cuando la evaluación de riesgo así lo requiera, se aplicarán medidas de debida diligencia ampliada o intensificada, incluyendo la verificación de beneficiarios finales, antecedentes reputacionales, situación regulatoria, listas restrictivas y sancionatorias, así como el monitoreo periódico de la relación comercial.
- Incluir como parte de los procesos de debida diligencia la búsqueda formal en las listas internacionales vinculantes para Colombia, de conformidad con el derecho internacional, con el fin de evitar el establecimiento de relaciones comerciales con personas naturales o jurídicas incluidas en dichas listas, sin perjuicio de la aplicación de otras listas de riesgo que se consideren necesarias para esta verificación.
- Disponer de ambientes presenciales y/o no presenciales para la vinculación de clientes mediante el uso de canales físicos y/o digitales que garanticen el contacto independiente. En ningún caso se omite realizar los procedimientos de identificación y verificación de los clientes.
- Desarrollar procesos especiales de vinculación y monitoreo de PEP locales y extranjeros, corresponsales, campañas políticas, entre otros que, por la naturaleza de sus actividades, exponen a un mayor riesgo frente a la posibilidad o facilidad para apropiarse de recursos, malversar y desviar fondos con destino a intereses particulares o a la financiación de estructuras o formas de asociación que hayan sido creadas con la intención de ocultar o dar apariencia de legalidad a operaciones de LA/FT/FPADM o delitos conexos.
- Obtener la aprobación de la alta gerencia (no incluye al Oficial de Cumplimiento) para la vinculación y continuación de la relación comercial o laboral de un PEP u otras contrapartes de países en donde no exista cooperación o no se apliquen las recomendaciones del GAFI, empresas y productos con mayor riesgo de blanqueo de dinero/financiación del terrorismo. Para estos casos, adoptar medidas para establecer el origen de los recursos; prever procedimientos más exigentes de vinculación; y realizar un monitoreo continuo e intensificado de la relación comercial.
- Optimizar los procesos de actualización de clientes y demás contrapartes entre las entidades vigiladas por la SFC, dadas las facultades otorgadas por el supervisor a los conglomerados financieros frente a la opción de compartir información obtenida durante los procedimientos de

debida diligencia. Esto siempre que se cuente con la autorización expresa del titular de los datos y se dé estricto cumplimiento a las normas relacionadas con protección de datos y habeas data.

- Mantener los registros físicos o electrónicos de la información relacionada con la gestión LA/FT/FPADM garantizando la integridad, oportunidad, confiabilidad y disponibilidad de la información allí contenida y acorde con los requerimientos legales y regulatorios.
- Monitorear regularmente los perfiles de riesgo y las exposiciones a pérdidas importantes asociadas a multas o sanciones, de acuerdo con el sistema de prevención de riesgo de LA/FT/FPADM aplicable.
- Asegurar la capacidad de operación ante impactos materiales y/o reputacionales y, ante eventos que pongan en entredicho el giro ordinario del negocio, llevando a cabo los planes de continuidad definidos.
- Identificar y cumplir las decisiones de bloqueo de fondos adoptadas por la autoridad competente y bajo ningún motivo deben 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.
- Identificar, bloquear y abstenerse de establecer o mantener relaciones con personas o entidades designadas como terroristas u organizaciones terroristas, de conformidad con la normativa nacional e internacional aplicable, mediante la verificación previa y el monitoreo continuo de clientes y transacciones, utilizando sistemas orientados a la detección de coincidencias en listas internacionales vinculantes y demás listas de control adoptadas por la entidad.

5. SANCIONES

El Grupo reconoce que en el evento de incumplimiento de esta política y demás actividades que se deriven de ella, las entidades y las personas responsables por su aplicación y cumplimiento deben someterse a sanciones administrativas, establecidas en las leyes locales e internacionales, así como al incremento del nivel de riesgo de la entidad y el estricto seguimiento y monitoreo de los órganos de control corporativos.

6. MODELO DE GESTIÓN

El modelo de gestión corporativa para la administración del riesgo de LA/FT/FPADM comprende, de manera general las siguientes etapas:

Identificación

Los riesgos a los que puede estar expuesto el Grupo, son: lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva; a partir de estos riesgos se debe establecer la segmentación de los factores de riesgo, teniendo en cuenta el contexto interno y externo de cada Entidad.

Medición

El modelo de medición utilizado corresponde a mapas de calor que, a través de su colorimetría, permite priorizar los riesgos que requieren atención inmediata, teniendo en cuenta los criterios de probabilidad e impacto, las mediciones cualitativas o cuantitativas, y sus escalas estén acordes con la naturaleza, complejidad y volumen de las operaciones de la Entidad.

Control

Las entidades deben tomar las medidas conducentes a controlar el riesgo inherente al que se ven expuestas, diseñando los controles que de forma efectiva y eficiente mitiguen los riesgos y causas de LA/FT/FPADM, disminuyendo la probabilidad e impacto de acuerdo con la efectividad de dichos controles.

Como resultado de esta etapa la Entidad establece el perfil de riesgo residual de LA/FT/FPADM, permitiendo identificar oportunamente la necesidad de planes de acción para corregir las desviaciones detectadas y cubrir de manera razonable y suficiente la exposición al riesgo.

Monitoreo

Se debe evaluar la evolución del perfil de riesgo de la Entidad tanto inherente como residual y su variación, de modo consolidado como discriminado por factor de riesgo y riesgo asociado, evaluando las calificaciones obtenidas y determinando los planes de acción o mejora para mantener y/o estabilizar el riesgo residual como aceptable.

Durante esta etapa las entidades implementan una matriz de riesgo y reportes que permitan establecer las evoluciones del riesgo de esta y la eficiencia de los controles implementados. Así mismo identifica, investiga y monitorea las transacciones, actividades inusuales, sospechosas o cualquier comportamiento irregular que indique posibles riesgos LA/FT/FPADM y generan informes para las autoridades pertinentes, como la UIAF (Unidad de Información y Análisis Financiero).

7. ROLES Y RESPONSABILIDADES

7.1 Modelo de las tres líneas

El Grupo debe estructurar las funciones y responsabilidades frente al LA/FT/FPADM, y en general frente a todos los riesgos, siguiendo el esquema de las tres líneas, esto es, considerando (i) la gestión por la línea de negocio, (ii) una función de gestión del riesgo LA/FT/FPADM independiente, y (iii) una revisión independiente, tal y como lo establece la Política Integral para la Gestión Integral del Riesgos y Cumplimiento.

Primera línea

Son las áreas que gestionan el negocio y las que tienen contacto directo con los clientes (p.ej. las actividades de cara al público y en contacto directo con los clientes). Sus responsabilidades son:

- Conocer y aplicar las políticas y procedimientos de LA/FT/FPADM y de conocimiento del cliente, así como disponer de los recursos suficientes para realizar eficazmente estas tareas. Aplicar la debida diligencia intensificada a los clientes PEPs y a aquellos con actividades económicas de mayor nivel de riesgo, conforme con los procedimientos y directrices internas.

Área: SARLAFT	Código: GRC-PO-SARLAFT-1	Versión: 8
---------------	--------------------------	------------

- Reportar y gestionar oportunamente las señales de alerta, garantizando su adecuado escalamiento a las instancias correspondientes.
- Conocer los riesgos inherentes asociados a los productos, actividades, procesos y sistemas a su cargo, así como ejecutar los controles definidos para su mitigación, asegurando su correcta aplicación en el desarrollo de las operaciones.
- Garantizar la calidad, integridad y actualización de la información suministrada por las contrapartes y utilizada en los procesos de vinculación, conocimiento y monitoreo.
- Colaborar activamente con la segunda y tercera línea, atendiendo oportunamente los requerimientos de información, revisiones y recomendaciones que se formulen.

Segunda línea

Son las áreas de riesgo y cumplimiento, la lidera el Oficial de Cumplimiento en las entidades obligadas y el líder de gestión LA/FT/FPADM (o quien haga sus veces) en las entidades no obligadas, encargadas de supervisar y fortalecer la gestión del riesgo. Sus responsabilidades son:

- Realizar el seguimiento continuo al cumplimiento de las obligaciones en materia de riesgo LA/FT/FPADM, de conformidad con la normatividad vigente, las políticas y los lineamientos internos.
- Definir, administrar y mantener la metodología de gestión del riesgo LA/FT/FPADM, incluida la identificación, medición y evaluación del riesgo.
- Identificar los riesgos y controles claves suficientes para su mitigación, así como en la calificación de los atributos de cada control a efectos de determinar el riesgo residual que debe ser sujeto a seguimiento de acuerdo con la metodología definida.
- Analizar y reportar a la Alta Dirección y a los Órganos de Gobierno el estado del riesgo LA/FT/FPADM, las principales exposiciones, tendencias, alertas relevantes y oportunidades de mejora del sistema.
- Emitir conceptos técnicos y recomendaciones para el fortalecimiento del sistema, sin asumir funciones operativas ni responsabilidades propias de la primera línea.

Tercera línea

- Evaluar de forma independiente la gestión del riesgo LA/FT/FPADM. Dichas evaluaciones podrán ser realizadas por la auditoría interna, por personal independiente del proceso o sistema evaluado siempre que actúe bajo un mandato formal, bajo un plan de auditoría o un encargo específico o por terceros externos debidamente calificados, garantizando en todos los casos la objetividad
- Rendir cuentas al Comité de Auditoría o al órgano de vigilancia equivalente mediante evaluaciones periódicas de la eficacia del cumplimiento de las políticas y procedimientos para la gestión del Riesgo LA/FT/FPADM.
- Emitir conclusiones, hallazgos y recomendaciones independientes, orientadas al fortalecimiento del sistema, y realizar seguimiento a la implementación de los planes de acción definidos.

7.2 Responsabilidades

Junta Directiva (u órgano que haga sus veces)

- Aprobar y velar por el cumplimiento de la Política LA/FT/FPADM o el documento equivalente de la Entidad, así como sus modificaciones posteriores.
- Asignar las competencias de manera explícita a los órganos y responsables definidos teniendo en la estructura de gobierno de la Entidad, garantizando así la gestión eficaz de las políticas y procedimientos.

Área: SARLAFT	Código: GRC-PO-SARLAFT-1	Versión: 8
---------------	--------------------------	------------

- Definir y aprobar el apetito, la tolerancia y los límites de exposición al riesgo de LA/FT/FPADM, y realizar seguimiento periódico a su cumplimiento.
- Comprender los riesgos de LA/FT/FPADM y asegurar que la información derivada de su evaluación sea recibida, de manera puntual, oportuna, completa, comprensible y precisa, a través del Comité de Auditoría, del Comité de Riesgo, y/o de cualquier otro Comité o instancia en la que participen miembros de la Junta Directiva.
- Recibir informes periódicos sobre los casos relevantes de LA/FT/FPADM identificados, incluyendo las investigaciones efectuadas y sus conclusiones y pronunciarse al respecto.
- Hacer seguimiento a la implementación de planes de acción derivados de hallazgos, incumplimientos o requerimientos de autoridades y órganos de control.
- Designar un Oficial de Cumplimiento en las entidades obligadas, o un Líder SARLAFT (o quien haga sus veces) en las entidades no obligadas en materia de LA/FT/FPADM, con la preparación adecuada y con la categoría y autoridad necesarias para garantizar que las cuestiones planteadas en esta política reciban la atención correspondiente por parte de la Junta Directiva, la Alta Dirección y las líneas de negocio.
- Proveer los recursos técnicos y humanos necesarios para implementar y mantener en funcionamiento para la gestión de riesgos LA/FT/FPADM.

Comité de Riesgos y Comité de Auditoría (u órgano que haga sus veces) de Grupo Aval

- Asegurar la existencia de una política LA/FT/FPADM y velar por su cumplimiento.
- Hacer seguimiento al resultado de la evaluación de los controles LA/FT/FPADM.
- Proponer los ajustes y actualizaciones de la política LA/FT/FPADM.

Vicepresidencia corporativa de riesgos y cumplimiento de Grupo Aval

- Presentar a aprobación de la Junta Directiva y divulgar las políticas que permitan la adecuada gestión del riesgo de LA/FT/FPADM.
- Remitir la información sobre la evaluación de riesgos LA/FT/FPADM a la Junta Directiva, Comité de Riesgos y/o Comité de Auditoría (u órganos que haga sus veces) de forma puntual, oportuna, completa, comprensible y precisa.
- Diseñar y realizar seguimiento al cumplimiento de la presente Política con el apoyo del equipo de la Dirección Senior de Cumplimiento, así como con la colaboración y coordinación de los Oficiales de Cumplimiento en las entidades obligadas y el líder de gestión LA/FT/FPADM (o quien haga sus veces) en las entidades no obligadas.
- Establecer directrices de acuerdo con las mejores prácticas definidas en el Comité de Riesgos / Comité de Auditoría (u órganos que haga sus veces) y considerando las diferentes jurisdicciones y tipo de entidades que conforman el Grupo.
- Definir y comunicar a los Oficiales de Cumplimiento de las entidades directas las instrucciones y políticas de cumplimiento, cronograma detallado anual, modelos y periodicidad de reporte, niveles de revisión y aprobación de cada entregable definido.

Oficial de Cumplimiento, Líder SARLAFT o responsable de la gestión LA/FT/FPADM

- Velar por el efectivo, eficiente y oportuno funcionamiento de las etapas que conforman el sistema de gestión de riesgo LA/FT/FPADM.
- Presentar los informes a la junta directiva u órgano que haga sus veces informando los temas relevantes del sistema.

Área: SARLAFT	Código: GRC-PO-SARLAFT-1	Versión: 8
---------------	--------------------------	------------

- Presentar a la Junta Directiva, o a quien haga sus veces, los requerimientos de recursos informáticos, tecnológicos, físicos, humanos y financieros necesarios para el cumplimiento de sus funciones.
- Evaluar los informes presentados por la auditoría interna o quien ejecute funciones similares o haga sus veces, y los informes que presente el revisor fiscal y adoptar las medidas del caso frente a las deficiencias informadas.
- Diseñar las metodologías de segmentación, identificación, medición y control para la gestión del riesgo LA/FT/FPADM.
- Diseñar y someter a la aprobación de la junta directiva u órgano que haga sus veces, los procedimientos establecidos para la aplicación proporcional basada en riesgos y los criterios para la determinación de las operaciones sospechosas y para la consolidación, monitoreo y análisis de inusualidad de operaciones.
- Aprobar si una operación inusual debe ser considerada como sospechosa y determinar el respectivo reporte ante la UIAF, con base en la información disponible y en el conocimiento sobre las tipologías y demás conceptos relacionados con LA/FT/FPADM.
- Asegurar que las actividades que resulten del desarrollo de la gestión LA/FT/FPADM se encuentran debidamente documentadas, de modo que se permita que la información responda a criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad.
- Cumplir las obligaciones relacionadas con sanciones financieras dirigidas.
- Adoptar y socializar las mejores prácticas, atendiendo los lineamientos Corporativos.
- Acompañar a los dueños de proceso en la evaluación de riesgos de LA/FT/FPADM e identificación de controles y apoyar a la primera línea, en la realización de la debida diligencia.
- Desarrollar y ejecutar planes de capacitación periódicos a todas las personas vinculadas mediante un contrato de trabajo y planes de comunicación, y establecer mecanismos para que, por lo menos, las personas vinculadas mediante un contrato de trabajo certifiquen anualmente el cumplimiento de la política y de los planes de capacitación.
- Desarrollar e implementar metodologías que permitan monitorear e identificar señales de alerta y/o transacciones inusuales para gestión de riesgos LA/FT/FPADM.
- Reportar periódicamente los informes requeridos, de acuerdo con el alcance y frecuencia definida en instrucciones o lineamientos corporativos.
- Presentar informes de gestión a la Vicepresidencia Corporativa de Riesgos y Cumplimiento de Grupo Aval con la periodicidad que éste le indique.
- Informar al Comité de Auditoría o comité que haga sus veces en las entidades, al menos semestralmente, los resultados del perfil de riesgo.
- Orientar y ejecutar al interior de su entidad los cambios en los lineamientos Corporativos asegurando su adecuado cumplimiento.
- Preparar el Informe de Gestión conforme a la aplicabilidad de los requerimientos, atendiendo la actividad principal de la entidad, su estructura y enfoque regulatorio.

Comité Corporativo SARLAFT de Grupo Aval

- Definir y evaluar las directrices en Grupo Aval para el mejoramiento de la metodología frente a la gestión del riesgo LA/FT/FPADM.
- Conocer la gestión de riesgos realizada por parte de las entidades, así como los eventos de riesgo y los planes de acción llevados a cabo para la mitigación de estos.
- Presentar propuestas para fortalecer las políticas, formatos y metodología relacionados con la gestión del riesgo LA/FT/FPADM e implementar mejores prácticas en cumplimiento con los requerimientos legales y la adecuada y eficiente gestión de los riesgos.

- Realizar seguimiento a la gestión estratégica de los riesgos, así como formular recomendaciones y buenas prácticas para su adecuado manejo en las entidades. La modificación, ajuste o actualización de dichas recomendaciones será responsabilidad del mismo comité, en su calidad de grupo asesor conformado por los Oficiales de Cumplimiento de las entidades principales.

Entidades que conforman el Grupo

- Participar en el proceso de identificación y valoración de riesgos LA/FT/FPADM, definir y actualizar los lineamientos corporativos en la entidad y que sirven para identificar, valorar y mitigar dichos riesgos con el apoyo de las áreas de riesgo.
- Gestionar el riesgo LA/FT/FPADM bajo su entera responsabilidad conforme a las políticas internas definidas y la normatividad vigente de acuerdo con su industria, jurisdicción y ente de vigilancia.
- Adaptar el modelo de gestión de riesgo LAFT/FPADM atendiendo la normativa propia de su industria y jurisdicción, así como los lineamientos corporativos.
- 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.
- Aplicar las normas contra LA/FT/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.
- Realizar seguimiento continuo de todas las relaciones comerciales, laborales 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 de la contraparte y 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.
- Disponer de sistemas para detectar señales de alerta que puedan indicar LA/FT/FPADM a partir de la evaluación de riesgo de la entidad, los resultados de las consultas y debida diligencia, entre otros.
- Identificar transacciones inusuales o no relacionadas con el perfil de riesgo, mediante el uso de la información sobre conocimiento del cliente, personas vinculadas mediante un contrato de trabajo y terceros intermediarios.
- Aplicar procesos robustos de debida diligencia para las relaciones de naturaleza civil, comercial o laboral que representen una calificación alta del perfil del riesgo LA/FT/FPADM y reforzar su seguimiento y vigilancia transversal de los productos o servicios con el fin de identificar y mitigar los patrones de riesgo emergentes.
- Cotejar su(s) base(s) de datos de relaciones civiles, comerciales o laborales cuando haya modificaciones en los listados de sanciones y periódicamente con las bases PEP y otras cuentas de alto riesgo y practicarles una debida diligencia.
- Garantizar los recursos necesarios para asegurar el cumplimiento de los objetivos de la esta política, así como el adoptar las mejores prácticas internacionales y demás lineamientos corporativos.
- Disponer de sistemas de gestión de la información, proporcionales 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 comerciales) 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 cualquier indicio de temas LA/FT/FPADM.
- Asegurar la adecuada atención de los requerimientos de los entes de control, mediante la acreditación de la idoneidad de los sistemas de evaluación, gestión y mitigación del riesgo LA/FT/FPADM de la política de aceptación de clientes; de los procedimientos y políticas sobre

identificación y verificación de clientes; de los procesos de seguimiento continuo y de los procedimientos para notificar operaciones sospechosas, así como de todas las medidas adoptadas en el contexto de prevención del riesgo de LA/FT/FPADM.

- Reportar a Grupo Aval y a las entidades matrices directas de cada una de las subsidiarias los formatos aplicables y detallados en el Manual Corporativo de Lavado de Activos, Financiación del Terrorismo y de la Proliferación de Armas de Destrucción Masiva, en las fechas establecidas.
- Velar por mantener un proceso de mejora continua al Sistema.
- Evaluar periódicamente la efectividad del sistema de administración del riesgo de LA/FT/FPADM en la Entidad, mediante el seguimiento de indicadores de gestión e indicadores de riesgo, resultados de monitoreo, calidad de alertas, reportes regulatorios, hallazgos de auditoría, evaluaciones independientes, requerimientos de autoridades y el cumplimiento de los planes de acción definidos.
- Presentar los resultados de dichas evaluaciones a la Alta Dirección y a los órganos de gobierno correspondientes, con el fin de identificar oportunidades de mejora, fortalecer los controles existentes y garantizar la evolución del sistema frente a cambios regulatorios, operativos, tecnológicos y de riesgo.

Revisor Fiscal del Grupo

- Evaluar anualmente el sistema de prevención de riesgos LA/FT/FPADM del Grupo de forma independiente y presentar al máximo órgano de gobierno y al Oficial de Cumplimiento los resultados y conclusiones obtenidas en el proceso de revisión del cumplimiento del sistema.
- Reportar al Comité de Auditoría cualquier irregularidad o hallazgo que pueda comprometer el resultado de la gestión del riesgo LA/FT/FPADM del Grupo.
- Reportar a la autoridad competente la información que lleva a la sospecha de posibles actos de LA/FT/FPADM cuando en el curso de su trabajo descubre dicha situación a pesar de la obligación de guardar reserva profesional.

Auditoría Interna de cada Entidad

- Verificar la existencia de políticas y procedimientos que establezcan los lineamientos sobre la gestión LA/FT/FPADM debidamente aprobados e implementados.
- Verificar el diseño y efectividad de los controles detallados en la matriz de riesgo/control, de acuerdo con su plan de operación definido autónomamente.
- Reportar sus hallazgos tanto a los dueños de proceso para su remediación, como al responsable en la gestión del LA/FT/FPADM y a la Junta Directiva / Comité de Auditoría.

Gou Payments

Gou Payments es una entidad de Administradora de Sistemas de Pago de Bajo Valor y dentro de sus actividades tiene acceso a la información asociada a las transacciones de retiro de efectivo en los ATM de los Bancos del grupo AVAL por parte de usuarios con tarjetas emitidas en el extranjero, bajo este enfoque se encarga de suministrar esta información hacia los bancos y hacia la UIAF en el momento que se requiera.

Por esta razón, Gou Payments en su modelo de riesgo LA/FT/FPADM debe:

- Realizar seguimiento de las transacciones de tarjetas internacionales por medio de este canal, de acuerdo con el comportamiento identificado en las transacciones de retiro de efectivo en los ATM

de los bancos del grupo Aval y la aplicación de señales de alerta establecidas por parte de Gou Payments.

- Gestionar los requerimientos de los Oficiales de Cumplimiento de los Bancos del grupo Aval, asociados a tarjetas y bins internacionales que como resultado de sus transacciones de retiro presenten comportamientos inusuales, para la aplicación de medidas dispuestas por Gou Payments para la mitigación estos comportamientos.
- El Oficial de Cumplimiento de Gou Payments debe reportar las operaciones consideradas como 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. El detalle de estos reportes es transmitido a la UIAF, a los bancos se comparte la información de manera cifrada y enmascarada.
- Reportar a los entes de control (comités, junta directiva, etc.) las estadísticas de los ROS reportados a la UIAF.

Gestión de tecnología e informes – apoyo al modelo LA/FT:

- Suministrar a los Bancos acceso a la información transaccional requerida para la implementación del monitoreo.
- Implementar las acciones de mitigación o tratamiento de riesgo que sean requeridas por los Bancos de acuerdo con los lineamientos acordados.

Esta política se complementa con el Manual Corporativo de Lavado de activos y financiación del terrorismo y de armas de destrucción masiva que detalla y desarrolla las directrices aquí descritas.

8. REGULACIÓN

Normatividad utilizada en el desarrollo de la Gestión de Riesgo de LA/FT/FPADM:

- **Local:**
 - Circular Básica Jurídica de la Superintendencia Financiera de Colombia SFC, (Circular Externa 006 de 2025):
 - ✓ 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.
 - ✓ Parte III Mercado desintermediado, Título I Emisores de Valores, Capítulo VII Instrucciones en materia de prevención y control de lavado de activos y de la financiación del terrorismo a los emisores no vigilados por la Superintendencia Financiera de Colombia referente al SIPLA.
 - Circular Básica Jurídica de la Superintendencia de Sociedades (Circular Externa 100-000008 de 2022) en su Capítulo X Autocontrol y Gestión del Riesgo LA/FT y Reporte de Operaciones Sospechosas a la UIAF.
 - Resolución de la Superintendencia de Transporte, (Resolución 2328 del 6 de marzo de 2025, modificada posteriormente por la Resolución 16615 del 5 de noviembre de 2025).

- Resolución de la Superintendencia de Transporte, (Resolución 4607 del 9 de abril de 2026, Por la cual se modifica el capítulo 6 del Título V de la Circular Única de Infraestructura y Transporte).
- Circular Externa 010 de la Superintendencia Financiera de Colombia del 28 de agosto de 2025 donde se dan las instrucciones para la prestación de productos y servicios financieros a consumidores financieros con antecedentes penales o investigaciones penales en curso, en cumplimiento de la orden proferida por la Corte Constitucional en la sentencia T-113 de 2025.
- Circular externa 170 de 2022 DIAN donde se indica los procedimientos que deberán seguir los usuarios del servicio aduanero y cambiario, para prevenir, detectar, controlar y reportar operaciones sospechosas que puedan estar vinculadas con el lavado de activo.
- Estatuto Tributario Nacional, Artículo 631-5 Definición beneficiario final o cualquier norma que lo modifique o sustituya.
- 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
- Resoluciones 1267, 1989, 2253 Consejo de Seguridad de la ONU
- Demás normas de la materia aplicables a las Subsidiarias del Grupo

9. GLOSARIO

- **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. Son beneficiarios finales los mencionados en el artículo 631-5 Definición beneficiario final del Estatuto Tributario Nacional.
- **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.
- **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.
- **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.
- **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:** 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 LA/FT/FPADM. También se conoce como medidas intensificadas.

- **Factores de riesgo:** son los agentes generadores del riesgo de LA/FT/FPADM como los son: Clientes/usuarios, Productos, Canales de distribución y 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.
- **Financiación 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, transferencia, deposito o uso dual para propósitos ilegítimos en contravención de las leyes nacionales u obligaciones internacionales, cuando esto último sea aplicable.
- **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:** se considera operación sospechosa aquella transacción o conjunto de transacciones sobre activos, pasivos u otros recursos que, por su cuantía, frecuencia o características particulares, no guardan relación con la actividad económica del cliente o usuario y que pueden llevar razonablemente a pensar que la entidad está siendo utilizada para transferir, manejar, aprovechar o invertir recursos provenientes de actividades delictivas o destinados a su financiación.
- **Persona Expuesta Políticamente (PEPs):** 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.

- **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 Reporte de Operación Sospechosa (ROS) es la obligación legal que tienen los sujetos obligados en Colombia de informar a la Unidad de Información y Análisis Financiero (UIAF) cualquier transacción o conjunto de transacciones que, por su monto, frecuencia o características, no guarden relación con la actividad económica de sus clientes o usuarios y que puedan razonablemente hacer sospechar que la entidad está siendo utilizada para transferir, manejar, aprovechar o invertir recursos provenientes de actividades delictivas o destinados a su financiación. El ROS no constituye una denuncia penal, tiene carácter reservado y confidencial, no es prueba judicial ni testimonio, y no genera responsabilidad penal para quien lo reporta; su finalidad es servir como insumo de inteligencia financiera para prevenir y detectar el lavado de activos y la financiación del terrorismo.
- **SAGRILAF:** 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.

- **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 LA/FT/FPADM.
- **SIPLA:** es el Sistema Integral para la Prevención del Lavado de Activos y la Financiación del terrorismo. El SIPLA se compone del conjunto de políticas, procedimientos, mecanismos e instrumentos mínimos diseñados e implementados para prevenir y controlar el lavado de activos y financiación del terrorismo LA/FT/FPADM a los emisores no vigilados por la Superintendencia Financiera. Así mismo aquellas entidades que deben dar cumplimiento a la Circular externa 170 de 2022 de la DIAN.
- **SIPLA/FT:** Sistema de Prevención y Control del lavado de activos, la financiación del terrorismo y financiamiento de la proliferación de armas de destrucción masiva, el cual deben implementar todas las empresas habilitadas por el Ministerio de Transporte para la prestación del servicio público de transporte terrestre automotor de carga, sin importar si estas empresas se encuentran o no en operación (estén o no operando y/o activas), según los Artículos 1 y 2 de la Resolución 74854 de 2016 de la Superintendencia Transporte.
- **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 LA/FT/FPADM, 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.

- **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.