



Corporate Policy on Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction

1. OBJECTIVE

To establish the methodological guidelines, roles, and responsibilities of key stakeholders for the management of risks related to money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction (ML/TF/FPWMD).

2. SCOPE

This policy is geared toward comprehensive management to ensure compliance with international and local regulations applicable to Grupo Aval Acciones y Valores and its subsidiaries (the Group) regarding the prevention of ML/TF/FPWMD. It establishes the criteria that must be considered in managing the risks associated with ML/TF/FPWMD, in accordance with the specific characteristics and current regulations applicable to each entity.

3. STATEMENT OF COMMITMENT

Grupo Aval is committed to a zero-tolerance policy toward ML/TF/FPWMD offenses in any form and pledges to:

- Prioritize compliance with regulations regarding ML/TF/FPWMD risk management over the achievement of business goals.
- Manage, in a structured and strategic manner, the ML/TF/FPWMD risks associated with the business and its relationships with counterparties.
- Promote and maintain a robust and ethical risk culture as an essential element for the prevention, detection, investigation, and remediation of ML/TF/FPWMD risks.
- Prevent damage to its image and reputation by adopting and complying with provisions that prohibit actions associated with ML/TF/FPWMD.
- Refrain from establishing or maintaining business relationships with individuals or legal entities when, as a result of due diligence, monitoring, and control processes, ML/TF/FPWMD risks are identified that cannot be mitigated in accordance with the Group's defined risk appetite, or when there are objective grounds arising from decisions by competent authorities, binding lists, or other verifiable criteria established in regulations and internal procedures.

4. GENERAL GUIDELINES

- Comply with the general guidelines for conduct set forth in the Code of Ethics and Conduct.
- Report and/or disclose potential cases of ML/TF/FPWMD of which you may become aware, or conduct that jeopardizes the Group's integrity and interests, with the aim of promoting transparency.
- Maintain an adequate and effective internal control system that ensures all business or employment relationships have the appropriate approvals, are duly supported by the documentation required by current regulations and the Group's internal policies, and that the relevant enhanced or intensified due diligence measures are applied, in accordance with the identified risk profile.
- To ensure protection against retaliation against any person bound by an employment contract, executive, or third party who reports a violation or suspicion of ML/TF/FPWMD and provides information in good faith regarding unethical conduct or cooperates with a duly authorized

investigation. Any person who is subject to retaliation is responsible for communicating all relevant information and documentation to the Ethics Committee.

- Identify and manage any conflict of interest that may affect the objectivity and judgment of any person bound by an employment contract in the performance of their work and that could lead to personal interests conflicting with those of the Group.
- Establish and implement, periodically or when special circumstances arise, a process to identify, assess, document, manage, and mitigate ML/TF/FPWMD risks, taking into account risk-generating factors on a case-by-case basis.
- Conduct ML/TF/FPWMD induction training for new employees, as well as provide training—at least annually—to existing staff and other stakeholders, as defined by current regulations, to promote and strengthen a culture of ML/TF/FPWMD prevention. These processes must be guided and supported by clear guidelines that foster professional, ethical, and responsible behavior among all members of the entity.
- Maintain an information repository to support the elements of SARLAFT/SAGRILAFT/SIPLAFT/SIPLA, as well as tools to manage identified risks and implemented controls.
- Establish prevention, mitigation, and control strategies that enable adequate management of ML/TF/FPWMD risks should they materialize, with a focus on the source crimes.
- Report to the Crisis Committee or its equivalent at the relevant entity any act that may constitute extortion against the Group merely due to the exercise of its functions, and of which the entity becomes aware, in order to carry out the established procedure for addressing the incident, notify the competent authorities, and implement the necessary measures.
- Ensure a clear, effective, and robust management structure with well-defined, transparent, and consistent lines of responsibility, duly approved by the relevant senior management, and ensure the consistency and maintenance of policies, products, activities, processes, and systems for the proper management of ML/TF/FPWMD risk.
- Ensure the assessment and classification of the inherent ML/TF/FPWMD risk present in all processes, activities, systems, channels, customers, users, products, and jurisdictions, taking into account the core business, structure, and regulatory scope (whether the entity is a regulated or non-regulated entity).
- Identify, assess, and manage ML/TF/FPWMD risks associated with the implementation or use of new products, services, distribution channels, and emerging technologies, including digital transformation processes, artificial intelligence, automation, open ecosystems, virtual assets, and other innovations that may impact the risk profile defined by the Entity.
- Apply control measures in the management and administration of ML/TF/FPWMD to prevent the Entity from being used as an instrument for the concealment, handling, investment, or exploitation in any form of money or other assets derived from criminal activities or intended for their financing, or to give the appearance of legality to criminal activities or related transactions and funds, thereby

ensuring an adequate control environment, structured through policies, processes, systems, internal controls, and appropriate monitoring of the effectiveness of ML/TF/FPWMD risk control measures.

- Conduct the necessary due diligence for onboarding and periodically updating information on business counterparties, operations, services, and products, based on data and information from reliable and independent sources to verify the identity of the counterparty, beneficial owners, legal representative, statutory auditors, and other related parties.
- Implement due diligence procedures and continuous monitoring with respect to suppliers, contractors, correspondents, strategic partners, intermediaries, and other third parties with whom relationships are maintained, taking into account the nature of the services provided, the level of access to information, the impact on critical processes, and exposure to ML/TF/FPWMD risks; when the risk assessment so requires, enhanced or intensified due diligence measures shall be applied, including verification of ultimate beneficial owners, reputational background, regulatory status, and restrictive and sanctions lists, as well as periodic monitoring of the business relationship.
- Include, as part of the due diligence processes, a formal search of international lists binding on Colombia, in accordance with international law, in order to prevent the establishment of business relationships with individuals or legal entities included on such lists, without prejudice to the application of other risk lists deemed necessary for this verification.
- Provide in-person and/or remote environments for onboarding clients through the use of physical and/or digital channels that ensure independent contact. Under no circumstances shall the procedures for identifying and verifying clients be omitted.
- Develop special procedures for engaging with and monitoring local and foreign PEPs, correspondents, political campaigns, among others, which, due to the nature of their activities, pose a greater risk regarding the possibility or ease of misappropriating resources, embezzling, or diverting funds for private interests or to finance structures or forms of association created with the intent to conceal or give the appearance of legality to ML/TF/FPWMD operations or related crimes.
- Obtain approval from senior management (excluding the Compliance Officer) for establishing and continuing a business or employment relationship with a PEP or other counterparties from countries where there is no cooperation or where the FATF recommendations are not applied, as well as with companies and products posing a higher risk of money laundering or terrorist financing. In such cases, adopt measures to establish the source of funds; implement more stringent onboarding procedures; and conduct continuous and intensified monitoring of the business relationship.
- Optimize the processes for updating information on customers and other counterparties among entities supervised by the Finance Superintendence of Colombia, given the authority granted by the supervisor to financial conglomerates regarding the option to share information obtained during due diligence procedures. This is provided that express authorization is obtained from the data subject and that regulations related to data protection and habeas data are strictly complied with.
- Maintain physical or electronic records of information related to ML/TF/FPWMD management, ensuring the integrity, timeliness, reliability, and availability of the information contained therein, in accordance with legal and regulatory requirements.



Corporate Policy on Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction

- Regularly monitor risk profiles and exposures to significant losses associated with fines or sanctions, in accordance with the applicable ML/TF/FPWMD risk prevention system.
- Ensure operational capacity in the face of material and/or reputational impacts and, in the event of incidents that jeopardize normal business operations, implement the defined business continuity plans.
- Identify and comply with asset freeze orders issued by the competent authority; under no circumstances should the company maintain relationships with designated entities or individuals (e.g., terrorists, terrorist organizations), in accordance with relevant national laws (Colombian law and the laws of countries where the company has subsidiaries) and applicable U.S. legislation related to money laundering and terrorist financing.
- Identify, block, and refrain from establishing or maintaining relationships with persons or entities designated as terrorists or terrorist organizations, in accordance with applicable national and international regulations, through prior verification and ongoing monitoring of customers and transactions, using systems designed to detect matches against binding international lists and other watchlists adopted by the entity.

5. SANCTIONS

The Group acknowledges that in the event of non-compliance with this policy and other activities arising therefrom, the entities and individuals responsible for its implementation and compliance are subject to administrative sanctions established by local and international laws, as well as to an increased level of risk for the entity and strict oversight and monitoring by corporate governance bodies.

6. MANAGEMENT MODEL

The corporate management model for managing ML/TF/FPWMD risk generally comprises the following stages:

Identification

The risks to which the Group may be exposed are money laundering, terrorist financing, and financing of the proliferation of weapons of mass destruction; based on these risks, risk factors must be categorized, taking into account the internal and external context of each entity.

Measurement

The measurement model used consists of heat maps, which, through their color coding, allow for the prioritization of risks requiring immediate attention, taking into account probability and impact criteria, as well as qualitative or quantitative measurements, with scales that are consistent with the nature, complexity, and volume of the entity's operations.

Control

Entities must take appropriate measures to manage the inherent risk to which they are exposed by designing controls that effectively and efficiently mitigate the risks and causes of ML/TF/FPWMD, thereby reducing the probability and impact in accordance with the effectiveness of such controls.

As a result of this stage, the entity establishes its residual ML/TF/FPWMD risk profile, enabling it to identify in a timely manner the need for action plans to correct detected deviations and to address risk exposure in a reasonable and sufficient manner.

Monitoring

The evolution of the Entity's risk profile—both inherent and residual—and its variation must be evaluated, both on a consolidated basis and broken down by risk factor and associated risk, by assessing the ratings obtained and determining action or improvement plans to maintain and/or stabilize the residual risk at an acceptable level.

During this stage, institutions implement a risk matrix and reports that enable them to track changes in their risk profile and assess the effectiveness of the controls in place. They also identify, investigate, and monitor transactions, unusual or suspicious activities, or any irregular behavior that may indicate potential ML/TF/FPWMD risks, and generate reports for the relevant authorities, such as the UIAF (Financial Information and Analysis Unit).

7. ROLES AND RESPONSIBILITIES

7.1 Three-Lines Model

The Group must structure its functions and responsibilities regarding ML/TF/FPWMD—and, more generally, regarding all risks—in accordance with the three-lines framework, that is, by considering (i) management by the business line, (ii) an independent ML/TF/FPWMD risk management function, and (iii) an independent review, as established in the Comprehensive Policy for Integrated Risk Management and Compliance.

First Line

These are the areas that manage the business and have direct contact with customers (e.g., customer-facing activities and those in direct contact with customers). Their responsibilities are:

- To understand and apply ML/TF/FPWMD and know-your-customer policies and procedures, as well as to have sufficient resources to effectively carry out these tasks. To apply enhanced due diligence to PEPs and customers engaged in higher-risk economic activities, in accordance with internal procedures and guidelines.
- Timely reporting and management of red flags, ensuring they are properly escalated to the appropriate authorities.
- Understand the inherent risks associated with the products, activities, processes, and systems under their responsibility, and implement the controls defined to mitigate them, ensuring their proper application in the conduct of operations.
- Ensure the quality, integrity, and timeliness of the information provided by counterparties and used in the onboarding, due diligence, and monitoring processes.
- Actively collaborate with the second and third lines of defense, promptly addressing any requests for information, reviews, and recommendations that are made.

Second Line

Area: SARLAFT	Code: GRC-PO-SARLAFT-1	Version: 8
---------------	------------------------	------------

These are the risk and compliance areas, led by the Compliance Officer in regulated institutions and by the ML/TF/FPWMD management leader (or their designee) in non-regulated institutions, responsible for supervising and strengthening risk management. Their responsibilities are:

- Continuously monitor compliance with obligations regarding ML/TF/FPWMD risk, in accordance with current regulations, policies, and internal guidelines.
- Defining, administering, and maintaining the ML/TF/FPWMD risk management methodology, including the identification, measurement, and assessment of risk.
- Identifying key risks and controls sufficient for their mitigation, as well as assessing the attributes of each control to determine the residual risk that must be monitored in accordance with the defined methodology.
- Analyze and report to Senior Management and the Governing Bodies on the status of ML/TF/FPWMD risk, the main exposures, trends, relevant alerts, and opportunities for system improvement.
- Provide technical guidance and recommendations for strengthening the system, without assuming operational functions or responsibilities typical of front-line staff.

Third line

- Independently evaluate ML/TF/FPWMD risk management. Such evaluations may be conducted by internal audit, by personnel independent of the process or system being evaluated—provided they act under a formal mandate, an audit plan, or a specific assignment—or by duly qualified external third parties, ensuring objectivity in all cases
- Report to the Audit Committee or the equivalent oversight body through periodic assessments of the effectiveness of compliance with policies and procedures for ML/TF/FPWMD risk management.
- Issue independent conclusions, findings, and recommendations aimed at strengthening the system, and monitor the implementation of the defined action plans.

7.2 Responsibilities

Board of Directors (or equivalent body)

- Approve and ensure compliance with the Entity's ML/TF/FPWMD Policy or equivalent document, as well as any subsequent amendments thereto.
- Explicitly assign responsibilities to the bodies and individuals designated within the Entity's governance structure, thereby ensuring the effective management of policies and procedures.
- Define and approve the Entity's risk appetite, tolerance, and exposure limits for ML/TF/FPWMD and periodically monitor compliance with them.
- Understand ML/TF/FPWMD risks and ensure that the information derived from their assessment is received in a timely, complete, understandable, and accurate manner through the Audit Committee, the Risk Committee, and/or any other committee or body in which members of the Board of Directors participate.
- Receive periodic reports on identified relevant cases of ML/TF/FPWMD, including the investigations conducted and their conclusions, and issue a ruling on the matter.
- Monitor the implementation of action plans resulting from findings, non-compliance, or requirements from authorities and regulatory bodies.
- Appoint a Compliance Officer in regulated entities, or a SARLAFT Leader (or their designee) in entities not subject to ML/TF/FPWMD regulations, who possesses the appropriate qualifications and the necessary rank and authority to ensure that the issues addressed in this policy receive the appropriate attention from the Board of Directors, Senior Management, and the business units.

Area: SARLAFT	Code: GRC-PO-SARLAFT-1	Version: 8
---------------	------------------------	------------



Corporate Policy on Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction

- Provide the technical and human resources necessary to implement and maintain ML/TF/FPWMD risk management.

Grupo Aval's Risk Committee and Audit Committee (or equivalent body)

- Ensure the existence of an ML/TF/FPWMD policy and oversee compliance with it.
- Monitor the results of the assessment of ML/TF/FPWMD controls.
- Propose adjustments and updates to the ML/TF/FPWMD policy.

Grupo Aval's Corporate Vice Presidency of Risk and Compliance

- Submit for approval by the Board of Directors and disseminate policies that enable the proper management of ML/TF/FPWMD risk.
- Submit information on the ML/TF/FPWMD risk assessment to the Board of Directors, Risk Committee, and/or Audit Committee (or their respective equivalents) in a timely, complete, understandable, and accurate manner.
- Design and monitor compliance with this Policy with the support of the Senior Compliance Management team, as well as with the collaboration and coordination of the Compliance Officers at regulated entities and the ML/TF/FPWMD management leader (or their designee) at non-regulated entities.
- Establish guidelines in accordance with the best practices defined by the Risk Committee / Audit Committee (or equivalent bodies), taking into account the different jurisdictions and types of entities that make up the Group.
- Define and communicate to the Compliance Officers of the direct entities the compliance instructions and policies, a detailed annual schedule, reporting templates and frequency, and the review and approval levels for each defined deliverable.

Compliance Officer, SARLAFT Leader, or person responsible for ML/TF/FPWMD management

- Ensure the effective, efficient, and timely operation of the stages that make up the ML/TF/FPWMD risk management system.
- Submit reports to the board of directors or its designated representative, highlighting relevant issues pertaining to the system.
- Submit to the Board of Directors, or its equivalent, the requirements for IT, technological, physical, human and financial resources necessary to fulfill their functions.
- Evaluate the reports submitted by the internal audit department or whoever performs similar functions or acts in their stead, as well as the reports submitted by the statutory auditor, and take appropriate measures to address any reported deficiencies.
- Design methodologies for segmentation, identification, measurement, and control for the management of ML/TF/FPWMD risks.
- Design and submit for approval by the board of directors or the body acting in its stead the procedures established for risk-based, proportionate application, as well as the criteria for identifying suspicious transactions and for the consolidation, monitoring, and analysis of unusual transactions.
- Determine whether an unusual transaction should be considered suspicious and decide on the corresponding report to the Financial Intelligence Unit (UIAF), based on available information and knowledge of typologies and other concepts related to ML/TF/FPWMD.
- Ensure that activities resulting from the implementation of ML/TF/FPWMD management are properly documented, so that the information meets criteria for integrity, reliability, availability, compliance, effectiveness, efficiency, and confidentiality.



Corporate Policy on Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction

- Comply with obligations related to targeted financial sanctions.
- Adopt and disseminate best practices, in accordance with corporate guidelines.
- Assist process owners in assessing ML/TF/FPWMD risks and identifying controls, and support front-line staff in conducting due diligence.
- Develop and implement periodic training plans for all individuals bound by an employment contract, as well as communication plans, and establish mechanisms to ensure that, at a minimum, individuals bound by an employment contract annually certify their compliance with the policy and training plans.
- Develop and implement methodologies to monitor and identify red flags and/or unusual transactions for ML/TF/FPWMD risk management.
- Periodically submit the required reports, in accordance with the scope and frequency defined in corporate instructions or guidelines.
- Submit management reports to Grupo Aval's Corporate Vice Presidency of Risk and Compliance at the frequency specified by that office.
- Report the results of the risk profile to the Audit Committee or its equivalent in each entity at least semiannually.
- Guide and implement changes to corporate guidelines within your entity, ensuring proper compliance.
- Prepare the Management Report in accordance with applicable requirements, taking into account the entity's core business, structure, and regulatory approach.

Grupo Aval Corporate SARLAFT Committee

- Define and evaluate Grupo Aval's guidelines for improving the methodology for managing ML/TF/FPWMD risks.
- Review the risk management practices of the entities, as well as risk events and the action plans implemented to mitigate them.
- To present proposals to strengthen policies, forms, and methodologies related to ML/TF/FPWMD risk management and to implement best practices in compliance with legal requirements and the proper and efficient management of risks.
- To monitor strategic risk management and formulate recommendations and best practices for its proper handling within the entities. The committee itself, in its capacity as an advisory group composed of the Compliance Officers of the main entities, will be responsible for modifying, adjusting, or updating these recommendations.

Entities Comprising the Group

- Participate in the process of identifying and assessing ML/TF/FPWMD risks; define and update corporate guidelines within the entity that serve to identify, assess, and mitigate such risks with the support of the risk management departments.
- Manage ML/TF/FPWMD risk under their full responsibility in accordance with defined internal policies and applicable regulations specific to their industry, jurisdiction, and supervisory authority.
- Adapt the ML/TF/FPWMD risk management model in accordance with the regulations specific to its industry and jurisdiction, as well as corporate guidelines.
- Foster public and investor confidence; prevent the institution from being used for ML/TF/FPWMD, ensuring the preservation of the business's reputation, integrity, and transparency.
- Enforce regulations against ML/TF/FPWMD and implement appropriate controls to avoid penalties that supervisory and regulatory authorities may impose on financial institutions or bank employees.
- Continuously monitor all business and employment relationships and transactions, as this constitutes an essential aspect of sound and effective ML/TF/FPWMD risk management; The scope

Area: SARLAFT

Code: GRC-PO-SARLAFT-1

Version: 8

of this monitoring must be based on the risk identified in the risk assessment conducted by the institution as part of its know-your-counterparty procedures, and it must strengthen the monitoring of high-risk customers or transactions while maintaining cross-functional oversight of products or services to identify and mitigate emerging risk patterns.

- Have systems in place to detect warning signs that may indicate ML/TF/FPWMD based on the entity's risk assessment, the results of inquiries and due diligence, among other factors.
- Identify unusual transactions or those not consistent with the risk profile by utilizing information on customer due diligence, individuals linked through an employment contract, and third-party intermediaries.
- Apply robust due diligence processes to civil, commercial, or employment relationships that represent a high ML/TF/FPWMD risk profile and strengthen cross-functional monitoring and oversight of products or services to identify and mitigate emerging risk patterns.
- Cross-reference its database(s) of civil, commercial, or employment relationships whenever there are changes to sanctions lists and periodically against PEP databases and other high-risk accounts and conduct due diligence on them.
- Ensure the necessary resources are available to meet the objectives of this policy, as well as to adopt international best practices and other corporate guidelines.
- Maintain information management systems, commensurate with the company's size, organizational structure, or complexity, based on materiality and risk criteria, that provide business units (e.g., business managers) and those responsible for risk and compliance (including investigative staff) the timely information needed to identify, analyze, and effectively monitor any indications of ML/TF/FPWMD issues.
- Ensure that the requirements of regulatory authorities are adequately addressed by demonstrating the adequacy of the systems for assessing, managing, and mitigating ML/TF/FPWMD risks under the customer acceptance policy; of the procedures and policies regarding customer identification and verification; the ongoing monitoring processes and procedures for reporting suspicious transactions, as well as all measures adopted in the context of preventing ML/TF/FPWMD risks.
- Report to Grupo Aval and to the direct parent companies of each subsidiary using the applicable forms detailed in the Corporate Manual on Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction, by the established deadlines.
- Ensure a process of continuous improvement of the system.
- Periodically evaluate the effectiveness of the ML/TF/FPWMD risk management system within the Entity by monitoring management and risk indicators, monitoring results, alert quality, regulatory reports, audit findings, independent assessments, regulatory requirements, and compliance with defined action plans.
- Present the results of these evaluations to Senior Management and the relevant governing bodies in order to identify opportunities for improvement, strengthen existing controls, and ensure the system's evolution in response to regulatory, operational, technological, and risk-related changes.

Group Statutory Auditor

- Annually evaluate the Group's ML/TF/FPWMD risk prevention system independently and present the results and conclusions obtained during the system compliance review process to the highest governing body and the Compliance Officer.
- Report to the Audit Committee any irregularities or findings that could compromise the outcome of the Group's ML/TF/FPWMD risk management.
- Report to the competent authority any information that gives rise to suspicion of possible acts of ML/TF/FPWMD when, in the course of their work, they discover such a situation, notwithstanding the obligation to maintain professional confidentiality.

Area: SARLAFT	Code: GRC-PO-SARLAFT-1	Version: 8
---------------	------------------------	------------

Internal Audit of Each Entity

- Verify the existence of policies and procedures that establish guidelines for ML/TF/FPWMD management, duly approved and implemented.
- Verify the design and effectiveness of the controls detailed in the risk/control matrix, in accordance with its independently defined operational plan.
- Report its findings both to the process owners for remediation and to the person responsible for ML/TF/FPWMD management, as well as to the Board of Directors and the Audit Committee.

Gou Payments

Gou Payments is a Low-Value Payment Systems Administrator, and as part of its activities, it has access to information associated with cash withdrawal transactions at ATMs of Grupo Aval banks by users with cards issued abroad. In this capacity, it is responsible for providing this information to the banks and to the UIAF whenever required.

For this reason, Gou Payments, as part of its ML/TF/FPWMD risk model, must:

- Monitor international card transactions through this channel, in accordance with the patterns identified in cash withdrawal transactions at ATMs of Grupo Aval banks and the application of warning signals established by Gou Payments.
- Address requests from the Compliance Officers of the Grupo Aval banks regarding international cards and accounts that exhibit unusual behavior as a result of their withdrawal transactions, to implement measures established by Gou Payments to mitigate such behavior.
- The Gou Payments Compliance Officer must report transactions deemed suspicious to the Compliance Officers of the relevant institutions (as necessary) and to the UIAF, as applicable, so that they may take the measures they deem necessary. The details of these reports are transmitted to the UIAF; the information shared with banks is encrypted and masked.
- Report statistics on Suspicious Transaction Reports (STRs) submitted to the UIAF to oversight bodies (committees, board of directors, etc.).

Technology and Reporting Management – Support for the ML/TF Model:

- Provide banks with access to the transactional information required to implement monitoring.
- Implement the risk mitigation or treatment measures required by the banks in accordance with the agreed-upon guidelines.

This policy is supplemented by the Corporate Manual on Money Laundering, Terrorist Financing, and Weapons of Mass Destruction, which details and elaborates on the guidelines described herein.

8. REGULATIONS

Regulations used in the development of ML/TF/FPWMD Risk Management:

Area: SARLAFT	Code: GRC-PO-SARLAFT-1	Version: 8
---------------	------------------------	------------

- **Document:**

- Basic Legal Circular of the Finance Superintendence of Colombia (SFC), (External Circular 006 of 2025):
 - ✓ Part I General Instructions Applicable to Supervised Entities, Title IV Duties and Responsibilities, Chapter IV: Instructions Regarding the Management of Money Laundering and Terrorist Financing Risks.
 - ✓ Part III: Disintermediated Market, Title I: Securities Issuers, Chapter VII: Instructions on the Prevention and Control of Money Laundering and Terrorist Financing for Issuers Not Supervised by the Finance Superintendence of Colombia Regarding the SIPLA.
- Basic Legal Circular of the Superintendence of Companies (External Circular 100-000008 of 2022), Chapter X: Self-Monitoring and ML/TF Risk Management and Reporting of Suspicious Transactions to the Financial Intelligence Unit (UIAF).
- Resolution of the Superintendence of Transportation (Resolution 2328 of March 6, 2025, subsequently amended by Resolution 16615 of November 5, 2025).
- Resolution of the Superintendence of Transportation (Resolution No. 4607 of April 9, 2026, amending Chapter 6 of Title V of the Single Circular on Infrastructure and Transportation).
- External Circular No. 010 of the Finance Superintendence of Colombia, dated August 28, 2025, which provides instructions for the provision of financial products and services to financial consumers with criminal records or ongoing criminal investigations, in compliance with the order issued by the Constitutional Court in Ruling T-113 of 2025.
- DIAN External Circular 170 of 2022, which sets forth the procedures that users of customs and foreign exchange services must follow to prevent, detect, control, and report suspicious transactions that may be linked to money laundering.
- National Tax Code, Article 631-5: Definition of beneficial owner or any regulation that modifies or replaces it.
- Decree 830 of 2021 “amending and adding certain articles to Decree 1081 of 2015, regarding the regime for Politically Exposed Persons (PEPs).”

- **International:**

- Regulations regarding the management of money laundering and terrorist financing that apply to entities located abroad.
- Basel Committee: Guidelines for “Adequate Management of Risks Related to Money Laundering and Terrorist Financing.” Bank for International Settlements (BIS) (January 2014).
- FATF: List of relevant recommendations.
- New FATF recommendations (including their interpretive notes), among others:
 - ✓ R. 1: Risk assessment and application of a risk-based approach
 - ✓ R. 2: Domestic cooperation and coordination

- ✓ R. 9: Legislation on professional secrecy for financial institutions
- ✓ R. 10: Customer due diligence
- ✓ R. 11: Record-keeping
- ✓ R. 12: Politically Exposed Persons (PEPs)
- ✓ R. 13: Correspondent Banking
- ✓ R. 15: New Technologies
- ✓ R.16: Electronic Transfers
- ✓ R. 17: Use of Third Parties
- ✓ R. 18: Internal Controls, and Overseas Branches and Subsidiaries
- ✓ R. 20: Reporting of Suspicious Transactions
- ✓ R. 26: Regulation and Supervision of Financial Institutions
- ✓ R. 40: International Cooperation

- UN Security Council Resolutions 1267, 1989, and 2253
- Other relevant regulations applicable to the Group's subsidiaries

9. GLOSSARY

- **Beneficial owner:** the natural person(s) who ultimately owns or controls, directly or indirectly, a customer and/or the natural person in whose name a transaction is carried out. This also includes the natural person(s) who exercise effective and/or ultimate control, directly or indirectly, over a legal entity or other unincorporated structure. The beneficial owners are those mentioned in Article 631-5 Definition of Beneficial Owner of the National Tax Code.
- **Clients:** Any natural or legal person and unincorporated entities with which the entity establishes and maintains a contractual or legal relationship for the provision of any product related to its business activities.
- **Basel Committee (Basel Committee on Banking Supervision):** the global organization that brings together banking supervisory authorities, whose objective is to strengthen the soundness of financial systems and the prudential regulation of institutions in order to improve financial stability. Its primary function is to serve as an international forum for developing policy solutions and promulgating standards.
- **External context:** the external environment in which the organization seeks to achieve its objectives, which may include: (i) the cultural, social, political, legal, regulatory, financial, technological, economic, natural, and competitive environment, whether international, national, regional, or local; (ii) key drivers and trends that impact the organization's objectives; and (iii) relationships with individuals and organizations that may affect, be affected by, or perceive themselves as affected by a decision or activity, as well as their perceptions and values.
- **Internal context:** This refers to the internal environment in which the organization seeks to achieve its objectives, which may include: (i) governance, organizational structure, functions, and responsibilities; (ii) policies, objectives, and strategies implemented to achieve them; (iii) capabilities, understood in terms of resources and knowledge (e.g., capital, time, people, processes, systems, and technologies); (iv) information systems, information flows, and decision-making processes (both formal and informal); (v) the organization's culture; (vi) standards, guidelines, and models adopted by the organization; and (vii) the nature and scope of contractual relationships.

- **Due Diligence:** The principles of due diligence are risk-based and describe what an institution must consider when establishing a relationship with a customer to determine what types of activities it must carry out to know the customer. The depth of due diligence depends on the risk profile assessment and may include levels such as Simplified Due Diligence, Standard Due Diligence, Enhanced Due Diligence, and Intensive Due Diligence.
- **Enhanced or Intensified Due Diligence:** deepening the understanding of the customer for certain types of customers or activities, for which the institution will request additional information, independent of the documentation policy established for each product, thereby ensuring reasonable certainty regarding the origin and destination of funds, compliance with regulatory frameworks, and the adoption of best practices in the prevention of ML/TF/FPWMD. This is also known as enhanced measures.
- **Risk factors:** These are the agents that generate the risk of ML/TF/FPWMD, such as: Customers/users, Products, Distribution channels, and Jurisdictions. Other risk factors may be considered, which will be identified based on the evolving internal and external context.
- **Terrorist financing:** the set of activities aimed at channeling lawful or unlawful resources to promote, fund, or sponsor individuals, groups, or terrorist activities.
- **Financing of the Proliferation of Weapons of Mass Destruction (FPWMD):** any act that provides funds or uses financial services, in whole or in part, for the manufacture, acquisition, possession, development, export, transfer of materials, fragmentation, transportation, transfer, deposit, or dual-use for illegitimate purposes in violation of national laws or international obligations, where applicable.
- **Financial Action Task Force on Money Laundering (FATF):** an intergovernmental body that develops international standards and promotes policies to protect the international financial system against money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction. This group defines money laundering as the recycling of funds derived from criminal activities to conceal their illicit origin and works closely with other entities involved in these issues, particularly with its associate members and observers. The Basel Committee has observer status with the FATF.
- **Jurisdiction:** the scope or territory over which authority or power is exercised.
- **Money laundering:** the set of activities aimed at concealing the illicit origin of funds or giving the appearance of legality to funds obtained through the commission of illicit activities.
- **International lists binding on Colombia:** these are lists of individuals and entities associated with terrorist organizations that are binding under international law, including, but not limited to, United Nations Security Council Resolutions 1267/1999, 1988/2011, 1373/2001, 1718 and 1737/2006, and 2178/2014, as well as all subsequent, related, and complementary resolutions, and any other list adopted in the countries where the group's entities are located.
- **Risk Matrix:** a tool that facilitates holistic risk assessment.

- **Monitoring:** the stage in which the evolution of the inherent and residual risk profiles—and, in general, of the SARLAFT—must be compared and tracked.
- **Unusual transactions:** These are transactions that meet at least one of the following characteristics:
 - They are unrelated to the customer's economic activity, and no explanation has been found that is considered reasonable.
 - It falls outside the parameters set by the institution, and no explanation has been found that is considered reasonable.

In the case of identifying and analyzing user transactions (individuals or legal entities to whom the institution provides a service even though they are not customers), institutions must determine which of these are relevant, taking into account the risk to which they are exposed and based on criteria previously established by the institutions themselves.

Transaction alerts generated by the monitoring system may be evaluated by business units (first line) or compliance units (second line), and they facilitate the identification of unusual transactions. These alerts may lead to the identification of unusual transactions, which in turn may result in suspicious transactions.

- **Suspicious Transactions:** A suspicious transaction is defined as any transaction or series of transactions involving assets, liabilities, or other resources that, due to their amount, frequency, or specific characteristics, are not consistent with the economic activity of the customer or user and that may reasonably lead one to believe that the institution is being used to transfer, manage, exploit, or invest resources derived from criminal activities or intended to finance such activities.
- **Politically Exposed Persons (PEPs):** Public officials within any job classification and nomenclature system of the national and territorial public administration shall be considered PEPs when they are assigned or delegated functions involving: the issuance of rules or regulations; general management; the formulation of institutional policies and the adoption of plans, programs, and projects; the direct management of State assets, funds, or securities; the administration of justice or the exercise of administrative sanctioning powers; and private individuals responsible for the direction or management of resources within political movements or parties.

The status of Politically Exposed Persons (PEPs) shall remain in effect for the duration of their term of office and for an additional two (2) years following their departure from office, resignation, dismissal, or declaration that their appointment is null and void, or any other form of separation or termination of their contract.

- **Transaction:** These are legally authorized transactions that regulated entities may carry out through the execution of a contract (e.g., checking or savings accounts, insurance, investments, Certificates of Deposits, money orders, debt issuance, purchase and sale of securities, fiduciary transactions, etc.).
- **STR:** A Suspicious Transaction Report (STR) is the legal obligation of regulated entities in Colombia to report to the Financial Information and Analysis Unit (UIAF) of any transaction or series of transactions that, due to their amount, frequency, or characteristics, are not consistent with the economic activity of their customers or users and that may reasonably give rise to suspicion that the institution is being used to transfer, manage, benefit from, or invest funds derived from criminal

activities or intended to finance such activities. A STR does not constitute a criminal complaint; it is confidential and private in nature; it is not admissible as evidence in court or as testimony; and it does not give rise to criminal liability for the person filing the report. Its purpose is to serve as financial intelligence to prevent and detect money laundering and the financing of terrorism.

- **SAGRILAFT:** This is the comprehensive self-monitoring and risk management system for money laundering and terrorist financing applicable to entities regulated by the Superintendence of Companies.
- **SARLAFT:** The Money Laundering and Terrorist Financing Risk Management System is the integrated set of policies, procedures, infrastructure, controls, training, and outreach designed to address potential threats that entities may be used for criminal conduct aimed at channeling proceeds from criminal activities, and in particular to reduce exposure to ML/TF/FPWMD risks.
- **SIPLA:** The Comprehensive System for the Prevention of Money Laundering and Terrorist Financing. SIPLA consists of a set of minimum policies, procedures, mechanisms, and tools designed and implemented to prevent and control money laundering and the financing of terrorism (ML/TF/FPWMD) at issuers not supervised by the Finance Superintendence. It also applies to those entities required to comply with DIAN External Circular 170 of 2022.
- **SIPLA/FT:** System for the Prevention and Control of Money Laundering, Terrorist Financing, and Financing of the Proliferation of Weapons of Mass Destruction, which must be implemented by all companies authorized by the Ministry of Transportation to provide public motorized land freight transportation services, regardless of whether or not these companies are currently in operation (whether or not they are operating and/or active), pursuant to Articles 1 and 2 of Resolution 74854 of 2016 issued by the Superintendence of Transportation.
- **Segmentation:** the process by which elements are separated into groups that are homogeneous within themselves and heterogeneous among themselves. The separation is based on the recognition of significant differences in their characteristics (segmentation variables).
- **Services:** These are all interactions between entities subject to inspection and oversight by the Finance Superintendence of Colombia and individuals or entities without legal personality other than their customers.
- **Warning Signs or Early Warnings:** These are the facts, situations, events, amounts, quantitative and qualitative indicators, financial ratios, and other information that the entity determines to be relevant, from which one can infer, in a timely and/or prospective manner, the possible existence of a fact or situation that deviates from what the entity, in the course of its ML/TF/FPWMD efforts, has determined to be normal.

These indicators must take into account each of the risk factors and the characteristics of the entity's operations, as well as any other criteria that the entity deems appropriate.

- **Financial Information and Analysis Unit (UIAF):** This is an agency under the Ministry of Finance and Public Credit of Colombia. Its mission is to protect national security in the economic sphere through investigative and innovative processes aimed at preventing and detecting criminal activities related to money laundering and the financing of terrorism.



Corporate Policy on Money Laundering, Terrorist Financing, and the Proliferation of Weapons of Mass Destruction

- **Users:** These are individuals, legal entities, or unincorporated entities to whom the institution provides a service, even though they are not clients.