SARLAFT POLICY

Disclaimer Note

This text corresponds to an extract from the Policy of the Anti-Money Laundering and Countering the Financing of Terrorism Risk Management System (SARLAFT, for its Spanish acronym), prepared to inform third parties of the existence, scope, and robustness of the risk management system implemented by the entity.

In compliance with the provisions issued by the Financial Superintendence of Colombia, particularly the provisions set out in the Basic Legal Circular (Part I, Title IV, Chapter IV), SARLAFT constitutes a comprehensive set of policies, procedures, stages, elements, controls, and methodologies designed to prevent the entity from being used to channel resources derived from illicit activities, for the financing of terrorism, or for the financing of the proliferation of weapons of mass destruction.

In this context, the entity has adopted a risk-based approach that enables the identification, assessment, control, monitoring, and reporting of factors and events associated with ML/TF/PF, supporting adequate customer knowledge, the application of due diligence procedures, transaction monitoring, and compliance with regulatory reporting requirements, in line with international best practices and the standards established by the FATF.

This extract is provided for informational purposes and reflects the institutional commitment to effective risk management, transparency, and integrity in the conduct of its operations.

OBJECTIVE

The overall analysis of money laundering risk, terrorist financing, and financing of the proliferation of weapons of mass destruction (hereinafter ML/TF/PF) involves establishing an adequate organizational infrastructure and culture, as well as applying a systematic, logical, and structured methodology to identify, measure or evaluate, control, and monitor the risk of money laundering, terrorist financing, and financing of the proliferation of weapons of mass destruction to which Banco Popular (hereinafter “the Bank”) may be exposed.

In this regard, the objective of ML/TF/PF risk management is to prevent and control, including detecting and reporting, the use of the Bank, either directly or through its operations, as an instrument for the concealment, handling, investment, or utilization in any form of money or other assets derived from criminal activities, to give an appearance of

legality to transactions or resources linked to such activities. It also seeks to prevent the Bank from being used for the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

Based on the foregoing, in Part I Title IV Chapter IV of the Basic Legal Circular, the Financial Superintendence establishes the minimum criteria and parameters that supervised entities must observe in the design, implementation, and operation of an Anti-Money Laundering and Countering the Financing of Terrorism Risk Management System (hereinafter "SARLAFT"), which is addressed in this Manual.

POLICIES FOR ML/TF/PF RISK MANAGEMENT

These guidelines must be observed by the Bank to prevent its use to give an appearance of legality to assets derived from criminal activities (Money Laundering) or to channel resources toward the execution of terrorist activities (Financing of Terrorism and Proliferation of Weapons of Mass Destruction). These guidelines are reflected in rules of conduct and procedures that govern the actions of shareholders, directors, and employees of the Bank.

The Board of Directors and Senior Management of the Bank are committed to SARLAFT and recognize it as a tool that guides the actions of its employees, with clear and applicable policies supported by the technological infrastructure required for its effectiveness, and establish the duty of control bodies, the Compliance Officer, and all other employees to ensure compliance with internal regulations and other applicable provisions.

Policies on this matter must be approved by the Bank's Board of Directors, and any modification or change in their scope and objectives must be approved by the same governing body.

Likewise, the Bank applies the legal provisions related to SARLAFT and the provisions set out in the Organic Statute of the Financial System (hereinafter "EOSF," for its Spanish acronym), the Basic Legal Circular of the Financial Superintendence of Colombia, and any other rules that amend, supplement, or repeal them.

The policies for the prevention of ML/TF/PF risk approved by the Board of Directors are described below.

Priority

For the Bank and its subsidiaries, the definition, documentation, publication, and implementation of clear policies and all necessary procedures to prevent the possibility of loss or damage that may arise from ML/TF/PF risk.

The Bank promotes and strengthens an organizational culture oriented toward the proper management of ML/TF/PF risk in the performance of its employees' duties. In this regard, employees must give priority to compliance with the policies, procedures, and processes established for the prevention and control of ML/TF/PF over the achievement of commercial targets or any other institutional or personal interest, to ensure regulatory compliance and protecting institutional reputation.

Responsibility of All

The application of the preventive controls established in SARLAFT is not the exclusive responsibility of a specialized body; on the contrary, it is the responsibility of all operational executors, as well as each of the Bank's areas and subsidiaries. This commitment requires ensuring that all transactions are carried out in accordance with the guidelines and mechanisms established in SARLAFT.

New products or channels, including their modifications, must consider the stages of identification, analysis, evaluation, and monitoring of ML/TF/PF risks.

Regulatory Implementation

To adopt guidelines and general policies derived from regulatory changes issued by control authorities that apply to SARLAFT, the Compliance Management area analyzes regulatory updates, assesses risks and implementation alternatives jointly with the Bank's involved areas, to proceed with implementation and/or modifications within the terms and deadlines required by the supervisory authority.

Initial Information Collection

The Bank provides the Single Customer Onboarding and Banking Services Form, as well as all other documents and activities required in accordance with the customer onboarding policy, before the business relationship begins.

Customer Due Diligence

Customer due diligence serves as the backbone of SARLAFT. For this reason, the commercial team is responsible for understanding each customer's economic activity, verifying the information provided, and ensuring compliance with basic requirements. This information must be analyzed in relation to the customers' economic and business activities, to assess consistency and reaching a conclusion regarding the appropriateness of their onboarding, considering the risk profile and the established objective grounds.

This same responsibility applies, with respect to third parties involved, to those employees in charge of contracting goods and services, as well as for the execution of any type of agreement.

Banco Popular designs, develops, and implements simplified, enhanced, and intensified due diligence measures for the identification of natural and legal persons with whom it maintains civil, legal, contractual, commercial, or employment relationships. These due diligence measures include carrying out the necessary activities to determine identity, economic activity, economic profile, market segment with which they are associated, and the origin of their resources.

Likewise, in accordance with FATF recommendations, more stringent customer due diligence guidelines are implemented for onboarding and monitoring transactions involving domestic or foreign individuals who, due to their profile or the functions they perform, may present a higher degree of ML/TF/PF risk; in this regard, precautions shall be applied with respect to activities classified as having extreme risk levels.

The Board of Directors of the Bank has established an explicit prohibition against establishing or maintaining business relationships with persons who refuse to provide information on their economic activity, domicile, profession, or voluntary declaration of the origin of funds, or who provide false or difficult-to-verify information, as well as those who, without reasonable justification and after being evaluated by the Compliance Management in monitoring processes, refuse to update their basic and financial information when expressly required by the Bank.

Accordingly, the Bank shall not provide services to individuals or companies when elements exist that raise well-founded doubts regarding the legality of transactions or the lawfulness of their funds. Likewise, objective grounds for termination may include those contained in the Universal Regulation of Financial Products and/or Services of the Bank, referring to predicate offenses of ML/TF and/or those activities classified by the Colombian Penal Code as predicate offenses of money laundering and terrorist financing, as well as other applicable regulations.

The due diligence activities required to achieve effective customer knowledge are described in the customer onboarding and customer maintenance policy.

User Knowledge

The Bank shall maintain tools to identify and control users who interact in the Bank's operations, enabling analysis of their transactions for the purpose of assessing exposure to ML/TF/PF risk.

Supplier Knowledge

Banco Popular implements guidelines for the management and administration of third parties and intermediaries (TPI), as published in the ABAC Risk Management Manual and the Strategic Procurement Policy, which sets out the guidelines to be considered for the due diligence process for supplier due diligence.

Market Knowledge

To strengthen customer knowledge and risk management, the Bank analyzes the markets in which it operates, supporting proper segmentation and early identification of behaviors or transactions that may indicate a higher risk of ML/TF/PF. The Bank's characterization is conducted through the analysis of the segmentation of the customer risk-generating factor, thereby supporting compliance with this activity.

Named Accounts

The Bank maintains named accounts, meaning it does not create or accept anonymous accounts, and establishes controls to prevent accounts from being opened under fictitious names or with inaccurate data.

Employee Conduct

The conduct of the Bank's employees is governed by the behavioral standards defined in the Code of Ethics and Conduct. All employees, regardless of their role or functions, must remain alert to unusual or irregular behavior by customers, suppliers, or employees, and comply with the reporting duty through the established reporting channels, as indicated in the aforementioned Code.

List Screening

The Bank complies with obligations related to international lists that are binding on Colombia, in accordance with international law (those published by the United Nations, including the list of countries subject to sanctions imposed by the United Nations Security Council Committee)[1] and European terrorist lists[2]. Accordingly, it verifies current customers, prospective customers, and users. Likewise, validation is performed on shareholders, administrators, employees, suppliers, external lawyers, consultants, and all parties related in general to the acquisition of goods or services, to avoid establishing relationships or entering into contracts with persons included in the aforementioned lists, and, in the event that such persons are identified, proceeding with disengagement.

The Bank also maintains enhanced controls over the onboarding and continued relationship of customers, counterparties, and beneficial owners in order to prevent any direct or indirect relationship with Foreign Terrorist Organizations (FTO). This control is carried out with reference to the guidelines and communications issued by the Office of Foreign Assets Control (OFAC), and includes enhanced transactional monitoring based on continuous screening against sanctions and designation lists. Risk treatment arising from this control shall be documented in line with the provisions of A-ALF-0010 Protocol for the Treatment of Financial Products due to Inclusion in Targeted Financial Sanctions Lists.

The management of internal control lists is the responsibility of the Compliance Management, and at any time, once a transaction has been classified as suspicious and a customer or supplier has been disengaged, or an irregularity has been resolved, a change in status within the list may be made.

[1] https://www.un.org/securitycouncil/es/content/un-sc-consolidated-list

[2] It establishes the list of persons, groups, and entities involved in terrorist acts and subject to restrictive measures. https://ec.europa.eu/info/files/annex-commission-delegated-regulation-c-2019-1326-supplementing-directive-eu-2015-849-european-parliament-and-council-identifying-high-risk-third-countries-strategic-deficiencies_en

Targeted Financial Sanctions

To support compliance with Colombia's international obligations regarding the freezing and prohibition of handling funds or other assets of individuals and entities designated by the United Nations Security Council, the UN List Update process has been established. This process enables immediate compliance with the obligation to report to the Deputy Attorney General of the Nation and the Financial Information and Analysis Unit (UIAF) the existence of a customer who has been newly included in the aforementioned list.

Cash Transactions

The Bank shall retain evidence of the information related to cash transactions (physical movement of banknotes and coins) carried out in legal currency or foreign currency, whose value exceeds the thresholds established by the Financial Superintendence. The corresponding report shall be submitted, considering all requirements expressly established by the EOSF and other applicable regulations.

Determination of Unusual and Suspicious Transactions

The identification of unusual transactions begins with customer knowledge and, with the support of technological tools, supports the identification of unusual behavior patterns. The necessary analyses must be performed to enable the responsible parties to conclude whether or not the transaction is suspicious and therefore subject to reporting. To determine whether a transaction is suspicious, analysis by Compliance Management is required, and once it is classified as a suspicious transaction, the obligation to promptly report it arises to the UIAF.

Information Disclosure

All data and information contained in suspicious transaction reports are considered highly confidential and strictly restricted. Such information shall remain under the responsibility and custody of the Compliance Officer and the corresponding team within the Compliance Management area. Likewise, access shall be granted only to persons authorized by the Compliance Officer, or to State authorities that submit a formal request.

Independent evaluation bodies such as the Internal Audit Management and the Statutory Auditor shall be granted restricted access to suspicious transaction reports and to specific

data and information of reported individuals. If additional information is required, the technical justification must be provided explaining why access to such information is necessary, and the requesting party shall assume responsibility for its use.

In order to comply with the provisions set forth in paragraph 4.2.7 (Information Disclosure), Part I, Title IV, Chapter IV of the Basic Legal Circular of the Financial Superintendence of Colombia, and Article 97 of the EOSF, the Statutory Auditor's report shall provide the public with the information necessary to enable the market to assess the ML/TF/PF risk management strategies.

SARLAFT Reports

In accordance with current regulations, the Bank shall comply with, without exception, all internal and external reporting requirements, including those specifically required by the Financial Information and Analysis Unit (UIAF).

In order to safeguard the confidentiality of information, procedures have been established to ensure that the data provided has been previously authorized by the competent authority, in accordance with the confidentiality instructions stipulated in the EOSF and other applicable regulations.

Documentation

All documentation obtained, processed, and prepared in connection with activities related to the prevention of ML/TF/PF is classified as confidential under the terms and conditions established in the Information Security Manual, Personal Data Protection regulations, and applicable national regulations governing the matter.

The Compliance Management, in carrying out its monitoring and ML/TF/PF risk management activities, shall document all activities that evidence the due diligence performed by the Management area. Likewise, the established processes must provide the necessary documentation evidencing compliance and facilitates supervision and follow-up by those executing them, making such documentation available whenever required by control bodies.

Documentation and records related to customer due diligence and those designed for SARLAFT compliance shall be retained for the period established by the EOSF.

Response to Authority Requests

The Bank, in compliance with current regulations, shall have the necessary resources to compile of documentation and respond in a timely manner to requests related to ML/TF/PF offenses and related matters, which are handled exclusively by the competent authorities. Likewise, the necessary cooperation shall be provided to the administration of justice under the terms required.
In order to safeguard the confidentiality of information, procedures have been established to ensure that the data provided has been previously authorized by the competent authority, in accordance with the confidentiality instructions set forth in the EOSF and other applicable regulations.

ML/TF/PF Risk Measurement

For the measurement of ML/TF/PF risk, risk factors are considered, as well as associated risks and other requirements established in the regulations, to identify and assessing their potential impact on the Bank's activities.

Transactions with Shell Banks

Under no circumstances shall the Bank establish correspondent relationships with banks or branches of banks that qualify as shell banks.

Cross-border correspondent banking relationships are governed by the processes established in the Foreign Trade Manual, as well as the processes for International Correspondent Banking Relationships and Updating Information of Foreign Correspondents, under the responsibility of the Treasury Management area.

Transactions with Foreign Nationals

Banco Popular shall allow the onboarding of foreign nationals of legal age, for whom adequate knowledge of their location can be established, verifying their residency status, provided that their economic activity is determined to be lawful, and and that the required data and documents can be confirmed and verified the required data and documents, including links with national and multinational companies with which the foreign national may be related.

The Bank adheres to the international standards defined by the Financial Action Task Force (FATF); consequently, it shall refrain from conducting transactions with customers from countries where such recommendations are not applied (Black List and Red List). In cases where the existence of action plans is known (Grey List), Compliance Management must be consulted the Compliance Management in the manner established in this Policy and in accordance with the recommended course of action set forth in the standards assessed by the FATF.

POLICIES RELATED TO THE STAGES OF SARLAFT

Policies related to the identification stage

Before the launch or use of any product, the adoption of new business practices, including new service delivery channels, and the use of new or developing technologies for new or existing products; and the modification of product characteristics; entry into a new market; the opening of operations in new jurisdictions; and the launch or modification of distribution channels, the associated ML/TF/PF risks must be identified and assessed.

Policies related to the ML/TF/PF risk measurement or evaluation stage

The Bank's SARLAFT has methodologies defined in the Instruction Manual for the Development of SARLAFT Stages, which enable the measurement of the likelihood of occurrence of the inherent ML/TF/PF risk for each of the risk factors and its impact, if materialized through associated risks.
Measurement shall be carried out qualitatively in accordance with the adopted methodology. However, to the extent that the Entity has sufficient numerical data, quantitative measurements may be incorporated to strengthen the evaluation process.

Policies related to the ML/TF/PF risk control stage

The Bank shall implement the controls it considers necessary and strengthen existing ones in order to reduce the impact and/or likelihood of risk occurrence, so that they achieve the levels approved by the Board of Directors.

In addition, the Bank shall evaluate the effectiveness of existing controls and propose modifications or special treatments to mitigate identified risks.

Policy related to the ML/TF/PF risk monitoring stage

The Compliance Officer has the resources, mechanisms, methodologies, and procedures to perform the necessary monitoring of these stages, in order to identify potential failures or weaknesses in the system and coordinate corrective measures.

TECHNOLOGICAL INFRASTRUCTURE

The Bank has transactional and information applications enabled to support the following operations:

- Customer segmentation.
- Identification of warning signals.
- Recording of unusual transactions.
- Generation of internal and external reports.
- Screening against binding lists.
- Identification and verification of politically exposed persons (PEPs).
- Support for the generation and analysis of early warnings.
- Programming languages are used to complement the capabilities of core applications, data analysis, model development, and process automation that strengthen ML/TF/PF risk management.
- Use of artificial intelligence tools is subject to the provisions established in the Bank's Information Security and Cybersecurity Guidelines, complemented by data classification policies, access controls, and data governance, to ensure that all operations are carried out in secure, supervised environments with restrictions that prevent the transmission or exposure of sensitive data to external sources.
- The use of corporate artificial intelligence is governed under a "Human-in-the-Loop" scheme; therefore, it supports, but does not replace, the analyses, technical criteria, verification of accuracy, and formal reviews required by the Compliance Management.

POLICIES RELATED TO ML/TF/PF ASSOCIATED RISKS

Policy related to Legal Risk

The Bank is committed to compliance with current regulations; therefore, it shall respond efficiently and effectively to all requests from competent authorities, as well as cooperate with relevant investigations and ensure the proper conduct of inspections conducted.

Additionally, the Bank undertakes to ensure the inclusion and compliance with the minimum regulatory requirements of SARLAFT in relation to contractual relationships with customers and their transactions.

Policy related to Reputational Risk

The Compliance Management shall support reputational risk control that must be addressed within the Bank's Business Continuity System Crisis Management Committee.

Any statements concerning events that may affect the Bank's reputation are prohibited, as the only authorized spokesperson is the Legal Representative or the person delegated by them, in accordance with the provisions of the Business Continuity System Policies.

Policy related to Contagion Risk

The Bank shall take all necessary measures to ensure that, in the development of its activities, it does not incur losses directly or indirectly arising from the actions or experiences of its related parties or associates, understood as natural or legal persons who have the ability to exert influence over the Bank.

Policy related to Operational Risk

The Bank shall take all necessary measures to ensure that, in conducting its operations, it is not involved in criminal activities, particularly money laundering, terrorist financing, or financing the proliferation of weapons of mass destruction. For this purpose, the Bank implements mechanisms that enable it to avoid losses due to deficiencies, failures, inadequacies, or shortcomings in human resources, processes, technology, infrastructure, or the occurrence of external events.

POLICIES FOR THE PREVENTION AND RESOLUTION OF CONFLICTS OF INTEREST

The guidelines concerning the management of conflicts of interest are established in the Anti-Bribery and Anti-Corruption Risk Management System (ABAC) and in the Code of Ethics and Conduct adopted by the Bank.

Situations that may give rise to conflicts of interest in relation to the prevention of ML/TF/PF include, among others, the following:

Analysis of unusual transactions

A conflict of interest is considered to exist in the analysis of unusual transactions when such transactions have been carried out by an employee or administrator of the Bank on their own account, by their spouse or permanent partner, by relatives within the second degree of consanguinity, second degree of affinity, or first civil degree, or in those transactions in which any of the persons participating in the analysis process have a personal interest or may seek to benefit another person.

Determination of suspicious transactions – reports to the UIAF and handling of information requests from competent authorities

A conflict of interest is considered to exist when the transactions under analysis, for the purpose of deciding on regulatory reporting or in the information requested by any competent authority, are related to employees linked to the Compliance Management area, their spouse or permanent partner, relatives within the second degree of consanguinity, second degree of affinity, or first civil degree, or in those transactions in which any of the persons participating in the respective analysis or decision-making process has a personal interest or seeks to favor another person.

Other Situation Constituting a Conflict of Interest

A conflict of interest exists when a Bank employee is directly or indirectly related to a customer or company included in any of the control lists.

Cases or situations in which a Bank employee or administrator is found to be in a conflict-of-interest situation shall be addressed and resolved by the Bank's Ethics and Conduct Committee.

Conflict of Interest of the Compliance Officer and/or Deputy Compliance Officer

In the event that the Compliance Officer and/or Deputy Compliance Officer, in performing SARLAFT-related functions or any additional assigned duties, is exposed to an actual or potential conflict of interest, they must disclose it to their immediate supervisor and/or to the Bank's Ethics and Conduct Committee, where it shall be addressed in accordance with the established guidelines.

SARLAFT STAGES

For the implementation and administration of the Anti-Money Laundering and Counter-Terrorist Financing Risk Management System, the regulatory guidelines of the Basic Legal Circular, Part I, Title IV, Chapter IV of the Financial Superintendence of Colombia were used as the basis, as well as the measurement methodology and foundations set out in the conceptual model known as COSO and in the ISO 31000 technical standard.

The methodologies for the application of each of the SARLAFT stages are described in the Annex on Methodology for the Development of the SARLAFT Stages and are intended for the exclusive use of the Compliance Management area.

In the identification, measurement or evaluation, control, and monitoring, the general and follow-up activities for carrying out of the SARLAFT stages are described, and they are managed in accordance with the provisions established in the SARLAFT Manual.

PROCEDURE FOR ENSURING EFFECTIVE, EFFICIENT, AND TIMELY KNOWLEDGE OF CURRENT AND PROSPECTIVE CLIENTS

PARAMETERS OF CUSTOMER DUE DILIGENCE PROCEDURES

The Bank has established procedures and controls for ML/TF/PF risk that enable it to identify:

a) Who the customer is,
b) What their economic activity is,
c) The origin of their funds,
d) The risk profile of the prospective customer and the existing customer.

To ensure adequate customer due diligence, the Bank has implemented the following policies and procedures:

- Customer Onboarding Policies.
- Onboarding of Individual Customers at Branches.
- Maintenance of Individual Customers.
- Onboarding of Legal Entity Customers.
- Maintenance of Legal Entity Customers.
- Required Documents by Product.

The Bank verifies information from customers, suppliers, and counterparties using a risk-based approach, based on reliable sources and robust authentication mechanisms, which

supports segmentation and monitoring of the risk profile. Data updating is essential for customer due diligence and may affect the continuity of the business relationship, and it is the responsibility of the first line of defense to maintain up-to-date information, particularly when relevant changes occur such as shareholding structure. This update must be performed periodically according to the risk level (annually for high/extreme risk and at least every three years for low/moderate risk), or whenever significant changes occur in the customer's profile, including inactive products or variations that increase their risk level. Non-compliance with these guidelines may result in sanctions for employees in accordance with internal regulations.

The Bank prioritizes the rigorous management of jurisdiction risk and control over restrictive lists as pillars of SARLAFT, and establishes that any relationship or transaction with customers linked to high-risk jurisdictions or jurisdictions with deficiencies in international standards must be subject to prior assessments, enhanced controls, and continuous monitoring, with the possibility of suspending or terminating the relationship if the risk increases. In this context, screening against control lists is a mandatory requirement prior to onboarding, applicable not only to the customer but also to their related parties (legal representatives, shareholders, directors, and authorized persons), and constitutes a key mechanism to prevent exposure to illicit activities and support compliance with regulatory provisions and international standards.

Likewise, more stringent onboarding and monitoring procedures are established for customers, as well as transaction monitoring for domestic or foreign individuals who, due to their profile or the functions they perform, may expose the entity to a higher degree of ML/TF/PF risk. These concepts include:

Politically Exposed Persons (PEPs)
Economic activities considered to present higher ML/TF/PF risk
Special cases of extreme risk subject to enhanced due diligence
Rules for the management of Political Campaign and Political Party accounts

DETECTION AND ANALYSIS OF UNUSUAL TRANSACTIONS

The Bank maintains a comprehensive system for the detection, analysis, and reporting of unusual and suspicious transactions, supported by technological tools configured with warning signals and statistical and scoring methodologies that enable the identification of atypical behaviors based on the customer's risk profile. These transactions are automatically evaluated by the Compliance Management area and/or assigned to the commercial team, which determines their justification or potential classification as suspicious, with special

monitoring of defined higher-risk segments. The process is complemented by the monthly electronic consolidation of transactions through specialized tools that support transactional monitoring. When suspicious transactions are identified, they are analyzed and, where applicable, reported to the UIAF, ensuring the confidentiality of the process and compliance with regulatory obligations, as well as the implementation of early warnings that support the anticipation of ML/TF/PF risks.

ORGANIZATIONAL STRUCTURE

For the management of ML/TF/PF risk, the Bank has adopted an organizational structure that defines the functions and responsibilities of each of the bodies and individuals responsible for adopting and implementing of SARLAFT, including the Board of Directors, Senior Management, Compliance Officer, and the support committees in which they participate.

ADMINISTRATIVE MEASURES

Any Bank employee who fails to comply with any of the control mechanisms established in this Manual and/or with all matters related to customer due diligence and identification of beneficial owners may be subject to disciplinary sanctions. If such non-compliance is determined to be a serious misconduct, the employee's employment contract shall be terminated in accordance with Article 87, numerals 12 and 31, in conjunction with Article 107 of the Internal Labor Regulations and the provisions set forth in the Employment Contract regarding employee obligations, without prejudice to any legal actions that may apply.

The Bank, through the Human Talent and Administrative Vice Presidency, shall impose sanctions on employees who expose the entity to higher risk due to non-compliance with the regulations established in this Manual.

The disciplinary procedures applicable in the event of non-compliance with this Manual and the Code of Ethics and Conduct are established in the Internal Labor Regulations.

TRAINING

The Bank recognizes training as a fundamental pillar for the effective management of SARLAFT; therefore, it maintains a permanent program of awareness, training, and capacity-building activities aimed at all employees and third parties involved in functions related to

this system. This program includes onboarding processes for new employees, mandatory refreshers at least once a year, and specific training sessions based on identified needs, using various methods such as in-person sessions, e-learning, and self-study. Likewise, it incorporates evaluation mechanisms to ensure knowledge acquisition and includes periodic review and updating of the plan, ensuring alignment with regulatory changes and emerging risks, thereby strengthening the culture of compliance and the prevention of ML/TF/PF within the entity.