MANUAL OF THE SELF-CONTROL SYSTEM AND MANAGEMENT OF THE INTEGRAL RISK OF MONEY LAUNDERING, FINANCING OF TERRORISM, AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION SAGRILAFT

COMPLIANCE MANAGEMENT

BIOFIX CONSULTORIA SAS BIC

PREPARED BY: Sandra Milena González C. **Management Controller – Compliance Officer**
REVIEWED BY: Carlos Andrés Méndez **General Manager APPROVED BY:** Shareholders' Assembly **Biofix Consulting SAS BIC**

CONTENT

1. OBJECTIVE

Establish policies, guidelines, and procedures for the effective management of risks associated with Money Laundering (LA), Terrorism Financing (FT), and Financing the Proliferation of Weapons of Mass Destruction (FPADM), hereinafter **LA/FT/FPADM**[1]. These guidelines apply to all collaborators and counterparties of BIOFIX BIC, contributing to integrity, sustainability, and regulatory compliance.

2. SCOPE

This manual regulates the System of Self-Control and Comprehensive Risk Management for Money Laundering, Financing of Terrorism, and Proliferation of Weapons of Mass Destruction, hereinafter referred to as **SAGRILAFT**, which has been implemented by BIOFIX BIC.

This manual contains methodologies, policies, procedures, roles, annexes, and responsibilities of all counterparties, including administrative and management bodies, the Compliance Officer, control bodies, expanding the regulatory framework to any natural or legal person wishing to engage with the company.

These guidelines and directives apply to all processes in the value chain, especially those involving activities related to relationships, onboarding, and managing transactions with counterparties. This includes the management of information systems and all operations and/or processes where risk factors associated with **AML/CFT/FPADM** are present.

The content and its annexes are mandatory for compliance, and in case of omission, they will be subject to legal sanctions by control entities and internal sanctions in accordance with the internal work regulations established by the organization as just cause.

3. APPLICABLE LEGAL FRAMEWORK

The legal framework in Colombia regarding the prevention and control of **AML/CFT/FPADM** aims to prevent the Company from being used in its operations, resources, and relationships to give the appearance of legality to assets derived from illicit activities.

The System of Self-Control and Comprehensive Risk Management of Money Laundering, Terrorism Financing, and the Financing of the Proliferation of Weapons of Mass Destruction, **SAGRILAFT,** is based on the general and special normative content provided in the Constitution, laws, decrees, and administrative acts issued by the oversight and control entities.

The main regulations that frame the obligations contained in this manual are listed below:

[1] AML/CFT/FPADM Money Laundering, Terrorism Financing, and Financing of the Proliferation of Weapons of Mass Destruction.

3.1 INTERNATIONAL STANDARDS

- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988.
- Declaration of Principles 1988 and Customer Due Diligence 2002. Supervisory Committee Bank for International Settlements.
- United Nations Conventions for the suppression of terrorism financing from 1989.

- European Convention on Money Laundering, detection, seizure, and confiscation of the proceeds of crime, 1990.
- United Nations Vienna Convention 1988, Palermo 2000, and Mérida 200. 3.
- Inter-American Convention against Corruption of the OAS. -
International Convention for the suppression of terrorism financing, terrorism, 2000.
- United Nations Convention against Corruption, 2004.
- Resolution 1373 of 2001 of the Security Council Executive Directorate of the United Nations Counter-Terrorism Committee.

3.2 NATIONAL STANDARDS

- Law 526 of 1999, which establishes the Financial Information and Analysis Unit (UIAF). - Resolutions and documents from the Financial Information and Analysis Unit of the Ministry of Finance and Public Credit of Colombia – UIAF.
- Colombian Penal Code Law 599 of 2000 Article 441, which establishes the duty to report, article 323 Money Laundering, article 345 Terrorism Financing.
-Law 808 of 2003 and Ruling C-037 of 2004, through which Colombia approved the United Nations Convention for the Suppression of the Financing of Terrorism of 1989.
-Law 970 of 2005 and Ruling C-172 of 2006, through which Colombia approved the Mérida Convention of 2003, United Nations Convention against Corruption.
-Law 1121 of 2006 regulates the procedure for the publication and compliance with obligations related to binding lists for Colombia, international restrictive lists.
-Law 1186 of 2008 and Constitutional Review Ruling C-685 of 2009, through which Colombia approved the Memorandum of Understanding signed in Cartagena de Indias on December 8, 2000, which created and put into operation the Financial Action Task Force of South America against Money Laundering (now the Financial Action Task Force of Latin America GAFILAT) and determined as its objective to recognize and apply the FATF Recommendations against money laundering and the recommendations and measures t hat may be adopted in the future.
-CONPES 3793, National Anti-Money Laundering and Counter Financing of Terrorism Policy, December 18, 2013.
-Code of Extinction of Domain, Articles 7 and 119 of Law 1708 of 2014.
-External Circular 100-000006 dated August 19, 2016, and amended by Basic Legal Circular No. 100-000005 dated November 22, 2017, issued by the Superintendency of Companies of Colombia.

-Chapter X of the Basic Legal Circular of the Superintendence of Companies, in its latest modification through External Circular 100-000016 of December 24, 2020, and partially by External Circular 100-000004 of April 9, 2021. It contains the obligation to implement a SAGRILAFT and the other standards that modify or replace it.

-External Circular 100-000016 of November 17, 2021, through which the transmission of report 58 regarding the data of the Compliance Officer appointed in the company is requested. Furthermore, the transmission of report 75 is contemplated, which is submitted annually and compiles information that the company has regarding AML/CFT/FPADM.

-Decree 830 of 2021, which modifies and adds some articles to Decree 1081 of 2015, the Unique Regulatory Framework of the Presidency of the Republic, regarding the regime of Politically Exposed Persons (PEP).

-Law 2195 of 2022 through which measures are adopted in the area of transparency, prevention, and the fight against corruption, and other provisions are enacted.

3.3 INTERNAL STANDARDS:

- PTEE Manual - Code of Ethics, Transparency, and Anti-corruption - Procurement Manual - Approval Act Assembly Official Compliance Policies and Legality - Characterization of SAGRILAFT & PTEE Compliance Policies - Internal Regulations - Internal Processes and Procedures.

4. TERMS AND DEFINITIONS

Risk acceptance: an informed decision to accept the consequences and probability of a particular risk.

Assets: An economic resource currently controlled by the Organization as a result of past events.

Management of resources related to terrorist activities: Corresponds to the behaviors outlined i n Article 345 of the Penal Code, amended by Article 16 of Law 1121 of 2006.

Risk administration: the culture, processes, and structures directed towards the effective management of potential opportunities and adverse effects.

Risk Analysis: It involves determining all stages of risk through the review of available information and achieving an understanding of how frequently specific events may occur and calculating the magnitude of their consequences.

General Shareholders' Assembly or Highest Social Body: It is known as the shareholders' meeting or General Shareholders' Assembly and is made up of all the partners or shareholders of an organization.

Absence of Suspicious Operation Report: If a quarter passes without the Obligated Organization submitting a suspicious operation report, the Compliance Officer must present a report of "absence of Suspicious Operation Report" to the online reporting system within ten calendar days following the end of the respective quarter, in the manner and terms that correspond, according to the instructions of that platform.

Ultimate beneficiary: Refers to the natural person(s) who ultimately own or control a client or the natural person on whose behalf a transaction is conducted. It also includes the person(s) who exercise effective and/or final control, directly or indirectly, over a legal entity or another structure without legal personality.

Code of Ethics and Conduct: Serves as a guide for the management staff, employees, and agents of the organization in applying legal and ethical practices in the course of their daily tasks.

Counterparty: Refers to any natural or legal person with whom the Organization has commercial, business, contractual, or legal ties of any kind. Among others, counterparties include: **Partners – Shareholders. Employees – Collaborators. Passive Clients. Participating Clients. Suppliers. Contractors and/or Third Parties and/or Others.**

Counterparty Knowledge Control: Collection of all documents that allow for the verification of the identity and legal status of each counterparty involved in the processes of the company for onboarding and/or updating.
Risk Control: This includes the implementation of policies, processes, practices, or other existing actions that work to minimize risk in the transactions, business, or contracts carried out by the organization.

Customer Due Diligence Format Control: It is a structured document that gathers detailed information about the counterparties of an organization, allowing for the assessment of their identity, background, and the purpose of the business relationship. Requested during the onboarding stage, this format is key in preventing risks associated with **AML/CFT/FPADM,** corruption, and other illicit activities, enabling the organization to communicate its commitment to compliance policies, ethics, and other measures that ensure reliability with our counterparties, identifying analytical information while considering its application only for supplier counterparties based on the amounts approved in the materiality base.

Control Search in Binding Compliance Lists: A platform available for consultation in national and international databases that collect information, reports, and records from various entities r egarding natural and legal persons who may exhibit suspicious activities, investigations, processes, or convictions for the crimes of **AML/CFT/FPADM**.

Consequence: the result of an event expressed qualitatively or quantitatively, whether it is a loss, damage, disadvantage, or gain. There could be a range of possible outcomes associated with an event.

Due Diligence: It is the systematic process through which a company adopts measures for understanding the counterparty, its business, transactions, products, and the volume of its transactions, as established in numeral 5.3.1 of Chapter X of the external circular of the Superintendence of Companies, in order to prevent, minimize, and manage risks associated with LAFTPADM, Corruption, and Bribery.

Enhanced Due Diligence: It is the process by which the Organization adopts additional and more i ntensive measures for understanding the counterparty, its business, transactions, products, and the volume of its transactions. As established in numeral 5.3.2 of Chapter X of the external circular from the Superintendence of Companies.

Control Assessment: systematic review of the processes to ensure that the controls described in t he risk matrix are adequate.

Risk Assessment: the overall process of risk analysis and risk evaluation. The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels, or other criteria.

Event: an incident or situation that occurs in a particular place during a specific time interval.

Risk factors: agents that generate the risk of **AML/CFT**.

Terrorism Financing (TF): Crime committed by any person who engages in any of the behaviors described in Article 345 of the Penal Code.

Financing of the Proliferation of Weapons of Mass Destruction (FPADM): any act that provides funds or uses financial services, in whole or in part, for the manufacture, acquisition, possession, development, export, trafficking of materials, fragmentation, transportation, transfer, deposit, or dual use for illicit purposes in violation of national laws or international obligations, when applicable.

Risk management: culture, processes, and structures aimed at seizing potential opportunities while managing adverse effects.

Jurisdiction territorial: Geographical areas identified as exposed to the risk of **AML/CFT/TF M** where the organization offers or purchases its products.

Money Laundering (LA): A crime committed by any person who seeks to give the appearance of legality to assets or money derived from any of the activities described in Article 323 of the Penal Code.

AML/CFT/FPADM: Acronym for Money Laundering, Financing of Terrorism, and Financing of the

Binding Lists: These are lists of individuals and entities associated with terrorist organizations that are binding for Colombia under Colombian legislation (Article 20 of Law 1121 of 2006) and in accordance with international law, including but not limited to Resolutions 1267 of 1999, 1373 of 2001, 1718 and 1737 of 2006, 1988 and 1989 of 2011, and 2178 of 2014 from the United Nations Security Council, as well as all those that succeed, relate to, and complement them, and any other binding list for Colombia (such as the terrorist lists of the United States of America, the list of the European Union of Terrorist Organizations, and the list of the European Union of Individuals Designated as Terrorists). The Superintendence of Companies will maintain a list of the Binding Lists for Colombia on its website as a guide, without these being exhaustive.

Risk Matrix of LA/FT/FPADM: It is one of the instruments that allows an Organization to identify, individualize, segment, evaluate, and control the Risks **AML/CFT/PF** to which it may be exposed, according to the identified and analyzed Risk Factors based on the nature and processes of the company.

Monitoring or follow-up: It is the continuous and systematic process carried out by obligated subjects, through which the efficiency and effectiveness of a policy or process are verified, as well as the identification of its strengths and weaknesses to recommend corrective measures aimed at optimizing the expected results. It is a condition for rectifying or deepening execution and for ensuring feedback between objectives, theoretical budgets, and lessons learned from practice.

OFAC: Office of Foreign Assets Control of the United States.

Compliance Officer: This is the individual designated by the Organization who is responsible for promoting, developing, and ensuring compliance with the specific procedures for prevention, updating, and risk mitigation regarding **AML/CFT/FPADM**.

Unusual operation: This refers to an operation whose amount or characteristics do not relate to the ordinary or normal economic activity of the Organization, which, due to its number, amount, or characteristics, does not fall within the guidelines of normality or ordinary business practices in a sector, an industry, or with a class of counterparty.

Attempted operation: This occurs when there is knowledge of an individual or legal entity's intention to carry out a suspicious operation, but it does not materialize because the person attempting to execute it withdraws or because the established or defined controls did not allow it to be carried out. These operations must be reported solely and exclusively to the UIA when the Compliance Officer analyzes the situation and considers reporting it.

Suspicious operation: This is the unusual operation that, in addition, according to the practices and customs of the activity in question, has not been reasonably justified. This type of operation includes attempted or rejected operations that contain characteristics that give them the nature of being suspicious before, during, and at the conclusion of the relationship.

Politically Exposed Persons (PEP): This refers to politically exposed persons, meaning public officials from any nomenclature and classification system of national and territorial public administration, when in the positions they occupy, they have responsibilities directly or by delegation for the general direction, formulation of institutional policies, and adoption of plans, programs, and projects, as well as the direct management of state assets, funds, or securities. This can occur through expenditure management, public contracting, project management, payments, settlements, and administration of movable and immovable property. It also includes foreign politically exposed persons and politically exposed persons from international organizations.

Products: are the goods and services produced, marketed, transformed, or offered by the Organization, or acquired from a third party.

Probability: the probability of a specific event or outcome, measured by the coefficient of specific events or outcomes in relation to the total number of possible events or outcomes. Used as a qualitative description of probability or frequency.

FATF Recommendations: These are the 40 recommendations designed by the FATF along with their interpretative notes, aimed at preventing the risk of **AML/CFT/FPADM,** which were reviewed in February 2012 and updated in June 2019. The result of this review is the document titled "International Standards o n Combating **AML/CFT/FPADM**."

Risk: is the possibility of an event, action, or omission occurring that will have an impact on the objectives. It is measured in terms of impact and probability.

LA/FT/FPADM Risk: It is the possibility of loss or damage that an Organization may suffer due to its propensity to be used directly or through its operations as an instrument for Money Laundering and/or channeling resources towards carrying out terrorist activities or Financing of the Proliferation of Weapons of Mass Destruction, or when there is an intention to conceal Assets derived from such activities.

Contagion Risk: It is the possibility of loss that an Organization may suffer, directly or indirectly, due to an action or experience of a counterparty.

Legal Risk: The possibility of loss incurred by an entity when sanctioned or required to compensate for damages as a result of non-compliance with laws or regulations and contractual obligations. Legal risk also arises as a consequence of failures in contracts and transactions, resulting from malicious actions, negligence, or unintentional acts that affect the formalization or execution of contracts or transactions.

Operational Risk: The possibility of incurring losses due to deficiencies, failures, or inadequacies in human resources, processes, technology, infrastructure, or due to the occurrence of external eve nts. This definition includes legal and reputational risk associated with such factors.

Reputational Risk: The possibility of loss that an entity incurs due to disrepute, negative image, or negative publicity, whether true or not, regarding the institution and its business practices, which causes loss of clients, decrease in revenues, or legal proceedings.

Inherent risk: The level of risk inherent to the activity, without considering the effect of the controls.

RResidual risk: It is the resulting level of risk after applying the controls.

Report of suspicious operation: If unusual or suspicious operations are identified within the Company, a report of suspicious operations (ROS) must be made on the online reporting system platform of the Unit of Financial Investigation and Analysis.

Report of Attempted Operations: If a counterparty wishes to link and reports an alert in searches of lists, it must be reported by the Compliance Officer to the UIAF.

Warning Signals: Events, situations, transactions, amounts, quantitative and qualitative indicators, financial reasons, and any other information that the entity determines to be relevant, from which it can be inferred promptly or prospectively the possible existence of an event or situation that falls outside what the Company considers normal.

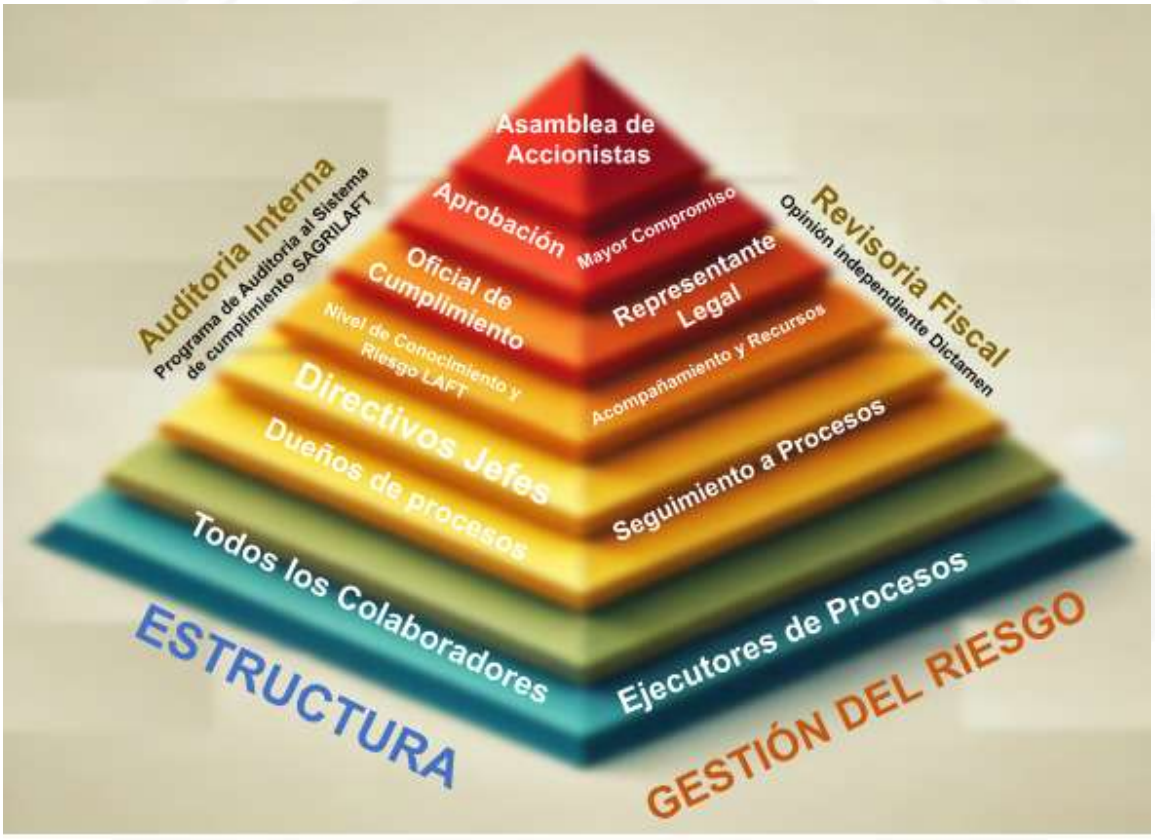
Online Reporting System (SIREL): An information system in a web environment, developed by the Unit of Financial Investigation and Analysis as the main mechanism to allow obligated subjects to report online the established information. It also allows for the consultation of upload certificates, of the reports uploaded, and to visualize the consolidation of the same.

Financial Information and Analysis Unit (UIAF): It is a special administrative unit of a technical nature, attached to the Ministry of Finance and Public Credit, created by Law 526 of 1999, modified by Law 1121 of 2006, which aims to prevent and detect transactions that may be used for money laundering or terrorism financing. It also imposes reporting obligations on certain economic sectors.

5. ASSIGNMENT OF FUNCTIONS

This manual establishes and clearly assigns who is responsible for exercising the powers and functions necessary for the execution of the different stages, elements, and other activities associated with SAGRILAFT. The interaction of all responsible parties is fundamental for the proper functioning, compliance, and effectiveness of SAGRILAFT. As part of this section, reference is made t o the internal processes and procedures established in the SAGRILAFT & PTEE Compliance Characterization Annex to this document.[2]

5.1 ROLES IN RISK MANAGEMENT



5.2 RESPONSIBILITIES OF ROLES

5.2.1 General Shareholders' Assembly:

The Shareholders' Assembly is the body responsible for implementing and ensuring the effectiveness of SAGRILAFT and has the following functions:

[2] Annex SAGRILAFT & PTEE Compliance Characterization

• Establish and approve the policies for the prevention and control of the comprehensive risk of money laundering, terrorism financing, and financing of the proliferation of weapons of mass destruction – SAGRILAFT.

• Approve the SAGRILAFT and the updates presented by the Legal Representative and the Compliance Officer.

• Designate the Compliance Officer and their respective deputy, when appropriate.

• Analyze and timely pronounce on the reports regarding the functioning of the SAGRILAFT, on the proposals for corrective actions and updates presented by the Compliance Officer, and make decisions regarding all the topics addressed therein, leaving an explicit record in the respective minutes.

• Timely analyze the reports and requests submitted by the Legal Representative.

• Make pronouncements on the reports submitted by the Fiscal Review or the internal and external audits related to the implementation and functioning of the SAGRILAFT.

• Conduct periodic follow-ups and progress on the system.

• Order and ensure the necessary technical, logistical, and human resources to implement and maintain the proper functioning of the SAGRILAFT, according to the requirements made by the Compliance Officer.

• Est ablish the criteria for approving the engagement of counterparties when it involves a PEP.

• Establish guidelines and determine the responsible parties for conducting audits on the c ompliance and effectiveness of SAGRILAFT.

• Verify that the Compliance Officer has the necessary availability and capacity to perform their functions.

• Confirm that the company, the Compliance Officer, the Legal Representative, and their employees, carry out the designated activities outlined in this Manual.

5.2.2 Legal Representative:

Within the framework of the implementation of SAGRILAFT, the legal representative will have the following functions:

• Present the proposal for the manual, the SAGRILAFT procedures, and their respective updates to the Compliance Officer for approval by the Shareholders' Assembly.

• Study the results of the LA/FT/FPADM Risk assessment conducted by the Compliance Officer and establish the corresponding action plans.

• Assign from efficiently the technical and human resources, determined by the Shareholders' Assembly Shareholders, n necessary to implement the SAGRILAFT.

• Verify that the Compliance Officer has the necessary availability and capacity to perform their functions.

• Provide effective, efficient, and timely support to the Compliance Officer in the design, direction, supervision, and monitoring of the SAGRILAFT.

• Present to the Shareholders' Assembly the reports, requests, and alerts that are deemed necessary to be addressed by these bodies and that are related to the SAGRILAFT.

• Ensure that the activities resulting from the implementation of the SAGRILAFT are properly documented, so that the information meets the criteria of integrity, reliability, availability, compliance, effectiveness, efficiency, and confidentiality.

• In case of requirements from the Superintendence of Companies, certify and attest to compliance with the SAGRILAFT, in accordance with the provisions of Chapter X of the Basic Legal Circular.

• Verify that the procedures of the **SAGRILAFT** develop the **AML/CFT/FPADM** Policy adopted by the Shareholders' Assembly.

5.2.3 Minimum Requirements and Official Compliance Functions:

Appointment of the Compliance Officer

The Shareholders' Assembly will appoint a responsible person who will participate in the design, direction, implementation, auditing, verification, and monitoring processes of the SAGRILAFT, and will also have the capacity to make decisions regarding the Comprehensive LA/FT/FPDAM Risk Management. Consequently, the Compliance Officer must meet the following requirements:

• Have the ability to make decisions to manage the LA/FT/FPADM Risk and maintain direct communication with and report to the Shareholders' Assembly.

• Possess sufficient knowledge in risk administration and understand the company's social purpose.

• Have the support of a human and technical work team, in accordance with the LA/FT/FPADM Risk and the size of the Company.

• Not to be listed in any of the restricted and/or binding lists for Colombia.

• You must have a professional title and demonstrate a minimum experience of six (6) months in the performance of and positions related to the administration of SAGRILAF.

• He must demonstrate knowledge in the administration of AML/CFT/FPADM Risk through specialization, courses, diplomas, seminars, conferences, or any other similar means.

• The Compliance Officer must not belong to the administration or the social bodies, nor to internal or external auditing or control (fiscal reviewer or linked to the fiscal review company performing this function, if applicable) or anyone performing similar functions or acting in their stead in the Company.

• Must not serve as Compliance Officer for more than ten (10) Obligated Companies. To serve as Compliance Officer for more than one Obligated Company, (i) the Compliance Officer must certify; and (II) the body that appoints the Compliance Officer must verify that the Compliance Officer does not act as such in competing Companies.

• When the Compliance Officer is not employed by the company, this individual and the legal entity t o which they are linked, if applicable, must demonstrate that in their professional activities they comply with the minimum due diligence measures.

• Be domiciled in Colombia.

Incompatibilities and disqualifications of the different bodies

In establishing the bodies and instances responsible for evaluating compliance and effectiveness of SAGRILAFT, the company must consider conflicts of interest, incompatibilities, and disqualifications of those responsible for performing their duties. In this regard, due to the differing functions involved, the Fiscal Reviewer, Internal Auditor, or Administrator should not be designated as the Compliance Officer.

Official Compliance Positioning

In accordance with External Circular No. 100-000016 of November 17, 2021, the company will sub mit the 'Report 58' via the Storm User with the information of the Compliance Officer appointed by the Shareholders' Assembly, and will subsequently send the following documents to the Superintendence of Companies through the Storm Web platform within fifteen (15) business days following the appointment of the Compliance Officer:

• Certification signed by the legal representative of the company stating expressly that the Compliance Officer meets the requirements set forth in Chapter X.

• The resume of the Compliance Officer.

• A copy of the document that provides evidence of the registration of the Compliance Officer with SIREL, managed by UIAF.

• A copy of the minutes extract from the Shareholders' Assembly that records your appointment.

• Document certifying knowledge in the management of LA/FT Risk or LA/FT/FPADM Risk; through specialization, courses, diplomas, seminars, congresses, or any similar means.

• Certificate of the verification of skills and incompatibilities of the Compliance Officer signed by the Legal Representative.

Functions of the Compliance Officer

The Compliance Officer or whoever performs those functions will be responsible for ensuring the efficient and timely operation of the SAGRILAFT and will have the following functions:

• Present at least once (1) a year reports to the Shareholders' Assembly. At a minimum, the reports must contain an evaluation and analysis of the efficiency and effectiveness of the SAGRILAFT and, if applicable, propose the respective improvements. Additionally, demonstrate the results of the Compliance Officer's management and the administration of the company, in general, in co mpliance with the SAGRILAFT.

• Promote the adoption of corrective measures and updates to the SAGRILAFT when circumstances require it and at least once every two (2) years. In this case, it must present to the Shareholders' Assembly the proposals and justifications for the suggested corrective measures and updates to the SAGRILAFT.

• Coordinate the development of internal training programs so that the employees of the Company are properly informed, updated, and trained to identify and report Unusual Operations or S uspicious Operations.

• Evaluate the reports submitted by the internal audit or those performing similar functions, as well as the reports presented by the fiscal reviewer or external audit, if applicable, and take reasonable measures in response to the reported deficiencies.

• Certify to the Superintendence of Companies the compliance with the provisions of Chapter X of t he Basic Legal Circular, fully amended by External Circular 100-000016/2020 and partially amended by External Circular 100-000004/2021, as required by the Superintendence of Companies.

• Supervise and direct the design of the system, taking into account the characteristics of the company, its activities, and the identification of its risk factors.

• Ensure the effective, efficient, and timely functioning of SAGRILAFT.

• Verify compliance with the due diligence and Enhanced Due Diligence procedures applicable to the Company.

• Ensure the proper filing of documentary supports and other information related to the management and prevention of LA/FT/FPADM risk.

• Conduct the assessment of the LA/FT/FPADM risk to which the company is exposed.

• Inform the Legal Representative and the Shareholders' Assembly about any possible failures and omissions in the established controls within the procedures, manuals, and/or system policies that could compromise any Company employee, in order to provide evidence and traceability regarding the occurrence of any event.

• Design the methodologies for segmentation, classification, identification, measurement, and control of LA/FT/FPADM Risk that will be part of the SAGRILAFT.

• Submit the Report of Suspicious Operations to the UIAF and any other report or document r equired by current regulations, in accordance with the provisions established by these norms and Chapter X of the Basic Legal Circular.

• Present the policies and procedures contained in the SAGRILAFT Manual for consideration by the Shareholders' Assembly, as well as all subsequent updates required.

• Address and coordinate any request, application, or action from a competent judicial or administrative authority regarding the prevention and control of LA/FT/FPADM activities.

In addition to the above, the Compliance Officer is obligated to continuously train through se minars, conferences, diploma programs, specializations, or similar activities that allow them to develop their skills and maintain updated knowledge in the field of **LA/FT/FPADM** to be prepared for any eventualities that may arise in the organization regarding these topics, and to support national training and dissemination plans for this regulation.

5.2.4 Functions of Employees

• Carry out the necessary activities to ensure compliance with internal and/or external standards related to the management of AML/CFT/PF risk.

• Comply with the policies, methodologies, procedures, and control activities outlined in this manual and report to the Compliance Officer any event that poses a risk of AML/CFT/PF to the company.

• Attend the training sessions called by the Compliance Officer.

• Report to the Compliance Officer any risks of AML/CFT/FPADM identified during the performance of their duties that are not included in the matrix, for analysis and treatment.

• Notify the Compliance Officer of any attempted, unusual, and suspicious operation that you are aware of in the course of your duties as defined in Chapter X of the Basic Legal Circular.

• Carry out the SAGRILAFT control activities incorporated in the procedures assigned to you in the course of your duties.

• Comply with and implement the action plans established to mitigate those risks where the initial controls have proven ineffective.

• Communicate to the Compliance Officer the progress in implementing the action plans assigned to them.

5.2.5 Fiscal Review:

In accordance with the provisions of numbers 1, 2, and 3 of article 207 of the Commercial Code, the fiscal reviewer must ensure that the transactions, businesses, and contracts entered into or fulfilled by the Company comply with the approved instructions and policies. Therefore, the fiscal reviewer will perform the following functions:

• They are obligated to maintain professional confidentiality in the exercise of their profession and in the performance of the functions they carry out within the Company.

• Report suspicious operations to the Financial Information and Analysis Unit (UIAF) when they detect them in the ordinary course of their duties, in compliance with number 10 of art. 207 of the Commercial Code. To this end, they must register on the Online Reporting System (SIREL), administered by the UIAF, to submit the report of suspicious operations.

• Report crimes, offenses, and disciplinary violations of which you have knowledge, except for legal exceptions.

• Pay attention to indicators that may raise suspicion of an act related to potential AML/CFT/FPADM.

5.2.6 Internal Audit:

Regarding the review of **SAGRILAFT**, this body must:

• Conduct at least one annual review of the effectiveness and compliance of the **SAGRILAFT**, and present the findings report to the Compliance Officer and the Legal Representative.

• Ensure the proper execution of processes, procedures, and controls with reference to the **SAGRILAFT**.

• Evaluate the execution of the controls implemented in business processes.

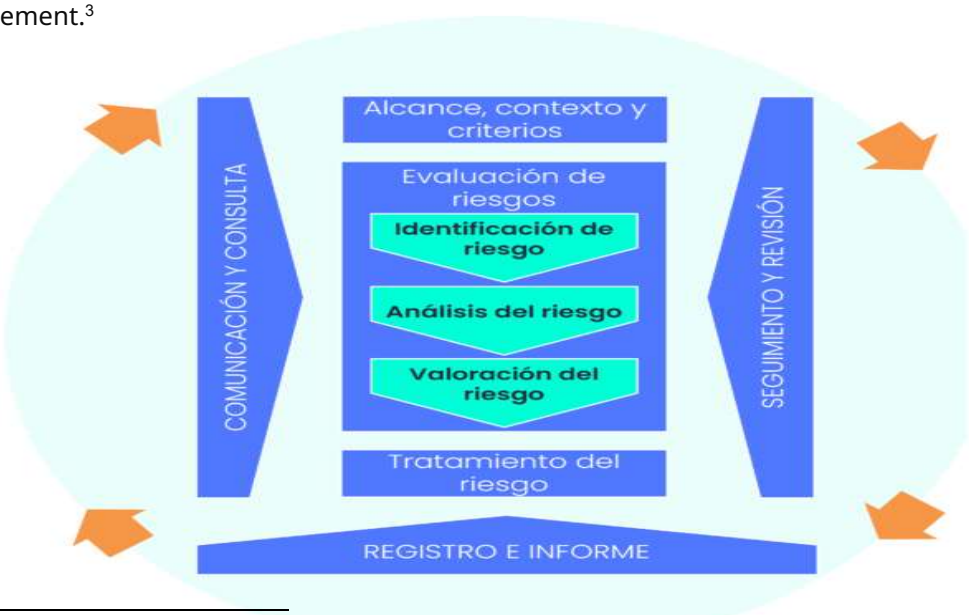
• Report the results to the Compliance Officer, Legal Representative, and the General Shareholders' Assembly, so that the corresponding analyses can be conducted, and necessary corrective actions can be adopted for compliance **SAGRILAFT**.

• You must report to the Compliance Officer when, in the course of your audit work, you identify unusual, suspicious, or attempted operations that may pose a risk to the organization in the terms of this manual.

• They may include improvement proposals when appropriate.

6. SAGRILAFT Risk Management

The SAGRILAFT implemented and designed by BIOFIX BIC includes the stages of identification, measurement, control, and monitoring of risks.
The risk management process is the systematic application of policies and procedures, aimed at transforming the inherent risk of an undesirable exposure condition into a level of tolerance accepted by the organization.
The methodology on which the identification, measurement, control, and monitoring of risks is based is provided under the methodological reference ISO 31000. See definitions related to risk management.[3]



[3]See 5. Terms and Definitions: Risk acceptance, Risk Administration, Risk Analysis, Risk Control, Consequence, Counterparties, Control Assessment, Event, Risk, Inherent risk, Residual risk

6.1 GENERALITIES RISK MANAGEMENT

Individual and consolidated exposure to residual risk must be maintained within the levels of tolerance accepted and approved by the General Shareholders' Assembly and specified in the Manual SAGRILAFT.

The level of risk exposure accepted by the General Shareholders' Assembly is supported through working meetings held by the Compliance Officer and the Area Managers or process leaders, as well as in the reports from control entities (UIAF, Superintendence). The Compliance Officer will review the stages of identification and analysis of the risks associated with the LAFTPADM Risk Matrix at least every six months, in accordance with the prioritization of risks.

- The risk exposure accepted by the General Shareholders' Assembly is supported through

Modification or elimination of LA/FT/FPADM controls

No BIOFIX BIC procedure with incidence and controls that contribute to the mitigation of the **LA/FT/FPADM** risk may be modified or eliminated without prior review by the Compliance Officer and the responsible control leader.

6.2 IDENTIFICATION OF LA/FT/FPADM RISK

In this first phase of the methodology, the specific concrete causes of the **LA/FT/FPADM** risks are systematically identified, as well as the various and possible effects that must be faced, in order to determine the origin or causes and consequences of the risks.

At this stage, the following activities are carried out:

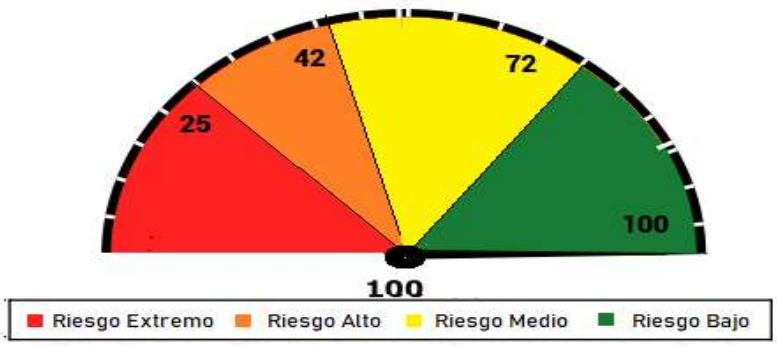
• Current or potential risks of processes sensitive to being used as mechanisms to facilitate illicit activities are characterized, regardless of whether they are controlled or not.

• Classification and analysis of risk factors through the information provided in the knowledge formats, documentary file, and consultation of restricted lists.

• Report of suspicious operations detected by the company, by the internal audit, or by the Fiscal Reviewer.

• Information from national and/or foreign media.

• The degree of risk for **LA/FT/FPADM** is classified as Extreme, High, Moderate, and Low. in each event depending on the risk factor



• The segmentation and classification of the LA/FT/FPADM risk factors is managed, which are determined according to the specific characteristics of each counterparty and as established in numeral 6.1.1. Segmentation of Risk Factors.

• Design and update of the Risk Matrix where the internal and external context of BIOFIX BIC is analyzed, allowing for the proper identification of risks, in accordance with the structure and processes of the company based on its environment and activities.

• The Compliance Officer manages the development, modification, and monitoring of the risk matrix, which is carried out with the risk management information generated in the Compliance **SAGRILAFT & PTEE** process, along with the leaders of the company's processes where relationships, connections, and transactions with counterparties are managed.

• In the event that the materialization of a risk is identified, the Compliance Officer must document the corrective, preventive, or improvement actions and their communication at the managerial and executive levels.

6.3 SEGMENTATION OF RISK FACTORS

Segmentation is a strategic process through which risk factors are grouped into homogeneous groups within each segment, while simultaneously ensuring heterogeneity among them, based on significant differences in their characteristics. This analysis allows for the optimization of risk management related to Money Laundering (LA), Terrorism Financing (FT), and Financing of the Proliferation of Weapons of Mass Destruction (FPADM). The main objective of conducting segmentation is to apply differentiated monitoring and follow-up strategies for counterparties, according to the combination of **LA/FT/FPADM** risk factors and other specific variables. In this way, segmentation facilitates:

1. Focusing efforts on segments with a higher risk profile. 2. Prioritizing monitoring for counterparties with a high probability of risk. 3. Optimizing resources by adjusting strategies to the

6.3.1 Segmentation Criteria

The main criteria for segmenting and profiling risk factors are described below:

a. Segmentation by Counterparty Type and its Nature

● Natural Persons: Individual clients, whether local or foreign .
● Legal Entities: Companies of various sizes, non-profit organizations, and government entities.

● High-Risk Clients:
○ Beneficial Owners: Natural persons who own or control an entity.
○ Politically Exposed Persons (PEPs).
○ Clients in high-risk areas or with unusual activities.

● Recurring vs. sporadic clients: Classification based on the frequency of the relationship and the connection with the organization.

b. Segmentation by Business Relationship

● Participating Clients: Those with high involvement in our mission and financial progress.

● Passive Clients: Counterparties with a high degree of importance in our transactions commercial.

● Suppliers: Entities that provide goods or services.

● Third Parties: Includes contractors, subcontractors, and other related parties.

● Collaborators: Internal individuals whose relationship may pose risks.

c. Segmentation by Geography

● High-Risk Areas: Regions identified by international organizations (FATF/GAFI) as vulnerable to AML/CFT/FPADM.

● Low-Risk Areas: Areas with strict regulations and a reduced history of illicit activities.

● Its National and/or International origin.

d. Segmentation by Transactional Characteristics

1. **Recurring Transactions**: Ongoing payments or activities. 2. **Unique Transactions**: Isolated operations, especially of high value. 3. **International Transactions**: Movements involving multiple jurisdictions.

6.3.2 PROFILING AND SEGMENTATION MODEL

A practical profiling and segmentation model can be structured in a spreadsheet (Excel) to record and analyze each criterion with specific scores that allow for categorizing the risk level of the management file called Compliance Control Dashboard.

6.4 MEASUREMENT OR EVALUATION

In the measurement stage, the possibility, probability, or frequency of occurrence of the inherent risk of AML/CFT/FPADM is measured against each of the risk factors, as well as the impact in case it materializes through the associated risks. These measurements are qualitative or quantitative in nature, described in the *Risk Matrix Controls and indicators.*

In this stage, a qualitative assessment of the identified risks is developed without considering the treatment actions designed for the process, for which measurement criteria for probability and impact are established, selected according to the experience of the process leaders and under the guidance of the Compliance Officer. This activity is described in the *risk analysis procedure.*

The following are the measurement criteria.

6.4.1 Probability or Frequency:

Probability or frequency is a qualitative variable for measuring risk, representing the number of times a specific risk event could occur over the course of a year.

The criteria for evaluating the probability in Biofix Consulting are detailed below: they will be as follows:

Table 1. Probability Measurement Criteria

FACTOR	RANGO	PUNTUACION
Complejidad del procedimiento	Muy facil de ejecutar	1
	Facil de ejecutar	2
	Complejo	4
	Muy complejo	8
	No aplica	0
Automatización	Automático	1
	Semiautomático	2
	Manual	4
	No aplica	0
Idoneidad del personal	Excelente	1
	Bueno	2
	Regular	4
	Deficiente	8
	No aplica	0
Materialización del riesgo	Ocurrrio una vez al año	1
	Ocurrrio dos veces al año	2
	Ocurrio una vez al mes	4
	Ocurio una vez a la semana	8
	No ha ocurrido	0
Frecuencia del procedimiento	Anual	0,5
	Semestral	1
	Mensual	2
	Semanal	4
	Diario	8
Calidad de la documentación	Muy completa	1
	Completa	2
	Aceptable	4
	Deficiente	8
	No aplica	0
Comunicación	Excelente	1
	Buena	2
	Moderada	4
	Deficiente	8
	No aplica	0

6.4.2 Impact:

In the risk analysis methodology, the impact reflects the effect that the presence of a risk event c ould potentially have on the process in qualitative terms, that is, the possible loss. The criteria used for its measurement include penalties for non-compliance with obligations and sanctions related to SAGRILAFT and PTEE according to Law 1908 of 2018 [4]:

Table 2 Impact Measurement Criteria

FINANCIAL LOSSES - Economic Quantification			
Value r	**Level**	**Minimum**	**Maximum**
5	Significant	10,000,001	99.999.999.999
4	High	7,500,001	10,000,000
3	Medium	5,000,001	7,500,000
2	Low	2,500,001	5,000,000
1	Insignificant	-	2,500,000
SOFT LOSSES - Quantification			
Value r	**Level**	**Image Impact**	**Legal**
5	Significant	Publication of news in media mass media (press, television, radio)	Significant accusations and fines by regulatory bodies, litigations very serious
4	High	National image impact (a media outlet)	Formal requirement or investigation by a regulatory body, litigations greater
3	Medium	Impact on image at the local level (guild group of clients)	Informal requirement by some regulatory body, minor litigations
2	Low	Impact on reputation before control entities	Informal requirement by some regulatory body, minor conciliations minor
1	Insignificant	Impact on image before one or several clients	Minor legal issues

6.5 RISK LEVEL:

Similarly, the risk level indicates the level of exposure to risk for the Company, through a valuation scale automatically generated from the combination of the Probability and Impact obtained for each risk, which is referred to as Inherent Risk, that is, the risk without considering the controls.

Once the treatment actions used to manage the risk are documented and assessed, the residual risk will be obtained, which results from the generation of deviations in the

4 According to the **Article** **Section 4 of Law 1908 of 2018**, the penalties for failing to comply with obligations to the SuperSocieties and the UIA F

probability, impact, or both variables of the inherent risk, in relation to the effectiveness of the treatment actions.

In the following table, the risk levels considered in the methodology of the Company are:

Table 3 Risk Exposure Level (Severity)

Value	Level	Min	Max
5	Highly probable	81%	100%
4	Very likely	61%	80%
3	Likely	41%	60%
2	Unlikely	21%	40%
1	Remote	0%	20%

6.6 CONTROL:

At this stage, measures are taken to control the inherent risk to which the organization is exposed, due to risk factors and associated risks.

By identifying the treatment actions being employed, the current level of exposure is reduced to accepted risk levels, that is,
Low Risk Zone: risks are mitigated and prevented from affecting the compliance with objectives, by mitigating risks through the identification of factors that may cause a risk to materialize. **LOW SEVERITY LEVEL Accounting Zone**

Accounting: Risk can be directly accepted, but it is necessary to implement additional controls Medium Severity Level.

Severe Risk Zone: More stringent control measures must be implemented to mitigate the risk, analyzing their cost/benefit. **HIGH SEVERITY LEVEL**

Unacceptable Risk Zone: This combination requires controls aimed at reducing the probability of occurrence and/or minimizing the severity of its impact or mechanisms must be implemented to avoid this risk or transfer it, defining coverage or treatment policies, and establishing exposure limits. **EXTREME SEVERITY LEVEL**

6.6.1 Class of Controls:

The adopted control measures will aim to result in a decrease in the likelihood of occurrence and/or the impact of the risk of **AML/CFT/FPADM** if it materializes.

Within the classes of controls that can be applied according to the particular case, we have:

Preventive Controls Refer to those

that prevent the materialization of risks by analyzing the causes that may generate them.

Defective Controls Refer to actions

for detection during the execution and development of the process; these can occur before or after the transactions. It is an alarm that is triggered in response to an abnormal situation, in situ.

Corrective Controlswhich allow to corr

identify deviations and errors in the operation or prevent them from occurring again. These controls are part of the Internal Control System of the organization duly supported by policies and procedures for its operation.

Within the types of controls that can be applied according to the particular case, we have:

6.1.2 Types of controls:

Manual Controls Control activities developed manually by one or more people.

Semi-Automatic Controls are procedures applied

from a computer in support software, designed to prevent, detect, or correct errors or deficiencies, but requiring human intervention in the process.

Automatic Controls are procedures applied

from a computer in support software, designed to prevent, detect, or correct errors or deficiencies, without the need for human intervention in the process.

The aforementioned control actions must be assigned a rating that evaluates whether they reduce probability, impact, or both, and assesses the effectiveness of the treatment action based on various variables mentioned below:

Table 4 Evaluation Variables of Control Effectiveness

FACTOR EVALUATED	CHARACTERISTIC OF effectiveness	scoring	weighting
class	corrective	1	20%
	detective	2	
	preventive	3	
audit tests of audit	Compliance with the control objective	3	20%
	Non-compliance of the control objective	2	
	An audit has not been conducted on the objective of the control	1	
Effectiveness of CONTROL	High	3	20%
	Acceptable	2	
	Low	1	
Type	Manual	1	20%
	Semi-automatic	2	
	Automatic	3	
Responsibility	Clearly assigned	3	10%
	Partially assigned	2	
	Not assigned	1	
Documentation of Procedure	Documented, Updated y Disclosed	3	10%
	Documented	2	
	Undocumented	1	

According to the rating obtained in the assessment of the treatment actions, the e effectiveness of each of these, according to the following table.

Table 5. Effectiveness of Treatment Actions

Name	Min >	Max <=	F	
Excellent	24	30	3	3
Good	19	24	2	2
Regular	14	19	1	1
Deficient	10	14	0	0

Once a treatment action is associated with a risk, the level of residual exposure will be automatically

6.7 RISK ACCEPTABILITY LEVEL OF AML/CFT/PF:

Risk acceptability level: It is the risk that the General Shareholders' Assembly decides to accept in the pursuit of achieving the objectives.

At Biofix Consulting, residual risks are accepted when their severity is at a low or moderate level, t hat is, if they are within the acceptability zone.

Efforts will be made to keep the residual risk below the moderate level, since in matters of risk **AML/CFT/FPADM**, although the probability of a risk event occurring may be low, the impact in case the risk materializes could be high.

Any residual risk that exceeds the acceptable level must be addressed, and the necessary action plans will be implemented to mitigate such risk.

SEVERIDAD DEL RIESGO		
NIVEL DE SEVERIDAD EXTREMO	E	Se percibe que es posible que el riesgo se presente con una probabilidad o impacto excesivo para la organización, generando pérdidas que exponen la continuidad de la Compañía. **Zona de Riesgo Inaceptable** que se encuentre en este nivel.
NIVEL DE SEVERIDAD ALTO	A	Se considera que el riesgo puede presentarse con una probabilidad o impacto representativo, afectando la adecuada operación de la compañía. Esta es una **Zona de Riesgo Grave** para que los riesgos se encuentren en este nivel.
NIVEL DE SEVERIDAD MEDIO	M	Se presentan eventos de riesgos que comprometen el resultado del proceso. Esta es la zona máxima de tolerancia para mantener los riesgos.**Zona de Aceptabilidad.**
NIVEL DE SEVERIDAD BAJO	B	Se presentan eventos en los procedimientos de baja criticidad para el negocio. Esta es una **Zona de Riesgo Bajo** para mantener los riesgos.

6.8 MONITORING

At this stage, the Compliance Officer monitors the evolution of the inherent risk profile, the AML/CFT/FPADM, and the effective detection of unusual and suspicious operations, allowing for corrective, preventive, and improvement actions to be taken on the SAGRILAF.

The self-assessment is based on the following mechanisms:
• Monitoring of the processes responsible for the relationship and engagement with counterparties in the company.
• Analysis of the benefits achieved.

• Monitor and compare the inherent and residual risk of each risk factor and the risks associated with AML/CFT/FPADM.
• Review that the residual risks are within the acceptance levels established by the company.

• Review the organization's level of learning regarding the management of its risks.

• Carry out an effective monitoring process that facilitates the rapid detection and correction of deficiencies identified in the risks associated with **AML/CFT**.
• It is essential to ensure that the controls are comprehensive of all risks and that they are functioning in a timely, effective, and efficient manner.

Likewise, use the following tools:

• Information gathering and classification.
• Annual work plan, audit activities for **SAGRILAFT,** analysis of the information generated in the management of counterparties, verification against restricted lists.
• Risk matrices. Update audited controls.
• Drafting of reports. UIAF, SUPER SOCIETIES, Response to requirements, internal and external audits of **SAGRILAFT**
• Presentation of reports to the legal representative and Shareholders' Assembly. Adoption of Action Plans and/or Recommendations
• Monitoring and evaluation of the functioning of the **SAGRILAFT** system.
• Automated System of Restricted or Informative Lists
• Risk Indicators **AML/CFT/FPADM.**
• Update of management tools, compliance control dashboard, risk matrix,
• Management of the Annex __ ***Procedure for Detecting Unusual and Suspicious Transactions***Annex __ Guide ***Warning Signals***

At this stage, the identification of new risks that may affect the objectives of the system is understood; therefore, methodologies (segmentation, request for reports, among others) are executed to update the risk profile at least annually or whenever business development requires it.

6.9 RISK TOLERANCE

Biofix Consulting defines that once risks (probability and Impact) are identified and assessed, it will assume those that fall within a medium and low range, which in terms of color coding in the risk matrix will be shown in yellow and green respectively. Accordingly, inherent and residual risks that fall into the extreme and high category (Red or Orange) will proceed with the implementation of controls in order to mitigate the risks.

However, if the controls do not ensure sufficient effectiveness to bring the risk(s) to the accepted and approved categories, it must be reported through periodic reports to Senior Management in order to propose action plans and risk mitigation or to define how to address them differently.

7. SAGRILAFT COMPLIANCE POLICIES

The Self-Control and Comprehensive Risk Management System for Money Laundering, Terrorism Financing, and Financing for the Proliferation of Weapons of Mass Destruction (SAGRILAFT) of BIOFIX BIC has been duly approved by the Shareholders' Assembly and implemented in the organization, in order to mitigate the risks associated with illicit activities. The system encompasses the following fundamental phases, in accordance with current regulations:

a. Risk Prevention: The main objective of this phase is to prevent the company from being used to channel resources from illicit activities. The actions implemented include:
- **Due Diligence:** Rigorous counterparty knowledge measures are applied, which include thorough identification of clients, analysis of beneficial owners, and risk assessment based on their profile, considering both clients and suppliers, business partners, and other relevant actors. -

- **Controls on Restricted Lists:** Continuous monitoring of counterparties using specialized technological tools that allow for the identification of alerts in national and international lists, both of the entity and its counterparties. -

- **Supervision of Relationships:** Detailed tracking of interactions with counterparties to ensure compliance with regulatory and ethical standards, with special emphasis on high-risk businesses or relationships with countries or jurisdictions with a high risk of money laundering or terrorism financing. -

b. Risk Control and Detection: In this phase, the focus is on the identification and reporting of suspicious activities related to Money Laundering (ML), Terrorism Financing (TF), and Financing for the Proliferation of Weapons of Mass Destruction (FPWMD). The main actions are:

- **Active Supervision by the Compliance Officer:** Continuous monitoring of the organization's transactions and activities is carried out by a Compliance Officer, who is responsible for the direct oversight of regulatory compliance.
- **Transaction Analysis:** Through internal and external audits, as well as the company's processes, a continuous analysis of financial transactions is conducted to identify unusual transactions or those that do not align with the profiles and behaviors of clients, detecting possible signs of illicit activities.

- **Report of Suspicious Activities:** Any generated alert is reported immediately both internally within the organization to the Compliance Officer and to the competent authorities, following the deadlines and procedures established by the regulations.
- **Timely Reporting Compliance:** Reports of suspicious activities must be submitted to the relevant authorities within the deadlines established by law, ensuring transparency and compliance with the regulatory framework.

c. Continuous Improvement: This phase aims to identify opportunities for continuous i mprovement in risk management, ensuring that procedures and tools are updated in accordance with regulatory changes and market conditions. The key actions are:

- **Evaluation and Update of Procedures**: The procedures and protocols used in SAGRILAFT are periodically reviewed to ensure they are aligned with best practices and current legislation.

- **Training and Capacity Building**: Continuous training programs are implemented for staff and counterparties to keep them informed about regulatory changes, new threats, and best practices in preventing money laundering, terrorism financing, and the proliferation of weapons of mass destruction.

- **Emerging Risk Analysis:** Continuous analysis of emerging risks is conducted, assessing new scenarios and adapting mitigation strategies to address unforeseen challenges that may arise in the future.

This comprehensive and constantly evolving approach ensures that BIOFIX BIC maintains effective risk management and meets regulatory requirements, contributing to the prevention of financial crimes and strengthening the trust of its clients, partners, and the market as a whole.

Therefore, BIOFIX BIC, in compliance with **SAGRILAFT**, is committed to the guidelines for preventing crimes associated with **AML/CFT/FPADM**, thus

● It has a methodology and procedures for the Management of Risk **AML/CFT/FPADM**, which allow for the identification, measurement, control, and monitoring of inherent and residual risks that may affect the Company.

● It will maintain the training program based on the regulations in permanent operation and development of the SAGRILAFT.

● Commercial negotiations will not take precedence over compliance with the policies and guidelines defined for the management of the risk of Money Laundering and Terrorism Financing established in this manual.

● Mechanisms will be adopted to preserve the documentary information of the associates, the movements of incoming and outgoing resources, the reports to the UIAF, the reports prepared by the Compliance Officer, the fiscal review, and other information generated in the execution of SAGRILAFT.

● It will report to the Financial Information and Analysis Unit (UIAF) the transactions that have been determined as suspicious for Money Laundering and Terrorism Financing.

● The information regarding attempted or suspicious transactions related to Money Laundering and Terrorism Financing will be treated with strict confidentiality, and therefore, the name or identity of the individuals for whom conduct has been determined that led to the generation of the report cannot be disclosed.

● Conduct due diligence on every natural or legal person who formalizes a contractual or legal relationship (Clients, Participants, Collaborators / Employees, Suppliers, Shareholders, Contractors).

● Any transaction in which the company is involved must have internal and/or external documentation that clearly explains the nature of the transactions, the date, and the approvals granted in accordance with the established policies and procedures for each area and process of the company.

● The Company will refrain from establishing links with clients, employees, suppliers, shareholders, and other related parties that are on any of the binding and restrictive lists, once due evaluation has been conducted in any case.

● Employees must immediately report any unusual or suspicious operation they identify in the course of their daily activities to the Compliance Officer.

● Employees and/or third parties who have any connection with the company assume the commitment and responsibility to promptly address the requests made by the Compliance Officer.

● Any situation or inquiry regarding a potential conflict of interest must be reported to the immediate superior, who should forward it to the authority responsible for resolving this conflict. This system aims to strengthen the company's capabilities in preventing these crimes and ensuring compliance with applicable regulations, promoting a safe and transparent corporate environment.

● The **non-compliance** with the policies, procedures, or guidelines of SAGRILAFT, especially those related to the prevention of **AML/CFT/FPADM**, corruption, or bribery, will be considered a serious offense. These cases will be analyzed in accordance with the **Internal Regulations of Work** and the current sanctioning regulations in Colombia, ensuring actions are aligned with the highest ethical and legal standards.

8. DUE DILIGENCE PROCEDURE

Due diligence is aimed at preventing the company from being used as an instrument to carry out activities or transactions related to **AML/CFT/FPADM**, allowing for the identification of unusual, suspicious operations and/or risks associated with compliance with SAGRILAF, where all employees and collaborators ensure compliance with all their processes and timely reporting of information for the management and analysis of the Compliance Officer.

This due diligence includes the controls Documentary File, Verification against restricted lists, and Enhanced Due Diligence in cases of news or alerts regarding counterparties that require it, utilizing the efficient and professional human resources of the company as well as the physical and technological resources available for risk management, such as the compliance application, information systems for managing process information, all to ensure compliance with the provisions contained in the regulation, which allow for the understanding of real and transparent information for decision-making and the inputs required for compliance with the SAGRILAFT System.

8.1 DOCUMENT FILE CONTROL:

The processes responsible for managing information with counterparties (passive clients, active clients, suppliers, employees, third parties, among others) are in charge of collecting, updating, and filing essential documents as applicable to each person or entity, whether national or foreign.

For national natural and legal persons, the required documents include: citizenship ID, RUT, Chamber of Commerce certificate, and bank certification. For foreign legal entities, the equivalent documents include: TAX ID, passport, Foreigner IN. The Customer Due Diligence Form duly filled out and other specific documents required by the process that leads the relationship and/or linkage, depending on the nature of the entity.

No exceptions are accepted in the minimum documentation, and no onboarding and continuity processes are managed if the counterparty does not comply with the due diligence controls that apply to it.

8.1.1 Customer Due Diligence Format Control:

This document is requested from all counterparties that engage with the company, which requests detailed information about the counterparties of an organization, allowing for the evaluation of their identity, background, accuracy according to the provided legal documents, and the purpose of the business relationship. This is requested at the relationship stage, and this format is key in preventing risks associated with **AML/CFT/FPADM,** corruption, and other illicit activities, allowing for the communication of the company's commitment to its compliance policies, ethics, and other measures that ensure reliability with our counterparties, identifying analytical information, considering that exceptions in the request for counterparties only apply to supplier clients and according to the amounts approved in the materiality basis. See*Numeral 9.1* ***Internal Reports - 9.1.7. Approval Materiality Basis***

8.1.2 Update Documentary File Counterparts.

This is carried out when counterparties report changes in legal representation, address, or other data, as well as upon requests from the Compliance Officer according to the risk management associated with each counterparty.
This documentary update process is carried out annually for recurring counterparties, such as the Participating Clients counterparties led by the Project Management Process, who report annual updates of information also for employees and collaborators in the documentary update process managed by Human Management.

This documentation must be supported in the folder of each counterparty as applicable and under the responsibility of the leaders of the onboarding and relationship processes according to our internal processes.

8.1.3 Final Beneficiary Identification

The compliance officer identifies all natural and legal persons associated with the counterparty; for the latter, he verifies the Beneficial Owners reported in the Customer Due Diligence Form FCC, which are part of the risk management and verification controls in restricted lists.

Therefore, it is important for the process leaders to ensure the proper completion and complete information of the legal entities and the beneficial owners reported in the FCC.

8.1.4 Management and Protection of Personal Data

BIOFIX CONSULTORÍA S.A.S. BIC, in compliance with Law 1581 of 2012 and its regulatory decrees, adopts technical, organizational, and legal measures to ensure the security, privacy, and confidentiality in the processing of personal data collected within the framework of SAGRILAFT. These actions include, among others, prior and express authorization from

the data subjects, the implementation of controls that ensure the integrity and accuracy of the information, and the limitation of access solely to authorized personnel. Additionally, mechanisms are established for addressing inquiries and complaints regarding the exercise of the rights of the data subjects, including requests for updating, rectification, and deletion of data, as provided for in current regulations.

BIOFIX CONSULTORÍA S.A.S. BIC reinforces its commitment to data protection through the adoption and dissemination of its data protection policies, ensuring compliance with the principles of purpose, necessity, and proportionality in the processing of information.

8.2 PROCEDURE FOR VERIFICATION IN RESTRICTED LISTS

The leading areas of engagement manage the SAGRILAFT and PTEE compliance management process approved by the company, making a formal request and reporting information to the compliance officer so that within their functions, they can validate against national and international restricted lists of the counterparties and beneficial owners identified in the documentary file to detect and manage risks associated with **AML/CFT/FPADM** and corruption.

8.2.1 Types of Concepts Issued by the Compliance Officer:

● **Eligible Counterparty**: A concept is issued for the continuity of the relationship and/or connection with the counterparty without risk and recommendations.
● **Ineligible Counterparty:** An unfavorable concept of connection is issued in case of alerts, a counterparty with risk, and requires management approval for its connection. At this stage, the Compliance Officer issues a written concept and reports via institutional email to the Process Leader for filing in the counterparty's compliance management evidence SAGRILAFT and PTEE.

The documentation associated with inquiries on lists and additional documentation generated from the risk analysis is under the custody and responsibility of the Compliance Officer. When there is no clarity to issue the concept, the Compliance Officer will determine to execute the **Enhanced Due Diligence.**

8.3 CL Contractual Clauses Associated with Ethical Policies and SAGRILAFT

In the process of onboarding and its legalization, the leading management ensures that each and every contractual document includes the clauses validated by the company that guarantee compliance with our SAGRILAFT and ethical policies.

If in the activities related to risk management **AML/CFT/FPADM** it is reported or detected that a counterparty violates the compliance of these clauses, the Compliance Officer will carry out the verification and consolidate the evidence to issue the respective communications, with a copy to the Legal Department and General Directorate to be treated as a serious offense, subject to sanctions in accordance with the Internal Work Regulations and/or legal regulations.

8.4 ENHANCED DUE DILIGENCE PROCEDURE:

This procedure applies to all third parties that generate any alert signal during the pre-contractual and/or contractual relationship that requires more information to objectively obtain an analysis of the identified alert and determine whether it should be reported to the Unit of Financial Investigation and Analysis or any internal or external control entity. The decision could lead to a determination that the relationship and/or affiliation is not appropriate and/or the discontinuation of the affiliation with the third party depending on the outcome.

Enhanced due diligence will be applied to counterparties identified as Beneficial Owners in cases of risk, as determined by the compliance officer's analysis.

Enhanced due diligence will be applied to counterparties identified as politically exposed persons (**PEPs)** who are in an active status and according to the analysis conducted by the compliance officer.

If a high variation in the risk profile is identified during the third-party profiling process (segmentation), enhanced due diligence must be considered, and appropriate measures should be taken based on the results.

If the report generated in the Verification of Restricted Lists does not clarify the risk associated with crimes related to **AML/CFT/FPADM**, corruption, or fraud where name similarities, inconclusive processes, or reputational risks in news and others without a clear connection to the counterparty are identified, the compliance officer considers enhanced due diligence for analysis and opinion.

To carry out this procedure, the compliance officer requests the process leader to manage with their counterparty: - the completion and signing of the Authorization for Data Processing format (***Annex Authorization Format for Data Processing***), - as well as additional information requirements and/or clarification of doubts and/or dismissal or confirmation of situations or risks identified in the initial due diligence.

The Compliance Officer will carry out the necessary follow-up in the **Compliance** application, using the available options to request an expanded compliance report.

8.4.1 Management of Additional Information:

● The Directorate Leader of the engagement will support the collection of the required information, ensuring direct communication with the counterparty to obtain the requested data.

● In cases where counterparties, due to their privacy policies, prefer to send the information directly to the Compliance Officer, the use of the email **sgonzalez@biofix.com.co** for this purpose is authorized.

This process ensures the necessary traceability and depth to mitigate identified risks, aligning with the highest standards of compliance and transparency, generating the respective alert reports and opinions as applicable.

8.5 Relationship and Linkage of Politically Exposed Persons (PEPs)

Regarding counterparties classified as politically exposed persons, they are managed as follows:

● Its linkage requires approval from the General Manager or a higher hierarchical level .
● Request the additional completion of the annexed Expanded PEPs Format Knowledge Format of the Client
● Ensure monitoring of the counterparty and follow-up over time during their engagement if approved.
.
● In accordance with the risk management of PEP counterparties, the Enhanced Due Diligence Procedure will be managed if the Compliance Officer requires it.

Enhanced Due Diligence if the Compliance Officer requires it.

9. COMPLIANCE REPORT MANAGEMENT

9.1 INTERNAL REPORTS

9.1.1 Annual Report Shareholders' Assembly:

The Compliance Officer, within their obligations, must prepare a report at least once (1) a year, addressed to the Shareholders' Assembly, in which they report on the progress made in the system, follow-up on continuous improvements, management of the officer, reports, regulatory changes, external and internal requirements, training, among others.

9.1.2 Report of Linkages

Monthly, the relationship leaders report to the compliance officer the updates on linkages approved by the company, a necessary input for the verification and validation of Sagrilaft controls, verifying the execution of preventive controls and/or management of compliance detective controls.

9.1.3 R Report on Warning Signals, Unusual, Suspicious, or Attempted Operations

At BIOFIX BIC, we consider warning signals to be those situations that, when analyzed, deviate from the normal behaviors of counterparties, internal processes, and/or the expected standards according to regulations, being deemed atypical and therefore requiring further analysis to determine if there is a possible **AML/CFT/FPADM** operation. Collaborators who detect unusual, suspicious, or attempted transactions should report to the Compliance Officer via the email sgonzalez@biofix.com.co and send the Annex Format FMT-GC-01-02 Internal Report Format for Unusual Operations for proper analysis and management. See Numeral

9.2 External Reports 9.2.1 Procedure for Reporting Suspicious Operations (ROS).

Below are some Alert Signals that can be identified:

We detail some Warning Signals as a guide for risk management:

- Facing Clients, Suppliers, and other third parties Counterparties with judicial records of AML/CFT.
Natural or legal persons that are not fully identified
Situations in which the counterparty provides false, incomplete, or misleading business contact information.

Counterparties that have large sums of cash or foreign currency available for the transaction or business activity, and the type of business they conduct does not support such a situation.
Findings of false information from the counterparty in the due diligence processes.
When the counterparty seeks to have the payment of profits made to an account in a foreign country that is not the location of their business.
New associates who have been accepted or linked without prior verification of the source of the funds they contribute.
Clients or associates or counterparties who continuously change their address and phone number.
act on behalf of third parties trying to conceal the identity of the client or associate or counterparty co in which the transaction will take place.
Individuals who split transactions to avoid having to fill out the source of funds certificate. The income level is not consistent with the economic activity.
Individuals whose transactional amounts in savings accounts and the opening of CDTs do not align with the income level they receive from their economic activity.
Individuals who fill out forms with illegible handwriting and do not place the respective signature or fingerprint on the form.
Constant change in legal representatives.
Payment requests in accounts that are not in their name.
Clients whose financial statements reflect results that are very different compared to other companies with similar activity and in the same economic sector. Addresses in tax havens with different companies.

They provide false information that is difficult to verify or insufficient.
Legal representatives not meeting the required criteria.
Purchasing goods at prices that are notably lower than those offered in the market.

- Employees Employee who

avoids certain internal controls or approvals established for specific transactions, products, or services.

Employee who omits the identity verification of a counterparty or does not verify their data against the records provided in the onboarding forms or the company's databases.
Employees who frequently receive gifts, invitations, and gratuities from certain clients or counterparties without a clear and reasonable justification.
Employees, especially commercial advisors, who preferentially, exclusively, and permanently serve or exempt a client from certain controls with the argument that they are 'well-known', 'referred by another entity', 'only tr ust me', 'I advise them on all their business', or similar.
Employees who ha ve a lifestyle that does not correspond with the income level at the labor level, yes my reasonable justificatio n
.

- Regarding transactions, businesses, or contracts that represent, have as their object, or involve:

High volume of cash without apparent justification.

Movable or immovable property at prices significantly different from normal market values.
Donations that do not have an apparent ultimate beneficiary, whose origin is unknown or... and this is
located in a country or a high-risk jurisdiction. cited in a country or a high-risk jurisdiction.
Transactions, businesses, or relevant contracts that are not documented in writing.
Payments for transactions involving funds derived from international remittances from various senders to a single beneficiary, or from a single sender to multiple recipients, without an apparent relationship.

OCommercial transactions or businesses with individuals included in the binding lists.
Transactions conducted with counterparties domiciled or located in designated geographic areas. designated by
FATF as non c operating.
Transactions involving products derived from illegal activities (including, among others, smuggling).

Transactions involving products that have not been properly nationalized; and transactions involving restricted sale products that do not have the necessary authorizations or licenses.

- Regarding transactions with cash derived from, or related to: Countries with
high corruption levels and political instability.
Cash deposits in personal or business bank accounts from unexplained sources. Unjustified documentation regarding, or not corresponding with, the origin or ownership. Amount, value, or currency inconsistent with t he circumstances of the bearer. Hidden cash transportation; clear security risk in the transportation method. Transportation with costs significantly higher compared to alternative transportation methods. Unusual cash billing or sales in the economic sector. Large increase in cash billing or sales from unidentifiable clients; and loans from

foreign received in cash and in local currency.

Since there are many more warning signals, a Guide of warning signals is attached to this list, which aims to provide guidance for all employees of the company to consider when identifying unusual operations, which, once identified, should be reported to the Compliance Officer according to our internal procedures.

9.1.4 Internal Level Report:

At the moment they are presented, the Compliance Officer must be immediately informed of the ***detection of unusual and suspicious operations. According to the Warning Signals,*** *all* employees of the company who detect a warning signal, unusual operation, suspicious or attempted operation, must inform the Compliance Officer immediately via the institutional emailsgonzalez@biofix.com.co, attaching the respective evidence, which will then evaluate and analyze the reported operations to determine whether it is indeed an unusual or attempted operation.

In the event that Warning Signals are identified during internal and/or external audits (Fiscal Review), the Compliance Officer must be informed about the findings related to alerts and/or transactions of **LA/FT/FPADM** that violate our SAGRILAFT policies, managing the type of report. See Numeral 9.2 External Report 9.2.1 Procedure for Reporting Suspicious Operations (ROS).

9.1.5 Anonymous Report - Externals

If the employee and/or an external party prefers to report anonymously, they can do so using the email address lineaetica@biofix.com.co - Reporting channel, attaching to the report the documentary file evidence of the non-compliance and/or identified alert signal. See Numeral 9.2 External Report 9.2.1 Procedure for Reporting Suspicious Operations (ROS).

9.1.6 Case Files Reports.

The information required by the compliance officer related to the detection and reporting of the s uspicious operation attempted is provided with the original documents, which must be retained in accordance with the documentation policies established by the Company, with the necessary security measures, in order to ensure they are delivered completely and promptly to the competent authorities in the event that any of them request it.

The Compliance Officer may request additional information within the company, which must be accessible for analysis and risk management if required for reports to authorities and/or management of co mplaints. Therefore, the compliance officer must ensure the confidentiality of the report and, primarily, of the employee who detects it. Likewise, the employee who has identified and reported the unusual activity may not disclose such information.

The situations evidenced and reported are subject to confidentiality in accordance with Colombian legislation, and they will be maintained appropriately, with their documentation management

9.1.7 Counterparty Control Risk Management Register:

For the processes of monitoring and oversight of SAGRILAF controls, Updated Databases of Employees, Counterparties Participants, Passive Clients, and Contracts are managed according to t he information provided by the leaders of the onboarding and relationship processes.

The Compliance Officer maintains control over their database of counterparties, where they document compliance with SAGRILAFT and PTEE controls, risk management, and records of updates related to reported updates, internal transactions, unusual and suspicious activities in case they are reported or identified, to provide a record of the management and treatment of risk as applicable (internal communications, expanded due diligence, UIAF reports, internal report), for managing the risks of situations in which it is considered that a risk of **LA/FT/DPADM** may have materialized, along with the analysis and results obtained for each of them. Furthermore, this statistical information will allow for f uture improvements in the methodology for measuring the risk of **LA/FT/FPADM**.

9.1.8 Approval of Materiality Base

According to the financial information, the Materiality Base Report (FMT-GC-01-03 Biofix 2025 Materiality Report Format) is completed by the Financial Management, determining in agreement with the Compliance area, the approved value of the materiality base for the application of SAGRILAFT controls for applying FCC controls to suppliers and risk analysis for internal management.

The materiality base is calculated and approved after the approval of the financial statements for the previous period, which were approved in the minutes of the Shareholders' Assembly, and according to the report presented on SAGRILAFT compliance and PTEE risk management for the previous period. This process is confirmed through electronic communication and is attached to the working papers of SAGRILAFT and PTEE compliance via electronic communication. See the Characterization of the co mpliance process where this procedure is detailed.

9.2 EXTERNAL REPORTS

9.2.1 Procedure for Reporting Suspicious Operations (ROS)

This procedure applies to all areas and collaborators of the organization, starting with the detection and analysis of the situation or operation and concluding with the filing of the information. If the Compliance Officer considers that the operation is suspicious, it ends with the report to the Financial Information and Analysis Unit (UIAF).

The detection and subsequent reporting of an unusual operation can be carried out by any collaborator of the organization, as the source of this type of report is any atypical or unusual situation that may arise in the daily activities conducted in their work environment. See Annex PRO-GC-01-01 Procedure for Detecting Suspicious Unusual Operations.

Unusual operation: This is one whose amount or characteristics do not relate to the economic activity of the Third Party being analyzed, or that, due to its amount, the transacted quantities, or its particular characteristics, falls o utside the established or known parameters of normality. The report related to an unusual operation is called ROI.

Attempted operation: It is configured when there is knowledge of the intention of a natural or legal person to carry out a transaction, but it is not completed because the person attempting to do so withdraws from it or because the established controls did not allow it to be carried out. These transactions must be reported solely and exclusively to the UIAF.

Suspicious operation: It is one that, due to its number, amount, or characteristics, does not fit within the normal systems and practices of businesses, an industry, or a specific sector, and, furthermore, that according to the customs and practices of the relevant activity, it has not been reasonably justified. These transactions must be reported solely and exclusively to the UIAF. The report regarding a suspicious operation is called ROS.

Through the reporting format Annex Internal Report Format for Unusual Operations, any unusual, attempted, or suspicious situation will be reported, which will be submitted to the compliance officer for pertinent analysis.

The Compliance Officer must report all Suspicious Operations detected in the ordinary course of their business or activities to the UIAF. The report must be made in an

immediate manner and with the nature of a ROS, through the SIREL. It is important to mention that the report made to the entity does not constitute a criminal complaint. For the management of transactions

9.2.2 Reports of Absence of Suspicious Operation (AROS)

In the event that a quarter passes without the Company conducting a ROS, the Compliance Officer must submit a report of absence ROS or **AROS** within ten (10) calendar days following the end of the respective quarter, through the SIREL system.

9.2.3 Reports Superintendency of Companies

According to the provisions established by the Superintendence of Companies, the company is required to annually submit reports requested by SuperSocieties regarding the mechanisms implemented within the company concerning **AML/CFT/PADM**, using the Storm Web application of the Superintendence of Companies.

Each and every report is managed by the Compliance Officer, consolidating the information and requesting, if applicable, information from other process leaders according to their area of responsibility. Prior to submission, it will be validated and approved by the General Directorate.

Attention to requirements from control entities and oversight regarding SAGRILAFT

The reports required from the company BIOFIX BIC must account for the results, analyses, evaluations, and corrective actions in the implementation, management, progress, compliance, difficulties, and effectiveness achieved through **SAGRILAFT,** which are required from the Legal Representative, the Compliance Officer, or the internal control bodies, as applicable.

The Compliance Officer must be notified of any communication from control or oversight entities that require information related to the compliance system**SAGRILAFT**, which is submitted by BI OFIX BIC through the communication channelcorrespondencia@biofix.com.co or submitted directly to other internal instances such as shareholders, management, executives, and other departments.

The attention to these requests must be timely and must comply with the appropriate and complete response as requested.

The Compliance Officer may rely on the respective official for obtaining the required information; all external communication related to the management of SAGRILAFT and PTEE will be shared and approved by the General Directorate and/or legal representative with the approval of the Compliance Officer.

- **Internal Audit and Fiscal Review**

The audit requirements of the fiscal review and the internal audit will be managed through internal communications and/or a requirements platform, for management by the Compliance Officer.

The analysis results generate the report and may include improvement proposals when relevant.

10. OTHER PROVISIONS

10.1 CASH OPERATIONS AND VIRTUAL TRANSACTIONS

In order to minimize the risks associated with AML/CFT/FPADM, the company will not make payments to third parties with whom no negotiation has taken place or for whom the due diligence procedure defined by the company has not been carried out; all electronic payments made by third parties must be received in the bank accounts established by the company. The accounting area will be responsible for validating the payments received in the bank accounts and making the necessary accounting entries, keeping the respective reconciliation supports. The company does not engage in or conduct **transactions with virtual assets**.

10.2 DONATIONS

Donation requests from clients and/or partners in vulnerable conditions are managed, which must ensure that the beneficiary entities are legal and transparent, including the verification of:

● Recognition as a legal entity.
● Due Diligence Beneficiaries Donations
● Approval from the Managerial and Executive Level
● Tax Declarations.
● Certificates supporting tax benefits.
See Code of Ethics, Conduct, Transparency, and Anti-corruption Number 4.29 Donations Related to Vulnerable Clients and risk factors.

10.3 CONFLICT OF INTEREST RESOLUTION

BIOFIX BIC is aware that a conflict of interest is a situation where individuals favor their personal or professional interests, directing their decisions for their own benefit or that of a third party, conflicting with the responsibilities of their position. Therefore, the following guidelines are defined:

• Commercial negotiations will not take precedence over compliance with the policies and guidelines defined for the management of the risk of AML/CFT/PF established in this manual.

• Any situation or inquiry regarding a potential conflict of interest must be reported to the i mmediate superior, who should forward it to management in order to evaluate and establish the respective actions.
• The Compliance Officer shall refrain from participating in decisions or activities involving the engagement of clients, partners, suppliers, collaborators, or any counterparty when it concerns family members or there is a personal interest in any business or project with BIOFIX BIC. In the event that both the legal representative and the compliance officer are impeded, they

must escalate the situation to the General Shareholders' Assembly, and it will be the members who provide the corresponding instructions and/or approvals.

In accordance with these provisions, it is regulated from an internal level with the family protocol and Corporate Governance Manual; likewise, at an external level, relationship documents are guaranteed to validate that all relationships and/or affiliations manage and report situations of conflicts of interest.

11. TRAINING, EVALUATION, AND INFORMATION DISCLOSURE

The Company, along with the compliance officer, will carry out training activities related to SAGRILAF for all employees and stakeholders, which meet the following characteristics:

• Induction Training will be provided to new employees, both permanent and temporary, upon their entry, either in person or through alternative methods such as e-learning. These will be accompanied by evaluations to assess the knowledge acquired about the System.

• Training for external third parties aims to inform about the SAGRILAFT system through mass communications via email.

• The training and education process will take place at the time of onboarding and at least once (1) a year, either in person or virtually.

• Training plans must be reviewed and updated in accordance with any changes presented.

• In evaluations conducted during induction or knowledge enhancement, if an employee does not pass the first (1) evaluation, a re-evaluation will be conducted. If they fail again, they will receive feedback from the Compliance Officer. If this issue is recurrent, administrative measures deemed appropriate will be taken. Evaluations conducted physically, once graded, will be sent to the human resources manager for filing and custody.

• It must maintain a record of the trainings conducted, which should include the date, topic treated and the names of the attendees and evidence of the evaluation.

• As a result of the training, the staff will be capable, at a minimum, of identifying unusual or suspicious transactions within the operations of the Company.

BIOFIX BIC promotes the proper officialization, publication, implementation, and functioning of its policies, procedures, and other documentation related to the **SAGRILAFT,** ensuring that they can be consulted on the institutional website and also within the company.

12. DOCUMENT CONSERVATION

Documents related to the SAGRILAFT must be retained in accordance with the provisions of Article 28 of Law 962 of 2005 for a period of ten (10) years. Once this period has expired, the documents may be destroyed as long as exact reproduction is guaranteed by any digital means. All necessary supports will be retained, and the company has the following documents for the management of the System.

- Manual of system policies for the Self-Control and Comprehensive Risk Management System LA/FT/FPADM approved by the Shareholders' Assembly.
- Reports submitted by the Compliance Officer to the Shareholders' Assembly.
- Reports submitted by the Fiscal Reviewer regarding the operation of the Self-Control and Comprehensive Risk Management System LA/FT/FPADM.
- Reports issued to the Financial Information and Analysis Unit (UIAF).
- Certificates of training conducted for the employees of the Company.
- Documentation related to the management and control of the Self-Control and Comprehensive Risk Management System LA/FT/FPADM.

Once these periods have expired, they may be destroyed in accordance with the policies established by the Company.

Protection, retention, and confidentiality of information regarding SAGRILAF T

BIOFIX BIC and each and every one of the employees and collaborators are responsible for ensuring that the information collected for the management of the risk of **AML/CFT/FPADM** (own, from clients, users, providers, suppliers, partners, collaborators, and reports) is confidential and are committed to maintaining its confidentiality; except for the exceptions contemplated or provided by law or with the corresponding authorizations from senior management and/or a judicial authority order.

No collaborator has the authority to provide information to third parties regarding the investigation, analysis, and monitoring procedures that are conducted on their transactions, as well as the communications and/or reports that, in compliance with the relevant provisions, are sent to the Financial Information and Analysis Unit, the Unit of Financial Investigation and Analysis, or to other competent authorities.

Due to the above, it is the duty of employees to maintain absolute confidentiality regarding such information.

13. SANCTIONS AND INCOMPATIBILITIES TO SAGRILAFT

Failure to comply with the orders and instructions issued in Chapter X by the Superintendence of Companies will lead to the relevant administrative investigations and the imposition of the pertinent administrative sanctions on the Company, the Compliance Officer,

the fiscal reviewer, or its administrators, in accordance with the provisions of numeral 3 of Article 86 of Law 222 of 1995, without prejudice to the actions that correspond to other authorities.

Failure to comply with or omission of the guidelines established in this Manual and in the procedures set forth related to SAGRILAFT will result in the disciplinary process provided for in the contract and current labor regulations, and if applicable, the imposition of the disciplinary sanction that may apply.

Noncompliance with this SAGRILAFT Manual will be considered a serious offense in labor matters and grounds for dismissal with just cause against employees.

• Failing to inform the Compliance Officer of the identification of suspicious or unusual transactions in the due diligence process.
• Not informing the Compliance Officer about the identification of warning signals regarding changes in the behavior of linked third parties.
• Omission of controls related to AML/CFT/FPADM.
• Being a facilitator in AML/CFT/FPADM transactions to benefit oneself or third parties.

In case of non-compliance with the provisions set forth in this Manual by clients, suppliers, and third parties, the contractual relationship will be terminated immediately.

14. UPDATE AND DISCLOSURE

This manual must be reviewed and updated at least once (1) a year by the Shareholders' Assembly and the Compliance Officer and/or when new legal or internal regulations of the Company need to be considered.

15. VALIDITY

This manual will come into effect once it is published and approved by the Shareholders' Assembly of the Company.

16. CONTROL OF UPDATES

This SAGRILAFT Manual will be updated as needed; in this regard, the Shareholders' Assembly of BIOFIX BIC will be responsible for approving all changes proposed by the Compliance Officer regarding the current policies, guidelines, methodologies, processes, and procedures.

The process of reviewing and updating the manual will be the responsibility of the Compliance Officer in coordination with the Managerial and Executive Level, taking into account international standards and regulations issued by local authorities in the jurisdictions where there are transactions.

as well as in accordance with changes in the internal policies of BIOFIX BIC.

Annexes Code d

and Ethics Transparency and Anti-corruption Transparency and Business Ethics Program Characterization Compliance SAGRILAFT and PTEE.pdf Risk Matrix 2024.pdf FMT-GC-01-03 Materiality Report Format Biofix 2025 Annex Authorization Format for Data Processing.docx Annex PRO-GC-01-01 Procedure Detection of Suspicious Unusual Operations Annex FMT-GC-01-02 Internal Report Format Unusual Operations

DATE	VERSION NA		OBSERVATIONS
June 2021	1	Initial documentation	
2022	2	Manual update validity	
2023	3	Manual update validity	
2024/12	4	Manual Update valid until 2025	