


Manual of the Comprehensive  
Self-Control and Risk  
Management System for Money  
Laundering, Financing of  
Terrorism and Financing of the  
Proliferation of Weapons of Mass  
Destruction




	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 2 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

**CONTENT**

---

1.	<b>GLOSSARY</b>	<b>3</b>
2.	<b>INTRODUCTION</b>	<b>6</b>
3.	<b>SCOPE OF APPLICATION</b>	<b>8</b>
4.	<b>APPLICABLE REGULATIONS</b>	<b>8</b>
5.	<b>ANTI-MONEY LAUNDERING POLICY, AGAINST THE FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION ALA/CFT/CFPADM</b>	<b>11</b>
6.	<b>ORGANIZATIONAL STRUCTURE AND CONTROL BODIES</b>	<b>18</b>
7.	<b>MECHANISMS AND PROCEDURES FOR COMPLIANCE WITH THE LA/FT/FPADM POLICY</b>	<b>22</b>
8.	<b>STAGES OF SAGRILAFT</b>	<b>24</b>
9.	<b>CONSERVATION OF DOCUMENTATION</b>	<b>25</b>
10.	<b>REQUIREMENTS OF THE AUTHORITIES</b>	<b>46</b>
11.	<b>TRAINING AND DISSEMINATION</b>	<b>33</b>
12.	<b>SANCTIONS</b>	<b>48</b>
13.	<b>WARNING SIGNS</b>	<b>fifty</b>

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 3of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

## 1. GLOSSARY

### Virtual Asset

It is the digital representation of value that can be traded or transferred digitally and can be used for payments or investments. Virtual assets do not include digital representations of fiat currency, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

### DNFBP:

They are the designated non-financial activities and professions of Companies, which for the purposes of this circular are the following: i) real estate agent sector; ii) precious metals and precious stones marketing sector; iii) accounting services sector; and iv) legal services sector.

### HOOPS:

In the event that a quarter passes without the Obligated Company making a ROS report, the Compliance Officer, within ten calendar days following the expiration of the respective quarter, must present a report of "absence of Suspicious Transaction report" or "Hoops" before SIREL, in the corresponding form and terms, in accordance with the instructions of that platform.

### Final beneficiary:

It is the natural person(s) who ultimately owns or controls a client or the natural person on whose behalf a transaction is made. It also includes the person(s) who exercise effective and/or final control, directly or indirectly, over a legal entity or other structure without legal personality. The following are the Final Beneficiaries of the legal entity:

to. Natural person who, acting individually or jointly, exercises control over the legal entity, under the terms of article 260 et seq. of the Commercial Code; either

b. Natural person who, acting individually or jointly, owns, directly or indirectly, five percent (5%) or more of the capital or voting rights of the legal entity, and/or benefits five percent (5%) or more of the income, profits or Assets of the legal entity;

c. When no natural person is identified in paragraphs a and b, the natural person who holds the position of legal representative, unless there is a natural person who has greater authority in relation to the management or direction functions of the legal entity.


The Final Beneficiaries of a trust contract, of a structure without legal personality or of a similar legal structure, are the following natural persons who hold the status of:

Yo. Trustor(s), trustor(s), constituent(s) or similar or equivalent position;

ii. fiduciary committee, financial committee or similar or equivalent position;

iii. Trustee(s), beneficiary(s) or conditional beneficiaries; and

iv. Any other natural person who exercises effective and/or final control, or who has the right to enjoy and/or dispose of the Assets, benefits, results or profits.


	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 4of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

<b>Critical area</b>	It corresponds to all areas in which legal, reputational, operational and/or contagion risks could materialize.
<b>Close Associates</b>	Close associates will be understood as legal entities that have as administrators, shareholders, controllers or managers any of the PEPs listed in the previous definition or that have established autonomous assets or trusts for their benefit, or with whom commercial relations are maintained, to whom due diligence will be applied in accordance with current regulations
<b>Associates/Partners</b>	They are the so-called partners or shareholders, that is, those people who hold ownership of the company quotas, interest parts or shares in a commercial company.
<b>Self-control</b>	It is the will of the employer and administrators to detect, control and manage efficiently and effectively the risks to which the company is exposed.
<b>Critical positions</b>	They are those that, due to their activities, involve possible ML/TF risks.
<b>Counterpart:</b>	It is any natural or legal person with whom the Company has commercial, business, contractual or legal ties of any kind. Among others, counterparties are associates, employees, clients, contractors and suppliers of Company Products.
<b>ML/FT/FPADM Control</b>	<b>Risk</b> It includes the implementation of existing policies, processes, practices or other actions that act to manage the ML/FT/FPADM risk in the operations, negotiations or contracts carried out by the company.
<b>Due diligence</b>	It is conceived as acting to reduce the possibility of being considered guilty of negligence and incurring the respective administrative, civil or criminal responsibilities. It is also considered as the set of processes necessary to make informed decisions.
<b>Enhanced Diligence</b>	<b>Due</b> It is the process through which the Company adopts additional and more intense measures to understand the Counterparty, its business, operations, Products and the volume of its transactions.
<b>Event</b>	ML/TF/FPADM incident or situation that occurs in the company during a particular time interval.
<b>ML/TF/FPADM Factors:</b>	<b>Risk</b> They are the possible elements or causes generating the ML/FT/FPADM Risk for any Obligated Company. The Obligated Company must identify them taking into account the Counterparties, the Products, the activities, the channels and the jurisdictions, among others.
<b>Financing of Terrorism</b>	Terrorist financing includes any support, conspiracy or assistance, directly or indirectly, to obtain funds that will be used in terrorist acts, especially those described in Article 345 of the Penal Code.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 5 of 52
		VERSION: [DOCUMENTVERSION:MN-004]


- Financing the Proliferation of Weapons of Mass Destruction or FPADM**      **the of Mass**      It is any act that provides funds or uses financial services, in whole or in part, for the manufacture, acquisition, possession, development, export, transfer of material, fractionation, transportation, transfer, deposit or dual use for illegitimate purposes in contravention of the national laws or international obligations, when the latter is applicable.
- ML/TF/FPADM risk management**      **risk**      It consists of the adoption of policies that allow preventing and controlling the risk of ML/FT/FPADM
- International Financial Action Task Force – FATF -**      Intergovernmental body established in 1989, whose mandate is to set standards and promote the effective implementation of legal, regulatory and operational measures to combat Money Laundering, the Financing of Terrorism and proliferation and other threats to the integrity of the financial system.
- Risk identification**      The process of determining what can happen, why and how.
- Territorial jurisdiction:**      Geographic areas identified as exposed to the risk of ML/FT/FPADM where the businessman offers or buys his products.
- LA/FT/FPADM**      refers to Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction.
- Money Laundering**      Money laundering is a crime that is committed when seeking to give the appearance of legality to resources originating from illicit activities described in Article 323 of the Penal Code.
- National and international lists**      **and**      List of people and companies that, according to the body that publishes them, may be linked to Money Laundering or Terrorist Financing activities, such as the lists of the United Nations Security Council. Additionally, the OFAC, INTERPOL, National Police lists, among others, can be consulted on the website of the Superintendence of Companies.
- Binding lists**      They are those lists of people and entities associated with terrorist organizations that are binding on Colombia under Colombian law and in accordance with international law.
- ML/FT/FPADM Matrix**      **Risk**      It is one of the instruments that allows a Company to identify, individualize, segment, evaluate and control the ML/TF/FPADM Risks to which it could be exposed, in accordance with the identified ML/TF/FPADM Risk Factors.

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 6 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

- Reasonable Measures** They are sufficient, appropriate and measurable actions in quality and quantity to mitigate the ML/TF/FPADM Risk, taking into account the Obligated Company's own risks and their materiality.
- Monitoring or tracking** It is the continuous and systematic process carried out by obligated subjects, and through which the efficiency and effectiveness of a policy or process is 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 to rectify or deepen execution and to ensure feedback between objectives, theoretical budgets and lessons learned from practice.
- Compliance officer** Official designated by the Board of Directors, in charge of verifying adequate compliance with the policies and procedures adopted for the control and Risk Management of ML/FT/FPADM.
- Attempted operation** It is that obtained when the intention of a natural or legal person to carry out an operation related to an illegal activity is frustrated, through a direct or indirect relationship with the company. These operations must be reported solely and exclusively to the UIAF.
- Unusual operation** Situation that is not related to the normal activities of clients, generating a warning signal for the company.
- Suspicious operation** It is one that, due to its number, quantity or characteristics, does not fall within the normal systems and practices of business, an industry or a specific sector and, furthermore, that in accordance with the uses and customs of the activity in question. , could not be reasonably justified. These operations must be reported solely and exclusively to the UIAF.
- Politically Exposed Persons (PEPs)** It means politically exposed people, that is, they are public servants of any nomenclature and job classification system of the national and territorial public administration, when in the positions they occupy, they have the functions of the area to which they belong or those of the job description they hold, under their direct responsibility or by delegation, the general management, formulation of institutional policies and adoption of plans, programs and projects, the direct management of assets, money or values of the State. These can be through expenditure management, public procurement, investment project management, payments, settlements, administration of real estate and personal property. It also includes Foreign PEPs and PEPs of International Organizations.
- PEP of International Organizations** They are those natural persons who exercise management functions in an international organization, such as the United Nations, Organization for Economic Cooperation and Development, the United Nations Children's Fund (UNICEF) and the Organization of American States, among others. others (vr.gr. directors, deputy directors, members of the Members' Assembly or any person who performs an equivalent function).
- Foreign PEP:** They are those natural persons who perform prominent and distinguished public functions in another country. In particular, the following people:

(i) heads of state, heads of government, ministers, undersecretaries or secretaries of state;

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 7 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

- (ii) congressmen or parliamentarians;
- (iii) members of supreme courts, constitutional courts or other high judicial bodies whose decisions do not normally admit of appeal, except in exceptional circumstances;
- (iv) members of courts or the boards of directors of central banks;
- (v) ambassadors;
- (vi) chargé d'affaires;
- (vii) senior officials of the armed forces;
- (viii) members of the administrative, management or supervisory bodies of state-owned enterprises;
- (ix) members of reigning royal families;
- (x) prominent leaders of political parties or movements; and
- (xi) legal representatives, directors, deputy directors, members of senior management and members of the Board of an international organization (e.g. heads of state, politicians, senior government, judicial or military officials and senior executives of state-owned enterprises ).

**Contractual parties** For JGB, contractual parties are: suppliers, clients, contractors, employees, investors, grantees or any form or person that implies a contractual or commercial relationship with the company.


**Policy** These are the guidelines, orientations or aspects that underpin the prevention and control of ML/TF/FPADM risk in the company. They must be part of the ML/FT/FPADM Risk Management process.

**Unusual Operations Report (ROI)** Report made by the company areas to the Compliance Officer, reporting an unusual operation.

**Suspicious Operations Report (ROS)** Report of a suspicious operation that the Compliance Officer makes to the UIAF.

**ML/TF/FPADM Risk** Financing. It is the possibility of loss or damage that a Company 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 the Proliferation of Weapons of Mass Destruction, or when the concealment of Assets from such activities is intended. The contingencies inherent to ML/FT/FPADM materialize through risks such as Contagion Risk, Legal Risk, Operational Risk, Reputational Risk and the others to which the Company is exposed, with the consequent negative economic effect that this may cause. represent for its financial stability, when it is used for such activities.

**Risks associated with ML/FT/FPADM** Risks through which the risk of ML/TF/FPADM materializes; These are: reputational, legal, operational and contagion

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 8of 52
		VERSION: [DOCUMENTOVERSION:MN-004]


<b>Risk of contagion</b>	It is the possibility of loss that a company may suffer, directly or indirectly, due to an action or experience of a customer, employee, supplier, associate or related party, linked to ML/FT/FPADM crimes. The related or associated includes natural or legal persons who have the possibility of exerting influence over the company.
<b>Inherent risk</b>	Level of risk inherent to the activity, without taking into account the effect of controls.
<b>Legal risk</b>	It is the eventuality of loss incurred by a company, its associates, its administrators or any other related person, when being sanctioned, fined or forced to compensate damages as a result of non-compliance with rules or regulations related to the Prevention of ML/TF.
<b>Operational risk</b>	It is the possibility of being used in ML/TF activities due to deficiencies, failures or inadequacies in human resources, processes, technology, infrastructure or due to the occurrence of external events.
<b>Reputational risk</b>	It is the possibility of loss incurred by a company due to discredit, bad image, negative publicity, true or not, with respect to the institution and its business practices, which causes loss of clients, decrease in income or connection to judicial processes.
<b>Residual risk:</b>	It is the resulting level of risk after applying controls.
<b>SAGRILAFT</b>	It is the self-control and comprehensive risk management system for ML/FT/FPADM established by the Superintendence of Companies.
<b>Warning signs</b>	Particular behaviors of the counterparties and atypical situations that they present in their operations that can conceal operations related to Money Laundering and Terrorist Financing. They are the facts, situations, events, amounts, quantitative and qualitative indicators, financial ratios and other information that the company determines as relevant, from which the possible existence of a fact or situation can be inferred opportunely and/or prospectively. It goes beyond what the company determines as normal.
<b>SIREL</b>	UIAF Online Reporting System
<b>UIAF</b>	Financial Information and Analysis Unit. It is the special administrative unit attached to the Ministry of Finance and Public Credit that aims to prevent and detect Money Laundering operations or the Financing of Terrorism in the different sectors of the Colombian economy.

## 1. INTRODUCTION

The ML/FT/FPADM phenomena are risks that have a great impact on the economy and society, since they constitute tools with which criminal organizations seek to use companies to achieve their illicit purposes. This situation requires that companies participate in its prevention, through the implementation of systems that mitigate this risk.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--



	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 9of 52
		VERSION: [DOCUMENTVERSION:MN-004]

By virtue of the above, it is worth highlighting the Financial Action Task Force (FATF), which is an intergovernmental entity established in 1989, whose objective is to set standards and promote the effective implementation of legal, regulatory and operational measures to combat money laundering, assets, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, and other threats to the integrity of the international financial system. Its recommendations constitute a complete and consistent international scheme of measures that countries should implement adapted to their particular circumstances to combat these crimes.

Consequently, and taking into account the socio-economic reality of the country, the Superintendency of Companies, through the powers of surveillance and control of companies in the real sector, has required the implementation of the comprehensive risk prevention and control system for Money Laundering, Assets, Financing of Terrorism and Proliferation of Weapons of Mass Destruction.

The fundamental objective of the System of Self-Control and Comprehensive Management of the Risk of Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (hereinafter SAGRILAFT) is to minimize the possibility that, through the different activities of the company, introduce resources from money laundering, finance terrorism or the proliferation of weapons of mass destruction

This manual, which has the approval of the Board of Directors of JGB (hereinafter JGB or the company), constitutes one of the documents that ensures the proper development and compliance of the system and contains the general structure, procedures and policies . to effectively identify, measure, control and monitor the risk of Money Laundering, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction (ML/TF/FPADM).

The purpose of this Manual is to establish the procedures under which JGB operates for the prevention of the risk of money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction (hereinafter ML/TF/FPADM), taking into account as a system, the prevention, detection, control and reporting of unusual or suspicious operations.

This manual will be general knowledge and will be updated by the Compliance Officer in accordance with the needs of the company and regulatory developments.

The System has had evolutions indicated by the Superintendence of Companies, which have been incorporated in Chapter X of the basic legal circular.


## 2. Area of application

This manual is part of the Comprehensive Self-Control and Risk Management System for Money Laundering, Financing of Terrorism and Proliferation of Weapons of Mass Destruction that JGB has implemented, it is applicable to all the company's workers and all the processes in which ML/TF/FPADM risk factors arise and is composed of: stages, methodologies, policies, procedures developed by the company, functions (of the administration and management bodies, of the Compliance Officer, of the control bodies), and in general all the regulatory elements required by the Superintendence of Companies.

This Manual includes the operational aspects and procedures that must be carried out to ensure adequate compliance with what is established in the regulatory framework for self-control and comprehensive risk management of ML/TF/FPADM and with the policies established in this Manual to achieve this end. Therefore, all JGB workers are obliged to comply with this manual and the internal and external regulations that arise from it, specifically those whose activities are especially related to:

- Acceptance and binding of contractual parties (customers, suppliers and contractors)

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 10 of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

- Acceptance and engagement of employees.
- Treasury Operations.
- Foreign trade operations.
- Making donations in money or kind.
- Management of materials and products.
- Commercial agreements or agreements.

JGB must ensure correct compliance with internal and external regulations in relation to self-control and comprehensive risk management of ML/FT/FPADM, incorporating said policies and regulations into its work procedures. In the event of a conflict between internal and external regulations, those that establish the most stringent requirements will always prevail.

Critical areas identified according to JGB's operation and business

As part of JGB's operations in the daily development of its businesses and the roles played by each of the areas of JGB, the following areas are identified as the most susceptible to materialization of the risk of ML/TF /FPADM, these areas called "criticisms" are obliged to strictly comply with the controls described in this document. Without prejudice to the above, all JGB collaborators must fully comply with the provisions of this Manual, referring to the obligation of communication and/or information of suspicious or unusual operations of which they are aware, and other obligations contained in this document.

The critical areas identified are:

- Financial services – Treasury and portfolio
- People and Organization
- Services and Security
- Commercial
- Planning and purchasing
- Legal
- LogisticsWarehouse

### 3. Regulations and applicable legislation


This Manual is based on compliance with current Colombian legislation on self-control and comprehensive risk management of ML/FT/FPADM and will be executed in accordance with the JGB Transparency and Business Ethics Program . Thus, this manual is based in particular on the following laws, and any that modify, add or replace them .

#### 4.1. INTERNATIONAL

Regarding ML/FT/FPADM risk, Colombia, through various laws and rulings of the Constitutional Court, has ratified the following United Nations conventions and agreements, in order to confront criminal activities related to Money Laundering and Financing of Terrorism:

- Vienna Convention of 1988: United Nations Convention against Trafficking in Narcotic Drugs and Psychotropic Substances. (Approved by L. 67/93 - Sent. C-176/94).
- United Nations Convention for the Suppression of the Financing of Terrorism of 1989. (Approved by L. 808/2003 - Sent. C-037/2004).

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 11 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

- Palermo Convention of 2000: United Nations Convention against organized crime. (Approved by L. 800/2003 - Sent. C-962/2003).
- Mérida Convention of 2003: United Nations Convention against corruption. (Approved by L. 970/2005 - Sent. C-172/2006).

In addition to these Conventions and treaties, in 1990, the Financial Action Task Force (FATF) designed forty (40) recommendations to prevent money laundering and subsequently established nine (9) special recommendations against the financing of terrorism.


#### 4.2. NATIONAL

- Law 222 of 1995 dictates the imposition of sanctions related to non-compliance in matters of ML/FT.
- Law 1121 of 2006 Terrorism Financing Regulations
- Law 526 of 1999 by which the UIAF is created
- Law 599 of 2000 by which the Penal Code is adopted
- Law 1474 of 2011 by which the Anti-Corruption Statute is adopted
- Law 1621 of 2013 by which Law 526 of 1999 is updated.
- Law 1708 of 2014: new domain extinction law and its practical effects on ill-gotten assets
- Decree 1674 of 2016 by means of which the Politically Exposed Persons -PEP- are indicated, referred to in article 52 of the United Nations Convention Against Corruption.
- Decree 1068 of 2015 article 2.14.2, which provides that public and private entities belonging to sectors other than finance, insurance and stock exchange, must report Suspicious Transactions to the UIAF, in accordance with literal d) of numeral 2 of article 102 and articles 103 and 104 of the Organic Statute of the Financial System, when said Unit requests it, in the manner and opportunity indicated to them.
- Law 1778 of 2016 by which rules are issued on the responsibility of legal entities for acts of transnational corruption and provisions are issued regarding the fight against corruption.
- Basic Legal Circular of the Superintendence of Companies Chapter External No. 100-000015 of September 24, 2021.

#### **4. ANTI-MONEY LAUNDERING POLICY, AGAINST THE FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION ALA/CFT/CFPADM**

JGB SA is committed to complying with the regulations that are integrated into the SAGRILAFT Comprehensive Risk Management and Self-Control System for Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction, with the fundamental objective of protecting the company so that it is not used as a means for money laundering, financing terrorism and/or financing the proliferation of weapons of mass destruction, related activities or source crimes. Therefore, we will refrain from linking counterparties or strategic partners that are on binding lists, we will be careful with those that appear on informative (non-binding) lists due to processes that link them in criminal activities or associated with ML/TF/FPADM, and that may affect the company's reputation or possible risk of contagion. An attempt will be made to terminate legal or any other type of relationship with the natural or legal persons that appear on said lists, or to determine possible suspicious operations during the development of contractual activities and through due diligence. In accordance with the above, JGB SA will carry out the disclosure, monitoring and permanent control of all actions that lead to mitigating the legal, reputational and operational risk of contagion.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 12 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

## 5. ORGANIZATIONAL STRUCTURAL AND CONTROL BODIES

The company has the appropriate structure taking into account its size and operations to support the effective and efficient management of ML/FT/FPADM risk.

### ROLES AND RESPONSIBILITIES

#### 6.1. Steering Committee


In order to establish internal work mechanisms and allow accurate decision-making and in light of the regulations and ML/FT/FPADM prevention mechanisms, the compliance officer will bring to the Steering Committee the cases and/or developments that arise. consider relevant.

The Compliance Officer may invite whomever he deems appropriate to the Committee, as long as it is related to the topics or cases to be submitted for consideration.

Taking into account the above, in the event of cases, communications and/or news that are raised to the Steering Committee, the members of the Committee, together with the Compliance Officer and guests, if any, must make the pertinent decisions in accordance with the provisions of this Manual in the event of operations that have been considered “unusual” carried out with counterparties, establish policies, standards, procedures, modifications and controls regarding the Prevention of ML/TF/FPADM.

#### 6.2. Board of Directors

- a. Establish the policies of the Self-control and Management System for the Risk of Money Laundering and Terrorist Financing.
- b. Approve the SAGRILAFT Manual and its modifications and/or updates
- c. Approve the appointment of the main and alternate Compliance Officer.
- d. Decide on reports related to ML/FT/FPDAM, presented by the Compliance Officer.
- e. Timely analyze the reports and requests presented by the Legal Representative.
- f. Rule on the reports presented by the statutory auditor or the internal and external audits, which are related to the implementation and operation of SAGRILAFT, and follow up on the included observations or recommendations. This monitoring and its periodic progress must be indicated in the corresponding minutes.
- g. Organize and guarantee the technical, logistical and human resources necessary to implement and keep SAGRILAFT in operation, according to the requirements made for this purpose by the Compliance Officer.
- h. Establish the criteria to approve the Counterparty connection when it is a PEP.
- i. Establish guidelines and determine those responsible for carrying out audits on the compliance and effectiveness of SAGRILAFT if so determined.
- j. Verify that the company, the Compliance Officer and the Legal Representative carry out the activities designated in Chapter X of the basic legal Circular and in SAGRILAFT.

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 13of 52
		VERSION: [DOCUMENTVERSION:MN-004]

**6.3. Legal Representative (main and alternate)**

- a. Submit the SAGRILAFT Manual and its updates for approval by the Board of Directors, in coordination with the Compliance Officer.
- b. Adopt appropriate measures in response to the result of the evolution of risk profiles and associated risks.
- c. Provide technological, human and physical resources necessary for the implementation of the system.
- d. Provide reports to the Board of Directors on the implementation, development and progress of the ML/FT/FPDAM System, based on the reports of the Compliance Officer.
- e. Provide effective, efficient and timely support to the Compliance Officer in the design, direction, supervision and monitoring of SAGRILAFT.
- f. Verify that the Compliance Officer has the availability and capacity necessary to carry out his or her duties.
- g. Present to the Board of Directors the reports, requests and alerts that you consider should be processed by said bodies and that are related to SAGRILAFT.
- h. Ensure that the activities resulting from the development of SAGRILAFT are duly documented, so that the information meets criteria of integrity, reliability, availability, compliance, effectiveness, efficiency and confidentiality.
- i. Certify before the Superintendency of Companies compliance with the provisions of Chapter X of the basic legal circular, when required by the Superintendency of Companies.
- j. Verify that SAGRILAFT procedures develop the ML/FT/FPADM Policy adopted by the Board of Directors.


**6.4. Compliance officer**

He will be designated by minutes by the JGB Board of Directors who will be internally responsible for monitoring ML/FT/FPDAM risk management. The Compliance Officer must have the professional behavior, experience and knowledge appropriate to perform the functions of his or her position.

The compliance officer's main functions are the following:

- a. Ensure the effective, efficient and timely operation of SAGRILAFT
- b. Promote the adoption of correctives and system updates. when circumstances require it and at least once every two (2) years. To do this, you must present to the board of directors the proposals and justifications for the correctives and updates suggested to SAGRILAFT.
- c. Lead the development of internal training programs on ML/TF/FPADM matters
- d. Evaluate the reports presented by the internal audit or whoever performs similar functions or takes its place, and the reports presented by the Statutory Auditor or the external audit, if applicable, and adopt Reasonable Measures against the reported deficiencies. If the measures to be adopted require authorization from other bodies, you must ensure that these matters are brought to the attention of the competent bodies.
- e. Certify before the Superintendency of Companies compliance with the provisions of the regulations, as required by the control entity
- f. Ensure the proper archiving of documentary supports and other information related to the prevention and management of the risk of ML/FT/FPADM, using technological programs for information and/or archiving (emails, documents in digital format, etc. )
- g. Design the methodologies for segmentation, identification, measurement and control of ML/TF/FPADM risk that will be part of SAGRILAFT
- h. Report suspicious operations to the UIAF and any other report required by current provisions, as established by said regulations and Chapter X of the basic legal circular.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 14 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

- i. Present, at least once a year, reports to the board of directors or, failing that, to the highest corporate body. At a minimum, the reports must contain an evaluation and analysis of the efficiency and effectiveness of SAGRILAFT and, if applicable, propose the respective improvements. Likewise, demonstrate the results of the management of the Compliance Officer, and of the Company's administration, in general, in compliance with SAGRILAFT and, in such case, propose ideas for improvements.
- j. Verify compliance with the Due Diligence and Enhanced Due Diligence procedures applicable to the company.
- k. Carry out the evaluation of the ML/FT/FPADM Risk to which the company is exposed.
- l. Lead meetings and training that are associated with ML/FT/FPADM Risk Management, convened by the competent authorities, for consultative or informative purposes, whenever possible.
- m. Conduct massive annual validations of counterparties on binding lists .
- n. Share and submit for consideration for decision-making the operations that have been classified as unusual, before the Steering Committee

**6.5. Process Leaders**


- a. Support the Compliance Officer in the monitoring and compliance of policies, through the controls and personnel under his/her charge.
- b. Report to the Compliance Officer any unusual, attempted or suspicious operation that your process identifies.
- c. Do not allow or link counterparties without fulfilling the requirements, as the case may be: Client, supplier, partner or employee.
- d. Attend the ML/TF/FPADM risk identification sessions that are scheduled by the Compliance Officer.
- e. Actively participate in the meetings or conferences required by the Compliance Officer to determine action plans on ML/FT/FPADM matters.
- f. Update customer, supplier or employee data as appropriate when circumstances require it or at least every two years.
- g. Support the Compliance Officer to raise awareness among employees in each area of the ML/FT/FPADM risk prevention culture.
- h. Carry out the activities that the Compliance Officer requires for the adequate and preventive ML/TF/FPADM prevention system.
- i. Notify the Legal Representative of any inconsistency that is evident in the management of SAGRILAFT and that has not been addressed by the Compliance Officer.

**6.6. Other collaborators**

- a. Given the ethical principles that the Company professes, the policy that governs its operations and the philosophy on which it is based, all business carried out by the Company's employees on its behalf will be done with absolute transparency and seriousness.
- b. The main duty of the Company employee is to maintain a strict commitment to the policies of transparency, control and prevention of money laundering and financing of terrorism established by the Company. Know the provisions established by law on the risk of ML/FT/FPADM.
- c. preventing money laundering , financing of terrorism and/or financing of the proliferation of weapons of destruction from materializing through the operations carried out. massive.
- d. Comply with the principles and standards of conduct taught in the manual and through its internal work regulations.
- e. Put observance of ethical principles before achieving business goals.
- f. Report unusual and suspicious transactions to the Compliance Officer.

**6.7. Audit**

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 15of 52
		VERSION: [DOCUMENTVERSION:MN-004]

- a. Evaluate the effectiveness and compliance of the Comprehensive Self-Control and Risk Management System for Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction. The result of the internal audits must be communicated to the legal representative, the Compliance Officer and the Board of Directors.

**6.8 . Tax Auditor**

The functions of this body are expressly stated in the law, in particular article 207 of the Commercial Code, which especially points out the obligation to report Suspicious Transactions to the UIAF, when they are noticed within the business. ordinary part of their work, as stated in paragraph 10 of said article.

For the purposes of the provisions of paragraph 10 of article 207 cited, the tax auditor must request a username and password in the SIREL administered by the UIAF, to send the STRs.

In any case, the tax auditor, despite the obligation to maintain professional reserve in everything he knows due to the exercise of his profession, by virtue of the responsibility inherent to his functions and in accordance with the cases in which said reserve may be lifted, has the duty to disclose information when required by law. Thus, for example, when in the course of his work a tax auditor discovers information that leads to suspicion of possible acts of ML/FT/FPADM, he has the obligation to refer these suspicions to the competent authority.

Likewise, it must be taken into account that tax auditors are covered by the general duty to report to which citizens are subject (article 67 CPP12).

Additionally, paragraph of article 10 of Law 43 of 1990 establishes the following:

“(…) Public accountants, when they grant public faith in accounting matters, will be assimilated to public officials for the purposes of criminal sanctions for the crimes that they commit in the exercise of the activities of their profession, without prejudice to civil responsibilities that may arise in accordance with the laws (…)”.

“25. Report crimes, contraventions and disciplinary offenses of which you have knowledge, except for legal exceptions.”

To fulfill his duty, the tax auditor, in the analysis of accounting and financial information, must pay attention to the indicators that may give rise to suspicion of an act related to a possible ML/TF/FPADM. It is suggested that you take into account the International Auditing Standards NIA 200, 240 and 250 and consult the Guide on the role of the tax auditor in the fight against transnational bribery and ML/FT/FPADM, available on the Superintendency's website. .


**6. MECHANISMS AND PROCEDURES FOR COMPLIANCE WITH THE LA/FT/FPADM POLICY**

**DESIGN AND APPROVAL**

JGB will have the necessary resources, whether operational, economic, technological and other measures necessary for the efficient and proper functioning of SAGRILAFT, which was designed to suit the needs and size of the company.

Both the design and updates of the system will be under the responsibility of the Board of Directors together with the Legal Representative and Compliance Officer. Each adjustment or update that SAGRILAFT warrants must be recorded in the minutes, if required by the control and surveillance entities.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

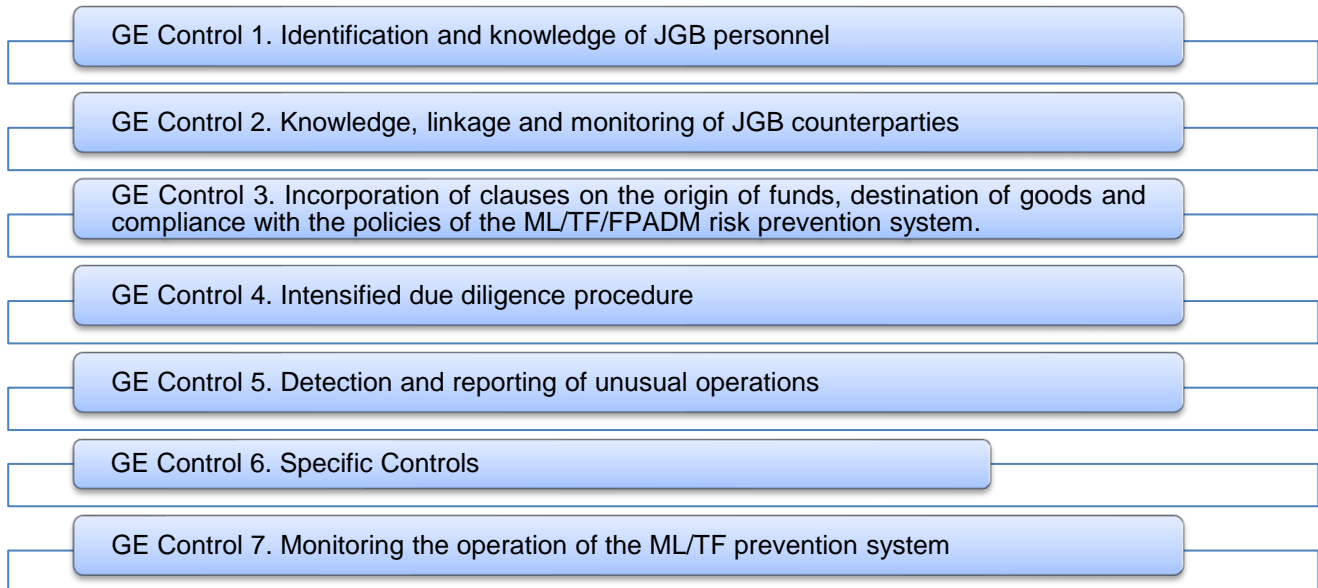
	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 16 of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

To comply with the policy, the following guidelines must be followed, which tend to promote at an institutional level the culture regarding Self-Control and Comprehensive Risk Management of ML/FT/FPADM, therefore, it is the duty of the legal representative, directors, administrators and JGB employees ensure compliance with internal regulations and other provisions related to this Manual.

The controls defined to prevent the risk of ML/TF are the following:

### 7.1. General Controls

The general controls defined for JGB are:



Each of the critical areas must define the person or persons responsible who must carry out the validation control in the binding lists for Colombia and public databases of the counterparties corresponding to their process. If a match is found on any of the binding lists, the person in charge of carrying out the search must immediately inform the compliance officer by email, who in turn will give his opinion regarding whether JGB will be able to bind the counterparty or if he must defect from the same. In any case, the respective Area will inform the counterparty of the decision made regarding their connection.


#### 7.1.1. Control GE 1 Knowledge and involvement of JGB staff

The People and Organization area, in company with the JGB Security Department, will apply the controls directed to the security study, personnel audit and consultation in binding lists and public databases, each time the feasibility of hiring a possible employee for JGB.

Knowledge of the Employees allows the Company to obtain information about the basic characteristics of potential employees before being linked, so the people in charge of the links are obliged to follow all the procedures provided and necessary to

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--



	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 17 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

achieve adequate knowledge of the Employees. employee candidate, even when they are referenced or recommended people. All controls established in relation to ML/FT/FPADM risk must be complied with.

Prior to linking a candidate, the People and Organization area, directly or through its service providers, will carry out the consultation on binding lists for Colombia and no candidate will be hired until the matches are validated, in case of exist, and the relevant risk analysis is carried out by the Compliance Officer. The third party in charge of security studies must follow its internal guidelines and proceed in accordance with the law and regulations, if applicable, and inform the area in charge at JGB about the coincidences found.

No candidate or employee is exempt from the provision of information contemplated in the formats and procedure for employment relationships.

If the hiring of personnel for JGB is carried out through a temporary company, it must certify that it has consulted binding lists of the employee during the selection process and that the result obtained is negative. In the event that the temporary company does NOT carry out consultations on lists binding for Colombia of workers who intend to join JGB, the company, through the People and Organization department, will be in charge of making the respective consultation, under penalty of the impossibility of continue with the process of linking the collaborator JGB, head of the People and Organization area, reserves the right to admit and/or hire people involved with any crime, and the area in charge will have the power to prevent access to the facilities of JGB personnel of contractors who are related to ML/TF/FPADM crimes, and will communicate these findings to the Compliance Officer.

The follow-up and monitoring for the prevention of ML/FT/FPADM risks of collaborators will be the responsibility of the People and Organization area and the Compliance Officer, who will ensure that active employees are consulted on binding lists at least annually.

In the event that the People Organization area directly carries out the security study, personnel audit and consultation on binding lists and matches are found on any of the binding lists, the Compliance Officer must be informed, who in turn will give its opinion regarding whether JGB will be able to carry out the contract, or failing that, it will have to abandon it; In this case, the Compliance Officer will inform the area in charge so that they can proceed to cancel the negotiations.

In accordance with the policies adopted by the Company, the People and Organization area will update employee data at least once a year.

All employment contracts incorporate clauses on the origin of funds and the use and destination of goods and compliance with the ML/FT/FPADM business ethics and risk prevention program.


### 7.1.2. Control GE 2 Knowledge, linkage and monitoring of JGB counterparties

Before establishing a legal or contractual relationship with a counterparty, in addition to the procedures for evaluation, selection and creation of counterparties (clients, suppliers, others) that JGB carries out, each of the areas in charge of these processes must execute the actions pertinent in accordance with the provisions of this Manual, and in the Function Manual of each position, in accordance with what is related to SAGRILAFT

The documents requested for the knowledge and connection of JGB counterparts will be:

- a. Identification of natural person. The following information will be requested from the counterparty:
  - Full name and surname

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 18of 52
		VERSION: [DOCUMENTOVERSION:MN-004]


- Identification number: Copy of the RUT, citizenship card (nationals), immigration card or passport (foreign).
  - Full name and surname of the representative, representative and identification number (if applicable) .
  - Residence address and telephone number
  - Description of activity: Main economic activity: commercial, industrial, transportation, construction, agribusiness, financial services, etc., in accordance with the provisions of the current ISIC international code.
  - Declaration of origin of goods and/or funds
  - Identification of the bank account(s) through which you will operate and bank certification of the account.
  - Authorization for consultation and reporting to risk centers
  - Form of payment for foreign trade operations identifying the means (if any)
  - Signature Date of completion
- b. Identification of legal entities . Legal entities must present documents that prove their name, company name, address and corporate purpose. As well as the respective certificates of existence and legal representation or documents that act in their place and the respective powers in case they act through attorneys-in-fact. Legal entities domiciled abroad will have to present the same or similar documents according to the legislation of each country.

Thus, the following information will be requested from legal entities:

- Business name
- Identification number: Copy of the RUT, citizenship card (nationals) or immigration card (foreigner) .
- Full name and surname of the legal representative, representative and identification number,
- Description of activity: Main economic activity: commercial, industrial, transportation, construction, agribusiness, financial services, etc.
- Address, telephone number, and city of the main office and the branch or agency .
- Certificate of existence and legal representation, or Power of Attorney deeds of the people acting on your behalf.
- Shareholder composition and identification of shareholders or associates who directly or indirectly hold more than 5% of the share capital, contribution or participation.
- Declaration of origin of the assets and/or funds.
- Declaration on the prevention of money laundering and financing of terrorism and proliferation of weapons of mass destruction.
- Beneficiary declaration of their status as PEP and identification of their relatives up to the second degree of consanguinity, second degree of affinity and first civil degree.
- Way to pay
- Identification of the bank account(s) through which it will operate and bank certification of the account, indicating the city in which it is located.
- Certified Financial Statements.
- Authorization for consultation and reporting to risk centers
- Form of payment for foreign trade operations identifying the means (if any)
- Signature and Date of completion

If the client or supplier is domiciled abroad, the equivalent documentation or necessary information will be collected and analyzed to validate the data described above.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 19of 52
		VERSION: [DOCUMENTVERSION:MN-004]

The initial knowledge of the counterparties will be understood as part of the due diligence and if at any time during the contractual relationship with JGB greater knowledge of these third parties is required, intensified due diligence must be carried out.

Thus, in the verification of the documents and data requested within the counterpart creation processes, each of the areas in charge must carry out a study of the documentation in light of this Manual and the objective of minimizing the risk of contagion. of activities related to money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction. In addition to the above, they must carry out at least one verification in lists binding for Colombia and public databases , making use of the technological and information resources that the Company provides, in which the background of the counterparties with which they are identified. A relationship is intended, whether these are natural and/or legal persons.

If the counterparties are legal entities, verification must be carried out in binding lists and public databases of:

- The company name of the legal entity
- Legal representatives
- Shareholders, partners or associates who have a participation in the capital stock equal to or greater than five percent (5%). In this case, the final beneficiary (natural person) must be reached; it is the duty of the Process Leaders to ensure that the final beneficiary is identified and leave evidence of the management carried out. In the extreme case in which it has not been possible to identify the final beneficiary, the Legal Representative of the Company to be linked must be taken as such.
- Of the other natural or legal persons, which appear in the document that certifies the existence of the counterparty. (Certificate of existence and legal representation or similar) which must be valid for no less than 30 days. In any case, the final beneficiary must be informed.

If matches are found with restrictive lists for Colombia, the relationship with the third party should not be formalized and the Compliance Officer must be notified by email sending evidence of the match. When the match is with another list, the Compliance Officer must be consulted about the action to follow.

To understand, link, monitor and update counterparts, the area in charge must:


- Identify the legal origin of the resources
- Request linking information from the counterparty: identification, economic and/or financial information and any other information that the critical area considers necessary, according to the activity carried out by the counterparty and location area, and the documents determined by the policies and procedures of the counterparty. JGB.
- Verify the identity of the counterparties, according to what is specified in this Manual, especially in the following section.
- Verify and confirm contact details and economic activity

In the event that a counterparty is reluctant to provide information and documentation required for its connection, this will immediately be taken as a warning signal for its non-connection with JGB, a circumstance that must be reported to the Compliance Officer so that the latter can evaluate the viability of the link.

#### 7.1.2.1. Verification of requested information

The critical area in charge will carry out procedures to verify the veracity of the identification documentation provided by the client/supplier, therefore, JGB reserves the right to request the documentation in original and copy when it deems necessary.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 20of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

The critical area in charge may carry out the consultations that it considers necessary in order to ensure and mitigate possible risks associated with Money Laundering, Financing of terrorism and Financing of the proliferation of Weapons of Mass Destruction.

From the moment the commercial relationship with the counterparty begins, the counterparty must declare the origin of the funds involved in the commercial relationship, by signing contractual clauses on the origin of funds and/or any other document that has this objective.

For those counterparties with whom there are contracts, the termination and/or suspension clause of the contractual or commercial relationship must be maintained when, as a result of intensified due diligence, circumstances of possible reputational risk or contagion for JGB are demonstrated.

**7.1.2.2 Identification of politically exposed persons – PEPs**

The involvement of any client, supplier and/or contractor called and/or identified as Politically Exposed Persons – PEP's, must have the approval and/or approval of the Legal Representative, because national and international experience has shown that they are third parties more prone to money laundering, therefore, the official who assists them must keep in mind that exceptions of information and documentation are not allowed for their connection, and furthermore, their connection is subject to the prior express and formal decision of the Legal Representative.

The identification of these people is initially contemplated in the forms that are filled out by clients, suppliers, employees and shareholders, so this information is based on good faith; However, the critical areas in charge may use the additional necessary resources for the identification and management of contractual activities that may be had with politically exposed persons. These activities are described in greater detail in the PEP linking procedure. It should be noted that, through the counterpart linking format, the third party is requested to identify whether or not they are PEP's and, if so, also identify their relatives up to the second degree of consanguinity, second degree of affinity or first civil relationship. However, through list queries, there is a list of PEPs, which will allow us to see if the third party is providing reliable information regarding their quality of PEPs, or not, through the form.

Likewise, authorization from the Area Director will be required to link a Publicly Exposed Person, that is, a natural person who enjoys public recognition and/or is considered an opinion leader.


In the event that the critical area identifies a match in the verification of binding lists, or finds an unusual operation in the process of knowing, linking and monitoring counterparties, it must immediately inform, by email, the Compliance Officer, who will analyze the feasibility of continuing or not the relationship with the counterpart, in accordance with the procedures established in this Manual.

Annually, each of the critical areas will carry out mass consultations in binding lists and public databases of counterparties and will share the results with the Compliance Officer, who will analyze them to minimize the risk of contagion ; In turn, each of the areas will update the information of third parties, in accordance with the provisions of the customer and supplier procedures that apply to them.

The updating of critical suppliers <sup>1</sup>will be carried out in accordance with the Procedure, selection, linking and updating of suppliers (annually) and the critical area in charge must carry out a complete validation (all natural or legal persons that appear in the creation documents, updated) on lists. binding, and inform the Compliance Officer if matches are found in the search.

<sup>1</sup>They are those suppliers that, due to the complexity of their operation, affect the risk of business continuity and are not easily replaceable immediately.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 21 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

Preferably, logistics and transportation operation agreements will be established only with companies that have ISO 28000 certification or are AEO Authorized Economic Operators.

For all donations that the Company intends to make, whether or not they require approval by the Board of Directors, the general management assistant must verify the information of the grantees prior to the donation, in binding lists and inform the Compliance Officer if necessary . to find a match.

### 7.1.3. Control GE 3 Incorporation of ML/FT/FPADM prevention clauses

The Legal Area must guarantee that in all contracts made by JGB, clauses for money laundering and financing of terrorism and/or financing the proliferation of weapons of mass destruction are incorporated, any other clauses that are considered necessary to ensure the due process. diligence in the lawful relationship with third parties.

If there is no contractual document, the purchasing and/or commercial area will require a certification of the origin of funds from all suppliers and clients.

### 7.1.4. GE Control 4 intensified due diligence procedure.

Commercial operations may not be carried out with counterparties (natural persons) that are not duly identified or counterparties (legal entities) that are not legally constituted.

Part of simple due diligence will be each defined mechanism that allows identifying, managing and monitoring ML/FT/FPADM risks, and keeping the counterparty, product, distribution channel or jurisdiction at low risk.

All areas of JGB that carry out relations with counterparties in the event of determining, in accordance with the provisions of this Manual and at their discretion, an operation as unusual or an operation of which it is not certain that it is not related to an ML/FT/FPADM event, you must immediately report it to the Compliance Officer through the established channels.


Some unusual or suspicious situations that may trigger heightened due diligence are:

- Matching on binding lists.
- Determination that the financial information presented presents inconsistencies
- That the counterparty to be linked is or has been investigated or sanctioned for corruption or bribery processes.
- Events in which a Legal Entity or natural person counterpart, after being linked to JGB, is investigated or linked in any process for illegal acts
- If the counterparty, its final beneficiaries and/or its administrators are identified as PEP
- If the counterparty and/or its final beneficiaries are in non-cooperative countries and high-risk jurisdictions.
- The others considered by both the Compliance Officer and each of the process leaders.

To carry out intensified due diligence, the following will be taken into account:

- Due diligence may have a different focus depending on whether the third party presents an alert from the perspective of bribery, corruption, money laundering, terrorist financing or proliferation of weapons of mass destruction.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 22 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

- If a third party represents a greater risk or if warning signs are identified, consideration may be given to sending the third party to complete questionnaires or certification regarding the possible situation.
- When a charitable donation approved by the Board of Directors is to be made, the information known to the third party must be expanded to identify the final beneficiaries.
- The warning signs in the SAGRILAFT manual must be considered.
- The evaluation of the linking of counterparties based on the analysis of the DDI will initially be the Compliance Officer's responsibility, and if he considers it pertinent, he will put the case under consideration of the Steering Committee, who will make the final linking decision.
- All DDI documents must be kept under the necessary security and will be kept for at least 10 years.
- The Compliance Officer must contact the UIAF if more information is required.
- The information obtained during the process may not be disclosed to third parties.

The Compliance Officer will evaluate the information and carry out intensified due diligence on the counterparty validation service provider, and together with the area in charge and/or the Steering Committee, they will define the need to exercise any of the following actions, as a due diligence plan. intensified diligence:


- Interviews and/or visits to contractor suppliers and/or clients.
- Periodic updating of information and documentation. The periodicity of the information will be defined by the Compliance Officer and the critical area must carry out the update. In the event that any supplier or client of this type does not update the information, this fact will be automatically interpreted as a "warning signal."
- Signature of the supplier or client on the registration form.
- Linking, continuation or termination of the relationship with the counterparty.
- Preparation of Suspicious Operation Report (ROS)
- Preparation of management reports for the Board of Directors.
- Design, execution and monitoring of action plans that are necessary to mitigate the risk that generates the alert signal.
- Archive of all documentation arising in the due diligence process.

For activities related to reports, reports, design of action plans and documentation filing, the person responsible will be the Compliance Officer. A written record of the completion of each of them will be left with the pertinent supports.

In the case of Politically Exposed Persons PEPs, if required, the following must be done:

- Approval of the connection must be obtained from the Legal Representative and monitoring procedures of its most demanding operations will be carried out.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 23of 52
		VERSION: [DOCUMENTOVERSION:MN-004]


- If the PEP is a shareholder, member of the Assembly of Partners or Board of Directors, if the Steering Committee so considers, it may request statements signed by them certifying that they are not immersed in situations of bribery, corruption, money laundering, financing of terrorism, or financing the proliferation of weapons of mass destruction.
- Obtain sufficient information from the counterparty (partner, customer, supplier, contractor, employee) and verify publicly available information to determine whether or not the customer is a PEP.
- In the Customer, Suppliers-Contractors knowledge form, the third party must record whether it has PEP status.
- Check your reputation in public sources.
- Investigate the source of your funds through the information recorded in the knowledge format and the requested supports.
- Obtain approval from the Legal Representative before engaging (or continuing, in the case of existing suppliers or contractors)
- If a PEP is accepted as a client, supplier or contractor, continuous supervision of the contractual relationship must be carried out.
- In case of being a Publicly Exposed Person, the director of the area in charge must approve the connection, and carry out the same controls to be carried out in case of PEP connection.

In the case of knowledge of partners or shareholders, the pertinent thing will be:

- If the new shareholder or partner is a legal entity, the final beneficiary must be identified.
- Consult lists of the new shareholder or partner.
- Legal entities and natural persons must be consulted. In the case of legal entities, the final beneficiary must be identified.
- It must be left annexed to the query in lists.
- If identified on binding or informational lists, any matches must be reported to the Compliance Officer.
- The Compliance Officer must manage the situation with senior Management and the Steering Committee and will provide support for said management.
- If the future partner or shareholder is a PEP, the provisions for the knowledge and connection of PEPs will apply, in addition to what refers to the due diligence necessary for people who hold such status.

At the time of linking suppliers and/or contractors that impact secure trade (Logistics Operators, packaging suppliers that manage JGB logos, IT suppliers that guard or have access to business information), they may be carried out selectively and according to the level of risk they represent, audits and/or visits by the area in charge, in order to validate aspects of security and interest, in accordance with JGB requirements .

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 24of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

**7.1.5. Control GE 5 Detection, analysis, communication and reporting of operations that may be linked to ML/FT/FPADM**

The owners of control and monitoring of the contractual parties are those employees who carry out operations with third parties, who must know the particular characteristics of the economic activities and the transactions they carry out; especially those related to the areas of Purchasing, Commercial, Logistics and other critical areas.

Unusual operations are considered to be those that may be outside the Market in which companies or individuals operate, generating a "Warning Signal" that is described in this manual.

Likewise, the critical area responsible for the process must consider as an "Unusual Operation" that operation whose amount or characteristics are not related to the economic activity of the contractual party, or those that do not fall within the normal systems and practices of the businesses of a specific industry or sector.

When the person responsible for the process detects an alert signal or unusual operation, they must immediately report to the Compliance Officer, through the email account oficialdecumplimiento@jgb.com.co, attaching all relevant information and documentary evidence that supports the signal. alert or unusual operation. In accordance with the management carried out by the Compliance Officer, in the company of the reporting party, if required, the Compliance Officer, if deemed necessary, will convene the Steering Committee and record the management and action plans to be taken through the format F-GF-06- 0 "*Internal reporting format for unusual operations* | "


The JGB official who detects an unusual operation will refrain from executing the operation and will immediately inform, through the communication channels provided, the Compliance Officer, who will send the corresponding acknowledgment of receipt to the communicating employee.

In any case, the compliance officer must be notified:

- Any operation carried out by a natural or legal person that, due to its number, quantity or characteristics, does not fall within the normal business systems and practices of a specific industry or sector and that, in accordance with the uses and customs of the activity in question, could not be reasonably justified.
- Any relevant information on the management of assets or liabilities or other resources, whose amount or characteristics are not related to the economic activity of its clients or suppliers, on transactions of its users that due to their number, the amounts traded or the particular characteristics of They may reasonably lead to suspicion that they are using the entity to transfer, manage, take advantage of or invest money or resources coming from criminal activities or intended for their financing.
- When it is detected that the nature or volume of a client's active or passive operations does not correspond to their activity or operational history, in accordance with the client profile established at the time of initiating the business relationship.
- Any change in customer or supplier behavior, such as:
  - a. Changes in the bank account from which you operate or to which you request the corresponding payments to be made, without prior communication and without sending the bank certification required for this purpose;
  - b. Sending payment from or requesting it to a tax haven;

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--



	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 25 of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

- c. Sending payment from or requesting it to a country other than that of origin or destination of the merchandise without there being a causal relationship that explains it;
- d. That the instrument or payment order, money order or remittance that cancels the import or export is issued or found to the order or in favor of a person other than the client or foreign supplier, without there being a causal relationship that explains it. .
- e. Clients or suppliers who repeatedly report loss or theft of merchandise during the journey from the place of arrival to the warehouse.
- f. Clients or suppliers who present allegedly false documents among the documents required for their identification and knowledge.
- g. Clients or suppliers, who have been sanctioned for violations of the exchange regime or the customs regime.
- h. Inconsistencies in information related to the existence, identification, home address, or location of the client or supplier.
- i. Inconsistencies in the information provided by the client or supplier, compared to that provided by other sources.

The mentioned operations are indicative, and may be modified or expanded, according to the new typologies that are detected in the future, according to the criteria of the critical area that may consider any activity as suspicious, or according to the Company's own experience.

The Steering Committee will adopt appropriate measures to maintain the confidentiality of the identity of workers and managers who have reported unusual or suspicious operations. To this end, the email address to which communications must be sent will be for the exclusive use of the compliance officer. If the communication is made by internal mail, it must be sent in a sealed envelope.


The actions that could be carried out as a result of investigations initiated by a suspicion about possible activities that could be related to ML/TF/FPADM should not be revealed to the client or third parties. Failure to comply with this duty of confidentiality may lead to sanctions as specified in the Colombian Penal Code, the JGB Code of Ethics and Conduct and the Internal Labor Regulations.

The communication in good faith of information related to activities related to ML/FT/FPADM does not constitute a violation of the restrictions on disclosure of information imposed by contract or by any legal or regulatory provision, and does not imply any type of responsibility for the communicating person. If it is found that the information was shared in bad faith or with objectives other than the prevention of contagion, it will be evaluated by the Administration and the Internal Work Regulations will be applied.

**7.1.5.1. REPORTS TO THE UIAF**

The UIAF Financial Information and Analysis Unit is the State entity, attached to the Ministry of Finance and Public Credit, in charge of detection, prevention and, in general, the fight against money laundering, financing of terrorism and the financing of proliferation of weapons of mass destruction in all economic activities. This Unit centralizes, systematizes and analyzes information on suspicious operations, cash transactions and exchange transactions of the subjects obliged to report to it. Reports to the UIAF must be made using the Online Reporting System (SIREL) on the entity's website following the formats and manuals published on the same page:

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--


	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 26 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

According to the regulations, the reports and frequencies that apply to JGB are:

NORMATIVITY		REPORT TYPE			
		Aim		Subjective	
		Individual Cash Transactions		Suspicious Operations Report (ROS)	
		Positive Report - Individual Cash Transactions	Report of Absence of Individual Cash Transactions	ROS Positive	Report of Absence of Suspicious Operations
DIAN Requirement Trusted Customs Users	UIAF Resolution 285 of 2007/017 of 2016	Monthly	Monthly	When it comes	Monthly
Superintendency of Companies Requirement Circular 100-000016 of 2020		Does not apply	Does not apply	When it comes	Quarterly basis

To prepare the report, the Compliance Officer will proceed as follows:

- **Detection of the unusual operation or situation:** the occurrence of an unusual operation or event must be reported to the Compliance Officer. Any coincidence with restrictive lists is considered an unusual operation and does not require completion of the unusual operations reporting form.
- **Report to compliance officer.** The person who identified the unusual situation must notify the Compliance Officer within a period of no more than 24 hours from its occurrence. It will attach all the documentary supports that may be required.
- **Analysis of the report.** Once the documentary supports have been received, the Compliance Officer must:
  - Evaluate whether the event is indeed a suspicious operation according to the information provided by the collaborator; likewise, you must determine if the information sent is sufficient or if it is necessary to request additional information.
  - The Confidentiality Policy will apply and will always tend to maintain the confidentiality of the communicator and the fact communicated.
  - Likewise, and in any case, additional procedures and investigations will be carried out using all available means.
- **Request additional information.** If in the previous activity it is determined that additional information is required, the Compliance Officer will complement the information through intensified due diligence. For this activity, he or she may rely on the immediate boss of the official who reported the event or on the available information.
- **Sending additional information.** The collaborator manages the request for additional information, which must be sent to the Compliance Officer immediately.

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 27 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

- **Document analysis.** Once the information is obtained, a detailed analysis will be carried out by the Compliance Officer with the support of the areas involved, which basically seeks to detect:
  - **Matches with suspicious profiles.**
  - **Inconsistencies and/or disproportionality with respect to the nature and/or volume of the current operation investigated, in relation to the commercial activity and/or operational history of the client.**
  - **Unusual operations that may be due to new channels used for ML/TF/FPADM.**
  - **The analysis techniques that may be used are: financial analysis and/or link analysis**

Once the analysis has been carried out, and based on the conclusions drawn from it, the compliance officer will inform the Steering Committee and present the file, if deemed necessary. As soon as the Steering Committee and the Compliance Officer conclude on the result of the analysis of the operation, the Compliance Officer will proceed to inform the critical area or communicating worker about the result of the analysis carried out. Said conclusion must be based on format F-GF-06-0 "Internal reporting format for unusual operations", which will be completed by the Compliance Officer, and also contain the recommendations and/or actions to be taken within the organization. .

Once the analysis has been carried out, the decision will be made on the treatment to be given to the file, assigning one of the following considerations:

***File under follow-up***

There are no signs, but it is an unusual operation. In accordance with the recommendations issued by the Compliance Officer in the Internal Report on Unusual Operations, the critical area in charge must comply with said recommendations, in the established periodicity, and must inform the Compliance Officer of any updates or news found in the file. , with obtaining complementary data that are appropriate, such as:

- Press clippings
- Information queries made on the internet and the tools provided by the Company
- Information reported on the UIAF page
- If indications or certainty of ML/TF/FPADM are observed, the UIAF will be immediately notified.
- Once it is confirmed that there is no risk of contagion, the file will be declared closed and will not have additional reviews other than those contemplated in this Manual and the applicable procedures .

***Failure to Report File:***


In the event that no signs are observed or it is not an unusual operation in the client's sector, or in the client's usual operations, the compliance officer will record in writing the information obtained regarding the knowledge of the client and the operation, the analysis carried out and the criteria by which it is decided not to communicate and finally the closing date of the file will be complemented, proceeding to file it.

***File to report***

If indications or certainty of your relationship with ML/TF/FPADM are observed, the following information will be requested:

- Photocopy of the Contracts related to the operation to be communicated
- Identification documents of the owners, payers or third parties involved.
- RUT, powers, certificate of existence and legal representation, if they are national legal entities, or similar documents, if they are foreign legal entities.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 28of 52
		VERSION: [DOCUMENTVERSION:MN-004]

- How much historical information is available on the client's activity in order to contextualize the client's global operational profile.
- If the critical area does not have and/or cannot locate this documentation, it should never be openly requested from the client, in order not to alert them. The critical area in charge must take note of this, to request it when appropriate, in order not to raise suspicions.

- **ROS suspicious operation report.** The Compliance Officer reports the suspicious operation to the UIAF through the SIREL online reporting system.

The report to the UIAF will be made exclusively by the compliance officer. The original documents that support the detection and reporting of the suspicious operation must be kept in the custody of the Compliance Officer, with due security, in order to make them reach the competent authorities in a complete and timely manner in the event that any of them request them. .

- **Archive.** The Compliance Officer generates the necessary reports to communicate them to the Board of Directors and archives all documentation of unusual operations reported by officials, as well as all supporting documentation of operations reported to the UIAF as suspicious. This file must have the necessary security measures to guarantee the confidentiality of the information.

The Compliance Officer must evaluate all operations reported as unusual. The first step to recognize if the operation is suspicious is to know enough about the third party (identification information, location, contracted products or services, start date of the contractual relationship with the company, information about transactions carried out between others). Suspicious operations are those operations that, according to good judgment, are considered in any case to be irregular or strange, to such an extent that they go beyond what is simply usual and that they lack support.

To develop the analysis, the Compliance Officer must carry out an intensified due diligence, exhaustive review, taking into account the information of the counterparty, the characteristics of the operation or situation detected and the warning signs described in this document, this in order to to discard any element of subjective judgment that contains any type of conflict of interest.

All collaborators are obliged to keep the reported information confidential and therefore will not be able to inform the third party about suspicious operation reports sent to the UIAF.


The original documents that support the detection and reporting of the suspicious operation must be kept in the custody of the Compliance Officer, with due security, in order to make them reach the competent authorities in a complete and timely manner in the event that any of them request them. .

#### 7.1.5.1.1. Objective Reports

They are the reports of those transactions that, due to their characteristics and in accordance with the conditions of the sector, constitute a source of information for the analysis developed in the UIAF. The "objective" nature of the report is due to the fact that it does not depend on the criteria of the person reporting, its preparation does not require any degree of suspicion.

Taking into account the import and export activities that JGB SA may carry out, and in compliance with Resolutions 285 of 2007 and 017 of 2016 of the UIAF, and Circular and 100-000016 of 2020 of the Superintendency of Companies, and any repeal, modify and/or complement, and any other regulation that imposes obligations on JGB SA in matters of money laundering and terrorist financing, JGB SA, through the Compliance Officer, must prepare the applicable objective reports, with the information that the critical areas supplied to you, within the terms stipulated for making the report (within the first 10 calendar days of each month).

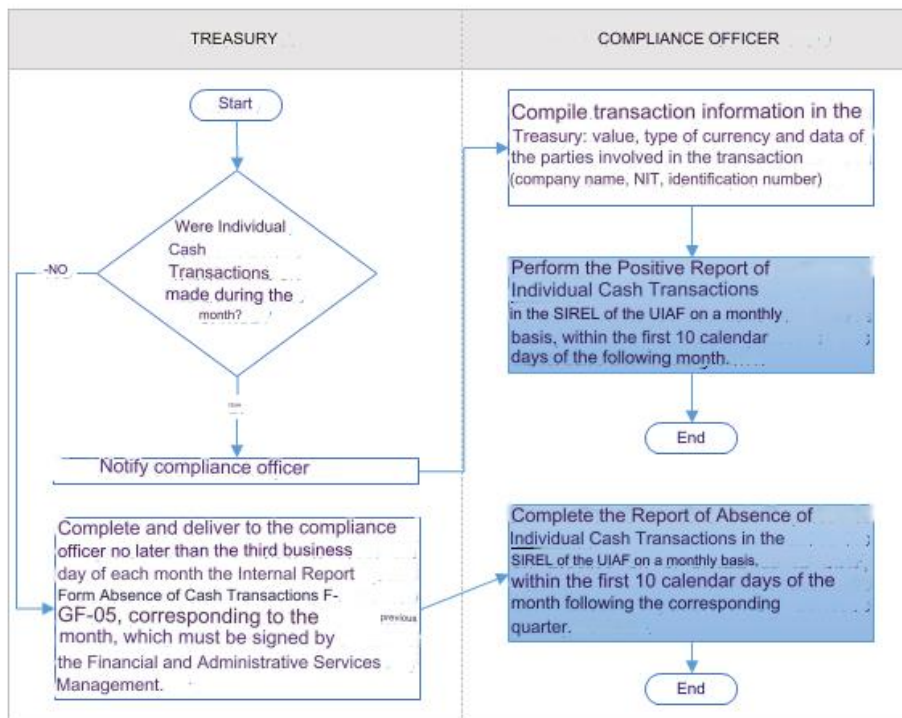
Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 29of 52
		VERSION: [DOCUMENTVERSION:MN-004]

JGB, in its capacity as a Trusted Customs User (or analogous quality, in accordance with the regulatory modifications, or certifications acquired by the company), will have to carry out the report on Individual Cash Transactions, which correspond to the transactions that are carried out in the development of the ordinary line of business and that involve payments through delivery or receipt of cash (bills or coins) for an amount equal to or greater than the sum of FIVE HUNDRED THOUSAND PESOS (\$500,000.00 M/CTE)


The information flow of **Individual Cash Transactions** within JGB is as follows:

The financial services area – Treasury must report to the compliance officer, no later than the sixth business day of each month, the existence or absence of individual cash transactions. In the event that individual cash transactions equal to or greater than \$500,000.00 (FIVE HUNDRED THOUSAND PESOS M/CTE) and/or multiple cash transactions equal to or greater than \$3,000,000.00 (THREE MILLION PESOS M/CTE) have been carried out, the following information must be attached for each transaction: Date, value, type of currency, type of identification, identification number, surname and first name, company name and municipality code.



### 7.1.5.1.2. Subjective Reports


Corresponds to Suspicious Transaction Reports (ROS). A suspicious operation is one that, due to its number, quantity or characteristics, does not fall within the normal systems and practices of business, an industry or a specific sector and, furthermore, is in accordance with the uses and customs of the activity that concerned, could not be reasonably justified.

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 30of 52
		VERSION: [DOCUMENTOVERSION:MN-004]


### 7.1.6. Control GE 6 Specific controls

All specific controls determined in this section, which generate a match, must be immediately reported to the Compliance Officer.

AREA	CONTROL	FREQUENCY
<i>Services and security</i>	Inspect the containers before loading merchandise, each time an export is carried out by filling out the F-NI-02-0 "Container Inspection" form. This inspection will be carried out by the security contractor, who must report to the area in charge. If nothing new is found, loading and placing any security seals is carried out.	Every time it occurs
	The security contractor must carry out verifications, in order to identify that an inspection is being carried out on the cargo vehicles parked outside the Company.	Random
	Perform background checks on binding lists of external personnel (contractors) who must enter the Company's facilities to provide services prior to their entry. Notify compliance officer when contractor employee matches occur on binding lists	Every time it occurs
<i>Financial Services - Treasury</i>	All collection operations will be channeled through entities supervised by the Financial Superintendency; any exception must be approved by the Financial Manager and must be brought to the attention of the compliance officer. The only cash payment operations will be those made through petty cash and/or travel expenses.	Every time it occurs
	Carry out monitoring and analysis of payments made through petty cash, in order to identify recurrences of payments or installments of unusual purchases to the same beneficiary (warning signs). The information can be obtained through SAP transaction FBCJ. When a red flag is identified, the case must be reviewed with the Financial Services Manager and subsequently with the Compliance Officer to determine if an unusual transaction is actually occurring, for which purpose one must proceed in accordance with what is defined in this Manual.	Every time it occurs
	Each time returns are made, the JGB treasurer disburses the money only to the registered account of the third party that is previously registered,	Every time it occurs
	Carry out monitoring in order to identify possible warning signs	Biannual
	Carry out random checks, in order to verify that only customer checks drawn directly to JGB are received.	Random
<i>Financial Services - Portfolio</i>	Update the information of all clients every two years, and carry out periodic updates of some clients where applicable, according to what is established by the Compliance Officer.	Biennial and/or periodic.
	Notify compliance officer when customer matches occur on binding lists .	Every time it occurs


	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 31 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

	Every time a check is received from a customer, the portfolio area makes sure not to receive checks that are not drawn directly to JGB	Every time it occurs
	Collection operations that are channeled through entities that are not supervised by the Financial Superintendence must be approved by the Financial Manager and must be brought to the attention of the compliance officer.	Every time it occurs
Legal	Ensure that contracts signed with third parties contain ML/FT/FPADM prevention clauses	Every time it occurs
Commercial	Register any event or warning signal related to SAGRILAF in the client linking form "Master Client Information".	Every time it occurs
	Immediately share with the Compliance Officer information that they may obtain about clients that is related to crimes related to ML/FT/FPADM or activities that are related to unusual operations.	Every time it occurs
	Provide support to the Compliance Officer in investigative work and expansion of documentation in the management of reports of unusual operations.	Every time it occurs
Logistics	Ensure that the inventories of packaging or materials that contain the JGB brand have an adequate final disposal for the protection of the brand, health and is in accordance with the environmental requirements in force in the territory.	Every time it occurs
	Companies providing transportation services must have mechanisms to track vehicles that transport finished products for export or for national distribution, such as GPS in vehicles, monitoring groups, among others, and must submit a report on the developments to the logistics area.	Every time it occurs.
	Companies providing logistics operation services will carry out inspections on vehicles with imported raw materials from the Company, as well as on vehicles with export products leaving JGB facilities. The news must be reported to the logistics area.	Every time it occurs.
	The logistics area and/or the companies providing logistics operation services will receive and review the content to be received and dispatched, and if necessary, they will carry out quality analysis and container inspection, regarding imported and national raw materials. dispatch of finished product, POP material and any other that is received in or dispatched from JGB SA	Every time it occurs.

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 32of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

	Ensure due knowledge and consultation in binding lists of each of the suppliers related to the Foreign Trade operations carried out by the company.	Every time it occurs.
<i>Planning and purchasing</i>	Obtain information on the usual characteristics of the market of potential suppliers, in order to maintain knowledge of the industry in which they operate and be able to compare them with the operations of the third party that intends or has a relationship with JGB, which will allow establishing its normality. or possible abnormality of the operation.	
	Require the AEO, ISO 28000 and/or BASC Authorized Economic Operator certification from all logistics and transport operators that aspire to provide services to JGB and annually request the update of said certification from those who are linked, in order to prevent Possible contamination or contagion within logistics operation procedures	Every time it occurs
	Update supplier information in accordance with the provisions of the supplier selection, linking and updating procedure; and periodically, as determined by the Compliance Officer, in accordance with your ML/TF/FPADM risk level	Annual and/or periodic
	Notify the compliance officer when supplier matches occur on binding lists and when a red flag or unusual operation is deemed to exist	Every time it occurs
	Ensure that audits are carried out randomly on critical suppliers.	Random
Quality	Verify that weekly inventories of controlled substances are being carried out. Additionally, in the event of a spill of these substances, a report is prepared indicating the quantity that was lost or contaminated, signed by quality assurance, warehouse and production person. .	Weekly
	Monitor quotas for controlled substances so that the authorized monthly amount is not exceeded in the purchasing and consumption processes.	Weekly
Business intelligence	Monitor sales, in order to identify variations or unjustified increases in purchases by a specific customer.	Biannual
<i>People and organization</i>	Carry out, through third parties or using the tools provided by the Company, the search and validation in binding lists of candidates in selection processes, and notify the Compliance Officer about matches in binding lists associated with ML/TF/FPADM, regardless of the linking decision.	Every time it occurs
	Update employee information in accordance with the stipulated policies, and periodically, as determined by the Compliance Officer, in accordance with their ML/FT/FPADM risk level.	Annual
Audit	Carry out an annual audit on the operation of SAGRILAFT	Annual
Compliance officer	Those established in this manual	Periodically
Cross	Report any unusual operations detected to the compliance officer	Every time it occurs



	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 33of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

	Comply with the ML/FT/ FPADM policies contained in the manual	Permanent
	The only cash payment operations will be those carried out by petty cash and/or travel expenses, provided that the procedures allow it.	Every time it occurs

**7.1.7. Control GE 7 Controls to ensure compliance with the standards contained in the ML/TF Risk Management Manual /FPADM**

The Compliance Officer will ensure the training, induction and reinduction of the obligations of collaborators in matters of ML/TF /FPADM , with the aim of raising awareness about the importance of the content of this Manual, to avoid the risk of contagion.

At least annually, the Compliance Officer, with the support of critical areas, will carry out mass validation of counterparties linked to the company.

**7.1.8. General Controls for the prevention of ML/FT/FPADM in the Payment process**

- No financial product of the company will be lent to carry out financial operations of third parties.
- Management or its formal delegates will be responsible for authorizing transfers to third parties other than those with which it has a commercial or contractual relationship. The beneficiary must complete the third-party knowledge form (as applicable), in addition to attaching the supporting documents that are usually requested. It is worth clarifying that the process will be carried out as if it were a client or supplier.
- Checks must have restrictive stamps.
- Leave complete and sufficient evidence of all financial product transactions.
- Do not lend the name of the company to carry out business or money movements for third parties.
- Do not make payments or receive payments from third parties who do not have a contractual relationship with the company. Unless the Legal Representative approves the exception and the Compliance Officer carries out his intensified due diligence regarding the operation and the third parties comply with all the linking formalities described for clients or suppliers.
- All forms, forms and other documents completed by the counterparties must be reviewed by the Leader of the corresponding process and may not have amendments, blank spaces and will have all the additional information required for their connection.
- The updating of information for recurring counterparties must be carried out by the Process Leader, in accordance with the regulations of the Compliance Officer and the criteria established in the Risk Profile produced in the profiling model, mentioned below.
- All counterparties must be consulted on binding and informative lists.


**7.2. Reservation and Confidentiality**

All actions and/or activities derived from the application of this Manual may not be made known to clients, suppliers, contractors, consultants, employees, particularly unusual operations that have been identified or people who have carried out or attempted to carry out operations classified as suspicious operations, especially if they were subject to internal reporting or to the competent authority (UIAF).

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

**7.3. Interest conflict**

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 34 of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

Our commitment is to always act in the interest of the company and to avoid or disclose situations that involve a real or perceived conflict between personal interests and the interests of JGB.

When the Compliance Officer, due to his other functions, requires approval of an extraordinary operation that is immersed in the same SAGRILAF T procedures; They must immediately inform the Legal Representative and the Board of Directors , who will give their approval.

The Compliance Officer will refrain from participating in decisions or activities that involve the connection of Clients, Partners, Suppliers or Employees when it involves family members or personal interests in any business or project with JGB.

If necessary, when both the Legal Representative and the Compliance Officer are prevented, the situation must be escalated to the Board of Directors . It will be its members who give the corresponding instructions and/or approvals.

#### 7.3.1. Regime of incompatibilities and disabilities


The following situations listed below will be considered as disabilities or incompatibilities that prevent the Principal or Alternate Compliance Officer from carrying out their work with full independence. Therefore, the person who:

- ✓ Have relatives up to the third degree of consanguinity, second degree of affinity or first civil relation about whom any link with activities or operations related to Money Laundering or the Financing of Terrorism and proliferation of weapons of mass destruction has been known.
- ✓ Although the Superintendence of Companies does not note an express provision that defines and characterizes the Compliance Officer, which allows us to infer that it is the company's discretion to establish the conditions of the position, which is also predicated regarding the possibility that the internal auditor occupies the position of the Compliance Officer.
- ✓ Legal Representatives or directors who are not residents of Colombia.
- ✓ Employees who, although they are at the appropriate hierarchical level to be a Compliance Officer, carry out commercial and/or administrative activities.
- ✓ The others determined by the Board of Directors .


#### 7.4. Classification of counterparties according to risk

With this information collected by the critical areas in charge, third parties must be classified into the following categories:

CATEGORY	CHARACTERISTICS	TREATMENT
Contractual parties with high risk	<ul style="list-style-type: none"> <li>• Third parties with nationality or residence in a 'high risk country'. A country considered high risk corresponds to any country registered on the restricted lists published by the OECD and the FATF.  <a href="http://www.fatf-gafi.org/countries/#high-risk">http://www.fatf-gafi.org/countries/#high-risk</a></li> <li>• Third parties, who, being on the list of "Specially Designated Nationals and Blocked Persons" published by OFAC, had obtained a license from OFAC to be managed by the State.</li> </ul>	<p>The case will be presented to the Steering Committee by the Compliance Officer.</p> <p>The Steering Committee must analyze the case and decide whether or not to accept the counterparty (or its continuity in case it is already linked to JGB). In the event that the committee decides to initiate or maintain a relationship with the third party, specific quarterly monitoring and control of the third party and the operations</p>

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 35of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

CATEGORY	CHARACTERISTICS	TREATMENT
	<p>Politically exposed persons (PEP). The following are considered PEPs from their appointment until two years after their retirement from office:</p> <p>PEP from international organizations: Foreign PEPs: Publicly Exposed People</p> <ul style="list-style-type: none"> <li>Investigated for the crime of money laundering and any of its underlying crimes, in accordance with the Colombian penal code and/or its analogous regulations in other jurisdictions</li> <li>Investigated for activities related to prostitution or pornography.</li> <li>Persons who are known to be under investigation for any type of criminal act associated or underlying money laundering in Colombia or other jurisdictions.</li> </ul>	<p>carried out by them in this period will be carried out .</p> <p>Your connection will be approved by a higher authority than the one that normally approves the connection, and there must always be a written contract.</p> <p>The case will be presented to the Steering Committee by the Compliance Officer. The Steering Committee must analyze the case and decide whether or not to accept the counterparty (or its continuity in case it is already linked to JGB). In the event that the committee decides to initiate or maintain a relationship with the third party, specific periodic monitoring and control of the third party and the operations carried out by them in this period will be carried out by the area in charge.</p>
Non-admitted counterparties	<ul style="list-style-type: none"> <li>Convicted of the crime of money laundering and any of its underlying crimes, in accordance with the Colombian penal code and/or its analogous regulations in other jurisdictions</li> <li>Convicted of activities related to prostitution or pornography.</li> <li>Persons who are known to be convicted of any type of criminal act associated or underlying money laundering in Colombia or other jurisdictions.</li> <li>Persons who are included in the lists binding for Colombia or any information list directly associated with money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction, regarding which they have been consulted at the time of verification.</li> <li>People with businesses whose nature makes it impossible to verify the legitimacy of their activities or the origin of the funds.</li> <li>People who refuse to provide the required information or documentation. <ul style="list-style-type: none"> <li>People who have businesses whose nature makes it impossible to verify the legitimacy of the activities they carry out or the origin of the funds.</li> </ul> </li> <li>Persons who, having presented the documentation that allows full identification of the owner and/or the final</li> </ul>	They will not be admitted as counterparties.

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 36of 52
		VERSION: [DOCUMENTVERSION:MN-004]

CATEGORY	CHARACTERISTICS	TREATMENT
	beneficiary, refuse to allow the Company to obtain a copy of the document that is necessary in light of the ML/TF/FPADM prevention system <b>for</b> their commercial link <ul style="list-style-type: none"> <li>• Persons who present manifestly false documents or whose external characteristics allow serious doubts about their legality or legitimacy.</li> <li>• Any other category not contemplated in the previous ones that is conveniently approved by the internal body, for illegitimate purposes by people, or organizations, with criminal purposes that lead to the exposure of the Company to legal and/or reputational risks.</li> </ul>	

One of the controls established by the Company in terms of prevention and control of ML/FT/FPADM is to have information on counterparties with whom commercial or contractual links are maintained in general. For this purpose, procedures for knowing counterparties have been established, which require completion of the format for the creation of third parties defined for this purpose.

For no reason can the word of mouth be accepted exclusively in the counterparty admission process and the established controls be omitted.

Process Leaders will ensure that their designated collaborators in their area correctly and completely complete the counterparty linking forms in the performance of their work, and collect the necessary information from counterparties, in accordance with this Manual and its procedures.

**profiling and segmentation model** was established , which must be completed and updated periodically for each critical area, in order to determine its risk profile.

The profiling model will allow establishing a low, medium and high risk level based on the basic information provided in the first instance. This scoring will locate the counterparty's risk profile in such a way as to generate early warning signals. For all recurring counterparties, the information and profiling model must be updated in accordance with the policies established for each area, without prejudice to the fact that, during their commercial stay with JGB, they present any warning signs that require intensified due diligence, through which requires requesting updated information from the third party.

All those counterparties that, through the profiling model, show a medium or high risk profile, in the first instance, the transactions carried out as a result of the contractual relationship will be monitored.


This information update includes the completion of the customer knowledge form, request for additional documentation described in the knowledge form.

For those counterparties with whom there are contracts, the termination and/or suspension clause of the contractual or commercial relationship must be maintained when, as a result of intensified due diligence that demonstrates circumstances of possible reputational risk or contagion for JGB.

**7.5. Market knowledge**

The portfolio, commercial and purchasing areas of JGB must obtain information on the usual characteristics of the market of potential clients and suppliers respectively, in order to maintain knowledge of the industry in which they operate and be able to

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 37 of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

compare them with the operations of the third party that intends or has a relationship with JGB, which will allow defining its normality or possible abnormality of the operation.

### 7.6. Updating documentation for clients, suppliers and active employees

Each of the critical areas of JGB must keep the identification documentation of clients, suppliers and employees updated throughout the duration of the relationship with the counterparty, in accordance with the applicable procedures for each critical area. Without prejudice to the above, if significant changes occur in the client's or supplier's data, or in their activity, the critical area in charge of managing the counterparty must carry out the update immediately.

Employee information must be updated annually or in accordance with current Company policies.

## 7. STAGES OF SAGRILAFT

---

The ML/TF/FPADM Self-Control and Comprehensive Risk Management System implemented in JGB will be guided for all its purposes by Chapter and Proliferation of Weapons of Mass Destruction (ML/FT/FPADM)"; and other regulatory standards issued by the Superintendency of Companies on the matter.

The methodology used for risk management will be carried out by the ISO31000 reference. The reasonable measures taken through the methodology must be documented and preserved in the event that any internal or external control body requests it.

### 8.1. ID

In this first phase of the methodology, the possible specific causes of ML/TF/FPDAM risks are systematically identified, as well as the various possible effects that must be addressed. Likewise, through this first stage, the segmentation and classification of ML/TF/FPDAM risk factors is contemplated.

It is necessary to maintain the internal and external context of JGB, in such a way that it allows adequate risk identification.

### 8.2. Measurement or Evaluation

In this stage, the possibility, probability or frequency of occurrence of the inherent ML/TF/FPADM risk is measured against each of the risk factors, as well as the impact if it materializes through the associated risks. These measurements are qualitative or quantitative in nature, described in the **Risk Matrix**.

In this stage, a qualitative assessment of the identified risks is developed without taking into account the treatment actions designed for the process, for which probability and Impact measurement criteria are established, which are selected according to the experience of the process leaders and under the guidance of the Compliance Officer.


The measurement criteria are detailed below.

#### 8.2.1. Probability or Frequency:


Probability or frequency is a qualitative risk measurement variable, which represents the number of times a certain risk event could occur over the course of a year.

The criteria to evaluate the probability in JGB will be the following:

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 38of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

FACTOR	WEIGHTING RANGE	PUNCTUATI	WEIGHTING	TOP SCORE
Complexity of the procedure	Very easy to execute	1	8	64
	Easy to run	2		
	Complex	4		
	Too complex	8		
	Does not apply	0		
Automation	Automatic	1	4	16
	Semi-automatic	2		
	Manual	4		
	Does not apply	0		
Staff suitability	Excellent	1	8	64
	Good	2		
	Regular	4		
	Deficient	8		
	Does not apply	0		
Risk Materialization	It happened once a year	1	8	64
	Happened twice a year	2		
	It happened once a	4		
	It happened once a week	8		
	It hasn't happened	0		

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 39of 52
		VERSION: [DOCUMENTVERSION:MN-004]

Procedure frequency	Annual	0.5	8	64
	Biannual	1		
	Monthly	2		
	Weekly	4		
	Diary	8		
Documentation quality	Very complete	1	4	32
	Complete	2		
	Acceptable	4		
	Deficient	8		
	Does not apply	0		
Communication	Excellent	1	4	16
	good	2		
	Moderate	4		
	Deficient	6		
	Does not apply	0		
Top Score				320


### 8.2.2. Impact:

In the risk analysis methodology, the impact reflects the estimated effect that the presence of a risk event could have on the process in qualitative terms, that is, the possible loss. The criteria used for its measurement are:

**Table 2. Impact measurement criteria.**

FINANCIAL LOSSES			
ECONOMIC QUANTIFICATION			
Worth	level	Minimum	Maximum
5	Significant	10,000,001	999,999,999,999
4	High	7,500,001	10,000,000
3	Half	5,000,001	7,500,000
2	Low	2,500,001	2,500,000
1	Insignificant	0	0

SOFT LOSSES			
ECONOMIC QUANTIFICATION			
Worth	level	Affect to the image	Legal
5	Significant	Publication of news in national mass media (press, television, radio).	Significant accusations and fines by regulatory bodies, very serious litigation.
4	High	Affecting image at the national level (a media outlet).	Formal request or investigation by a

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 40of 52
		VERSION: [DOCUMENTVERSION:MN-004]

			regulatory body, major litigation.
3	Half	Affectation to the image at the local level (client group union).	Requirement by a regulatory body, litigation Minors.
2	Low	Less impact on reputation before control entities	Informal requirement by a regulatory body, minor conciliations.
1	Insignificant	Image damage to one or more clients	Minor legal matters.

### 8.2.3. Risk level:

Likewise, the risk level shows the company's level of risk exposure, through a rating scale automatically generated from the combination of the Probability and Impact obtained for each risk, which is called Inherent Risk. that is, the risk without considering the controls.

Once the treatment actions used to manage the risk are documented and qualified, the residual risk will be obtained, which is the result of the generation of deviations in the probability, the impact or both variables of the inherent risk, in relation to the effectiveness of treatment actions.

The following table shows the risk levels considered in the company's methodology:

**Table 3 Risk Exposure Level (Severity)**

Worth	Level	min	Max
5	Highly probable	81%	100%
4	Very likely	61%	80%
3	Likely	41%	60%
2	Unlikely	twenty-one%	40%
1	Remote	0%	twenty%


### 8.2.4. Control

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

#### ML/TF/FPADM Risk Treatment

- **Acceptability Zone:** The risk can be directly admitted, but additional controls must be implemented.



	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 41 of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

- **Serious Risk Area:** More demanding control measures must be implemented to mitigate the risk, analyze their cost/benefit.
- **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, define coverage or treatment policies, define exposure limits. .

**Control classes**

The control measures adopted will seek to reduce the possibility of occurrence and/or the impact of the risk of ML/TF/FPADM if it materializes.

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

- **Preventive Controls :** These correspond to those that prevent risks from materializing by analyzing the causes that may generate them.
- **Detective Controls :** These refer to detection activities during the execution and development of the process, these can be prior or after operations. It is an alarm that is activated in the event of an abnormal situation, on site.
- **Corrective Controls :** Which allow deviations and errors in the operation to be corrected or prevent their recurrence. These controls are part of the company's Internal Control System duly supported by policies and procedures for its operation.


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

- **Manual Controls :** Control activities carried out manually by one or more people.
- **Semi-Automatic Controls :** These are procedures applied from a computer in support software, designed to prevent, detect or correct errors or deficiencies, but which require human intervention in the process.
- **Automatic Controls :** These are procedures applied from a computer in support software, designed to prevent, detect or correct errors or deficiencies, without requiring human intervention in the process.

The aforementioned control actions must be assigned a rating where it is evaluated whether it reduces the probability, the impact or both and the effectiveness of the treatment action is assessed, based on different variables which are mentioned below:

**Table 4 Variables for Evaluation of the Effectiveness of Controls**

EVALUATED FACTOR	EFFECTIVENESS FEATURE	PUNCTUATION	WEIGHING
Class	Corrective	1	twenty%
	Detective	2	
	Preventive	3	
Audit tests	Compliance with the control objective was evident	3	twenty%

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 42of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

	Non-compliance with the control objective was evident	2	
	No audit has been carried out for the control objective	1	
Control effectiveness	high	3	twenty%
	Acceptable	2	
	Low	1	
Guy	Manual	1	twenty%
	Semiautomatic	2	
	Automatic	3	
Responsibility	Clearly assigned	3	10%
	Partially assigned	2	
	Not assigned	1	
Procedure Documentation	Documented, Updated and Disclosed	3	10%
	Documented	2	
	Not documented	1	

According to the rating obtained in the evaluation of the treatment actions, the effectiveness of each of these is determined, according to the following table.

Table 5 Effectiveness of Treatment Actions

Name	Min >	Max <=	Frequency	Impact	Excellent	24	30	3	3
					Well	19	24	2	2
Regular	14	19	1	1					
Deficient	10	14	0	0					


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

#### ML/FT/FPDAM Risk Acceptance Level

Level of risk acceptability: This risk is decided by the Board of Directors that is willing to accept in the pursuit of achieving the objectives.

In JGB, residual risks are accepted when their severity is at a low or moderate level, that is, if they are in the acceptability zone.

Care will be taken to keep the residual risk below the moderate level, since in ML/TF/FPADM risk issues, although the probability of a risk event occurring may be low, the impact in the event of the risk materializing could be tall

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 43of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

Any residual risk that exceeds the level of acceptability must be addressed and the necessary action plans will be taken to mitigate said risk.

### 8.2.5. Monitoring

Monitoring will be carried out at least annually and during this the following should be ensured:

- ✓ Carry out an effective monitoring process that facilitates the rapid detection and correction of deficiencies identified in the risks associated with ML/TF/FPADM.
- ✓ Monitor and compare the inherent and residual risk of each risk factor and the risks associated with ML/TF/FPADM.
- ✓ It must be ensured that controls are comprehensive of all risks and that they are operating in a timely, effective and efficient manner.
- ✓ It must be ensured that residual risks are within the acceptance levels established by JGB .

Monitoring must be carried out by the Compliance Officer based on the following activities:

- ✓ Binding or Informative List System
- ✓ SAGRILAFI audit
- ✓ Report of the Compliance Officer to the Board of Directors
- ✓ Adoption of Action Plans and/or Recommendations
- ✓ Reports to the UIAF
- ✓ ML/TF/FPADM Risk Indicators
- ✓ Update audited controls

Additionally, the updated information will be used to carry out analysis of variations in the main financial figures for those Clients and/or Counterparts that, according to the segmentation exercise, are located in a high-risk area.

### 8.3. Methodology for segmentation of risk factors

Segmentation is the process by which risk factors are separated into homogeneous groups that must be treated differently for the purposes of risk management of money laundering, financing of terrorism and proliferation of weapons of destruction. massive (LA/FT/FPADM). The separation is based on the recognition of significant differences in their characteristics.

Segmentation must seek homogeneity within each of the identified segments and heterogeneity between them. The objective of segmentation is to apply differentiated monitoring strategies for counterparties according to the combination of each ML/TF/FPADM risk factor and other variables.


Segmentation allows us to focus on those segments whose risk profile is highest. In this way, special monitoring is carried out on those third parties who, due to their characteristics, are classified with a higher probability regarding the risk of ML/TF/FPADM.

According to the company's analysis, the following ML/TF/FPADM risk factors have been determined:

- a. Customers
- b. Suppliers
- c. Jurisdiction
- d. Services and products

Segmentation will be carried out on these identified factors. **Expert segmentation guide and segmentation model.**

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 44of 52
		VERSION: [DOCUMENTVERSION:MN-004]

## 8. DOCUMENTATION CONSERVATION

JGB SA will keep for ten years the documents that support the SAGRILAFT compliance procedures, as well as the corresponding records that adequately prove the completion of operations with all counterparties.

The period indicated above will be counted from the day on which relations with a client and/or supplier end for the documents related to their identification and from the execution of each operation for the conservation of the documents or records that accredit it.

The documents that prove the identity of Clients, Suppliers, Investors, Contractors or contractual relationships with third parties, as well as the documents related to the operations with them, carried out by JGB, will be kept physically or virtually during the period previously provided. The central archive area of JGB will be responsible for the custody of the documentation.

For each JGB counterparty that has been reported to the UIAF as a suspicious operation, the Compliance Officer will open a file (physical or digital) in which all the documentation collected will be collected, which includes at least:

- Copy of identity documents
- Form for creating and updating clients and suppliers
- Contracts
- Search in a public database or binding list where the match found is observed.
- Intensified due diligence
- Newspaper or news clippings or impressions.

For cases of internal reporting of suspicious operations, the compliance officer will have custody of the documents related to: statements, external reports made, electronic communications, information management protocol, responses received on information requests, reports from external entities. related to the background of the person or company evaluated and other information that was considered to support JGB's decision.


Each area of the company will be responsible for the custody and conservation of each record related to the activities established in this manual, and will be subject to the document management provisions that the company has.

Notwithstanding the above, the conservation of documents will be subject to the provisions of article 28 of Law 962 of 2005, or the rule that modifies or replaces it, on the conservation of books and business papers.

## 9. REQUIREMENTS OF THE AUTHORITIES

The commercial reserve is not opposable to requests for information specifically formulated by the judicial, tax, customs or exchange supervision authorities and the UIAF within the investigations of its jurisdiction, in accordance with the provisions of article 15 of the National Constitution. and in articles 63 of the Commercial Code, 275 of the Code of Criminal Procedure and 288 of the Code of Civil Procedure.

The requests made by the aforementioned authorities in matters of ML/FT/FPADM to JGB, received at the registered office or in any of the companies or branches of the company, will be immediately sent to the compliance officer, who must respond to such requirements in the times established by law.

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 45of 52
		VERSION: [DOCUMENTVERSION:MN-004]

Attention to these requirements must be timely and comply with the appropriate and complete response according to the request.

The Compliance Officer may rely on the respective official to obtain the required information.

Through the report of the Compliance Officer to the Board of Directors, the receipt of the request and its response must be notified.

The procedure established by JGB to respond to requests for information received is as follows:

- Check the file of existing files, in case it is a new requirement or is the continuation of a previous requirement or communication. In the latter case, the file will be reviewed.
- It is registered and assigned a reference number, made up of a code followed by the year of production.
- As a matter of urgency, the necessary documentation and information will be requested from the corresponding area to respond to the requirement. The response requested by the compliance officer will be due within the period requested by the Compliance Officer.
- The compliance officer will respond to the requesting authority within the deadline granted by the control body and through the means indicated by the same. The Compliance Officer will verify that the information to be delivered is reliable, complete, clear, precise and is framed in the context of what is requested. The file will then be closed and archived.
- In his periodic report, the Compliance Officer will update the Highest Administration Entity, the status of receipt/sending of responses to requirements from control entities and/or UIAF.

## 10. TRAINING AND OUTREACH

---

In the induction processes of employees entering JGB, the objective, scope and policies of SAGRILAFT are socialized. The area in charge of inductions, training and training will ensure that the induction of this Manual and the associated policies is socialized to all workers who join the Company. These trainings will be carried out with the help of digital platforms and tools.


Annually, training sessions will be held for collaborators and especially for those who are part of critical areas of the Company (those that have a relationship with counterparties and therefore execute critical and high-risk processes regarding ML/FT/FPADM risk). To the extent possible, JGB may make use of information technologies to carry out training. These trainings and reinductions will be led by the JGB training and training area, in the company of the Compliance Officer.

Periodically, as defined by the Company, re-induction sessions will be held for all employees, making use of information technologies.

When modifications and/or additions are made to the policies applicable to ML/FT/FPADM, and to this Manual, the Compliance Officer must disseminate the relevant updates to the entire Company.

The training must be duly evidenced through the physical or electronic documents used for its development and registration of attendance.

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 46of 52
		VERSION: [DOCUMENTVERSION:MN-004]

JGB S.A. is available to interested parties and promotes the proper officialization, publication, implementation and operation of its policies, procedures and other documentation related to SAGRILAFI.

Additionally, it will design strategies to report on the policies, standards and their updates implemented within the company regarding the prevention and control of ML/FT/FPADM.

## 11. SANCTIONS

All JGB workers have the institutional and personal obligation to comply with all the activities, processes and procedures contained for the control of ML/FT/FPADM and in current legal regulations. Any deliberate non-compliance or omission of the controls established here will result in sanctions.


The company will apply the necessary measures to impose criminal, administrative and labor sanctions, when necessary, on workers who directly or indirectly facilitate, allow or assist in the use of the company as an instrument for carrying out money laundering, financing of terrorism and proliferation of weapons of mass destruction.

### 12.1 WORK DISCIPLINARY OFFENSES:

Failure to comply with the provisions of the manual by a company worker will be considered a serious offense, in accordance with the definition contained in the Internal Labor Regulations and the Employment Contract.

#### 12.1.1 SCALE OF SANCTIONS FOR OFFENSES RELATED TO THE LA/FT/PADM CONTROL SYSTEM

DISCIPLINARY FAULT	GRADUATION CRITERIA	TYPE OF FAILURE	SANCTION
Incurring infractions related to processes and procedures contained for the control of ML/FT/FPADM, in the current legal regulations and the declarations under the severity of oath that are detailed in the individual employment contract for the first time	The collaborator's omission did not generate any of the risks contemplated in the system for the control of ML/FT/FPADM	MILD	<b>For the first time:</b> Verbal attention call with function reminder.
		SERIOUS	<b>For the second time:</b> Suspension of the employment contract for up to 8 days <sup>i</sup>
	The omission of the collaborator generated the risks contemplated in the system for the control of ML/FT/FPADM.	SERIOUS	<b>For the first time:</b> Suspension of the employment contract for up to 8 days <sup>ii</sup>
			<b>For the second time:</b> Termination of the contract with just cause
			<b>For the first time:</b>

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 47 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

	The omission of the collaborator led to the materialization of one or more of the risks contemplated in the system for the control of ML/FT/FPADM	SERIOUS	Termination of the contract with just cause
--	---	---------	---


After three years from the occurrence of the sanction, a new period is reestablished in which previous offenses will not be taken into account to determine the sanctions. This implies that any sanction prior to the aforementioned period of time will not be considered when evaluating future offenses, allowing the employee to start with a clean record and no repercussions for previous violations. However, it is important to highlight that previous sanctions could still be taken into account for other purposes, such as performance evaluation or in cases of recurrence of similar offenses.

## 12. WARNING SIGNS

This list is illustrative, the activity does not in itself establish that it is a suspicious operation, so it is necessary to verify other elements related to the questioned activity that support this perception.

GENERAL <sup>2</sup>
<ul style="list-style-type: none"> <li>• Unusual characteristics of activities, products or places of origin</li> <li>• Attempt to fail to comply with customs, tax or exchange rules or procedures or that have already been sanctioned for violations of the exchange regime or the customs regime</li> <li>• Inconsistencies in information related to the existence, identification, bank account, home address, or location of the user</li> <li>• Inconsistencies in the information provided by the user compared to that provided by other sources</li> <li>• Economic sectors likely to be used as a mechanism to carry out money laundering operations or for the financing of terrorism, such as: metals, precious jewelry, transportation, taxi service, gambling, auto parts, foreign currency intermediary companies, foundations, chemicals, cooperatives of any level, motels, network marketing companies.</li> <li>• Company that, without apparent justification, begins to receive transfers from abroad of high amounts or with high frequency.</li> <li>• Increase in the turnover of a company's business, without a justified reason.</li> <li>• Operations that do not match the economic capacity of the company.</li> <li>• Company that in a short period of time appears as the owner of important new businesses and/or assets.</li> <li>• Company that sends or receives frequent money transfers from or to territories or countries considered non-cooperative by the Financial Action Task Force (FATF, <a href="http://www.fatf-gafi.org/countries/#high-risk">http://www.fatf-gafi.org/countries/#high-risk</a>) or paradises harmful tax regimes or preferential tax regimes, by the Organization for Economic Cooperation and Development (OECD), without an apparent economic justification.</li> <li>• Companies that have been established with low capital and that promptly receive large amounts of foreign investment.</li> <li>• Companies that present non-operating income higher than operating income.</li> <li>• Companies whose financial statements reflect very different results compared to other companies in the same sector or with similar economic activity.</li> </ul>

<sup>2</sup>Taken from the "Risk Management Model for money laundering, terrorist financing (ML/FT) and smuggling for the Foreign Trade Sector" – DIAN and the United Nations Office on Drugs and Crime (UNODC).

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 48of 52
		VERSION: [DOCUMENTVERSION:MN-004]

- Companies whose operations do not correspond to normal market conditions
- When the same person acts as legal representative or owner of different companies, they all have the same address or telephone number.
- Register a post office box as an address or the company address matches that of other companies with no apparent link.
- That the person or company or some of the administrators or partners appear on the control lists adopted by the company or have appeared in the media or on the control lists
- The financial situation of the company does not match the type of income from the activity of the company or its partners
- Companies little recognized in the market that make high volumes of purchases and the date of incorporation of the company is recent.
- Companies whose sources of financing may come from illegal fundraising resources or money desks not authorized to manage public resources.
- Several companies have partners, managers, administrators or legal representatives in common, without having been reported as a business group, nor with a clear justification.
- Companies whose operations do not correspond to the financial information
- Companies that frequently change their data; address, telephone, etc.
- Companies that have a very low subscribed capital and/or a very broad corporate purpose.
- It presents debt that does not correspond to the income declared by the company.
- Companies that do not have agencies or branches, however, carry out several operations involving large sums in different cities or countries, which do not have a clear relationship with their economic activity.
- Companies that have a high degree of liquidity and their activity according to market evaluation normally do not maintain or generate it.
- Companies older than one year with significant assets without justification.
- Companies with income higher than the average of the economic sector to which it belongs.
- Companies that have been established with low capital, receiving large sums of investment shortly after, whose origin is unknown
- Companies with operating margins very far from the average.
- Significant change in declared assets from one year to another.
- Assets not declared in a fiscal period.
- The company was acquired being in financial difficulties in meeting its obligations
- The company presents overwhelming profits in a short period of time
- The company was established with little capital, shortly after receiving large sums of investment, mainly foreign.
- They make large investments despite having been created very recently
- Companies receive non-operating income in greater amounts than operational income
- Substantial and sudden changes in liquidity volumes, particularly in cash, compared to the normal development of business
- Companies that present high volumes of cash purchases and a high percentage do so in cash
- Unjustified growth in revenue when you do not have important or stable clients
- Early cancellations of obligations for important values.
- Unexpected payment of an overdue debt, without plausible explanation.
- Prepayment of obligations, without justification
- Early cancellation of obligations without reasonable justification of sources of income.
- Companies that sell merchandise unrelated to their corporate purpose.
- Companies with low capital and assets, which carry out operations for high amounts.



	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 49of 52
		VERSION: [DOCUMENTVERSION:MN-004]


### SUPPLIERS AND CUSTOMERS<sup>3</sup>

#### LINKAGE AND ANALYSIS OF SUPPLIER INFORMATION

- That in the interview, the Supplier appears reluctant or annoyed to answer questions, or that his answers are evasive in the face of knowledge of the same
- That shows reluctance to provide identification documents of its owners or references
- The data provided is not consistent or true, it is outdated, unverifiable or insufficient and the Provider insists on not clarifying or completing it.
- Potential suppliers whose business or financial sources are unclear, or who are reluctant to provide details about the source of their funds
- That they refuse to reveal relationships with other companies or financial institutions
- Threat or attempt to bribe the entity's official in order to get him or her to accept incomplete or false information
- Supplier whose operations do not correspond to those of the market
- Carry out operations through an agent without there being a valid reason to use this mechanism
- When the same person acts as legal representative or owner of different companies, they all have the same address or telephone number.
- Register a post office box as an address or the company address matches that of other companies with no apparent link
- That the Supplier or some of the administrators or partners appear on the control lists adopted by the company or have appeared in the media or on the lists classified as allegedly linked to illegal activities
- The financial situation of the company does not match the type of income from the activity of the company or its partners
- Supplier that refuses to inform the origin of its resources
- Supplier without the minimum required information
- Information is not consistent with that obtained by the company
- Little recognized suppliers in the market that make high volumes of purchases and the date of incorporation of the company is recent
- Suppliers who refuse to sign the declaration on ML/TF prevention defined by the company
- Suppliers whose sources of financing may come from illegal fundraising resources or money tables not authorized to manage public resources
- Disinterest in obtaining financial advantages
- Companies that have as owners or directors people from lower strata and with economic difficulties and that handle large volumes of money
- Several companies have partners, managers, administrators or legal representatives in common, without having been reported as a business group, nor with a clear justification.
- Supplier whose operations do not correspond to the financial information provided
- They frequently change their data; bank account number, address, telephone, etc.
- Companies that have a very low subscribed capital and/or a very broad corporate purpose.
- Presents a debt that does not correspond to the declared income
- Companies that do not have agencies or branches, however, carry out several operations involving large sums in different cities or countries, which do not have a clear relationship with their economic activity.
- In the financial study, the company has a high degree of liquidity and its activity, according to market evaluation, normally does not maintain or generate it.
- The company refuses to receive company officials in its offices
- Supplier who, having the status of subjects obliged to adopt ML/TF prevention systems, refuse to subscribe to the certification required by the company
- Suppliers who request the transfer of the contract or the economic rights of the contract, without clear justification.

<sup>3</sup> Taken from the "Risk Management Model for money laundering, terrorist financing (ML/TF) and smuggling for the Foreign Trade Sector" – DIAN and the United Nations Office on Drugs and Crime (UNODC).

Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 50 of 52
		VERSION: [DOCUMENTVERSION:MN-004]

- Suppliers who refuse to provide the list of partners who have 10% or more of the share capital.
- Greater weight in the composition of assets for non-essential goods for the company
- Significant amounts of accounts payable to individuals when they do not have a clear link with the company or defined economic activity
- Companies older than one year with significant assets without justification.
- Companies with income higher than the average of the economic sector to which it belongs.
- Companies that have been established with low capital, receiving large sums of investment shortly after, whose origin is unknown
- Companies with operating margins very far from the average
- Significant change in declared assets from one year to another. Assets not declared in a fiscal period.
- The Supplier is a politically exposed person - PEP (for example: people who hold public positions, with public recognition, who manage public resources)
- Sources of capital are not clear or justifiable


- EXECUTION OF THE CONTRACT**
- The company has new owners
  - The company was acquired being in financial difficulties in meeting its obligations
  - The company presents overwhelming profits in a short period of time
  - The company was established with little capital, shortly after receiving large sums of investment, mainly foreign.
  - They make large investments despite having been created very recently
  - Companies receive non-operating income in greater amounts than operational income
  - Supplier that initially carries out transactions for low amounts, but in a short time they increase them to high amounts
  - The company's inventories do not match the information held by the company
  - Untimely request for an increase in space and its sales are not related to the request.
  - Substantial and sudden changes in liquidity volumes, particularly in cash, compared to the normal development of business
  - Provider who refuses to update basic information.
  - Suppliers that present high volumes of cash purchases and a high percentage do so in cash
  - Entry of unknown partners
  - Capital injection without justification
  - Substantial change in the participation of the company with the entry of a new partner when there is no capital injection (regardless of family ties)
  - Unjustified change in liabilities from a larger amount to a much smaller one or vice versa
  - Unjustified growth in revenue when you do not have important or stable clients

- PAYMENTS**
- Request for early cancellations of obligations for important values.
  - Request for payment with endorsed checks
  - Request for large, non-usual cash payments
  - Request for unexpected payment of an overdue debt, without plausible explanation.
  - Request for prepayment of obligations, without justification
  - Request for early cancellation of obligations without reasonable justification of sources of income.
  - Request for payment of obligations in favor of third parties

- EMPLOYEES<sup>4</sup>**
- Official who:
- Frequently processes operations in which they accept or make exceptions for a specific client or user.

<sup>4</sup>Taken from the "Money Laundering Risk Manual in Financial and Commercial Instruments" prepared by the United Nations Office on Drugs and Crime (UNODC).


Revision date:[DOCUMENTDATEVISION:MN-004] Reviewed by:[USERDOCUMENTREVIEW:MN-004]	Approval date:[DOCUMENTAPPROVALDATE:MN-004] Approved by:[USERDOCUMENTAPPROVAL:MN-004]
--	--

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 51 of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

- Avoids certain internal or approval controls established for certain transactions, products or services.
- They frequently make errors, mismatches or inconsistencies and their explanations are insufficient or inadequate.
- It omits verification of a person's identity or does not compare the data and/or fingerprints with the records provided in the entity's formats or databases.
- Prevents other colleagues from serving certain clients or users without apparent justification.
- Frequently serves the same client or user whom he or she appears not to know (especially a commercial advisor)
- Documents or partially supports the information or transactions of a client or user without a clear and reasonable justification (especially commercial advisor)
- Serves preferentially, exclusively and permanently or exempts a client from certain controls with the argument that he is "quite well known", "referred from another entity", "he only trusts me", "I advise him on all his businesses" or similar. (especially business advisor)
- He is frequently absent from his workplace without a clear and reasonable excuse.
- Frequently receives gifts, invitations, gifts or other presents from certain clients or users, without a clear and reasonable justification.
- Who frequently remains at the workplace after the usual time or attends it outside normal working hours without a clear and reasonable justification.
- You are reluctant to take your vacation or accept changes or promotions in your work activity without a clear and reasonable justification.
- You have a lifestyle or carry out financial and investment transactions that do not correspond to the amount of your income (work or other known) without a clear and reasonable justification.

#### SUMMARY OF MODIFICATIONS AND UPDATES

MODIFICATION DATE	RESPONSIBLE	MODIFICATIONS
July, 2020	Nelson Montezuma / Elsa Paez	<ul style="list-style-type: none"> <li>• Area identification update</li> <li>• Adjustment of functions and procedures according to the current situation of the Company</li> <li>• Clear identification of those responsible in each critical area.</li> <li>• Steering Committee as a control body: The compliance officer will raise the cases that he considers relevant to the Steering Committee, to make the pertinent decisions in accordance with the Manual, regarding operations that are considered unusual, with third parties.</li> <li>• Relation of responsibilities of the Manual with policies of critical areas (purchasing policy, customer creation policy, etc.)</li> <li>• Identification of specific controls by critical area</li> <li>• Update of criteria for identification of non-admitted counterparties.</li> <li>• Updating information on induction, re-induction and training programs, according to the e-learning program of the G&amp;O Training area</li> </ul>
August, 2021	Nelson Montezuma / Elsa Páez Sarmiento	<ul style="list-style-type: none"> <li>• Regulatory update</li> </ul>

	MANUAL	NUMBER: [DOCUMENTCODE:MN-004]
	<b>SELF-CONTROL AND COMPREHENSIVE RISK MANAGEMENT SYSTEM OF MONEY LAUNDERING, FINANCING OF TERRORISM AND FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION</b>	PAGE: 52 of 52
		VERSION: [DOCUMENTOVERSION:MN-004]

September, 2023	Nelson Montezuma / Laura Rodríguez Mayor	<ul style="list-style-type: none"> <li>• Inclusion of definition of close associates.</li> <li>• Decrease in the limit amount of individual and monthly cash operations allowed by JGB.</li> <li>• Modification of the treatment given to counterparties linked to crimes related to ML/FT/FPADM.</li> <li>• Inclusion of labor disciplinary offenses applicable to non-compliance related to processes and procedures contained for the control of ML/FT/FPADM</li> </ul>
-----------------	---	--

<sup>i</sup>When the sanction consists of suspension from work, it cannot exceed eight (8) days for the first time, nor two (2) months in case of recidivism of any degree. (Art 112 CST)

<sup>ii</sup>When the sanction consists of suspension from work, it cannot exceed eight (8) days for the first time, nor two (2) months in case of recidivism of any degree. (Art 112 CST)