



DeepL

Subscribe to DeepL Pro to edit this document.  
Visit [www.DeepL.com/pro](https://www.DeepL.com/pro) for more information.



Rymel

Nos mueve crear juntos

SA-CER505894

SC278-1

OS-CER617167

CERTIFICADO BASC  
COLUMBEO0328-1  
COPACABANA

## **SAGRILIFT AND BUSINESS ETHICS MANUAL**

### **MANUAL OF THE SELF-CONTROL AND INTEGRAL RISK MANAGEMENT SYSTEM FOR MONEY LAUNDERING, FINANCING OF TERRORISM AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION AND BUSINESS ETHICS PROGRAM**

## Table of Contents

INTRODUCTION.....	5
Title .....	6
Key words.....	6
Scope .....	10
Objectives.....	11
General .....	11
Specific .....	11
Regulatory Framework.....	11
SAGRILAFT Stages and Business Ethics .....	13
Identification of ML/FT/ATF/MFATF, bribery and corruption risks.....	13
Measurement or assessment of ML/FT/AMLF risk.....	13
Probability assessment .....	13
Impact assessment .....	15
Inherent risk assessment .....	16
Control of ML/FT/ATF/MFATF, bribery and corruption risks .....	16
At the time of the business partner's engagement .....	16
Updating and follow-up.....	17
Analysis of findings .....	17
ML/FT/ATF/MFATF, corruption and bribery Risk Monitoring .....	20
Risk Factors .....	21
SAGRILAFT Structure .....	22
Policies.....	23
LA/FT/FPADM Policies.....	23
General AML/CFT/ATF/MFATF Policy .....	23
Conflict of interest policy .....	24
Due diligence policy and knowledge of counterparties .....	25
Aspects that represent greater exposure to ML/FT/ATF/MFATF risk.....	25
Documentation storage and handling policy.....	26
Policy on suspicious transaction reporting .....	26
Risk factor management policy .....	27

Cash Management Policy .....	27
Virtual Assets Transaction Policy .....	27
Policy for entering new markets .....	27
Outreach and training policy.....	27
Reservation policy on the request for information by authorities .....	28
SAGRILAFI Non-Compliance Consequences Policy .....	28
Anti-corruption and bribery policy.....	29
Reach .....	29
Performance parameters .....	29
Relationship to other policies and codes .....	30
Non-compliance.....	30
Procedure .....	30
Documentation and due diligence .....	30
Knowledge of business partners, customers and/or suppliers .....	30
Simplified due diligence on customers and suppliers.....	32
Enhanced due diligence.....	33
Employee knowledge .....	34
Employee control and monitoring.....	34
Knowledge of shareholders .....	34
Knowledge of compliance officer and alternate compliance officer .....	34
Knowledge of Publicly Exposed Persons (PEP).....	35
Detection, determination and analysis of unusual and suspicious transactions .....	35
Detection and analysis of unusual transactions .....	35
Warning Signs.....	36
Transactions or activities with counterparties, related to: .....	36
Transactions, businesses or contracts that represent, have as their object or involve..	38
Warning signs employees .....	39
Internal reporting of red flags and unusual transactions .....	41
Determination of suspicious transactions .....	41
Suspicious transaction report .....	41
Other external reports.....	42

Report of absence of attempted or suspicious transaction ("A-ROS") to UIAF .....	42
Documentation and archiving of the cases analyzed.....	42
Organizational structure and functions .....	43
Roles and responsibilities.....	43
Functions of the board of directors .....	44
Functions of the legal representative .....	44
Compliance officer functions .....	45
Functions of the statutory auditor .....	47
Purchasing functions.....	48
Human resources functions .....	49
Employee functions .....	49
Attention to requests from authorities .....	50
Imposition of penalties .....	50
Disclosure.....	50
Training .....	51

## INTRODUCTION

Money laundering and terrorist financing represent a significant threat to the economic and reputational stability of Rymel Ingeniería Eléctrica S.A.S., and of the companies and markets in which it develops its commercial activity.

The high international exposure and the trade of its products in the different jurisdictions of the country make it more vulnerable and it is essential that the company's management implements good practices to prevent criminal organizations from using its operations and resources for money laundering or for channeling assets to terrorist activities.

In order to create this conviction and culture in the organization and generate a commitment to prevention beyond legal compliance, this manual establishes the criteria and parameters to be taken into account for the involvement of our business partners and the follow-up controls to guarantee the operation of the system.

## Title

SAGRILIFT manual and business ethics (manual of the self-monitoring and integral risk management system for money laundering, financing of terrorism, proliferation of weapons of mass destruction and business ethics program).

## Key words

**Shareholder:** The natural person or legal entity that owns the shares of Rymel S.A.S.

**Administrator:** The legal representative, liquidator, member of the Board of Directors who, in accordance with the bylaws, will perform these functions.

**Beneficial owner:** The natural person who controls 5% or more of the shares, voting rights or yields, profits or assets of the legal person, or on whose behalf a transaction is carried out; it is also the person who exercises ultimate effective control over a legal person.

When no natural person is identified who complies with the preceding paragraph, he/she will be the one 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 person.

**Business partners:** Any natural or legal person that maintains a commercial, contractual or any other type of relationship, framed within the national and international supply chain of Rymel S.A.S.; that is to say: shareholders, partners, employees, intermediaries, clients and/or suppliers of goods and services.

**Critical client:** A client that, when evaluated according to the criteria of jurisdiction risk, country risk, amount, frequency of transactions and legal nature, is rated as such in the risk matrix.

**Critical supplier:** A critical supplier is one that, when evaluated according to the criteria of jurisdiction risk, country risk, amount, frequency of transactions and legal nature, trajectory and dependence of its product, yields this rating in the risk matrix.

**Distribution channel:** The means by which products or services are offered or marketed.

**Financing of terrorism:** Financial support in any form to terrorism or to those who encourage, plan or are involved in it.

**Jurisdiction:** It is the geographical location where the service is provided and the commercial relationship with the business partner is legalized.

**Money laundering:** This is known as money laundering, money laundering and includes all actions to give the appearance of legality to resources of illicit origin.

**Binding lists:** These are those lists of entities binding Colombia, where persons associated with terrorist organizations are listed.

**Compliance Officer:** The person in charge of overseeing the System, promoting and developing specific procedures for the prevention, updating and mitigation of ML/FT/FPADM risk, as well as the transparency and business ethics program.

**Unusual transaction:** A transaction whose amount or characteristics are not related to the company's investments, or which does not fall within the normal patterns or ordinary business practices in the sector, industry or counterparty.

**Suspicious transaction:** An unusual transaction that, according to the uses and customs of the type of investment or relationship with a counterparty, could not be reasonably justified.

**Politically Exposed Person (PEP):** Public servants of any nomenclature and job classification system of the national and territorial public administration. When in the positions they occupy, they have in the functions of the area to which they belong or in those of the employment record they occupy, under their direct responsibility or by delegation, the general direction, formulation of institutional policies and adoption of plans, programs and projects, direct management of goods, money or securities of the State; these may be through expenditure management, public procurement, management of investment projects, payments, liquidations, administration of movable and immovable property.

**PEPs of international organizations:** Those individuals who perform managerial functions in an international organization, such as the United Nations, the Organization for Economic Cooperation and Development, the United Nations Children's Fund (UNICEF) and the United Nations Development Program (UNDP).

Organization of American States, among others (directors, assistant directors, members of the board of directors or any person exercising an equivalent function).



**Foreign PEP:** Those natural persons who perform prominent and outstanding public functions in another country. In particular, the following persons: heads of state, heads of government, ministers, undersecretaries or secretaries of state, congressmen or parliamentarians, members of supreme courts, constitutional courts or other high judicial instances whose decisions do not normally admit of appeal, except in exceptional circumstances; members of courts or boards of directors of central banks, ambassadors, chargés d'affaires, senior officials of the armed forces, members of administrative, management or supervisory bodies of state-owned enterprises, members of reigning royal families, prominent leaders of political parties or movements, legal representatives, directors, deputy directors, members of senior management and members of the board of an international organization.

**Internal reports:** These are reports made within the company by any employee who becomes aware of a possible unusual or suspicious operation; internal reports are also those that the compliance officer must submit at least once a year to the board of directors.

**Reputational risk:** The possibility of loss incurred by an entity due to loss of prestige, bad image, negative publicity, whether true or not, with respect to the institution and its business practices, causing loss of clients, decrease in income or legal proceedings.

**Legal risk:** The possibility of loss incurred by a company when it is penalized, fined or required to pay damages as a result of non-compliance with rules or regulations and contractual obligations.

**Operational risk:** The possibility of incurring losses due to deficiencies, failures or inadequacies in human resources, processes, technology, infrastructure or the occurrence of external events.



**Contagion risk:** Possibility of loss that a company may suffer directly or indirectly from an action or experience related to ML/FT/AML/CFT. The business associate includes natural or legal persons who have the possibility of exercising influence over the company.

**ML/TF/ATF/AMLF risk:** It is the possibility of loss or damage that the company may suffer as a result of being used as an instrument for ML/TF/AMLF. It is expressed in terms of probability (opportunity or frequency of occurrence of the risk) and impact (consequence in case of occurrence or materialization of the event).

**Risks associated with ML/TF/TFTPDM:** These refer to the consequences or impact that the Company may suffer, derived from the materialization of the ML/TF risk; these may be:

**Legal risk:** The possibility of loss or damage incurred by the company, its shareholders, its administrators or any other related person, being sanctioned, fined or obliged to compensate damages as a result of non-compliance with rules or regulations related to the prevention of ML/FT/FPADM.

**Inherent risk:** This is the level or profile of risk inherent to the company's activity, without taking into account the effect of ML/TF/TFATF/MFATF risk controls.

**Residual risk:** It is the level or profile resulting from the company's risk after applying controls to ML/FT/FPADM risk.

**Warning signs:** These are particular circumstances that attract attention and warrant further analysis.

**SAGRILAF:** This refers to the company's system of self-monitoring and management of ML/FT/ATF/MFATF risk.

**Business ethics and transparency program:** This is the transparency and ethics program managed by the company's management to ensure regulatory compliance and preserve the good name of the organization by avoiding corruption and always acting ethically and transparently.

**Terrorism:** **Terrorism** is defined as any act intended to keep the civilian population in a state of anxiety through acts that endanger life, integrity or freedom by using instruments capable of causing havoc. The instruments used may originate from both legitimate and illegitimate sources.

**UIAF:** Acronym for the Financial Information and Analysis Unit and refers to the entity attached to the Colombian Ministry of Finance and Public Credit in charge of centralizing, systematizing and analyzing data related to ML/FT/FPADM operations.

**Bribery:** It is a crime when an official, collaborator or any member of the company accepts or demands a bribe to carry out or omit an action.

**Transnational bribery:** The act by virtue of which the company, through its employees, senior management, associates, contractors or subordinate companies, gives, offers or promises to a public servant, directly or indirectly: (i) sums of money, or objects of pecuniary value or (ii) any benefit or utility in exchange for said public servant performing, omitting or delaying any act related to his functions and in connection with an international business or transaction.

**Corruption:** It is any act, attempt or deliberate omission to obtain a benefit for oneself or for third parties to the detriment of organizational principles, independent of the financial effects on companies. These are actions that can be presented under the following modalities:

**Internal:** Acceptance of bribes from third parties to company employees, so that their decisions, actions or omissions benefit that third party.

**Corporate:** acceptance of bribes from company employees to government officials or third parties, directly or through agents, so that the third party's decisions, actions or omissions benefit the company or an official of the company.

## Scope

This manual involves all shareholders, employees, customers, suppliers and other

strategic allies commercially or contractually linked to the company's operations. In order to prevent money laundering, terrorist financing, corruption and bribery, policies and guidelines are established to mitigate these events.

## Objectives

### General

To implement the guidelines and controls to comprehensively develop the necessary elements for the prevention of risks associated with corruption, bribery and money laundering in Rymel S.A.S., through a system of ML/FT/FPADM risk management, business ethics in the execution of contractual activities.

### Specific

- Establish procedures to minimize the probability of reputational risk to which the company is exposed in the event of being subject to fraudulent operations.
- Define the methodology for linking and monitoring business partners, identifying the origin of the resources.
- Implement linkage, follow-up and control policies applicable to the conduct of business associates.
- Evaluate the operation of the system to ensure legal compliance.

## Regulatory Framework

The main rules that govern legal compliance for Rymel S.A.S., and integrate the set of guidelines to be followed to conduct business with ethics and transparency are:

**Law 1778 of 2016, Congress of the Republic:** known as the "anti-bribery law", whereby rules are issued on the liability of legal persons for acts of transnational corruption and other anti-corruption provisions.

**Resolution 100-006261 of October 2, 2020:** The Superintendence of Companies issued this resolution that expands the criteria to determine which companies are obliged to adopt transparency and business ethics programs.

**Circular 100-000003 of 2016 Superintendency of Companies:** Guide aimed at implementing business ethics programs for the prevention of the conducts provided for in Article 2 of Law 1778 of 2016.

**Circular 100-000016 of 2020 Superintendency of Companies:** Integral modification of Chapter X of the basic legal circular of 2017, aims to deepen the risk-based approach, both in the supervision of this entity and in the creation of policies and matrices by commercial companies and companies obliged to comply with the SAGRILAF regime and reports to the UIAF of suspicious transactions.

**Chapter X of the Basic Legal Circular of the Superintendence of Corporations ("Circular"):** This rule obliges supervised companies to design and implement a SAGRILAF when they meet the criteria of economic activity and total income defined in the Circular. Specifically, the regulation states that companies in the real sector that, as of December 31 of the immediately preceding year, have obtained total revenues equal to or greater than 40,000 SMLMV, are obliged to implement the SAGRILAF.

**Resolution 285 of 2007 UIAF:** Whereby public and private warehouses, customs brokerage companies, port companies, free zone users, transportation companies, international cargo agents, permanent customs users and highly exporting users are required to report directly to the Financial Information and Analysis Unit.

**Circular 170 of 2002:** Prevention and control of money laundering. By which the procedure to be followed by the users of the customs and exchange service to prevent, detect, control and report suspicious operations that may be linked to money laundering is indicated.

**Law 1708 of 2014 Code of Extinction of Ownership:** According to Article 119 of the Code of Extinction of Ownership, every person, including the company, has the obligation to inform the Attorney General's Office of the Nation about the existence of assets that they have detected in the course of their activities and that may be subject to the action of extinction of ownership.

**Law 1121 of 2006:** Establishes that individuals, including the company, must report to the UIAF and the Attorney General's Office when they have knowledge of the presence or transit of a person included in one of the international lists binding Colombia in accordance with international law. In this sense, the company must make periodic

consultations in the list issued by the United Nations Security Council (UN); as well as the restrictive list of individuals and entities linked to terrorist activities approved by the National Security Council Act of January 17, 2020, regarding the persons with whom it maintains any type of link.

## **SAGRILIFT stages and business ethics**

### **Identification of ML/FT/ATF/MFATF, bribery and corruption risks**

Aware of the economic, reputational and legal impact generated by the materialization of the ML/FT/FPADM risk, as well as the risk of corruption, bribery and contagion caused by involvement with counterparties that may be related or affected by crimes associated with such risks; Rymel S.A.S., performs the due diligence process identifying the alerts raised for control, monitoring and follow-up.

It also assesses and controls them by means of the company's general risk matrix, which contains the sources, main areas where they are generated, the impact, causes, probability of occurrence and possible consequences.

### **ML/FT/AMLF risk measurement or assessment**

The inherent risk rating is obtained from the weighting of the probability and impact analysis, calculated based on the probability of occurrence. Therefore, the following valuations are defined:

### **Probability assessment**

The probability of occurrence refers to the possibility of the occurrence of a ML/FT/AML/CFT, bribery or corruption risk event. This can be measured based on frequency criteria or taking into account the presence of internal and external factors that may favor the risk, even if it has not materialized.

<b>PROBABILITY</b>		
<b>Score</b>	<b>Rating</b>	<b>Description</b>

5	Highly probable	The situation has frequent and continuous occurrence. The materialization of the risk occurs frequently or permanently.
	Likely	The situation occurs frequently but not continuously. The materialization of the risk may occur several times in a period.
	Occasional	The situation has an average occurrence. The materialization of the risk may occur sometime.
	Remota	The situation has a sporadic occurrence. Materialization is to be expected at a minimum level.
1	Improbable	The situation has never occurred or is unlikely to occur. Nevertheless, the risk is conceivable.



## Impact assessment

The impact is the consequence that may result from the materialization of the risk.

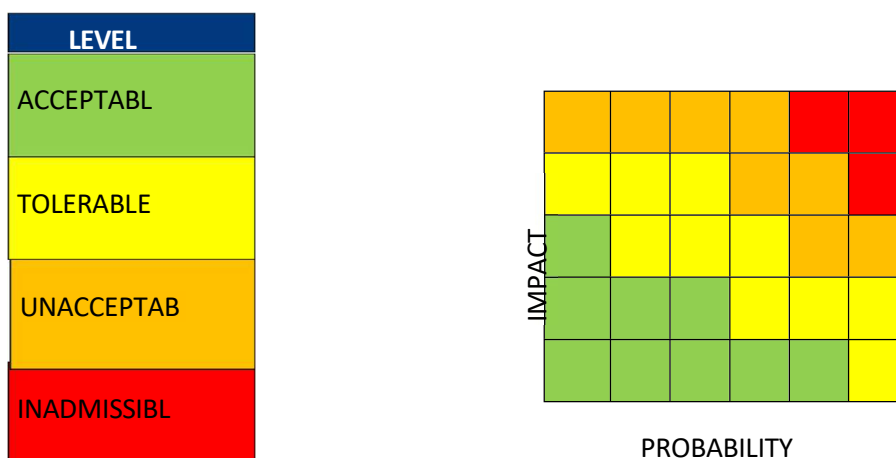
IMPACT		
Score	Rating	Description
5	Catastrophic	The materialization of the risk causes substantial economic losses and can lead to the total suspension of the company's activities.
	Mayor	The materialization of the risk causes considerable economic losses and may result in the temporary suspension of several of the company's activities.
	Moderate	The materialization of the risk causes economic losses and may result in the temporary suspension of one or more of the company's activities.
	Menor	The materialization of the risk has an impact and may generate indirect economic losses, but does not cause a suspension of the company's activity.
1	Insignificant	The materialization of the risk does not have a significant impact on the Company's business.

These probability and impact criteria will be reviewed periodically to adjust, increasingly, the risk matrix according to the corporate purpose of Rymel S.A.S., and the characteristics of its processes so that these are adjusted to the risk identified.



As a result of this stage, the company is able to establish its inherent risk profile by multiplying the probability score by the impact score, as follows:

### Inherent risk assessment



### Control of ML/FT/ATF/MFATF, bribery and corruption risk.

The company initiates the system with the ML/FT/FPADM, bribery and corruption risk control mechanisms described in this manual to prevent, control or mitigate the risk. These controls will be strengthened according to the result of the follow-ups, with the purpose of establishing the residual risk profile.

The objective is to mitigate the risk, taking the necessary measures to reduce the probability of occurrence and/or the impact to which Rymel S.A.S. is exposed, for which the following controls are established:

### At the time of the business partner's engagement

- Minimum documentation, detailed in the due diligence procedure (see business partner procedure A-GL-06).
- Queries in restrictive lists: A detailed report of the different lists is generated and, in addition, if there is any investigation process for corruption or similar offenses, it is reflected in the query and the table of matches for follow-up is filled in.
- PEP Declaration: If you are a PEP, you must fill out the PEP declaration form and

- Declaration of origin of funds: This is contained in the F-GL-04 and by means of it, the business partner declares that its resources come from a lawful origin.
- The code of ethics and this manual define the term conflict of interest, which is disclosed and prohibits employees from receiving gifts, gifts, incentives, among others, in order to purchase a good or award supply contracts to Rymel S.A.S.
- Corruption and bribery policy: This policy is disclosed to employees, suppliers, contractors and in general to all counterparties.
- Verification of referrals: References are verified by telephone to business associates of den as critical results. If this is not possible, an observation is made in the respective linkage form.
- Home visits to critical suppliers in the supply chain.
- Preservation and enumeration of the folders with documentation of each business associate.
- Record in the F-GL-08 format "registration of domestic customers", F-GL-32 "registration of foreign customers and suppliers", F-SC-02 "registration of domestic suppliers".
- Record of the coincidences found for later analysis and follow-up.
- Approval of entry into the ERP system.

## Updating and follow-up

It is required to update the business partner annually; identifying administrative and financial changes complying with the same procedure as at the time of linkage.

## Analysis of findings

Business associates with inconsistencies or any report in a restrictive list are subject to the respective analysis and consultation process in the different pages. If pertinent, the board of directors will be informed.

Each year the effectiveness of controls will be evaluated according to the following risk measurement table:

Level	Action Plan
<b>Under</b>	Risks at this level are a minor threat to the company and do not require additional measures or controls. They should be monitored at least every two years. This level of residual risk can be accept, mitigate or transfer.
<b>Medium</b>	Risks at this level affect the company and must be dealt with by the employee or area affected in the medium term, applying satisfactory measures to mitigate them. Its monitoring must be done at a minimum annually. This level of residual risk must be mitigated or transferred.
<b>High</b>	Risks at this level represent a significant threat to the company's The company and must be treated in the short term to ensure a decrease in its level or its causes must be avoided. Likewise,

	must be permanently monitored, at least once a once on a semi-annual basis. This level of residual risk must be mitigated, transferred or avoided.
<b>End</b>	Risks at this level represent a high threat to the company and must be treated immediately to ensure a decrease in their level or their causes must be avoided. Likewise, they must be monitored permanently, at least quarterly. This level residual risk should be avoided.

Rating of the risk	Description
<b>Under</b>	Risk is considered tolerable for the organization, its occurrence may cause non-significant losses. These risks can be accepted or treated with control actions to reduce the probability of occurrence. of occurrence or impact.
<b>Moderate</b>	The risk is moderate, its occurrence could cause losses of some consideration. It requires response actions to reduce it.
<b>High</b>	The risk is very significant and requires response actions for and transfer it. Its occurrence could cause serious losses to the Company.
<b>End</b>	The risk is unacceptable or critical because, if it were to materialize, its consequences would destabilize the company. It requires actions immediate response to prevent and/or reduce it.

**ML/FT/ATF/MFATF, corruption and bribery Risk Monitoring**

The compliance officer shall continuously monitor the system in order to evaluate the timeliness, effectiveness and efficiency of the controls, ensuring that they are comprehensive and address all identified ML/TFTP/AML/CFT, bribery and corruption risk events. This monitoring shall be performed at least annually. Any deviation shall be reported to the board of directors.

Monitoring should be the responsibility of the compliance officer with the respective collaboration of the committee and the leaders of the processes, and its purpose is to apply and suggest corrective actions and adjustments necessary to ensure effective management of ML/TFTP/ATF, bribery and corruption risk.

After monitoring, the compliance officer will evaluate the results and, together with the committee, will make proposals for improvement and treatment of the situations detected to the legal representative and the board of directors.

The statutory auditor will also conduct periodic reviews to facilitate the detection and correction of deficiencies in SAGRILAF and the transparency and business ethics program, the results of which are communicated to the board of directors, the legal representative and the compliance officer so that he/she may take the necessary measures to address the deficiencies reported.

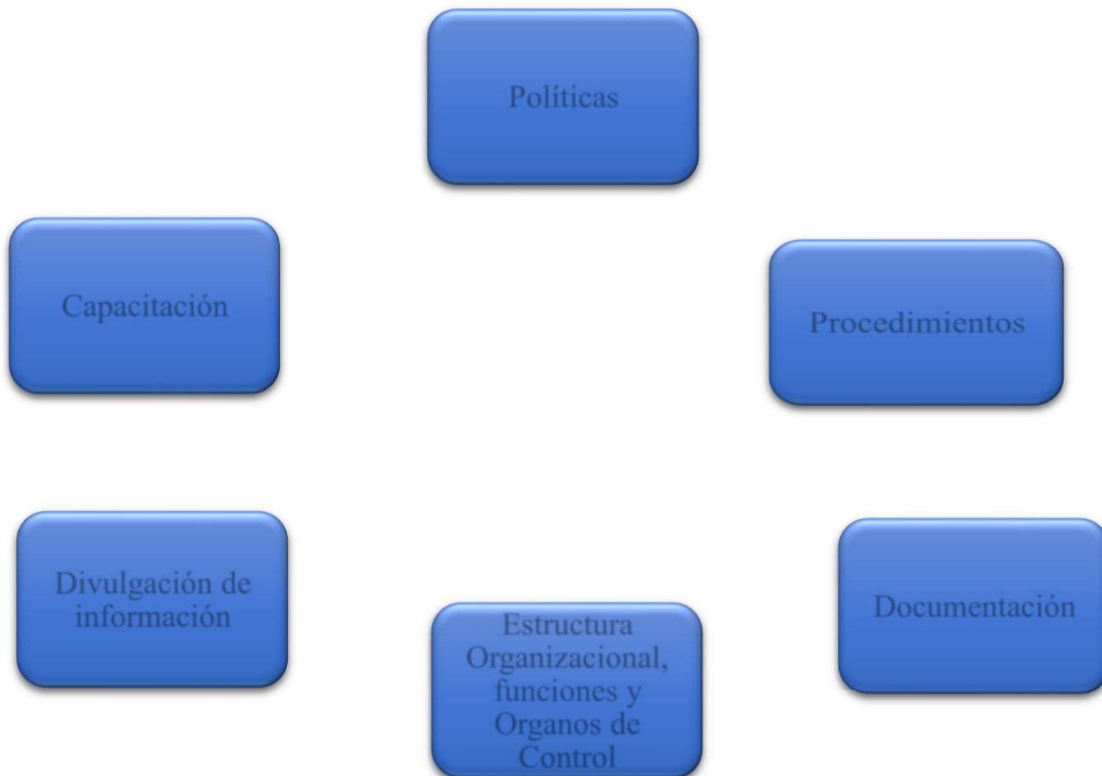
## Risk Factors

Rymel S.A.S. identified the following risk factors in its operations, business and/or contracts:

Factor of Risk	Description
Counterparts	These are all those natural or legal persons with whom the organization establishes or maintains some type of contractual or legal relationship in the development of its activities, such as shareholders, contractors, employees, suppliers and customers.
Jurisdiction or Areas geographic	It is the geographic location where the operations of the organization's object are carried out and in which a higher or lower level can be determined. risk to ML/FT/ATF/AMLF.
Services and/or Products	These are legally authorized operations that may be carried out by supervised entities through the execution of contracts.
Channels from distribution	These are the channels used by the organization to distribute its products and services. products.

## Structure of SAGRILIFT

Taking into account the identification of risks, and the fact that a system is an ordered module of elements that are interrelated and interact with each other, the following structure is established for SAGRILIFT:





## Policies

### LA/FT/FPADM Policies

#### General ML/FT/FPADM Policy

- The board of directors, and the administrators of Rymel S.A.S., declare and state that the company:
- Compliance with ML/FT/ATF/ AML/CFT prevention regulations is prioritized over the achievement of investment goals. The prevention, detection and monitoring of ML/FT/ATF/MFATF risk shall be applied to all business activities.
- It has the duty and commitment to ensure compliance with the law and regulations aimed at preventing and detecting ML/TF/TFTPDM, with a view to protecting its image and reputation.
- It may refrain from carrying out any operation, and shall report it to the competent authorities as soon as it can reasonably determine that the monies related thereto are the proceeds of or are intended to finance or support illicit activities.
- The Company declares that its employees and other counterparties are aware of, apply and comply with the provisions of this manual, under penalty of the respective sanctions set forth herein and the appropriate criminal and administrative consequences.
- Actively collaborate with the competent authorities in relation to the prevention and control of ML/FT/AML/CFT, giving timely response to their requirements, providing them with all the information considered pertinent and complying with the corresponding legal and regulatory provisions.

## Conflict of interest policy

No business or transaction may be carried out that puts the company at risk of ML/FT/AML/CFT, nor shall the omission of ML/FT/AML/CFT risk control procedures and measures be authorized in order to favor any investigation case.

The following situations shall be considered conflicts of interest related to LF/FT/FPADM:

- In the consultation in control lists, the analysis of unusual operations, the study of suspicious operations and making STRs: When the consultation, study, analysis or report has been made by an employee on the spouse or permanent partner, relatives within the fourth degree of consanguinity, second degree of affinity or first civil degree, in which the person in charge of making the consultations has any personal interest, direct or indirect, on the result.
- In making reports to the authorities: When in the decision making on the origin of the external report affects the person in charge, directly or indirectly, or when the report or the decision on the operations carried out, are carried out by the spouse or permanent partner, relatives within the fourth degree of consanguinity, second degree of affinity or first civil degree.
- In any of the above events, the person in conflict of interest shall report it directly to the compliance officer. In the event that the person in conflict of interest is the compliance officer and it is the compliance officer who notices the conflict of interest, he/she must immediately withdraw from the situation and delegate all his/her functions in relation to the matter to the alternate compliance officer. In the event that a third party becomes aware of the compliance officer's conflict of interest, he/she shall notify the board of directors so that the board may designate another person to carry out these tasks.

## **Due diligence policy and knowledge of counterparties**

Rymel S.A.S., has as one of its main mechanisms of control and prevention of ML/FT/FPADM risks the adequate knowledge of its counterparties, at the moment of their engagement and during the contractual relationship.

It will make its best effort to obtain the documentation according to the due diligence, for the linking or updating of the business partner. In those cases in which it is not possible to obtain complete documentation, the process of getting to know the client will be carried out to the extent possible and will be submitted for approval by the board of directors, the convenience or not to continue with the commercial transactions with such business associates.

Likewise, it shall verify that the information provided by the counterparty is updated at least every two years (according to the criticality of the business partner, see detailed controls in the selection and linkage procedure), in order to know the possible changes in its activity and financial information; however, some counterparties may expose the company to greater ML/TF/TFTPDM risks than others; therefore, the management and the compliance officer shall take into account the following aspects that represent

The company performs due diligence by identifying its counterparties, according to the following criteria:

- Source of resources.
- Jurisdiction in which they operate.
- Final beneficiaries of economic resources (shareholder composition).
- Economic and legal impact according to the amount of commercial operations.
- Continuous monitoring of management changes through data updates.
- Rating according to the criticality matrix.
- Consultations in binding and restrictive lists.

The findings or coincidences will be evaluated by the compliance officer taking into account the impact they may cause; they will be submitted to the evaluation of the management for its decision to link or continue with the commercial relationship between the two parties.

## **Aspects that represent greater exposure to ML/FT/ATF/MFATF risk**

**Jurisdiction:** Counterparties located in non-cooperative countries and high-risk

jurisdictions that are listed by the Financial Action Task Force (FATF)<sup>6</sup> and the Basel index<sup>7</sup> ; on the latter, high-risk jurisdictions will be considered those with an overall rating above 6.5.

**PEP:** Due to the high risk posed by the relationship with publicly exposed persons, monitoring processes will be carried out periodically, in accordance with current regulations.

**Binding lists:** Rymel S.A.S., will investigate the matches of its counterparts thrown in the consultation in lists to determine their veracity, seriousness and impact they may cause in the company.

The pertinent supports will be submitted for analysis by the committee and the board of directors will be the one to approve the continuity of the commercial relationship with the business partner.

### Documentation storage and handling policy

The Company shall keep the manuals, code of ethics, policies, documents and records related to the system for the time defined in the standard, in order to ensure the integrity, timeliness, reliability and availability of the information contained therein.

At the end of this term, the documents may be destroyed, provided that the following conditions are met:

- That there is no request for the delivery of the same, formulated by the competent authorities.
- That they are kept in a medium that guarantees their subsequent accurate reproduction and the preservation of their probative value.

The information and documents submitted to the UIAF as support shall be under the safekeeping of the compliance officer and for no reason shall the counterparties have access and knowledge of them. Likewise, the information requested by said entity shall be kept confidential.

Rymel S.A.S., will keep a file in which it will keep all the documents of the system, guaranteeing the integrity, opportunity, reliability and availability of the information contained therein.

### Policy on suspicious transaction reporting

The company shall report to the UIAF those operations that, due to their amount,

characteristics and other elements, may qualify as suspicious operations. It is not required to be certain that it is a criminal activity, nor to identify the criminal type or that the resources involved come from such activities.

### **Risk factor management policy**

In cases where the residual risk is high or extreme, the operation or related transaction that may be affected by this risk shall be restricted until such time as the risk is reduced by the application of additional controls. The company's priority is the management of ML/FT/FPADM risk over the achievement of commercial or financial goals.

### **Cash management policy**

All payments to counterparties shall be made through the means provided by the financial system and in favor of the holder of the obligation. No cash will be received for amounts greater than COP 10,000,000.

### **Virtual asset transaction policy**

The company does not receive contributions, make investments or provide services related to virtual assets.

### **Policy for entering new markets**

Prior to entering new markets, the company shall identify the ML/TF/TFTPDM risk factors and events specific to the new market and define the relevant ML/TF/TFTPDM risk controls.

### **Outreach and training policy**

Management and the compliance officer shall promote a culture of AML/CFT/AML/CFT risk prevention through all means available in the company, down to the business

partners.

Rymel S.A.S., will disclose the policies and procedures for the prevention and control of ML/TF/ATF/ATF, through a training program directed to all the company's employees.

This manual will also be disclosed on the company's website for external counterparties.

Inductions will be carried out at the beginning of the relationship with the employee and a training schedule will be established periodically for all personnel.

### **Reservation policy on the request for information by authorities**

The company's employees will keep confidential reports and requests for judicial inspections by the authorities, as well as reports made to the UIAF.

### **Policy on consequences for non-compliance with SAGRILAF**

Non-compliance with this manual will be verified in accordance with the company's internal or contractual rules that regulate the relationship with counterparties. Any serious non-compliance in relation to the policies and/or procedures established in this manual, whether intentional, due to carelessness or negligence of any business associate, will be sanctioned in accordance with the commitments subscribed contractually, and in accordance with labor law; without prejudice to the civil, administrative and criminal consequences that such conduct may entail.



## Anti-corruption and bribery policy

Rymel S.A.S., committed to the security systems that integrate the company in order to preserve its reputation, that of its business partners and the commitment to act ethically and transparently, has created guidelines to conduct its business in a socially responsible manner, acting with a philosophy of transparency in everything related to corruption and bribery.

## Scope

The anti-corruption policy is applicable to all Rymel employees, administrators, business advisors and directors, regardless of the area or jurisdiction in which they provide their services; it is also applicable to contractors, suppliers, representatives or third parties acting on its behalf.

## Performance parameters

The main measures to prevent corruption and bribery are related to contracting, procurement and administration, and are strictly enforced in such a way that:

- No gifts or other offers that may interfere with healthy competition and free awarding of contracts are allowed.
- Commission rates or fees paid to distributors, agents, commission agents or consultants shall be reasonable in relation to the value of the service, product or work actually performed.
- Purchasing procedures will be carried out in accordance with the law, price lists and healthy competition. Therefore, purchasing decisions will be made objectively and based on the company's interests.
- Suppliers are bound by contract with Rymel, in which the commercial conditions, the service or product to be provided, the applicable rate or fees, terms of delivery and quality must be specified.
- Purchase agreements shall be clearly documented and identified, and must be kept on file in a secure location within the company's facilities.
- Representation expenses will be allowed only in accordance with the due attention inherent to the commercial relationship with our business partners.



- Employees and managers are obliged to strictly comply with their duties without incurring in acts such as money laundering, drug trafficking, bribery or any other act that may affect the reputation and good name of the company.

## **Relationship to other policies and codes**

This Policy complements and supports the terms defined in the code of ethics, business ethics program and the SAGRILAF policy manual, which contain guidelines to prevent and detect bribery and corruption.

## **Noncompliance**

Failure to comply with the anti-corruption policy is considered a violation of the employment or commercial contract with Rymel and will lead to the application of sanctions that may result in the termination of the contract. Ignorance of the policy does not exempt any recipient from its due compliance or the sanctioning regime.

This policy will be subject to the respective update for greater regulatory compliance or to prevent the occurrence of events of high reputational risk.

## **Procedure**

One of the main mechanisms to control and prevent money laundering, corruption and bribery operations will be the adequate knowledge of counterparties; therefore, procedure A-GL-06 "Selection, Evaluation and knowledge of business partners, customers and suppliers" is established.

## **Documentation and due diligence**

### **Knowledge of business partners, customers and/or suppliers**

The process of getting to know the counterpart arises in the initial contact, for its linkage, and is sustained in the process of updating information.

The person in charge shall ask the business partners (Customers, Suppliers and Contractors) to fill out the linking forms, including the following documents contemplated in the selection and evaluation procedure.

Natural Person	National Legal Entity	Foreign Legal Entity
Legible photocopy of citizenship or foreigner's identification card, in case you do not have one and you are a foreigner, a passport is requested.	Certificate of existence and legal representation not older than 30 days or legal document that certifies the existence of the associate's organization.	Document, depending on the country, that accredits the legal conformation of the organization.  Analogous duly authenticated in the case of legal entities
Signed manifestation of association form, F-GL-04, F-GL-25, forms for foreign associates and F-GL-16, F-GL-16-1 duly signed.	Format of linkage And signed statement F-GL-05 and F-GL-25 duly signed by the legal representative or alternate.	Form duly completed and signed, F- GL-16-1, F-GL-17 (in Spanish), F-GL-16, F-GL-17-1 (English), F-GL-16, F-GL-17-1 (English)

	Registration Unique Tax Registration Number (RUT)	Register of incorporation, RUC, company ID.
	Photocopy of the identification document of the person who sign the form	Photocopy of the identification document of the person who sign the form
	Shareholding composition if the shareholders are legal entities (if they are not authorized to share this information, please reply to the mail or letter signed by the legal representative or person in charge	Shareholder composition if the shareholders are legal entities (if they are not authorized to share this information, please reply to the mail or letter signed by the legal representative or person in charge

As an optional good practice, financial statements for the immediately preceding period and commercial references will be requested.

### **Simplified due diligence on customers and suppliers**

The due diligence process can be simplified in the linking of clients and suppliers, to expedite the commercial transaction, depending on the amount and frequency of the negotiation; taking into account that the overall impact, if the ML/FT/ATF/MFATF risk materializes, would be insignificant.

For this purpose, the following transaction classification table is defined:

Frequency	Total amount	Minimum documentation
Once or several times a year	< 50 million per year	*RUT
Once or several times a year	> 50 million per year	Complete documentation

These business associates will be registered separately with the objective of monitoring the criticality matrix of customers and suppliers every six months to verify compliance with the parameters.

### Enhanced due diligence

The enhanced due diligence process involves an advanced knowledge of the third party. It should be applied when the awareness or update process yields a finding that requires expansion and reasonable measures according to the compliance officer's criteria. In the event that the counterparty, or its beneficial owners, are included in one of the risk lists that may generate a significant contagion or legal risk for the company, the case will be documented and presented to the board of directors and the legal representative to evaluate whether or not to link it.

If the compliance officer proceeds with the linkage, he/she must request from the counterparty a certification, signed by its legal representative, or directly by the counterparty (in case it is a natural person), in which he/she declares in writing:

- That all its resources come from lawful activities.
- That the resources resulting from the relationship with Rymel S.A.S., will be destined for equally licit purposes.
- That it has procedures to prevent risks of corruption, bribery, money laundering required by law or regulation, or if not required, that it has suitable processes to prevent such risks.
- If the case is under investigation, it should be followed up until the case is resolved or the contractual relationship is terminated.

## **Employee knowledge**

Rymel S.A.S., before initiating an employment contract, performs a complete due diligence process through a detailed analysis of the documents submitted by the applicant, as well as the consultation of the lists, using the resources assigned by Rymel S.A.S., for such purpose.

In the event that the candidate or a current employee is included in one of the control lists that may generate a risk of contagion, his or her hiring or continuation of the employment contract will be submitted to the Board of Directors for approval.

## **Employee control and monitoring**

Home visits to employees with critical positions, both at the time of joining the company, as well as follow-up visits. These visits are the basis for socio-economic studies where unjustified changes in assets can be evidenced.

Carefully monitor behaviors, especially those of employees who have positions related to the handling of money, products, customers, suppliers and control of information.

Establish disciplinary actions to employees who do not comply with the processes contained in this manual and enshrined in the internal work regulations.

Massive consultation in lists every two years

Analysis of results

## **Knowledge of shareholders**

Rymel S.A.S. has a long history in the market, it is a family company and has kept the same partners during its commercial history.

Each partner must undergo the respective study of the entry or update and have at least: Form of linking business partner, contains declaration of origin of resources, consultation in control lists and background analysis on an annual basis. If there is a finding in control lists that represents a direct risk of money laundering, bribery and corruption, the case will be presented to the legal representative for evaluation.

The documentation provided by the shareholders must be filed in an adequate manner, so that it can be easily consulted by the competent authorities in case they request it.

## **Knowledge of compliance officer and alternate compliance officer**

In the event that the compliance officer and the alternate are not bound by an employment contract, the due diligence process must be carried out in the same way as for other business associates.

**Updating:** The monitoring and updating of the due diligence process to active business associates shall be done at least every two years, except, when there are changes in the corporate names and basic information of the companies and/or there is a high risk according to the criticality matrix.

### **Knowledge of Publicly Exposed Persons (PEP)**

In case the client is considered or is identified as a politically exposed person, the processes for knowing the client must be stricter, and therefore it will be essential to require more controls: An intensified due diligence, declaration format of the person as PEP, background check in public information media.

### **Detection, determination and analysis of unusual and suspicious transactions**

#### **Detection and analysis of unusual transactions**

The procedure for detection and analysis of transactions is understood as the series of activities carried out to identify unusual behavior of counterparties to be analyzed, documented and, if determined as suspicious transactions, to report such behavior to the UIAF.

The identification of warning signs and unusual transactions is performed by the company's employees, during the performance of their job functions and, in particular, during the application of controls in due diligence and updating procedures.

Warning signs and unusual or suspicious transactions are identified through the use of the following tools:

- **Binding and control lists.** Through their use, possible links with individuals related to money laundering, corruption and bribery are identified.
- **Monitoring against the counterparty's profile.** It is used to identify atypical behavior with respect to the characteristics of each counterparty. It is performed by comparing the behavior of the counterparties to infer the existence of atypical



## Warning Signs

The warning signs allow identifying unusual situations linked to the procedures that Rymel S.A.S. develops in an ordinary way, with its suppliers and clients, which will constitute a background at the moment of making the evaluation of a fact that could contaminate any process of the company; they help to identify or detect conducts, activities, methods or situations that can conceal operations of ML/FT/FPADM.

The fact that an operation is qualified as unusual does not mean that it is linked to illicit activities. For this reason it is necessary to study each of the operations, businesses and contracts in order to verify its unusual character.

The following warning signs, among others, can be established, which should be brought to the attention of the compliance officer and which should be subject to an evaluation process.

### Operations or activities with counterparties, related to:

- Natural or legal persons who are not fully identified.
- Shareholders or employees with a judicial record of ML/FT/AML/CFT.
- Potential shareholders who have been accepted or linked without previously verifying the origin of the resources they contribute.
- Delivery of erroneous, inaccurate or unverifiable information, or the filling out of forms without complying with all the requirements.
- Coincidences of the counterparty, or related to it, in reports of national or foreign competent authorities, regarding ML/FT/ATF/MFATF.



- Non-compliance with contract clauses, especially those related to the prevention and mitigation of ML/FT/FPADM risks.
- Presents an unjustified increase in net worth.
- Acting on behalf of third parties in an attempt to conceal the identity of the client.
- Fractionate transactions to avoid document requirements.
- Threaten or attempt to bribe sales representatives to accept incomplete documentation or to not fill out the binding documents completely.
- They carry out operations for small amounts, but over time they increase in size.
- They record addresses or telephone numbers that are different from the current location or are unrelated.
- Frequent change of address.
- They make all their transactions for the purchase or sale of goods in cash.
- They show preference to be served by a single salesperson.
- They offer products or services at prices below the normal price.
- Companies that frequently change their corporate name or obtain profits that are not in line with the market.
- Companies incorporated with small capital and receiving large investments.
- They receive large non-operating income in excess of their operating income.
- They have a very low subscribed capital and a very broad corporate purpose.
- They have partners, managers or representatives in common with other companies.
- They register the data of only one address, but request deliveries in different parts of the country.

- Customers who only provide cellular numbers to locate them and not landlines.
- They threaten to buy elsewhere just because general data and verifications are requested.
- Customers presenting false identity documents or documents that do not correspond to the person being traded.
- Humble-looking executives doing business for very large sums of money in cash.
- Request for payment or money transfers to third parties that are not related as customers or suppliers.

**Transactions, businesses or contracts that represent, have as their object or involve**

- High cash volume with no apparent justification.
- Movable or immovable property at prices considerably different from normal market prices.
- Donations that have no apparent final beneficiary, whose origin is unknown or who is domiciled in a high-risk country or jurisdiction.
- Relevant transactions, business or contracts that are not in writing.
- Operations with subcontractors that have not been identified.
- Commercial transactions or business dealings with persons included in the control lists
- Transactions with counterparties domiciled or located in geographic areas designated by the FATF as non-cooperative.
- Operations with products originating from illegal activities (including, among others, smuggling).
- Operations with products that have not been duly nationalized.

- Operations with restricted sale products that do not have the proper authorizations or licenses.
- Transactions with cash from or related to:
- Countries with a high level of corruption and political instability.
- Cash deposits in personal or corporate bank accounts from unexplained sources.
- Amount, value or currency not in accordance with the circumstances of the bearer.
- Concealed cash transportation.
- Costly transportation compared to alternative transportation methods
- Invoicing or cash sales not expected in the sector.
- Large increase in turnover or cash sales from unidentifiable customers.

### Employee warning signs

- **They** have a lifestyle that does not correspond to the salary they earn.
- They try to serve specific customers.

- They are reluctant to take vacations or to change activities within the company.
- They are frequently absent from the workplace.
- They always stay on the job overtime or come in before the starting time.
- If they have money management, they often get out of hand without sufficient explanation.
- Officials who do not request complete documentation from clients for their own benefit.
- They handle a lot of cash without supporting the same with their operations.

## Internal reporting of red flags and unusual transactions

Whenever a company employee, in the performance of his duties, detects a warning signal or an unusual operation, he must report this fact to the compliance officer so that he may initiate the respective analysis and investigation.

The form in which the compliance officer will be notified is by e-mail [lineaetica@rymel.com.co](mailto:lineaetica@rymel.com.co) with the respective evidence.

## Determination of suspicious transactions

The compliance officer is responsible for analyzing unusual operations for the purpose of:

- Verify that activities were carried out to deepen the warning signal and knowledge of the counterpart.
- Request additional information when the analysis warrants it.
- Determine if the situation is of an unusual nature that generates a suspicion that is not clarified or justified and is susceptible of being reported to the UIAF as a suspicious operation.

The compliance officer shall determine the suspicious operation and make the corresponding report to the UIAF. Suspicious operations are determined once the unusual operation has been compared with the counterparty's information and its normality parameters.

## Suspicious transaction report

In accordance with the decision taken in the previous step, the compliance officer must immediately, that is, from the moment the company makes the decision to classify the operation as suspicious, make the report through the UIAF web page, following the guidelines established in the "SIREL User Manual", which is published on the UIAF web page.

Attempted transactions that have characteristics that make them suspicious should be reported.

As the suspicious transaction report (STR) does not constitute a criminal complaint, it does not need to be signed by any officer, but is made at the institutional level. The STR will not give rise to any type of liability for the company, nor for the administrators or collaborators who have participated in its determination and reporting.

The STR does not exempt from the duty to report, if applicable.

### **Other external reports**

#### **Report of absence of attempted or suspicious transaction ("A-ROS") to the UIAF.**

In the event that a quarter elapses without STR reports, the compliance officer shall report this fact to the UIAF within the first ten (10) calendar days of the month following the expiration of the respective quarter, through the online reporting system (SIREL) of the UIAF.

### **Documentation and archiving of the cases analyzed**

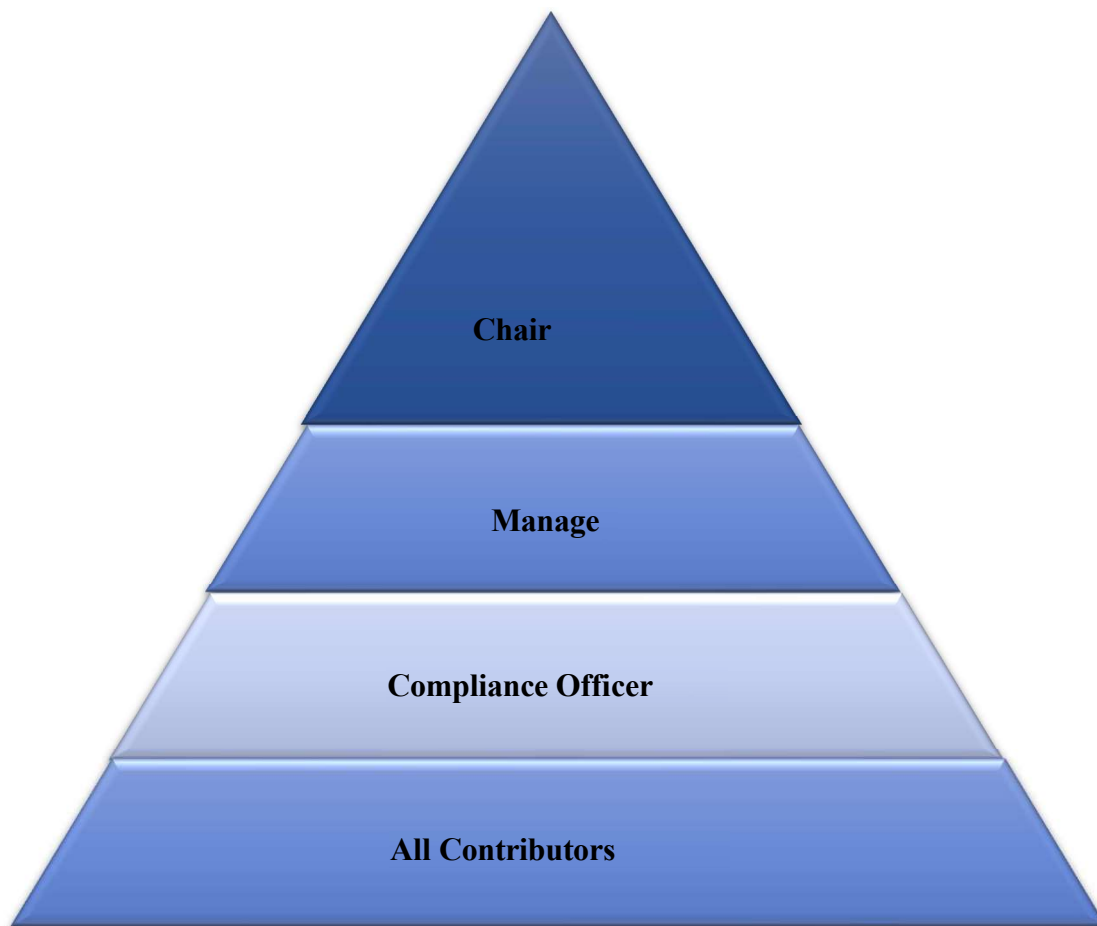
Following the completion of the report, the compliance officer must keep the supports (file) that led to the qualification of the operation in one category or another in a file that must be cataloged and filed according to security and confidentiality standards.

These files must be centralized and organized together with the respective report to the UIAF, adopting adequate security and confidentiality measures for such purpose, in order to make them available in a complete and timely manner to the authorities when requested.

This information shall be managed by the compliance officer, who shall regulate the positions authorized to consult this information and shall be kept for the term established in this manual.



## Organizational structure and functions



## Roles and responsibilities

In Rymel S.A.S., the following functions are established for the compliance of the system, taking into account the regulations issued by the Superintendence of Corporations, as follows:

## Functions of the board of directors

- Define and approve anti-corruption, bribery and ML/FT/AML policies.
- Approve the business ethics program presented by the legal representative.
- Discuss and approve the SAGRILIFT manual and business ethics, other documents of the System presented by the legal representative and the compliance officer, as well as their updates.
- Appoint the compliance officer for the two programs and verify that he/she has the necessary availability, experience and qualifications to perform his/her duties.
- To arrange the operational, economic, physical, technological and resource measures necessary and required by the compliance officer to carry out his/her functions.
- Receive, analyze and make timely decisions on the compliance officer's reports and define, when necessary, a proposal for improvement to the system.
- Follow up on the critical points contained in the reports submitted by the legal representative, the compliance officer or the statutory auditor on the company's two systems, leaving an express record in the respective minutes.
- Verify that the company, the compliance officer and the legal representative carry out the activities designated to them.

## Functions of the legal representative

- Present to the board of directors, together with the compliance officer, the SAGRILIFT manual and business ethics and other system documents.
- Efficiently allocate the operational, economic, physical and technological resources necessary and required for the compliance officer to implement the system and develop the follow-up and compliance tasks.

- Verify that the compliance officer has the necessary availability and capacity to perform his/her duties.
- Support the compliance officer in the design, direction, supervision and monitoring of the two systems.

### **Compliance officer functions**

- Supervise and direct the design of the system, taking into account the company's own characteristics, its activity and the identification of its risk factors.
- Submit to the Board of Directors, together with the legal representative, the SAGRILIFT manual and business ethics for its consideration and approval, by means of the respective minutes.
- Implement, with the support of the legal representative, the Manual and ensure that employees apply it effectively.
- Assess bribery and ML/TFTP/ATF/MFATF risk with employees before entering new markets.
- Ensure the effective, efficient and timely operation of SAGRILIFT and business ethics.
- Promote the adoption of corrective measures and updates to the system when circumstances so require, and at least every two years. To this end, it shall submit to the Board of Directors the proposals and justifications for the suggested corrective measures and updates to SAGRILIFT and business ethics.
- Inform the legal representative about possible failures or omissions in ML/FT/AML/CFT risk controls and business ethics of which he/she becomes aware.
- Submit at least once a year to the Board of Directors a report on compliance with SAGRILIFT and business ethics that, at a minimum, contains an evaluation and analysis of the efficiency and effectiveness of the system and, if required, the respective proposals for improvement, as well as a demonstration of the results of its management.

- Develop an internal disclosure and training program when necessary so that company employees are properly informed, updated and trained to identify and report unusual and suspicious transactions, as well as to avoid bribery.
- Receive from the different processes of the company the internal reports of attempted, unusual or suspicious transactions so that, if appropriate, report suspicious transactions to the UIAF.
- Register the compliance officer and the company in the SIREL administered by the UIAF and request a user name and password to enter this platform in order to be able to comply with the submission of mandatory reports.
- To report suspicious transactions (hereinafter "STR") or absence of suspicious transactions ("A-ROS") to the UIAF and any other report or report established by the rules applicable to the company in terms of prevention and control of ML/FT/FPADM in Colombia. For the fulfillment of this function, the compliance officer shall inform, prior to the report, the legal representative of the company of the content of the STR, provided that the legal representative does not have a conflict of interest in this decision.
- Report to the UIAF, through electronic channels determined by these authorities, coincidences of persons identified in the binding lists.
- For the fulfillment of this function, the compliance officer shall inform, prior to the report, the legal representative of the company about the matches of persons identified in the binding lists, provided that the legal representative does not have a conflict of interest in this decision.
- To report to the competent authority, when in the course of its activities of supervision of the system it becomes aware of the commission of crimes related to ML/FT/FPADM and bribery activities.
- Attend and coordinate any requirement, request or diligence of judicial or administrative authority in matters of prevention and control of ML/TF/AML/CFT and bribery activities.
- To certify to the Superintendency of Corporations, when required by this authority, the company's compliance with the provisions of Chapter X and Circular 100-

00003 (business ethics program).

- Evaluate the reports of the statutory auditor regarding SAGRILAFT and the company's business ethics program and adopt the necessary measures to provide solutions required for the proper functioning of the system.
- Ensure the proper filing of documentary supports (STRs and Internal Reports), as well as any information related to the management and prevention of ML/FT/ATF/AMLAP and bribery risk of the company.
- Receive and answer inquiries from counterparties in all matters related to the company's system.
- Verify compliance with the company's due diligence and enhanced due diligence procedures.
- Design the methodologies for classification, identification, measurement, evaluation and control of ML/FT/ATF/ATF risks and bribery that will be part of the SAGRILAFT and business ethics.

## Functions of the statutory auditor

As part of the tax functions established for the statutory auditor by Article 207 of the Commercial Code, the statutory auditor must ensure that the operations entered into or carried out on behalf of the company are in accordance with the bylaws and the decisions of the shareholders' meeting, as well as that any irregularities in the operation of the company and in the development of its business are reported to the shareholders' meeting in a timely manner. In this sense, the statutory auditor shall:

- Report to the UIAF the suspicious operations that they notice within the ordinary course of their work, and report to the criminal, disciplinary and administrative authorities, the alleged commission of a crime against the economic and social order. They must also bring these facts to the attention of the company's corporate bodies and management.
- Verify compliance with current regulations applicable to the company in terms of self-monitoring and management of ML/TF/TFPA and business ethics risks, as

well as the controls established by the company to protect itself from these risks.

- Submit reports, at least annually, on the results of system reviews, as well as recommendations to correct deficiencies, to the board of directors, with a copy to the legal representative and the compliance officer.

## Purchasing functions

- Comply with the guidelines of the present manual and other procedures for the linking of the business associate.
- Request timely, from the time of the order, due diligence documentation in accordance with A-GL-06 "Business Associate Procedure".
- Verify that it is complete and transfer it to the SAGRILAF area to expedite the creation of the business partner in a timely manner.
- Classify and monitor business associates according to risk assessment criteria to evaluate behavior and take the necessary measures to ensure security in commercial transactions.
- Visit the business partner according to the level of criticality shown in the matrix, to ensure compliance with the standard and procedure A-GL- 06 "Selection, evaluation and knowledge of business partners".
- Abide by the guidelines of the transparency and business ethics program, avoiding conflicts of interest.
- Preventing transnational bribery.
- Timely inform the compliance officer of significant changes in the organizational structure associated with the business, such as:
  - High asset growth.
  - Constant location changes in nomenclatures
  - Changes in legal representation and its directors



- Changes in corporate purpose or economic activity
- To maintain absolute confidentiality regarding any information on investigations that the Company is conducting.

### **Human resources functions**

- Support the compliance officer in the training to be given to employees on ML/FT/AML/CFT and transparency and business ethics program.
- Incorporate into the induction and re-induction manual of its employees the guidelines set forth in the business ethics program and SAGRILAFIT.
- Carry out the security study and consultations in lists to timely notify the compliance officer of any indication or suspicion of unusual activity with personnel directly or indirectly related to the company.
- Monitor the behavior of employees, especially those in critical positions.

### **Employee functions**

All company employees are obliged to carry out their work in strict compliance with the rules established in this manual and the code of ethics, and to immediately inform the compliance officer of any suspicious activity of which they are aware and which they consider may jeopardize the good name of the organization, regardless of whether it has been committed by another employee.

## Attention to requests from authorities

Any request for information from competent authorities in matters of ML/FT/AML/CFT prevention and control shall be dealt with by the compliance officer.

The compliance officer shall gather the necessary information and draft the response to the requirement within the established terms, and submit it to the company's general manager and the area in charge of the process for approval. He/she shall ensure that it is filed on time and kept in the system's documentation.

## Imposition of sanctions

In case of non-compliance and depending on its seriousness, the company will apply disciplinary sanctions in accordance with the internal documents provided by the company.

In case of detecting any irregularity or failure to comply with the policies and procedures defined in this manual, all employees must report the offense immediately, even if committed by their immediate superior, to the compliance officer at [lineaetica@rymel.com.co](mailto:lineaetica@rymel.com.co). Rymel S.A.S., will guarantee no retaliation against those who report misconduct in good faith.

In the event of a complaint, the compliance officer will be responsible for carrying out a preliminary investigation process, taking the results and the concept to the legal representative, who will apply the disciplinary procedure established in the disciplinary action procedure.

In the event that the complaint is against the legal representative, the compliance officer shall submit the result of the investigation to the board of directors.

## Disclosure

This manual will be available on the web page for all business associates, in order to guarantee their knowledge and compliance with the guidelines established to properly manage resources, control the risk of money laundering, financing of terrorism and avoid corruption.

In addition, it will be made known internally to all company personnel through induction at the time of hiring.

## Training

The compliance officer in collaboration with the human resources area will be responsible for designing, scheduling and coordinating the training, coaching and awareness-raising plans in relation to the contents of this manual. This program will be aimed at the company's employees, following the general training plan for the system. When a new employee is hired, the human resources manager shall inform him/her about the application of the system in the company.

A record shall be left in each employee's résumé, as a record of the reading of the manual and attendance at the induction. The compliance officer shall be informed of the entry of new employees, so that, if deemed appropriate, the compliance officer may provide special support during the induction, due to the sensitivity of the area to which the new employee will be assigned.

Employee attendance at training events is mandatory and everyone should be allowed the necessary time for participation, depending on the overall plan and coordination with the compliance officer.

In general terms, the general plan meets the following conditions:

Be taught in the form of awareness during the induction process of new employees, so that the system becomes part of the company's culture.

To be given in the form of intensified training to those employees whose duties include the execution of system controls, thus ensuring adequate compliance with them.

Be constantly reviewed and updated.

To have mechanisms in place to evaluate the results obtained, in order to determine the effectiveness of these programs and the achievement of the proposed objectives.

Elaboro		I review	Approved	Version
<b>NAME</b>	Martha Vasco	Veronica Monsalve	Board of Directors	
<b>POSITION</b>	Compliance Officer	Alternate compliance officer	Members of the board of directors	
<b>DATE</b>	October/2022	October/2022	October/2022	