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

Contents

1. Introduction

CERREJÓN, a Glencore company, is a company mainly engaged in the extraction, transportation, and export of coal in the department of La Guajira, Colombia.

CERREJÓN's activities are not exempt from the risks of money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction (hereinafter ML/FT/FPWMD), and that is why the Board of Directors, in observance of CERREJÓN's policy concerning strict compliance with all laws applicable to its business and contained in the document called Code of Conduct, and aligned with Glencore's policies and controls, approved the policy designed by the Legal Representative and the Compliance Officer, for the self-monitoring system and comprehensive risk management of ML/FT/FPWMD, which is developed through the procedures described in this document, in order to prevent and avoid the commission of these crimes within CERREJÓN, as well as to mitigate the consequences that these criminal behaviors may cause to the competitiveness, productivity and durability in the market of the COMPANY.

2. Regulatory Framework

The following standards are applicable to THE COMPANY, and CERREJÓN is developing this document based on these standards:

- **Law 1121 of 2006:** Duty to consult counterparties in the binding list for Colombia.
- **Law 1708 of 2014:** Duty to report illicit goods. Duty to act with good faith exempt from guilt.
- **Law 2195 of 2022**: Principle of due diligence.
- **CONPES 4042 of 2021**: National policy against ML/FT/FPWMD.
- **Article 441 of the Criminal Code:** Duty to report ML/FT crimes.
- **External Circular 170 of 2002 issued by DIAN.** Duty to implement a SIPLA, as a permanent customs user (UAP), high exporter user (ALTEX) and private warehouse.
- **Resolution 285 of 2007 issued by UIAF.** Imposes on companies required to comply with DIAN External Circular 170/02, the duty to transmit to the UIAF the report of suspicious transactions and cash transactions.
- **Resolution 212 of 2009 issued by UIAF.** Imposes on companies required to comply with DIAN Circular 170/02, the obligation of transmitting to the UIAF a report on the lack of suspicious transactions and the lack of cash transactions.
- **Resolution 17 of 2016 issued by UIAF.** Whereby Resolutions 285 of 2007 and 212 of 2009 of the UIAF are amended.
- **Chapter X of the Basic Legal Circular of the Superintendency of Corporations, as amended by Circular 100-000016 of December 24, 2020.** Mandates companies to adopt the stipulations of the circular, related to SAGRILAFT, when they comply with certain assumptions mentioned in the regulation.

3. Scope of application

CERREJÓN is compelled to adopt the provisions of Chapter X of the Basic Legal Circular of the Superintendency of Corporations, as it is subject to the supervision and control exercised by this entity and

because it has total revenues and/or assets equal to or greater than forty thousand (40,000) SMLMV, as of December 31 of the immediately preceding year.

This document also complies with the stipulations of Circular 170 of 2002 issued by the DIAN.

4. System objectives

CERREJON's self-control and comprehensive ML/FT/FPWMD risk management system has the following objectives:

- Prevent the entry into CERREJÓN of persons identified as money launderers or financiers of terrorism or of the proliferation of weapons of mass destruction, as clients, suppliers, employees, shareholders, donors, or beneficiaries of social responsibility programs.
- Prevent assets of illicit origin from infiltrating CERREJÓN's transactions and commercial activities.
- Prevent CERREJÓN from being used as an instrument for laundering assets, financing terrorism, or financing the proliferation of weapons of mass destruction.
- Maintain a good reputation at the local, national, and international levels in the prevention of money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction.
- Comply with current regulations on ML/FT/FPWMD risk management.
- Create an organizational culture of legality, dedicated to stopping ML/FT/FPWMD crimes from being committed within the COMPANY and supported by the company's core values of integrity, accountability, and transparency.
- Contribute to the fulfillment of the commitment against ML/FT/FPWMD outlined in our Code of Conduct.

5. Definitions

For the purposes of this manual the following definitions apply:

Virtual Asset: 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.

Assets: is a present economic resource controlled by the Company as a result of past events.

Geographical Area: is the area of the territory where the Company carries out its activities.

Final Beneficiary: is the individual(s) who ultimately owns or controls a customer or the individual on whose behalf a transaction is conducted. It also includes the person(s) exercising effective and/or ultimate control, directly or indirectly, over a legal entity or other unincorporated structure. The following are Final Beneficiaries of the legal entity:

a. Individual who, acting individually or jointly, exercises control over the legal entity, under the terms of Article 260 and subsequent articles of the Code of Commerce, and the Article 631-5 of the Tax Statute; or,
b. Individual who, acting individually or jointly, holds, directly or indirectly, five percent (5%) or more of the capital or voting rights of the legal entity, and/or benefits from five percent (5%) or more of the income, profits or assets of the legal entity.
c. When no individual is identified in a) and b), the individual who holds the position of legal representative, unless there is an individual who has greater authority in relation to the management or direction duties of the legal entity.

The Final Beneficiaries of a trust contract, of an unincorporated structure or of a similar legal structure, are the following individuals who hold the status of:

- Trustee(s), settlor(s), constituent(s) or similar or equivalent position.
- Trust committee, finance committee or similar or equivalent position.
- Trustee(s), beneficiary(ies) or conditional beneficiaries; and
- Any other individual exercising effective and/or ultimate control or having the right to enjoy and/or dispose of the assets, benefits, results or profits.

Counterpart: any individual or legal entity with which CERREJÓN has commercial, business, contractual or legal ties of any kind. Among others, counterparties are associates, employees, customers, contractors and suppliers of the Company's products.

Due diligence: is the process through which the Company adopts measures for the knowledge of the Counterparty, its business, operations, and products and the volume of its transactions, which is developed in accordance with the stipulations of Article 12 of Law 2195 of 2022, *numeral 5.3.1 of Chapter X of the Basic Legal Circular of the Superintendence of Companies and numeral 5 of Circular 170 of 2022 of the DIAN*.

Intensified Due Diligence: is the process by which the Company adopts additional measures and with greater intensity for the knowledge of the Counterparty, its business, operations, products, and the volume of its transactions, **as established in section 5.3.2 of the Basic Legal Circular of the Superintendency of Companies.**

Company: is the commercial company, sole proprietorship or branch of a foreign company supervised by the Superintendence of Companies.

Financing of Terrorism or FT: is the crime regulated in article 345 of the Colombian Criminal Code (or the norm that replaces or modifies it); which consists of providing, collecting, delivering, receiving, administering, contributing, guarding or storing funds, goods or resources or performing any act that promotes, organizes, supports, maintains or economically sustains organized crime groups, illegal armed groups or their members, or national or foreign terrorist groups, or national or foreign terrorists, or terrorist activities.

Financing of Proliferation of Weapons of Mass Destruction (FPWMD): is any act that provides funds or uses financial services, in whole or in part, for the manufacture, acquisition, possession, development, export,

material transfer, fractioning, transportation, transfer, deposit or dual use for illegitimate purposes in contravention of national laws or international obligations, where the latter is applicable.

ML/FT/FPWMD risk factors: are the possible elements or causes that generate ML/FT/FPWMD risks. The Company must identify them considering the Counterparties, products, activities, channels and jurisdictions, among others.

FATF: The Financial Action Task Force. Intergovernmental group created in 1989 to issue standards to countries for the fight against ML, FT and FPWMD.

GAFILAFT: It is the Latin American Financial Action Task Force, the FATF's regional umbrella organization.

ML/FT/FPWMD Risk Management: Consists of the adoption of policies and procedures to prevent and control the ML/FT/FPWMD risk at CERREJÓN.

Total Revenues: are all revenues recognized in the statement of income for the period, as the main source of information on CERREJÓN's financial activity for the reporting period. In accordance with the disclosure criteria these include Income from Ordinary Activities, other income, gains (other items that meet the definition of income but are not Income from Ordinary Activities) and financial income.

Income from ordinary activities: The income generated in the course of the main activities of CERREJÓN's business.

ML/FT/FPWMD: Acronym for Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction.

Money laundering or ML: is the crime typified in article 323 of the Colombian Criminal Code (or the norm that replaces or modifies it). In particular, it is the crime committed by any person who seeks to give the appearance of legality to goods or money derived from any of the activities described in the aforementioned article. According to Article 323 of the Criminal Code, the crimes that are the source of money laundering are: smuggling of migrants, trafficking of persons, extortion, illicit enrichment, extortive kidnapping, rebellion, arms trafficking, trafficking of minors, financing of terrorism and administration of resources associated with terrorist activities, trafficking of toxic drugs, narcotics or psychotropic substances, crimes against the financial system, crimes against the public administration, or conspiracy to commit a crime.

Binding Lists: are those lists of persons and entities associated with terrorist organizations that are binding on Colombia under Colombian law (Article 20 of Law 1121 of 2006) and under international law, including but not limited to Resolutions 1267 of 1999, 1373 of 2001, 1718 and 1737 of 2006, 1988 and 1989 of 2011, and 2178 of 2014 of the United Nations Security Council, and all those that succeed, relate to and complement them, and any other list binding on Colombia such as terrorist lists of the United States of America, the European Union list of Terrorist Organizations and the European Union list of Persons Listed as Terrorists.

- The United Nations (UN) Security Council list of individuals and entities that are members of the Taliban, the AL-QAIDA Organization or associated with them, which under international law is the only binding list for Colombia.
- The U.S. Government's Office of Foreign Assets Control (OFAC) periodically publishes the Specially Designated Nationals (SDN) list, which lists individuals and organizations associated with drug trafficking crimes with whom U.S. persons and those with interests in the United States are prohibited from doing business. This is a restrictive list.
- INTERPOL's database of the most wanted persons in the world.

At the national level, among others, the following are available:

- The list of the Office of the Comptroller General of the Nation, regarding persons who have had contractual relations with that agency and have been sanctioned, better known as the bulletin of persons responsible for fiscal matters.
- - The database of the General Prosecutor of the Nation, related to the disciplinary records of individuals in general.
- The Colombian National Police's database on the judicial records of individuals in general.

Risk Matrix for ML/FT/FPOWMD: one of the instruments that allows CERREJÓN to identify, individualize, segment, evaluate and control the ML/TF/FPWMD Risks to which it could be exposed, according to the ML/TF/FPWMD Risk Factors identified.

Reasonable Measures: are the sufficient, appropriate and measurable actions in quality and quantity to mitigate the ML/FT/FPWMD Risk, taking into account the Bound Company's own risks and their materiality.

Compliance Officer: the individual designated by CERREJÓN to promote, develop and ensure compliance with the specific procedures for the prevention, updating and mitigation of ML/TF/FPWMD risk.

Monitoring and/or follow-up: is the continuous and systematic process by which the efficiency and effectiveness of a policy or process is verified by identifying its achievements and weaknesses in order to recommend corrective measures to optimize the expected results.

Unusual Operation: is the transaction whose amount or characteristics are not related to the ordinary or normal economic activity of the Bound Company or, due to its number, quantity or characteristics, does not fall within the guidelines of normality or ordinary business practices in a sector, industry or with a type of Counterparty.

Suspicious Operation: is the Unusual Transaction which, in addition, in accordance with the customs and practices of the activity in question, could not have been reasonably justified.

Politically Exposed Persons (PEP): means, Politically Exposed Persons, i.e., they are public servants in any type of position and job classification of the national and territorial public administration, when in the positions they occupy, they have in the duties 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, the direct management

of goods, money or securities of the State. These may be through expenditure management, public contracting, management of investment projects, payments, liquidations, administration of movable and immovable property. It also includes Foreign PEPs and PEPs of International Organizations. PEP status is retained for two years after the date on which the person has ceased to perform the duties by virtue of which he/she may be considered a political or publicly exposed person. In Colombia there is an official list of PEPs, available on the web for consultation by the general public.

PEPs of International Organizations: individuals who exercise managerial duties 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 Organization of American States, among others (e.g., directors, deputy directors, board members or any person exercising an equivalent duty).

Foreign PEP: individuals who perform prominent and outstanding public duties in another country. In particular, the following persons: (i) heads of state, heads of government, ministers, undersecretaries or secretaries of state; (ii) congressmen or parliamentarians; (iii) members of supreme courts, constitutional courts or other high judicial instances whose decisions do not normally admit appeal, except in exceptional circumstances; (iv) members of courts or the boards of directors of central banks; (v) ambassadors; (vi) chargés d'affaires; (vii) senior officers of the armed forces; (viii) members of the administrative, managerial 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, senior management and board members of an international organization (e.g. heads of state, politicians, senior government, judicial or military officials and senior executives of state-owned enterprises).

ML/FY/FPWMD Policy: These are the guidelines, orientations or aspects that support the prevention and control of ML/FT/FPWMD risk in CERREJÓN. They are part of the ML/FT/FPWMD risk management process.

Products: The goods and services produced, marketed, transformed, or offered by CERREJÓN or acquired from a third party.

FATF Recommendations: The recommendations designed by the FATF with its interpretative notes, to prevent the ML/FT/FPWMD risk, and the document published by the FATF called International Standards for the Fight Against Money Laundering, Terrorist Financing, and the Financing of the Proliferation of Weapons of Mass Destruction.

Self-control and Integral ML/FT/FPWMD Risk Management Regime: is the SAGRILAFT and the Minimum Measures Regime, as a whole.

ML/FT/FPWMD risk: the risk of harm or loss that CERREJÓN might experience if it is used to finance crimes such as money laundering, terrorism, or the proliferation of weapons of mass destruction. It is described in terms of impact (consequence) and probability (frequency).

ML/FT/FPWMD risk: the risk that CERREJÓN may sustain loss or damage as a result of its propensity to be used directly or through its operations as a tool for the laundering of assets and/or channeling of resources towards financing terrorist activities or the proliferation of weapons of mass destruction, or when it intends to conceal assets from such activities. The risks that the Company is exposed to, including contagion risk,

legal risk, operational risk, reputational risk, and others, are what cause the ML/FT/FPWMD contingencies to materialize, with the consequent potential for harm to the company's financial stability.

Legal Risk: the possibility of loss incurred by CERREJÓN when it is sanctioned or obliged to compensate damages as a result of non-compliance with rules or regulations and contractual obligations. It also arises as a consequence of failures in contracts and transactions, derived from malicious actions, negligence or involuntary acts that affect the formalization or execution of contracts or transactions.

Reputational Risk: the potential for loss or harm to Cerrejon owing to diminished reputation, a bad public image, unfavorable press regarding the company and its business practices, whether real or untrue, which could result in a decline in clientele, a drop in revenue, or being involved in legal proceedings.

Operational Risk: the potential for losses brought on by deficiencies, failures, or limitations in infrastructure, technology, procedures, individuals, or other external events. This term covers the accompanying legal risks and reputational risks.

Risk of Contagion: the possibility of loss that CERREJÓN may suffer, directly or indirectly, due to an action or experience of a counterparty, related to ML/FT/FPWMD offenses.

Inherent Risk: the level of risk inherent in the activity, without considering the effect of controls.

Residual Risk: is the resulting level of risk after the application of controls.

RSA: Report on Suspicious Activities. An operation that, due to its size, scope, or other characteristics, deviates from the standard operating procedures and business, industry, or sector practices, as well as from the uses and norms of the relevant activity, so much so that it could not be reasonably justified.

SIREL: is the Online Reporting System, which the UIAF oversees. It is a WEB application that enables organizations to securely upload and/or report online any information of the obligations established in the regulations of each sector, in an efficient and secure manner. It is available 24 hours a day, 7 days a week and 365 days a year.

SAGRILAFT: the Comprehensive ML/FT/FPWMD Self-Control and Risk Management System established in the Basic Legal Circular of the Superintendence of Corporations.

SIPLA: is the Comprehensive System for the Prevention and Control of Money Laundering, in accordance with DIAN Circular 170.

SMLMV: is the current legal monthly minimum wage.

Terrorism: Terrorism is defined as any act intended to keep the civilian population in a state of anxiety by means of acts that endanger their life, integrity or freedom by using instruments capable of causing havoc. Terrorism is financed through both legitimate and illegitimate sources. Illegitimate activities include extortion, kidnapping and drug trafficking. Legitimate sources include donations to organizations that appear to be humanitarian non-profit entities and the sponsorship of foreign governments.

UIAF: is the Financial Information and Analysis Unit, which is Colombia's financial intelligence unit, with the duties of intervening in the economy to prevent and detect ML/FT/FPWMD. Entity attached to the Ministry of Finance and Public Credit of Colombia.

6. Roles and Responsibilities for the SAGRILAFT

The operation of SASGRILAFT requires the participation of multiple parties, and while each party has been given a distinct duty, the collaboration of all parties involved is crucial to the system's efficient operation.

In general, the SAGRILAFT must be known, assimilated, and applied by all the instances related to this program within CERREJÓN and especially by the Compliance Officer.

6.1 Duties of the board of directors or the highest corporate body

The Board of Directors, or the highest corporate body when there is no Board of Directors, is the body responsible for the implementation and effectiveness of the SAGRILAFT in CERREJÓN. In addition to the duties established by other external or internal regulations, the following are specifically established in relation to the Self-Control System and Integral ML/FT/FPWMD Risk Management System:

a. Establish and approve the LA/FT/FPWMD Policy.
b. Approve the SAGRILAFT and its updates, presented by the Legal Representative and the Compliance Officer.
c. Approve the SAGRILAFT Procedures Manual and its updates.
d. Selecting and appointing the Compliance Officer and his/her respective alternate, when appropriate.
e. Analyze in a timely manner the reports on the operation of SAGRILAFT, on the proposals for corrective actions and updates submitted by the Compliance Officer and make decisions /statements regarding all the issues discussed therein. This shall be recorded in the minutes of the corresponding body.
f. Analyze in a timely manner the reports and requests submitted by the Legal Representative.
g. Provide inputs on the reports submitted by the statutory auditors or the internal and external audits, which are related to the implementation and operation of SAGRILAFT, and to follow up on the observations or recommendations included. This follow-up and its periodic progress shall be recorded in the corresponding minutes.
h. Order and guarantee the technical, logistical, and human resources necessary to implement and maintain the SAGRILAFT in operation, according to the requirements made by the Compliance Officer for this purpose.
i. Establish the criteria for accepting the Counterparty's linkage when it is a PEP.
j. In the event that it decides to do so, establish rules and choose who will be in charge of performing audits on the SAGRILAFT's efficacy and compliance.
k. Verify to find out if the compliance officer is capable and available to carry out his or her responsibilities.

l. Verify that the assigned activities are carried out by the Company, the Compliance Officer, and the Legal Representative in line with the rules and the SAGRILAFT.

6.2 Duties of the Legal Representative

In addition to the duties established by other external or internal regulations, the following duties are specifically established in relation to the Self-Control and Integral ML/TF/FPWMD Risk Management System:

a. Together with the Compliance Officer, present the proposed SAGRILAFT and any revisions, along with the associated procedure manual, for the Board of Directors' approval.
b. Examine the findings of the Compliance Officer's LA/FT/FPWMD risk assessment and establish the corresponding action plans.
c. Efficiently distribute the technical and human resources required to implement the SAGRILAFT, as determined by the Board of Directors.
d. Verify to see if the compliance officer is capable and available to do his / her duties.
e. Provide effective, efficient, and timely support to the Compliance Officer in the design,
f. direction, supervision and monitoring of SAGRILAFT.
g. Submit to the Board of Directors the reports, requests and alerts that it considers should be addressed by such bodies and that are related to SAGRILAFT.
h. Ensure that the activities resulting from the development of the SAGRILAFT are duly documented, so that the information meets the criteria of integrity, reliability, availability, compliance, effectiveness, efficiency, and confidentiality.
i. Attest that this entity complies with the requirements of Chapter X of the Basic Legal Circular and submit the corresponding certification to the Superintendency of Corporations.
j. Verify that the SAGRILAFT practices adhere to the LAFT/FT/FPWMD Policy that the Board of Directors adopted.

6.3 Duties of the Compliance Officer

a. Actively participate in SAGRILAFT design, management, implementation, auditing, compliance verification and monitoring procedures.
b. Make decisions on the risk management of SAGRILAFT and issue recommendations as it deems appropriate.
c. Ensure the effective, efficient, and timely operation of SAGRILAFT.
d. Promote the adoption of corrections and updates to SAGRILAFT, when circumstances so require and at least once every two (2) years. For this purpose, it shall submit to the Board of Directors, the proposals and justifications of the corrections and updates suggested to the SAGRILAFT.
e. Design the methodologies for classification, identification, measurement, and control of ML/FT/ATF/ATF risk that will be part of SAGRILAFT.
f. Certify to the Superintendence of Corporations the compliance with the stipulations of Chapter X of the Basic Legal Circular issued by this entity or any regulation that totally or partially modifies or substitutes it.

g. Submit, at least once a year, reports to the Board of Directors. As a minimum, the reports shall 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 Compliance Officer's management, and of the Company's management, in general, the compliance with the SAGRILAFT.
h. Submit, in accordance with DIAN Circular 170, a monthly report addressed to the legal representative, with the activities carried out by the Compliance Officer and other relevant data that should be known to him/her.
i. Design, program and coordinate the development of internal training plans.
j. Evaluate the risk to which the company is exposed from LA/FT/FPWMD.
k. Conduct the necessary studies to determine whether an unusual operation is suspicious.
l. Present the Suspicious Transactions Report before the UIAF and any other report or information required by the stipulations in force, or by the competent authorities as established by such regulations or authorities, the DIAN and Chapter X of the Basic Legal Circular of the Superintendence of Companies or the regulation that modifies or substitutes it totally or partially.
m. Receive and resolve queries from all CERREJÓN employees in all matters related to the Self-Control System and Integral Risk Management of ML / FT / FPWMD
n. Verify compliance with the procedures of Due Diligence and Enhanced Due Diligence, applicable to CERREJÓN.
o. Perform additional activities of knowledge and review for due diligence considered high risk ML/FT/FPWMD and the acceptance as a counterparty to a PEP in CERREJÓN.
p. Evaluate the reports submitted by the internal audit or whoever performs similar duties or takes their place, and the reports submitted by the statutory auditor or the external audit, if applicable, and adopt Reasonable Measures to address the deficiencies reported. If the measures to be adopted require authorization from other bodies, it shall promote that these matters be brought to the attention of the competent bodies.
q. Ensure the proper filing of documentary supports and other information related to ML/FT/FPWMD risk management and prevention.
r. Verify the timely and strict compliance with the legal norms and reports established for the prevention of criminal activities in international trade.
s. Attend and coordinate any requirement, request, or diligence of judicial or administrative authority regarding prevention and control of criminal activities.

6.4 Other duties

6.4.1 Statutory auditors

Statutory Auditors: The duties of this body are specifically outlined in the law, most notably in Article 207 of the Code of Commerce, which states specifically, the obligation to report Suspicious Transactions to the UIAF when they are detected in the ordinary course of the work, as stated in paragraph 10 of said article.

a. In any case, the statutory auditor has a duty to disclose information when required by law, despite the professional obligation to maintain confidentiality in matters that are known to him/her in the performance of his/her profession. This duty arises from the responsibility inherent in his/her functions and in accordance with the circumstances in which such confidentiality may be lifted.

Thus, for instance, a statutory auditor is required to report his concerns to the appropriate authority when he comes across material during the course of his work that raises the possibility of an ML/FT/FPWMD act.

b. Even in the face of professional confidentiality, he or she must report to the appropriate criminal, disciplinary, and administrative authorities any suspected money laundering or other crimes against the economic or social order. Additionally, he or she must alert the corporate bodies and the management of the business regarding these facts.

c. When analyzing accounting and financial information, attention should be paid to the indicators that may give rise to suspicion of an act related to a ML/FT/FPWMD fact.

6.4.2 Internal audit

In order to provide the Compliance Officer and CERREJÓN management with a foundation upon which to assess the existence of problems in the SAGRILAFT and their potential remedies, the internal audit will include an evaluation of the efficacy and compliance of the SAGRILAFT in its yearly audit plans.

The result of such internal audits shall be communicated to the Board of Directors, the Legal Representative and the Compliance Officer. The Compliance Officer shall follow up on the execution of the action plans derived from the audit.

6.4.3 Duties of the people in charge of areas and processes with their work teams

All CERREJÓN personnel have a responsibility to report any anomalous operations, businesses, or contracts relating to their work to their immediate supervisor and the Compliance Officer. Additionally, they must refrain from alerting anyone who has engaged in or plans to engage in suspicious activity that information about them has been shared with the UIAF. This will help determine whether the operation qualifies as suspicious.

It is the responsibility of the process owners and/or Area Managers to:

- Inform all employees under their charge of the policies and procedures and due diligence standards contained in this manual.
- Promote attendance to the training scheduled in CERREJÓN on the policies and procedures of the system of self-control and comprehensive risk management of ML / FT / FPWMD.
- Participate in the working groups convened by the Compliance Officer for the identification, evaluation, control, and follow-up of identified risk situations.
- To avoid or lessen the effects of identified risk scenarios, propose and carry out action or treatment strategies. Failures or flaws in the System should be reported to the Legal Representative or his or her designee and the Compliance Officer in order to coordinate corrective actions.

7. Profile, incompatibilities, and exclusions of the Compliance Officer.

7.1 Compliance Officer Profile

Those who serve as principal or deputy Compliance Officer must meet the following requirements and competencies:

a. Professional in Law, Engineering, Business Administration or Accounting.
b. Have sufficient knowledge of risk management and understand the ordinary course of CERREJÓN's activities and its processes.
c. At least six months of experience in the performance of positions related to the administration of SAGRILAFT.
d. Proof of ML/FT/FPWMD risk management expertise obtained through specialization, education, training, congresses, or other related activities.
e. Know the fundamentals, guidelines, and regulations relating to anti-corruption, money-laundering, and terrorist financing (such as the UK Bribery Act, FCPA, and Anti-Corruption Statute), as well as the basic norms in effect at the national and international levels that govern the topic.
f. Have knowledge of data management and analysis.
g. Have the capacity to make decisions to manage the ML/FT/FPWMD Risk and have direct communication with the Board of Directors, as well as to report to this body.
h. Have the support of a human and technical work team, in accordance with the ML/FT/FPWMD risk and the size of the Company.
i. have the capacity for analysis and synthesis, high ethical sense and confidentiality management.
j. Communication skills (verbal and written), customer orientation (at all levels), attention to simultaneous requirements and adaptation to changing priorities.
k. Residence in Colombia.

7.2 Incompatibilities and grounds for disqualification of the Compliance Officer

May not serve as CERREJÓN's Chief Compliance Officer:

a. Whoever has been sanctioned or is being investigated for the commission of the crimes of Money Laundering, Financing of Terrorism, and/or Corruption or any of its related crimes or source crimes.
b. Whoever is a close relative of approvers of the different processes of the Company.
c. Whoever belongs to the administration or corporate bodies, audit or internal or external control.
d. Whoever belongs to the statutory auditors (statutory auditor or linked to the statutory audit firm that performs this function) or whoever performs similar functions or acts as such in the Bound Company.
e. Not acting as Compliance Officer in more than ten (10) Bound Companies. To serve as Compliance Officer of more than one Bound Company, (i) the Compliance Officer must certify; and (ii) the body that appoints the Compliance Officer must verify that the Compliance Officer does not act as such in competing Companies.

f. When the Compliance Officer is not employed by the Company, this individual and the legal entity to which he/she is linked, if applicable, must demonstrate that in their professional activities they comply with the minimum characteristics established in the rules governing the matter.
g. The Compliance Officer of the parent or controlling company may be the same person for all the companies that make up the group or conglomerate, regardless of how many companies comprise the group or conglomerate, depending on how the situation of a business group or a declared situation of control is configured.

If the Compliance Officer finds himself or herself in any of the aforementioned scenarios after being assigned to the position as a result of a supervening circumstance, he or she must notify the Board of Directors and provide a copy to the Presidency.

The Compliance Officer must notify the Board of Directors of any conflicts of interest they may have at the time that they are reviewing, endorsing, or issuing a concept, along with a copy to the President's Office. They must also declare themselves ineligible to hear the matter. This kind of circumstance may occur, among other things, when the Compliance Officer holds stock in or serves on the board of directors of a company for which due diligence is being conducted, or when the candidate employee, supplier, or contractor for whom due diligence is being performed is a close relative of the Compliance Officer.

The deputy Compliance Officer will independently assume the analysis and study of the problem if the conflict of interest or inability generated is in the head of the main Compliance Officer in a specific instance. If this is not possible due to the existence of an impediment or conflict of interest of the deputy Compliance Officer, or in the case of a situation of inability of the principal Compliance Officer that is likely to last over time and is generated not only in a specific case, the Board of Directors of CERREJÓN may make decisions aimed at ensuring impartiality in the processes and functions assigned to the Compliance Officer, without necessarily implying the removal of the Compliance Officer from the position.

In the event of absence of the Chief Compliance Officer, the Deputy Compliance Officer shall assume his or her duties until the Board of Directors appoints the new Chief Compliance Officer.

8. Policy of the Integral ML/FT/FPWMD Self-Control and Risk Management System

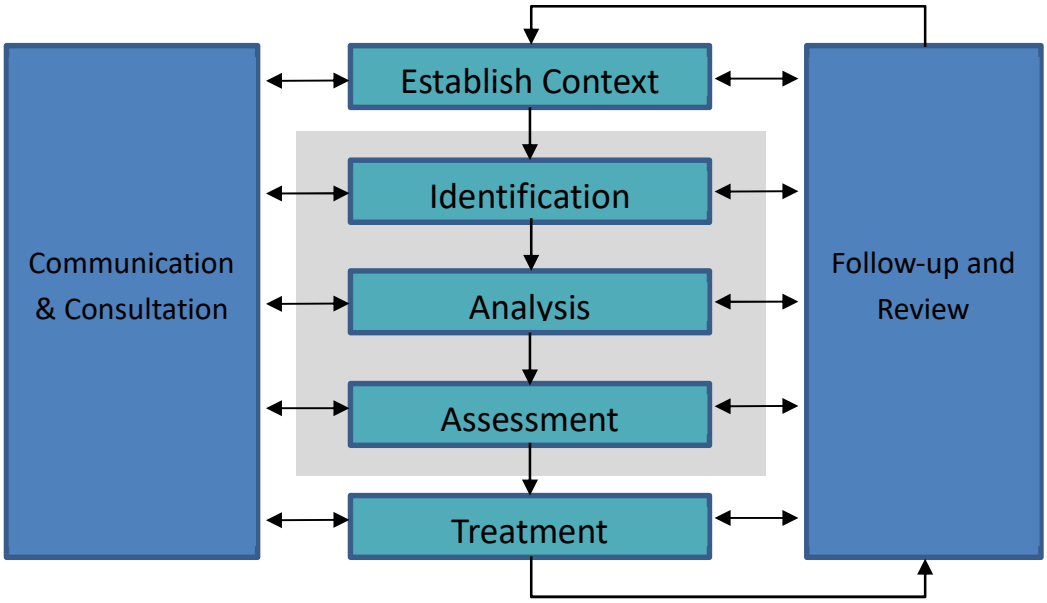
The system's policy is described in the document entitled **Policy of the System of Self-Control and Integral Risk Management of Money Laundering, Financing of Terrorism and Financing of the Proliferation of Weapons of Mass Destruction (ML/FT/FPWMD)**, which is developed through the procedures described below.

In any case, the Self-Control and Integral ML/FT/FPWMD Risk Management System is integrated to the guidelines imparted through the document called Code of Conduct and thus the controls implemented here must be applied by all employees, in line with the principles and values that guide their actions.

9. Procedures of the Integral ML/FT/FPWMD Self-Control and Risk Management System

9.1 Risk Management[1]

In accordance with the Risk Management Manual MA-DCI-RSK001, at CERREJÓN each functional area of the company is responsible for identifying and evaluating the risks inherent to its operations and implementing adequate controls. All risk management processes must follow the same basic steps indicated in the aforementioned manual and which are shown in the following diagram:



CERREJÓN will apply the methodology described in the Procedure for risk analysis and assessment MA-DCI-RSK001, which follows the ISO 31000 standard.

9.1.1 Segmentation methodology

Understanding segmentation as the identification of representative differences to group the elements that interest us from the point of view of SAGRILAFT (customers, suppliers, etc.), CERREJÓN uses the clustering technique on the segment, for all historical values, organizing it into 15 clusters. Each cluster's average is determined, and the derived cluster average is applied to all observations contained inside the same cluster. It is then normalized, giving each cluster a score between 0 and 100. The cluster with the lowest average will receive a value of 0, while the cluster with the greatest will receive a score of 100., the intermediate ones will be calculated with the expression:

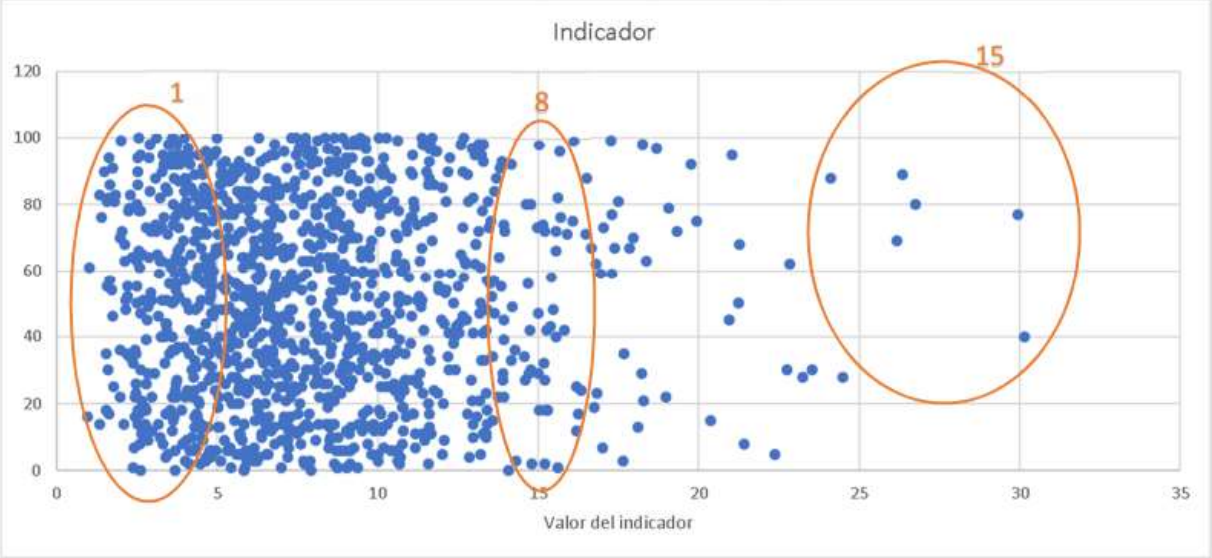
The rating of the supplier is determined by adding up its ratings for each indicator, each factor, and its total in accordance with the weights specified in the parameters. The value of the observation is categorized in

[1] Refers to the application of a methodology to effectively manage ML/FT/FPWMD risk.

the previously assembled clusters and assessed in the same manner for the present rating. Finally, if the difference between the historical and present ratings for any factor exceeds a predetermined threshold, an alert will be created.

Additional alerts are generated due to supplier characteristics or product-related activities:

- Supplier's business activity
- Country of import of the product
- Country of registration of the supplier
- Import of dangerous product



When segmenting, we will differentiate our counterparties into homogeneous subsets, grouped according to criteria related to geographic location, sector, type of product or good offered and handled by the company. The grouping is based on their characteristics, which will constitute the segmentation variables.

In accordance with the definitions in this Manual, counterparties are shareholders, employees, customers and suppliers of goods and services.

Following the list of segmentation criteria defined by the Superintendence of Corporations, we have:

9.1.1.1 Customers, Product and Distribution Channels

The product extracted by CERREJÓN is thermal coal; all the coal extracted is exported for power generation and most of the customers belong to the Power Generation Sector, therefore, the general profile of the coal buyers are foreign legal entities from the mentioned sector.

Considering the above, the level of ML/FT/FPWMD risk is considered low to medium for the case of the product and customers. The business partner/intermediary that markets our coal is a company of the Glencore Group, which performs the due diligence process and classifies customers into the following groups, considering different internal criteria:

- Clients with Low to Medium risk
- High risk clients

The criterion is determined according to the knowledge of the customer, where the evaluation is made based on due diligence and the risk level is assigned to each one. In this way, customers that are classified as having "High Risk" will require more in-depth due diligence analysis and enhanced due diligence will be performed.

9.1.1.2 Suppliers

Since CERREJÓN's universe of suppliers is varied and broad, it is considered that the ML/TF/FPWMD risk is latent in this segment and is the one that requires further analysis. The company's current suppliers are national and international individuals and legal entities that carry out activities that are specific and not specific to the coal industry, aimed at leveraging the extraction, transportation, and marketing of coal, as well as goods and supplies for the development of CERREJÓN's activity.

The Supplier Master File (SMF) is the basis for understanding supplier information.

Performing primary statistical checks, the Segmentation Variables established for the Company's suppliers are:

Jurisdiction or Geographic Area: CERREJÓN has national and international suppliers. For this analysis, the segmentation is defined according to the geographical location of the counterparty's operations, firstly, whether it is national or foreign, and locally, the Department of its domicile.

For the purposes of the Jurisdiction variable, the following fields are included in the SMF:

Counterparty by Origin (Supplier Typex4): classification according to whether the supplier is domestic or foreign.
PN = Domestic Supplier
PX = Foreign Supplier

Country code: contains the two-letter country code according to ISO 3166-1 standard.

Payment Address (Payment Addr 3): for national suppliers it contains the municipality and department; for international suppliers it contains the city and country.

This information will make it possible to compare with geographic areas that historically present high rates related to crimes associated to money laundering, terrorism, and proliferation of weapons of mass destruction or which have been identified as not having sufficient controls, in order to determine the associated ML/TF/FPWMD risk.

- **At the national level,** the statistical tables of crimes by department, published by the National Police are used, specifically data related to crimes against the economic order and terrorism.

Subsequently, the risk zones are classified according to the percentage of crimes of this type presented by department**.**

- **At the international level**, the Basel Anti-Money Laundering (AML) Index report produced by the Basel Institute on Governance as well as the list of non-cooperative and high-risk countries published by the Financial Action Task Force - FAFT for the classification of countries with the highest risk of ML/FT/FPWMD.

Economic activity or corporate purpose (Mark Sect Typex1): this is basically the sector to which the business is directed, since the type of economic activity carried out by the counterparty is an extremely key factor in the evaluation of its risk profile:

- Industrial
- Commercial
- Service Industry
- Financial / Banking / Insurance
- Government / Military
- Education
- Non-Profit
- Special Regime / Other
- Employee

Market Sector (Mark Sect Typex6): this classification is complementary to the previous one and is associated to the main economic activity according to the RUT for the case of national suppliers (See Table MARKET SECTOR 6) in the Vendor Master File.

For the classification of the economic activities vulnerable to ML/TF/FPWMD, those defined in the document Vulnerable Activities for ML/TF, "ML/TF Risk Management Model in the Real Sector", created under the "Responsible and Secure Business" program, led by the United Nations Office on Drugs and Crime (UNODC), the Bogota Chamber of Commerce and the British Embassy, were used as a basis.

- Corporations, foundations, or non-profit entities (Identified in the **Mark Sect Typex1** variable).
- Publicly or politically exposed persons (PEP) (Identified in the **Mark Sect Typex1** variable).
- Entities engaged in high-risk economic activities:

  - Companies or persons who commercialize products controlled by the National Narcotics Directorate.
  - Hotels and travel agencies.
  - Professionals and exchange houses.
  - Motor vehicles, boats, and aircrafts dealers/leasing companies.
  - Multilevel or pyramidal sales scheme marketers.
  - Arms, explosives, or ammunition dealers.
  - Construction companies.
  - Real estate agencies or real estate agencies.
  - Sports entities.
  - Gasoline stations.
  - Dealers in antiques, jewelry, precious metals and stones, coins, art objects and postage stamps.

- Moneylenders.
- Transportation sector.
- Money or value transporters.
- Companies located in free trade zones.
- Companies engaged in the transfer or remittance of funds or remittances.
- Border exchange operators.

Business Allies / Intermediary (Mark Sect Typex5): Special attention is given to individuals and legal persons hired to interact with national or foreign public officials or who generate business on behalf of or in representation of CERREJÓN, directly or indirectly, whose capacity to represent CERREJÓN is expressly stipulated or is implied in the terms of the agreement they have entered into.

Method of payment to Customers and Suppliers

The acquisition by coal customers, of products such as surplus and scrap is made with direct payments from them to CERREJÓN's bank accounts through electronic transfers.

Likewise, payment to suppliers is made through the national and international banking system, duly regulated, and recognized. According to CERREJON's procedures, cash transactions are not allowed since there are no petty cash accounts.

9.1.2 Identification of situations that may generate ML/FT/FPWD risk for CERREJÓN in new markets.

Each time CERREJÓN enters a new market, the President or whoever acts as Legal Representative or whoever he/she designates, will prepare a list of ML/FT/FPWMD risk situations, and will evaluate them. The result of the analysis shall be documented in accordance with CERREJÓN's risk management methodology and the procedure for risk analysis and evaluation.

9.1.3 Identification, evaluation, control, and follow-up of situations that may generate ML/FT/FPWMD risk.

9.1.3.1 Identification of situations that may generate ML/FT/FPWMD risk.

In accordance with CERREJÓN's methodology, this stage, which includes personnel from different areas and levels, involves the identification, classification and determination of the causes and consequences of incidents or specific and easily manageable events derived from an internal[2] or external [3]source that, in the development of the Company's corporate purpose, may generate ML/TF/FPWMD risk.

Once the identification procedure has been developed, those responsible for the areas associated with the sources of ML/TF/FPWMD risk and the Compliance Officer will list the situations that may generate ML/TF/FPWMD risk to CERREJÓN in the technological tool designed for this purpose, and will include the following information in the Bow Tie:

[2] LA/FT/FPWMD: Employees, Shareholders
[3] LA/FT/FPWMD: Customers, Suppliers, Donors and Beneficiaries of social programs

Causes: Situations that may generate the risk event.

Impacts: Estimation of the consequences generated by the materialization of a risk event. For LA/FT/FPADM it is measured in the dimensions of Financial, Legal, Reputation **(Consequence Criteria Table).**

9.1.3.2 Analysis and evaluation of situations that may generate ML/FT/FPWMD risk.

The purpose of the stage of analysis and evaluation of the risk situations identified is to determine the degree or level of CERREJÓN's exposure to the general risk of money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction, in each of the activities of its corporate purpose.

According to CERREJÓN's methodology, in this stage, which includes personnel from different areas and levels, the analysis of each risk situation identified from the information obtained in numeral 9.1.3 is carried out and includes the controls that contribute to prevent the occurrence of the event and/or help mitigate the impact/consequence in case the risk event occurs.

To document the result of the analysis, the Bowtie is completed, which includes the following items:

Estimate the PMC (Possible Maximum Consequence) or inherent risk. For each of the identified impacts/consequences, estimate the PMC and determine the level according to the Consequence Criteria Table and select the impact/consequence with the highest severity factor. The PMC is estimated by identifying the reasonably possible, credible, worst-case scenario when critical preventive and mitigating controls are missing or fail. The scenario should be described in a detailed manner such that the potential event under consideration is clear. The impacts/consequences should be assessed by representatives of the expert areas.

Estimate Severity: For the same scenarios selected in the PMC calculation, calculate the impacts/consequences in the presence of mitigation controls and determine the level according to the **Consequence Criteria Table**. Select the impact/consequence with the highest severity factor**.**

In order to calculate the PMC or Financial Severity, the following must be considered:

- Tonnage no longer produced and exported.
- Other costs generated by the discontinuation of production and exports, such as infrastructure repair, delays, etc.
- Fines for non-compliance
- Contracts for crisis management or for handling legal cases, cost overruns on purchases and/or contracts, etc.
- Should work with coal sales prices and production costs from the last forecast (Budget, Q1, Q2 or Q3) issued by the Finance area

- Affectation time period (days/months/years).
- With the above information, calculate the net present value of not producing and exporting the corresponding tonnage in the determined time.

Estimate the Probability Factor: Assign a probability to the highest severity scenario and determine the probability factor according to the **Probability Table**. The probability value is determined by the actual occurrence or materialization of the event, with the loss associated to the severity scenario.

The value of the probability is determined by the actual occurrence or materialization of the event with the loss associated with the severity scenario.

Determine the Residual Risk Value: The residual risk value results from the matrix relationship between the consequence and probability defined in the Enterprise Risk Matrix Table found in the Risk Management Manual.

9.1.3.3 Control of situations that may generate ML/FT/FPWMD risk.

The purpose of the control stage is to take measures to address the risk inherent in the risk situations to which CERREJÓN is exposed. The control must allow a decrease in the probability of occurrence or in the impact/consequence of the risk situation if it materializes and must always be applied in the corresponding process.

In order to reduce residual risks (those that remain after risk responses have been implemented) controls will be regularly reviewed and evaluated following CERREJÓN's risk management methodology.

Critical Controls will be identified which are those controls that, if they fail, the probability of the event materializing is very high.

A **Performance Standard** will be established for these Critical Controls, which are the minimum requirements that a critical control must meet. It contains information on the design of the control, who executes it, how it is executed and how often it is evaluated.

- The effectiveness of the critical control must be verified at least once a year, the result of the evaluation is a rating of "Adequate" or "Not Adequate" according to the methodology applied by CERREJÓN. If the result of the Risk Control Assessment (RCA) is not "Well Controlled" or the result of the Critical Control Evaluation (CCE) is not "Adequate" an alert must be raised before closing the risk assessment cycle.
- If a material risk is not tolerable, remediation plans should be identified within one month of the alert being raised. Once the remediation plan is completed and closed, the risk owner must re-perform the Risk Control Assessment (RCA) and revalidate the tolerability of the Material Risk.

9.1.3.4 Follow-up or monitoring of situations that may generate ML/FT/FPWMD risk.

The monitoring of risk situations seeks to evaluate the evolution of CERREJÓN's risk profile, both inherent and residual, and its variation.

The following activities will be carried out by the Compliance Officer and his team, with the support of CERREJÓN's areas from which collaboration is required, as follows:

- **Compliance Management:** will conduct at least once a year a review of the risk analysis, in order to evaluate the effectiveness of the controls to ensure that they address all risks and that they operate adequately, timely and efficiently. Additionally, it will verify that residual risks are within CERREJÓN's acceptance levels.

  On the other hand, Compliance Management will conduct a quarterly review of the due diligence performed during said period to verify compliance with the stipulations contained in this manual.

- **Process managers and their work teams**: those responsible for each process must permanently monitor the systems and activities of the specific process they are in charge of, to ensure that there are no ML/FT/FPWMD risk situations and that the controls in place are operating effectively and efficiently. The results of these activities must be reported to the Compliance Officer.

- Audit area: The audit areas carry out periodic reviews, the results of which are reported to the President or whoever acts as Legal Representative and to the Compliance Officer, who determine the corrective actions to be taken.

9.1.4 Due diligence in the knowledge of Counterparties

No activities, business or contracts may be carried out with any of the counterparties without compliance with the following rules.

In order to identify the final beneficiaries of CERREJÓN's counterparts, the criteria established in Article 12 of Law 2195 of 2022 will be considered, such as:

- Identify the individual, legal party, unincorporated or similar structure with which the legal transaction is entered into.

- Identify the beneficial owner(s) and the ownership and control structure of the legal party, unincorporated entity or similar structure with which the legal transaction is entered into and take reasonable steps to verify the information reported.

- Request and obtain information that allows to know the intended purpose of the legal business.

- Conduct ongoing due diligence of the legal business, examining the transactions carried out throughout that relationship to ensure that the transactions are consistent with the knowledge of the individual, legal party, unincorporated or similar structure with which the legal business is conducted, its business activity, risk profile and source of funds.

In the event that a relationship with a third party or counterparty mentioned below must be initiated, without the due diligence process having been fully and previously carried out, the area in charge or interested party must request written authorization from Compliance Management to continue with the linking or relationship process without complying with the strict procedure of knowledge of the counterparty, indicating the reasons for the urgency of the operation or the calamity situation, in which case the due diligence must be carried out as soon as possible. If after establishing the relationship with the third party, due diligence is not completed within a maximum period of one month after the beginning of the relationship or the occurrence of the calamity, Compliance Management will review the situation and may recommend not to continue having any relationship with such third party and, if necessary, will proceed to make a STR in relation to the counterparty.

The verification of each counterparty shall be carried out prior to the beginning of the commercial relationship and the information shall be kept in accordance with the provisions of Article 12 of Law 2195 of 2022. If the term of an agreement is for several years, the due diligence will be updated according to the level of risk and at least every 24 months.

9.1.4.1 Customer Knowledge

Coal Sales

CERREJÓN or the third party mandated to carry out this activity, will verify the identity and background of all customers, for which it will request the following information:

- Name, address, and contact details of the entity.
- Certificate of Incorporation, Tax Identification Number or its equivalent (Tax Identification Number)
- Beneficial owners with 5% or more ownership interest in the company
- Other information deemed relevant and necessary.

Once the information is received, CERREJÓN or the third party mandated to carry out this activity, will analyze the documentation of the clients in order to carry out an objective and reasonable evaluation to establish the possible existence or not of a ML/TF/FPWMD risk. These verifications in relation to ML/TF/FPWMD will be carried out only to coal sales counterparties.

CERREJÓN or the third party mandated to carry out this activity, will aim to include in all coal sales contracts clauses to ensure compliance with the rules that apply to the client in terms of prevention and control of ML/TF/FPWMD.

Additionally, CERREJÓN or the third party mandated to carry out this activity, will verify each client and the legal representative who will sign the corresponding contract, in the sanctions lists (including the list of the Office of Foreign Assets Control of the United States - OFAC, the list issued by the Security Council of the United Nations) using an alert detection service. Beneficial owners with 5% or more ownership interest, as well as their directors, will also be verified. If it is determined that the entity is sanctioned on a list applicable to Colombia, the case will be reported to the CERREJÓN Compliance Officer. Verifications in the sanction lists will be made to the coal sales counterparties.

Sale of surplus

In the case of the sale of surpluses and in light of this manual, the buyer of surpluses who is not an employee of the Company will be considered a customer. Therefore, the buyer must fill out the attached format established by CERREJÓN in order to obtain information on knowledge of this type of third parties.

The employee responsible for CERREJÓN must request supporting documents that allow verification and/or confirmation of the information recorded in the form established by CERREJÓN.

The names of the persons appearing on the form and supporting documents, including the names of the final beneficiaries, must be consulted in the tool provided by CERREJÓN. With this information, due diligence will be performed in the technological tool established by CERREJÓN for this purpose, where all supporting documents must also be attached.

If the result of the due diligence is that the transaction is classified as high risk, a risk analysis by Compliance Management will be required.

9.1.4.2 Knowledge of Recipients of charitable contributions (donations), community investment beneficiaries and sponsorships.

The Vice-Presidency of Public Affairs and Communications and Compliance Management will work together to develop the due diligence process for this type of third parties that will receive charitable contributions or sponsorships or will benefit from investment projects in the CERREJÓN community. The completion of the forms/questionnaires designed for this type of third parties will be requested, as appropriate, as well as the relevant and necessary supporting documentation, and the due diligence will be carried out in the technological tool provided for this purpose, in order to identify alerts on such third parties and make the appropriate decisions or the necessary controls.

The entire due diligence flow indicated by Compliance Management, where each case is analyzed according to the level of risk, shall be followed.

Once the endorsement or approval has been received from Compliance Management, the corresponding approval process will continue, considering the recommendations, if applicable.

9.1.4.3 Knowledge of suppliers and contractors

The following due diligence activities are considered as part of the controls established for the knowledge of suppliers and contractors.

1. The corresponding analysts will ask basic questions previously established by the Compliance Management to identify whether to follow the course of a simplified due diligence (Know Your Client) or intensified due diligence (TPDDMP).
2. The supplier or contractor shall be requested to fill out the corresponding form and shall be required to send the necessary and relevant supporting documents for the knowledge of

the counterparty, in accordance with national regulations, such as information on final beneficiaries.

3. The due diligence information shall be filled out in the system provided by CERREJÓN for such purpose, identifying whether it is a simplified due diligence or an intensified due diligence in the case of PEPs, intermediaries, attorneys-in-fact, or representatives and for those who generate other types of alerts, and the corresponding risk assessment shall be made, including the consultation in lists.
4. Depending on the level of risk, approvals may be required from different CERREJÓN Compliance instances.
5. Considering the risk analysis, the linking of the third party will be approved or not from the point of view of Compliance Management and/or recommendations will be made if necessary.

9.1.4.4 Supplier and Contractor Data Update

Due diligence is valid for 20 months for low and medium risk third parties and one year for high and serious risk third parties.

In cases where the supplier or contractor reports a change of legal representative, final beneficiaries or company name, the due diligence must be performed again regardless of the time the previous due diligence has been in force.

In cases where the risk level changes due to a contractual modification, or any other type of alert, a new due diligence shall be performed regardless of the time the last due diligence has been in force.

9.1.4.5 Knowledge of workers or employees

The Vice-Presidency of Human Resources and Services, in charge of the process of selection, hiring and maintenance of human resources, will carry out the due diligence activities during the selection, hiring and maintenance of employees described in the Personnel Selection Manual.

In case of alerts that qualify the hiring as high risk, the due diligence must be sent to the Compliance Management for the performance of the corresponding enhanced due diligence and endorsement.

Ensure that all "red flags" are cleared before confirming the job offer.

9.1.4.6 Knowledge of shareholders

The register of shareholders and the register of directors (members of the Board of Directors) is managed by the Legal Vice-Presidency, who is responsible for keeping available the identification of the associate or

director, together with his or her address and telephone number. On the other hand, it shall ensure the updating of the information that may change over time.

The Legal Vice-Presidency will make a consultation of the persons on the binding and/or restrictive lists, contained in the tool provided for such purpose, leaving evidence of the result with date and time of the activity. The aforementioned result must be saved in the physical or electronic folder of the associate.

The matches found must be reported to the Compliance Officer.

When it is required to make dividend payments or other payments to shareholders, the Financial Accounting and Tax Department[4] shall fill in the information required to register them in the Suppliers master.

9.1.5 Knowledge of persons who may expose CERREJÓN to a higher risk.

9.1.5.1 Politically or Publicly Exposed Persons (PEP)

Pursuant to the definition of Politically or Publicly Exposed Persons (PEPs) as indicated in this document, PEPs are considered to be individuals who may expose CERREJON to a greater degree to the risk of money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.

Most PEPs are recognized members of society, and their involvement in a company is completely legitimate. The link with PEPs of any of the categories, may generate exposure to risks such as legal, reputational and contagion risks; they present a higher risk of involvement in money laundering and/or terrorist financing due to the position they hold. Situations may arise where it is discovered that the companies they manage are used for other purposes, such as hiding personal assets in offshore tax havens, or are involved in corrupt businesses.

The PEP may use its recognition to simplify know-your-customer and due diligence procedures, i.e., try to use its status and popularity to evade controls.

According to Colombian regulations, the PEP status is maintained until two years after leaving office.

By way of example, the following are politically or publicly exposed persons:

- **Persons who manage public resources:** included in this category are those who directly or indirectly have under their responsibility the administration of resources of public origin. For example: governors, mayors, State Contractors, Directors of Public Entities.

- **Persons who hold some degree of public power:** included in this category are those who have a level of influence over political decisions or strategies that have an impact on Society. These persons may or may not be directly or indirectly related to the public sector.

[4] Procurement and Contract Divisions

Likewise, PEPs are considered to be officials who legally represent Public Entities that may have any transaction with CERREJÓN, leaders of indigenous communities that enjoy public recognition within their organization, among others.

The PEP conditions are alerted in most cases, by the tool provided by CERREJÓN for consultation, or detected when reviewing the information that the third party declares in the forms provided for their knowledge. Any transaction involving a PEP requires enhanced due diligence.

9.1.6 Due Diligence

In the questionnaire of knowledge of third parties:

- The questionnaire asks if the legal entity has a PEP or if the natural person is a PEP or a family member of a PEP.
- It includes a statement of the legality of the origin of the funds and the lawful use of the resources received from Cerrejón in the event of a linkage.

The list and database consultation tool used by CERREJÓN generates:

- Alerts related to the quality of PEPs, including that defined by Colombian standards.
- Alerts for negative news databases.

9.1.6.1 Enhanced Due Diligence

This type of due diligence requires the completion of forms/questionnaires of knowledge of third parties where more information is requested compared to simplified due diligence. It may also happen that in the development of a simplified due diligence where the form of knowledge of the third party is simple, an alert is presented in the development of the due diligence, in which case it will be required to expand it and develop an enhanced due diligence procedure.

Through the intensified due diligence process a more exhaustive risk analysis is made in which the alerts are analyzed, as well as the type of service or good or the type of relationship that is intended to be established or has been established between the third party and CERREJÓN.

- Information from other sources such as the supplier's or contractor's website, information on stock quotes, news, legal proceedings, among others, is reviewed to decide whether it is possible to continue with the relationship and linkage process with each third party.
- Reasonable steps are taken to establish the source of wealth and source of funds.
- The origin of the contact with Cerrejón is verified (e.g., referred by someone, social investment project, donation, competitive process, direct contracting, delegated or major contracting).
- If necessary, the counterpart should be interviewed to clarify any doubts that may arise.
- Once all the information has been gathered, the situation and the possible impact/consequences should be analyzed.

- If the alerts are confirmed and the decision is not to take the risk, the reasons supporting the decision should be documented, attaching the documents obtained and rejecting the counterparty.
- If there is already a relationship with the counterparty, the scope of services and the impact/consequences of a possible need to terminate the contract should be reviewed with the area that hired the third party.

A PEP can appear in a relationship in any of the following ways:

- A link is being made with an entity that belongs to the State (national or foreign) totally or partially. In this case, the presence of the PEP as an official of that entity is justified.

- A relationship is being made with a legal entity where the presence of a PEP or family relationship with a PEP is identified.

- The linking of a natural person is being carried out where the PEP status is identified.

9.1.6.2 High Risk Transaction Analysis - Enhanced Due Diligence

The Compliance Officer in his role of analyzing transactions identified as high risk may make use of some enhanced due diligence practices for decision making regarding the linkage with that third party:

- ✓ Request and examine the financial statements to determine whether their financial situation is in line with that of the companies in the sector.
- ✓ Verify the background of legal entities incorporated abroad.
- ✓ Request certificates stating that the company has policies and procedures for the prevention and control of money laundering and financing of terrorism.
- ✓ Request from foreign companies the certificate of compliance with the measures for prevention and/or control of ML/TF/FPWMD that apply in the country of origin.
- ✓ Request from companies domiciled abroad the corresponding certificate of incorporation.
- ✓ Request the "Certificate of lack of reports for drug trafficking for the handling of controlled chemical substances", for companies producing or distributing controlled substances.
- ✓ Consult information of the potential counterparty in the databases of credit bureaus, upon request of the corresponding authorization.
- ✓ Verification of additional information through the web.
- ✓ For the purposes of the PEPs, verify the information about their position, date of employment and date of termination. Verify if he/she handles or handled public resources.
- ✓ Request information on whether it is an Authorized Economic Operator (AEO).

9.1.7 Handling of matches in binding, restrictive and other lists

The results of consultations in lists that show "positive" matches will be handled as follows:

- Binding list queries must be made through the tool CERREJÓN has available for this purpose. If an alert is generated, the due diligence should be directed to the Compliance Management for review

and evaluation of the risk level taking into account different aspects of each third party, to determine whether it was a case of homonymity, if it is possible to continue with the linkage or relationship with the third party that presented matches in the consultation in lists or if the recommendation is not to have any relationship with the third party. In applicable cases, CERREJÓN, through the Compliance Officer, will immediately report a suspicious transaction to the UIAF and/or the competent authorities.

If the person is involved in another list, in an adverse or negative news:

- If it is decided not to advance or close the relationship, the owner of the corresponding process, depending on whether it is a customer, supplier, employee or shareholder, will advance the information protocol to the counterparty as appropriate, citing strictly corporate reasons.

If it is an owner of an asset that is registered in a binding list (UN) or in the OFAC restrictive list:

- No property is acquired or taken on lease whose certificate of tradition shows as last owner a person who is on the restrictive lists.

- In the event that those who appear on the restrictive lists are previous owners, an analysis is made in each case as to whether or not to lease or purchase the property in view of the risk of forfeiture of ownership and the possibility that such a fact is indicative of the illegal origin of the property.

CERREJÓN, through the Compliance Officer, will carry out special monitoring of the behavior of persons with whom it has a contractual relationship and who have been identified in some of the non-binding lists or in adverse or negative news, reserving the right to terminate in advance its contractual relationship, in cases that do not contravene the law.

It is the obligation of CERREJÓN employees to keep confidential the results of the consultation of third parties in the lists.

9.1.8 Operations that may generate greater risk for the company

9.1.8.1 Handling of cash within the Company

At CERREJÓN, cash payments to third parties are not authorized. All operations will be carried out using the services of the financial system.

9.1.8.2 Virtual assets

CERREJÓN does not trade through virtual assets.

9.1.9 Management of funds deposited in the Company's bank accounts

CERREJÓN will receive in its bank accounts, the resources coming from the sales made to its counterpart clients, the income from other services rendered and any other income from transactions originating in its operation. Bank reconciliations will detect any resources that have entered the bank accounts and that are not supported by a business transaction. In the event that an unusual transaction is detected, it must be reported to the Immediate Supervisor and the Compliance Officer.

Unusual transactions that, after being analyzed by the Compliance Officer, are susceptible of being returned to the beneficial owner, must be duly documented and, if they are suspicious, must be reported to the UIAF by the Compliance Officer.

9.1.10 Foreign trade operations

According to the nature of the foreign trade operations carried out by CERREJÓN (import and export of products), the following activities must be carried out:

- Verify that the counterparty (customer, supplier) has satisfactorily completed the linking and/or updating procedure.

- Verify with the documents issued by the customs authorities, that the country of origin or the country of destination of the goods, complies with international recommendations against LAFT/FPWMD.

9.1.11 Acquisition of real estate property

The Legal Vice-Presidency, in charge of the review of titles and documents, must compile and keep available the identification of all owners or holders that appear in the certificate of tradition of the property. In these cases, due diligence must also be carried out as with any other matter, in the systems provided by CERREJÓN for this purpose, attaching the supporting documents, consulting restrictive lists and taking into account the concept of the Legal Vice-Presidency and the Standards Office.

9.1.12 Detection and analysis of unusual transactions

The procedure for detection and analysis of unusual operations is understood as the series of activities carried out in order to identify unusual behaviors of clients, suppliers, associates, and employees to be analyzed, documented and, in case of being determined as suspicious operations, to report such behaviors to the UIAF. These activities are described in the subtitles of this numeral.

The identification of warning signals and unusual operations is carried out by CERREJÓN employees, during the performance of their duties and especially during the application of controls in the procedures of knowledge (selection and linking) of the counterparties and at all times during the contractual relationship.

These operations are identified through the use of the following tools:

- ✓ **National and international lists.** By using them it is possible to identify links with persons or assets related to ML/TF/FPWMD crimes.

  The list query application performs a daily cross-check of information from the databases updated during the day against the CERREJÓN counterparty database. If there is a match, it generates an alert that is sent to the Compliance Management e-mails for verification and action. This process allows establishing whether the initial situation of the counterparties is maintained or has undergone changes in terms of the status in the consulted lists (UN, OFAC, PEPs, Comptroller's Office, and others).

  Once the alert is received, the verification process must be carried out, in case it is positive and it is decided that it is not possible to continue with the business relationship, it must be reviewed with the area that contracted the services and based on the unilateral termination clause contained in the contract, the contractual relationship will be automatically terminated, based on strictly corporate reasons.

  CERREJÓN through the Compliance Officer will immediately report a suspicious operation to the UIAF and/or the competent authorities.

  Matches found during the development of these activities will be handled as described in this manual.

- ✓ **Market Knowledge:** in order to facilitate the detection of unusual operations CERREJÓN will seek to learn about the usual characteristics of the market[5], in relation to the economic activities of its external counterparties (Customers and Suppliers). This review is conducted whenever a Foreign Trade activity or service has an alert signal activated and it is necessary to compare things to determine whether they are normal, maybe unusual, or have a suspicious character.

- ✓ **Non-transactional red flags.** By gathering information regarding the economic activity of the counterparty, knowledge of the business and the industry, the experience of the Business Partner / Intermediary, the Materials and Services Department, the Human Development Division of the Vice-Presidency of Human Resources, the Vice-Presidency of Public Affairs and Communications, the Legal Vice-Presidency and Compliance Management, warning signals are established related to atypical behavior that, if detected, must be reported to the Compliance Officer.

Listed below are a series of warning signs to watch out for:

Warning signs - Customers

[5] It involves inquiring into the characteristics of mode, time and place in which similar activities are usually carried out, in order to gather elements of judgment about the reasonableness of the operation being carried out by the customer or supplier.

- Refusal to provide information at the time of the engagement. This includes failure to provide the duly completed form or the required supports.
- Refusal to update the information when required.
- When there are matches in the identification number or name when validating with the binding or restrictive lists or other sources.
- Being linked to crimes related to ML/FT/FPWMD.
- When it is intended to acquire goods or services that do not correspond to the type of counterparty.
- When as a result of control and verification of the information differences are found.
- When upon request for information or clarifications the counterparty decides not to continue the process.
- When the usual characteristics of the counterparty's economic activity or transactions deviate from the defined profile.
- When the counterparty carries out transactions with large volumes of cash without apparent justification.
- Any other fact that is not expressly mentioned but that draws attention or generates distrust.

Warning Signs - Suppliers and Contractors

- Refusal to provide information at the time of the engagement. This includes not delivering the duly completed questionnaire or the required supports.
- Refusal to update the information when required.
- When there are coincidences in the identification number or name when validating with the binding or restrictive lists or other sources.
- Being linked to crimes related to LA/FT/FPADM.
- Identifying goods with prices notoriously lower than those offered by the market.
- Requesting payments in favor of third parties, without reasonable justification.
- Legal representative appearing in several supplier companies without apparent justification.
- That the goods or services supplied are not duly nationalized and therefore may come from contraband.
- That the goods being of restricted sale do not have the proper authorizations or licenses.
- In the case of real estate, that persons related to ML/FT/FPADM are included in its tradition certificate.
- That the company is insolvent or is in some type of liquidation.

Warning signs from workers or employees

- Refusal to provide information at the time of hiring. This includes the failure to provide the resume form duly filled out or the required supports.
- Refusal to update the information when required.

- When there are coincidences in the identification number or name when validating with the binding or restrictive lists or other sources.
- Current employees who are linked to ML/FT/FPWMD related crimes.
- Significant changes in the employee's quality of life without apparent justification.
- Employee who avoids certain internal or approval controls established for certain operations, products, or services.
- Employee who omits to verify the identity of a counterparty or does not confront their data with the records provided in the forms/questionnaires or databases provided.
- Employee who frequently receives gifts, invitations, and gifts from certain clients or counterparties, without a clear and reasonable justification.
- Employee who provides preferential, exclusive, and permanent service or exempts a counterparty from certain controls with the argument that he/she is "well known", "referenced from another entity", "he/she only trusts me", "I collaborate with him/her in all his/her business" or similar.

.

Partner warning signs

- Identify assets related to crimes associated with ML/FT/FPWMD that are intended to be received as contributions.
- Impossibility of identifying the origin of the contributions made by the partner or shareholder.

Warning signs in foreign trade operations

- That the export payment comes from a person other than the foreign buyer.
- That the export payment comes from a country qualified as a tax haven.
- That the export payment comes from a country other than the country of the buyer or the country of destination of the thermal coal, without reasonable justification.
- Inconsistencies between the deposited or supported values, with the values of the exchange declarations.
- Endorsements of the transport document to a third party with no track record in the sector.
- Lack of information in the transport document such as mentioning only the city, telephone number, incomplete addresses, names without surnames, etc.
- Difficulties to physically verify the merchandise, despite the fact that the documents are supported, and the import declaration complies with all customs formalities.
- Imports or exports of large volume or value that are not directly related to its economic activity or ordinary course of business.
- Imports or exports that are not directly related to CERREJÓN's economic activity.
- The importation of luxury goods, such as luxurious vehicles, works of art, precious stones, sculptures, etc., which are carried out sporadically or habitually and are not directly related to the economic activity or ordinary business of CERREJÓN.

- Re-shipment of goods without apparent cause or re-export of goods that if they had been nationalized would present any of the risk profiles noted above.
- Open smuggling or technical smuggling operations.
- The use of allegedly false documents or fictitious exports.
- Loss or theft of goods while being transported from the place of arrival to the warehouse.
- Merchandise that enters the country documentarily, but not physically without apparent cause.
- Over-invoicing or under-invoicing of imports.
- Physical entry of sums of money in containers

9.1.13 Internal reporting of red flags and unusual transactions

Whenever a CERREJÓN employee, in the performance of his/her duties, detects a warning signal or an unusual operation, he/she must immediately report this fact by e-mail to his/her superior and to the Compliance Officer so that he/she may initiate the respective analysis and investigation.

The e-mail must contain the following information:

- Date of report
- Reporting officer
- Name and identification number of the related counterparty
- Warning signal that generates the report
- Clear reasons why the operation is considered unusual.
- All relevant information of the case.

9.1.14 Analysis of warning signals and unusual transactions

The Compliance Officer is in charge of receiving the reports made by the processes and/or areas of CERREJÓN, together with the necessary supports, and in this way to advance the analysis jointly with the owners of the processes that affect the counterparties analyzed, with the following enhanced due diligence procedure:

- Request additional information when required, in order to examine more closely the warning signal and knowledge of the counterparty. Verify that the economic activity of the counterparty has a causal relationship with the operation, business, or contract. Verify that the operation, business, or contract is in accordance with the profile and usual characteristics of the counterparty. Verify the result against the consultation parameter in prevention lists and databases.
- In case of not finding reasonableness or logical explanation against the identified alert signal, the corresponding unusual operation report must be prepared and if applicable, must prepare a ROS.

9.1.15 Identification and determination of attempted or suspicious transactions

The Compliance Officer is responsible for analyzing unusual transactions in order to:

- Verify that in-depth activities have been carried out on the warning signal and on the knowledge of the counterparty.
- Request additional information when the analysis warrants it.
- Determine whether the situation, operation, contract, or business, due to its unusual nature, may be susceptible to be reported to the UIAF and, according to the moment in which it was detected, classify it as attempted or suspicious[6].

The Compliance Officer shall determine the suspicious operation and shall make the corresponding report to the Financial Intelligence and Analysis Unit (UIAF). The applicable criteria to determine if an operation is suspicious are:

- The principle of consistency[7].
- The knowledge of counterparties policy.
- Lack of a reasonable explanation for any of the warning signs indicated.

Attempted or suspicious transactions are determined once the unusual transaction has been compared with the counterparty's information and the defined normality parameters. In any case, CERREJÓN may consider as attempted or suspicious those operations of the counterparty that, being within normal parameters, are considered irregular.

9.1.16 Report of attempted or suspicious transaction

In accordance with the decision taken in the previous step, the Compliance Officer must make the suspicious transaction report following the guidelines established in Chapter X of the Basic Legal Circular of the Superintendency of Companies and DIAN Circular 170 of 2002, immediately, that is, from the moment the company makes the decision to classify the transaction as suspicious.

9.1.17 Documentation and archiving of the cases analyzed

Following the completion of the report, the supports (information from transaction records and documents of knowledge of the counterparty) that led to classify the operation or situation in one category, or another must be kept.

They must be centralized and organized in a sequential and chronological manner with the appropriate safeguards, together with the respective report to the UIAF, for the purpose of making them available in a complete and timely manner to the authorities when they request them.

[6] A transaction is attempted when it is known that the counterparty is going to carry out a suspicious transaction, but it is not completed either because the counterparty desists or because the controls in place do not allow it to be carried out.
[7] The amount or characteristics are not related to the counterparty's activity, or that due to their number, the amounts traded or their particular characteristics, are outside the established parameters of normality.

Said 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 the policy.

10. Disclosure and Documentation

10.1 LAFT self-monitoring and risk management system documents

As part of the simplified or enhanced due diligence processes, CERREJÓN may request from the counterparty, among others, the following documents:

- Certificate of existence and legal representation with an issue date of no more than three months or equivalent document(s) from the company's registry confirming the existence of the organization, corporate name, corporate purpose, registered address, country of incorporation/domicile, and a list of legal representatives, directors, or authorized persons. (Examples: Certificate issued by Chamber of Commerce, Sole Tax Registry RUT (for its Spanish acronym), Operating Agreement, Articles of Incorporation, Certificate of Formation, Bylaws).
- Certificate of shareholder composition.
- Copy of the Sole Registry of Beneficial Owners RUB (DIAN)[8] or certificate indicating full names, identification and nationality of the beneficial owners, natural persons, who own 5% or more of the shares or participation.
- Certification of the bank account with date of issue not older than three months.
- Copy of the valid official identity document of the beneficial owners, legal representatives, and directors.
- Photographs of the location of the counterpart's offices.
- Copy of the resumes or a description of the duties to be performed by the counterpart's employees who will foreseeably lead the relationship with CERREJÓN.
- Copy of the compliance policies of the counterparty, especially those associated with ethics, corporate transparency, prevention of corruption and bribery.
- Certificate or administrative act stating the appointment of the representative or director of the entity in case it is a government entity.
- Recent certificate of non-encumbrance and tradition.
- Sworn statement of non-existence of inabilities, impediments, incompatibilities, and conflicts of interest.
- If the counterparty is an individual, copy of its identity document and curriculum vitae.

CERREJÓN shall keep the documents and records related to compliance with the standards of the System of Self-Control and Integral Risk Management, according to legal provisions on personal data protection contained in Laws 1266 of 2008, 1581 of 2012, any norm that modifies or replaces them, and other applicable regulations; likewise, such media shall be kept in accordance with the provisions of Article 28 of Law 962 of 2005 (for a term of 10 years), or any norm that modifies or replaces it. The information obtained in due diligence shall be kept for the duration of the legal business and at least during the following five (5) years counted from January 1 of the following year in which the legal business or the state contract is terminated, or the occasional transaction is carried out, as established in Paragraph 3 of Article 12 of Law 2195 of 2022.

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

[8] Colombia's Department of Taxes and National Customs

- That there is no request for their delivery formulated by a competent authority.
- That they are kept in a technical medium that guarantees their subsequent accurate reproduction and the preservation of their evidentiary value.
- In cases of merger, the absorbing entity must guarantee the continuity of strict compliance with this stipulation.
- In the event of liquidation, the liquidator must adopt the necessary measures to guarantee the filing and protection of these documents.

The documentation related to the system includes:

- The manual with its respective annexes containing the policies and procedures.
- The documents that support the design, development, and implementation of the system's methodologies.
- The documents and records that evidence the effective operation of the system, which include, among others, the documentation and information of the counterparties and the documentation related to unusual operations and the report of suspicious operations.
- The Compliance Officer's report to the Board of Directors and the Legal Representative.
- Documents that support the evolution of controls.
- Documents by means of which the authorities require information together with their responses.
- The supports of the analysis of unusual and suspicious operations.
- Disciplinary processes carried out for eventual non-compliance with the system.
- Documents supporting the training and dissemination of the system.
- Internal reports of warning signals and unusual operations or external reports of the system to the UIAF and other authorities.
- All additional documentation that supports the system in any way.

The Compliance Officer will be in charge of the system documentation, who will ensure its integrity, availability, compliance, effectiveness, efficiency, reserve, reliability and updating. It shall be kept in a centralized and chronological manner with the security protocols either in written or magnetic media.

10.2 Internal and external reporting

10.2.1 Internal Reports

10.2.1.1 Regarding unusual transactions

Whenever any of the employees detects warning signs, unusual operations, or behaviors, they must report this fact to the Immediate Supervisor and to the Compliance Officer, indicating the reasons that determine the operation as unusual.

10.2.1.2 Internal reporting of suspicious transactions

Whenever an employee detects warning signs or inusuales operations, he/she must report it to the Immediate Supervisor and Compliance Management. Such report is reviewed by the Compliance Officer and if it is determined as suspicious, it must be immediately reported in writing to the UIAF.

The report must indicate the reasons that determine the operation as suspicious.

10.2.1.3 Reports from the follow-up or monitoring stage to the system.

Compliance Officer's Report

Annually, the Compliance Officer shall submit a report to the Board of Directors on the management carried out and the fulfillment of the tasks under his/her responsibility.:

- Evaluation and analysis of the efficiency and effectiveness of the system.
- Results of the Compliance Officer's management.
- Proposals for improvements, if identified.

Such report shall be delivered directly to the Board of Directors without any intermediation with the Legal Representative of the COMPANY, thus allowing the independence of the Compliance Officer in accordance with the stipulations of Chapter X of the Basic Legal Circular of the Superintendence of Corporations.

Likewise, in accordance with the provisions of DIAN Circular 170, a monthly report shall be submitted to the legal representative on the most important aspects related to the prevention of ML/FT/FPWMD risks in the company.

10.2.2 External Reports

10.2.2.1 Mandatory reporting of attempted or suspicious transactions (STR) to UIAF.

Once the operation is determined as suspicious, the Compliance Officer shall immediately and directly report it to the Financial Information and Analysis Unit - UIAF, following the instructions and technical specifications issued by the latter in this regard.

Attempted or rejected transactions that have characteristics that make them suspicious shall also be reported, as well as attempts of commercial linkage.

The ROS shall not give rise to any type of liability for the company, nor for the managers or collaborators who have participated in its determination and reporting. The ROS does not exempt from the duty to report, if applicable.

For control purposes and to support risk management, the Compliance Officer shall keep a record of the reports that have been sent to the UIAF.

The Compliance Officer and the Legal Representative shall ensure the timely submission of reports to the Superintendence of Corporations.

10.2.2.2 Report of absence of attempted or suspicious transaction (STR) to the UIAF.

The Compliance Officer is obliged to make timely reports of absence of suspicious transactions to the UIAF according to the applicable regulations.

10.2.2.3 Single and Multiple Cash Transaction Reporting

On a monthly basis within the first ten (10) calendar days of the following month or as indicated in the regulations in force, the Compliance Officer shall report to the UIAF the transactions involving collections or payments by means of delivery or receipt of cash for an amount equal to or greater than ten million pesos ($10,000,000) or transactions involving collections or payments by means of delivery or receipt of cash for amounts less than ten million pesos ($10,000,000) but which added together during a calendar month reach an amount equal to or greater than fifty million pesos ($50,000,000) for the same individual or legal person.

Cash payments channeled through the financial system shall not be reported to the UIAF.

10.2.2.4 Absence of single and multiple cash transactions reporting

In the event that during a month the existence of individual or multiple monthly cash transactions has not been determined, the Compliance Officer must report this fact to the UIAF within the first ten (10) calendar days of the month following the end of the period (quarterly) through the Online Reporting System (SIREL) of the UIAF or according to the periodicity indicated by the regulations in force.

10.3 Design and implementation of the management system training program and dissemination plan

10.3.1 Training Program

CERREJÓN, establishes as a mechanism for dissemination of policies and procedures for the prevention and control of money laundering, financing of terrorism and financing for the proliferation of weapons of mass destruction, the design and development of a training program that will allow awareness and training to employees at the beginning and during the duration of the contractual relationship.

The program will contemplate the frequency of the training, the scope, the forms of evaluation and the means to execute it.

The training program will be directed to third parties whenever CERREJÓN considers it appropriate.

The Compliance Officer, with the support of the Vice-Presidency of Human Resources and Services, is responsible for designing, scheduling, and coordinating training plans for CERREJÓN's employees on the Self-Control System and Integral ML/FT/FPWMD Risk Management.

The trainings must comply with the following conditions:

- The training for key positions in the Self-Control and Integral ML/FT/FPWMD Risk Management System will be carried out at least once a year.
- Communication of policies and procedures to all CEREJÓN employees will take place every two

years.

- Disclosure will be made during the induction process of new employees and to third parties (non-employees of the company).
- Be constantly reviewed and updated.
- Have mechanisms for evaluating the results obtained, in order to determine the effectiveness of these programs and the achievement of the proposed objectives.
- Indicate the scope of these programs, the means that will be used to implement them and the procedures that will be used to evaluate them.
- A record should be made of their execution, as well as the names of the attendees, the date and the topics covered.
- As a result of the training plan, the trained persons must be able to identify what is an Unusual Transaction and what is a Suspicious Transaction and the content and form in which they must be reported.
- The system will be disclosed annually through the company's internal mass media and in training sessions.

11. Attention to requests for information from competent authorities.

CERREJÓN will only lift the confidentiality of the information collected from its counterparties as a result of written requests specifically formulated by the competent authorities, with the fulfillment of the legal requirements and forms and in the cases indicated by the regulations.

Any request for information from competent authorities regarding the prevention and control of money laundering, financing of terrorism and financing for the proliferation of weapons of mass destruction will be handled by the Compliance Officer with the support of the Legal Vice-Presidency.

CERREJÓN employees will keep confidential all requests and judicial inspections carried out by the authorities, as well as reports made to the UIAF. Disclosure of such requests may result in administrative and criminal penalties.

Requests from government entities are received through the e-mail address registered in the RUNT: notificaciones.judiciales@cerrejon.com, which is under the responsibility of the company's Legal Vice-Presidency. Once received, the Legal Department reviews the scope of the requirement and forwards it to the area in charge; the latter analyzes the information, prepares the response, attaching the pertinent supports and forwards it to the legal area for review, approval and signature of the legal representative; finally, the responsible area is responsible for its formal filing with the entity within the terms established in the requirement.

12. Technological Infrastructure

CERREJÓN has different tools (software, hardware, data, and communications) that support the work of the Compliance Officer, such as:

Tool for consultation in lists
Tool for registration of suppliers and contractors
Tool for the registration and processing of due diligences.
Tool for virtual courses

These tools interact with CERREJÓN's existing systems and/or applications, mainly with the databases containing information on knowledge of risk factors and the transactional system.

On the other hand, the Compliance Officer can access external information such as lists, press, requests from authorities, verifications, audits, and evaluations, which strengthen his analysis work.

13. Imposition of sanctions

In case of non-compliance and depending on its seriousness, CERREJÓN will apply disciplinary sanctions in accordance with the provisions of the Internal Labor Regulations.