TRIADA EMA S.A. SUC. COLOMBIA SAGRILAFT MANUAL

Manual for the Comprehensive Self-Monitoring and Risk Management System for Money Laundering, Terrorist Financing and Proliferation Financing of Weapons of Mass Destruction – SAGRILAFT implemented and approved for TRIADA EMA S.A. SUC. COLOMBIA

GENERAL INDEX – Sections

1. INTRODUCTION.

TRIADA EMA S.A. SUC. COLOMBIA (hereinafter referred to as "**TRIADA"** or the "**Company"** or the **"Enterprise")**, is a branch of the Peruvian company TRIADA ES MAS AGRO S.A.C., domiciled in Lima, Peru, with 100% Colombian capital, whose operations in Colombia are carried out from its headquarters in the Pacific Free Trade Zone in Palmira, Valle; It is a company in the agro-industry sector that shares the concern expressed by both national and foreign authorities and agencies regarding the scourge of money laundering ("**ML"**), terrorist financing ("**TF"**), and the financing of the proliferation of weapons of mass destruction ("**FPWMD"**), criminal activities that are present and on the rise in our country.

As part of the commitment of TRIADA, its shareholders, and its administrators to Colombian society and the regulatory obligation of the Company led by the Superintendency of Companies to implement a Comprehensive LA/FT/FPWMD Self-Control and Risk Management System (hereinafter "**SAGRILAFT**"), the Company has adopted this SAGRILAFT Manual (hereinafter the "**Manual"**). This Manual seeks to ensure that TRIADA adopts the appropriate procedures to identify, measure, and control or mitigate its ML/TF/FPWMD risks, preventing its lawful business activity from being used to commit these prohibited or illegal acts.

TRIADA understands that the best way to contribute to the fight against ML/TF/FPWMD and comply with its regulatory obligations is to define clear and objective rules, processes, and procedures. In this way, TRIADA seeks to build an efficient and effective SAGRILAFT to manage its ML/TF/FPWMD risks, which is embodied in this manual.

2. PURPOSE OF THE MANUAL

Through this instrument, TRIADA establishes an active consultation and procedure tool so that in the various processes of its production and commercial operations that may be affected by ML/TF/FPAM risks, it allows its Administrators and Compliance Officer to review the policies and procedures that must be followed to prevent or control ML/TF/FPAM risk within the framework of their activities. In this way, the Company will be able to protect both its ability to operate legally in the market and its most valuable intangible assets, its reputation, its goodwill, and its brands.

This Manual seeks to define the rules of conduct that TRIADA expects from its employees, contractors, suppliers, customers, shareholders, and related third parties as part of its overall commitment to legality.

This Manual will serve as a letter of introduction to its customers, suppliers, counterparties, and all interested parties who need to know how TRIADA addresses ML/TF/FPWMD issues and risks as part of its corporate culture.

3. SCOPE OF THE MANUAL.

TRIADA aims to create a true culture of prevention, compliance, and legality within the organization and in its area of influence, supported by efficient and effective controls for ML/TF/FPTAM risks to which it may be exposed in the course of its commercial and productive operations. TRIADA's SAGRILAFT consists of a series of procedures and policies that define the appropriate stages, elements, and instruments for managing your ML/TF/FPWAP risk.

4. LEGAL OR REGULATORY FRAMEWORK.

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

(b) **External Circulars 100-000016 of December 24, 2020, and 100-000004 of April 9, 2021,** which comprehensively amended Chapter X of the Basic Legal Circular of the Superintendency of Companies, and other administrative acts that may amend it from time to time (hereinafter, "Chapter X").

(c) **Law 599 of 2000 Colombian Penal Code.** Classifies crimes in Colombia, including those related to ML/TF/FPWAP, and underlying crimes. Art. 323 C.P. and in accordance with Art. 441, all natural persons have the obligation to report when they become aware of the commission of ML/TF/FPWAP crimes, among others.

(d) **Law 1121 of 2006. Which establishes rules for the prevention, detection, investigation, and punishment of terrorist financing and other provisions.** Establishes our duty to immediately and sufficiently report to the Financial Information and Analysis Unit **(UIAF)** and the Attorney General's Office when we become aware of the presence or transit of a person included in one of the international lists binding on Colombia in accordance with international law.

(e) **Law 1708 of 2014 Code of Extinction of Ownership.** Article 119 establishes the duty to report illicit assets that may be subject to extinction of ownership, and Article 120 establishes a 5% reward for the person reporting such assets.

(f) **Decree 1068 of 2015:** Contains the Single Regulatory Decree for the Treasury and Public Credit Sector, which establishes the obligation of entities other than those supervised by the financial and insurance sector to report suspicious transactions to the UIAF when required to do so by that unit or by law (section 2.14.2.).

(g) **Decree 1736 of 2020:** Empowers the Superintendency of Companies to instruct, in the manner it deems appropriate, entities subject to its supervision on the measures they must adopt to promote transparency and business ethics in their business practices in order to have internal mechanisms for the prevention of acts of corruption, as well as management mechanisms for the prevention of money laundering and terrorist financing, and the financing of the proliferation of weapons of mass destruction by their supervised entities.

(h) **EXTERNAL CIRCULAR # 100-000008 OF JUNE 11, 2021 SUPERSOCIEDADES** Contains the Supervision Policy for the Self-Control and Comprehensive Risk Management Regime LA/FT/FPWMD

5. SCOPE OF APPLICATION.

This Manual is intended for administrators, employees, shareholders, members of the Board of Directors, suppliers, contractors, customers, and other third parties who have a legal or contractual relationship with TRIADA. Therefore, TRIADA will make every effort to structure the appropriate contractual instruments to ensure compliance with this Manual by its recipients or counterparties.

6. DEFINITIONS.

Without prejudice to the terms defined throughout the Manual, the glossary applicable to this document is set out below. The definitions provided herein apply and are interpreted regardless of whether the term is used in the singular or plural.

(a) **Shareholder:** The natural or legal person who is the owner of shares in the company that owns TRIADA EMA S.A. SUC. COLOMBIA, duly registered in the Shareholders' Register.

(b) **Virtual Asset (VA):** is the digital representation of value that can be traded or transferred digitally and can be used for payments or investments. In practice, they create opportunities for ML/TF. Virtual assets do not include digital representations of currency, securities, and other financial assets that are already covered elsewhere in the Recommendations of the FATF (Financial Action Task Force).

(c) **Administrator(s):** The legal representative, principal or substitute, liquidator, member(s) of the Board of Directors or shareholders' meeting and who, in accordance with TRIADA's bylaws, exercise or hold these functions legally and statutorily.

(d) **Counterparty:** Refers to any natural or legal person with whom TRIADA has civil, commercial, business, contractual, or legal ties of any kind. Examples of these Counterparties are TRIADA's Shareholders, Administrators, Employees, Suppliers, Contractors, and Clients.

(e) **Customer:** The natural or legal person with whom TRIADA establishes and maintains a contractual or legal relationship, or business relationship for the sale or supply of any product or service from the portfolio of TRIADA EMA S.A. SUC. COLOMBIA.

(f) **Contractor:** A natural or legal person with whom TRIADA establishes and maintains a contractual or legal relationship for the acquisition of products or services.

(g) **ML/TF/FPWMD Risk Control:** The implementation of procedures or policies that seek to prevent, reduce, or neutralize ML/TF/FPWMD operational risk.

(h) **Due Diligence:** The set of processes carried out by TRIADA on its Counterparties that seek to prevent ML/TF/FPWMD Risks in their interaction with them. The 40 recommendations of the FINANCIAL ACTION TASK FORCE – FATF – will be taken into account for this process.

(i) **Event**: An ML/TF/FPWMD risk situation that occurs or may occur.

(j) **Operational Risk Factors**: These are the sources of ML/TF/FPWMD risk for the Company during its operations, from which Events are identified within the framework of TRIADA's policies.

(k) **Terrorist Financing - FT**: A crime committed by any person who engages in any of the conduct described in Article 345 of the Criminal Code.

(l) **Financing of the Proliferation of Weapons of Mass Destruction (FPWMD):** Any act that provides funds or uses financial services, in whole or in part, for the manufacture, acquisition, possession, development, export, transfer of material, fractionation, transport, transfer, deposit, or dual use for illegitimate purposes in violation of applicable national and international laws.

(m) **Money Laundering - ML**: Money laundering is the process by which criminal organizations seek to give the appearance of legality to the proceeds of their illicit activities. In practical terms, it is the process of making dirty money look clean, allowing criminal organizations or criminals to use these resources and, in some cases, to profit from them. This crime is committed by any person who seeks to give the appearance of legality to property or money derived from any of the activities described in Article 323 of the Penal Code.

(n) **Restrictive Lists:** These are national and international risk lists that collect information, reports, and background information from different agencies, individuals, and legal entities that may be related to suspicious activities, investigations, proceedings, or convictions for conduct and crimes related to ML/TF/FPWMD.[1] **Vgr.** CLINTON, OFAC, UN, EU, DEA, INTERPOL, and others.

(o) **Compliance Officer**: The individual appointed by TRIADA who will be responsible for monitoring compliance with this SAGRILAFT Manual and for promoting, developing, and ensuring compliance with specific procedures for the prevention, updating, and mitigation of ML/TF/FPWMD risk. He or she is appointed by the Board of Directors and must meet the profile or conditions established by the Superintendency of Companies in External Circular 100-00000016 of 2020, amending Chapter X of the 2017 Basic Legal Circular of the Superintendency of Companies.

(p) **Unusual transaction:** A transaction whose amount or characteristics are not related to the economic activity of the customers, or which, due to its amount, the quantities traded or its particular characteristics, falls outside the established parameters of normality.

(q) **Suspicious transaction**: A transaction that, due to its number, amount, or characteristics, does not fall within the normal systems and practices of a business, industry, or r a specific sector and, furthermore, cannot be reasonably justified according to the customs and practices of the activity in question. These transactions must be reported solely and exclusively to the UIAF.

(r) **Politically Exposed Person (PEP):** Public servants in the national, departmental, or municipal public administration with positions of direct responsibility or by delegation in the formulation of institutional policies and the adoption of plans, programs, and projects, or the management of State assets. Applies to all branches of the State: Legislative, Executive, and Judicial.

[1] TRIADA uses a third-party restrictive list verification service.

(s) **Suppliers** or **Contractors**: All individuals or legal entities that provide goods and/or services necessary for the Company's activities.

(t) **Internal Reports:** These are reports made within the Company by any employee who has knowledge of a possible Unusual or Suspicious Transaction. Internal Reports also include those that the Compliance Officer must submit at least once a year to TRIADA's Board of Directors.

(u) **ML/TF/FPWMD Risk:** This is the possibility of loss or damage that the Company may suffer by being used as an instrument for ML/TF/FPWMD. It is expressed in terms of probability (opportunity or frequency of occurrence of the risk) and impact (consequence if it occurs or materializes).

(v) **Risks Associated with ML/TF/FPWMD:** These refer to the consequences and effects for the Company arising from the materialization of ML/TF Risk. These may include:

- **Legal Risk:** The possibility of loss or damage affecting the Company, its Shareholders, its Directors, or any other related person, by being sanctioned, fined, or forced to pay damages as a result of non-compliance with rules or regulations related to the prevention of ML/TF/FPAM.

- **Reputational Risk:** The possibility of loss or damage affecting the Company due to disrepute, bad image, negative publicity, loss of goodwill with respect to the Company and its business practices, causing loss of investment opportunities or a decrease in income;

- **Operational Risk:** The possibility that the Company may be used in ML/TF/FPT activities due to deficiencies, failures or errors in human resources, processes, technology, infrastructure, or due to the occurrence of external events;

- **Contagion Risk:** The possibility of loss that the Company may suffer, directly or indirectly, due to an action or experience of a Shareholder, customer, employee, Supplier, Contractor, or related party, linked to ML/TF/FPWBP crimes. Related parties include individuals or legal entities that have the potential to influence the Company or its business operations.

- **Inherent Risk**: The level or profile of risk inherent in the Company's activity, without taking into account the effect of ML/TF/FPY controls.

- **Residual Risk**: The level or profile of risk remaining after applying ML/TF/FPTD risk controls.

(w) **Red Flags:** These are particular circumstances that fall outside normal parameters and attract attention and warrant further analysis in the event of an unusual or suspicious transaction, and must be reported.

(x) **System** or **SAGRILAFT**: refers to the ML/TF/FPWMD Self-Control and Risk Management System adopted by TRIADA EMA S.A. SUC. COLOMBIA and which must be applied in all its commercial operations and relations with its counterparties.

(y) **Terrorism**: Defined as any act intended to keep the civilian population in a state of fear through acts that endanger life, integrity, or freedom using instruments capable of causing havoc. The instruments used may originate from both legitimate and illegitimate sources. See Art. 343 of the Penal Code.

(z) **UIAF**: FINANCIAL INFORMATION AND ANALYSIS UNIT is the technical investigation office attached to the Ministry of Finance, the state financial intelligence body created to prevent, detect, and combat money laundering and terrorist financing.

7. FUNCTIONS AND RESPONSIBILITIES TOWARDS SAGRILAFT.

Without prejudice to the other functions assigned internally within TRIADA to the various persons and bodies described below**,** the following functions are established for the implementation and application of the System.

7.1 <u>FUNCTIONS OF THE BOARD OF DIRECTORS</u>.

In addition to the functions statutorily assigned to the Board of Directors, this body shall specifically perform the following functions with regard to SAGRILAFT:

(a) Define and approve the Company's LA/FT/FPWMD Policy.

(b) Discuss and approve the SAGRILAFT manual and other System documents submitted by the Legal Representative and the Compliance Officer, as well as any updates thereto.

(c) Appoint the Compliance Officer and verify that he or she has the availability, experience, and qualifications necessary to perform his or her duties.

(d) Provide the operational, economic, physical, technological, and resource measures necessary and required by the Compliance Officer to perform their duties.

(e) Receive, analyze, and respond in a timely manner to reports from the Compliance Officer and define, when necessary, a proposal for improvement to the System.

(f) Follow up on critical issues contained in reports submitted by the legal representative, the Compliance Officer, or the tax auditor on the Company's SAGRILAFT, making express mention thereof in the respective minutes.

(g) The above shall be recorded in the respective minutes.

7.2 <u>FUNCTIONS OF THE LEGAL REPRESENTATIVE</u>

In addition to the duties that statutorily correspond to the Legal Representative, in other documents such as Board of Directors' Instructions and applicable legal regulations, the Legal Representative shall specifically perform the following duties with respect to SAGRILAFT:

(a) Submit to the Board of Directors, together with the Compliance Officer, the SAGRILAFT manual and other documents of the System.

(b) Efficiently allocate the necessary and required operational, financial, physical, and technological resources so that the Compliance Officer can implement the System and carry out the monitoring and compliance tasks thereof.

(c) Verify that the Compliance Officer has the necessary availability and capacity to perform his or her duties.

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

(e) Follow up on critical points contained in reports submitted by the compliance officer or the statutory auditor on the Company's SAGRILAFT, with the obligation to report to the Board of Directors anything that it deems should be brought to the attention of that body.

(f) Ensure that SAGRILAFT activities are properly documented.

(g) Certify to the Superintendency of Companies, when required by that authority, compliance with the provisions regarding SAGRILAFT and the approved policies.

7.3 QUALIFICATIONS AND DUTIES OF THE COMPLIANCE OFFICER.

The Board of Directors of the company shall appoint a natural person to serve as Compliance Officer, principal and alternate, who shall have at least the following qualifications:

(a) Hold a professional degree.

(b) Demonstrate knowledge and at least six (6) months of experience in positions related to ML/TF/FPWAP risk management.

(c) Be domiciled in Colombia.

The Compliance Officer shall have the following duties:

(a) Supervise and direct the design of the System, taking into account the specific characteristics of the Company, its activity, and the identification of its Risk Factors.

(b) Submit the SAGRILAFT manual to the Board of Directors, together with the Legal Representative, for consideration and approval, and ensure that such approval is recorded in the respective minutes of the meeting.

(c) Implement the Manual with the support of the legal representative and ensure that employees apply it effectively.

(d) When required, assess ML/TF/FPTADM risk with employees for current and new operations.

(e) Ensure the effective, efficient, and timely operation of SAGRILAFT.

(f) Promote the adoption of corrective measures and updates to SAGRILAFT when circumstances require it, and at least once every two (2) years. To this end, it shall submit to the Board of Directors the proposals and justifications for the suggested corrective measures and updates to SAGRILAFT.

(g) Inform the Legal Representative of any possible failures or omissions in the ML/TF/FPWMD risk controls of which it is aware.

(h) Submit at least once a year to the Board of Directors a report on compliance with SAGRILAFT that, at a minimum, contains an evaluation and analysis of the efficiency and effectiveness of the System and, if required, the respective proposals for improvement, as well as a demonstration of the results of its management and that of the Company's administration with respect to the System.

(i) Develop an internal dissemination and training program when necessary so that Company employees are properly informed, updated, and trained to identify and report Unusual and Suspicious Transactions.

(j) Receive internal reports of Unusual or Suspicious Transactions from the heads of the different areas of the Company so that, if appropriate, Suspicious Transactions can be reported to the FIU.

(k) Register themselves and the Company in the SIREL administered by the UIAF and request a username and password to access this platform in order to comply with the submission of mandatory reports.

(l) Submit the Report of Suspicious Transactions (hereinafter "**STR**") or Absence of Suspicious Transactions ("**A-STR**") to the UIAF and any other report or information required by the regulations applicable to the company in relation to the prevention and control of ML/TF/FPT in Colombia. In order to fulfill this function, the Compliance Officer must inform the company's Legal Representative of the content of the SAR prior to the Report, provided that the Legal Representative does not have a conflict of interest regarding this decision under the terms of section 10.2 below.

(m) Report to the UIAF and the Attorney General's Office, through the electronic channels determined by these authorities, any matches of persons identified in the Binding Lists. In order to fulfill this function, the Compliance Officer must inform the company's Legal Representative, prior to the report, of any matches of persons identified in the Binding Lists, provided that the Legal Representative does not have a conflict of interest regarding this decision under the terms of section 10.2 below.

(n) Report to the competent authority, when in the course of its system supervision activities, it becomes aware of the commission of crimes related to ML/TF/FPWMD activities.

(o) Respond to and coordinate any request, application, or proceeding from judicial or administrative authorities regarding the prevention and control of ML/TF/FPWAP activities.

(p) Certify to the Superintendency of Companies, when required by that authority, that the company complies with the provisions of Chapter X.

(q) Evaluate the reports of the statutory auditor regarding the company's SAGRILAFT and take the necessary measures to adopt solutions required for the proper functioning of the system.

(r) Ensure the proper filing of documentary evidence (ROS and Internal Reports), as well as any information relating to the management and prevention of ML/TF/FPWMD risk in the company.

(s) Receive and respond to inquiries from counterparties regarding all matters related to the company's system.

(t) Verify compliance with the company's Due Diligence and Enhanced Due Diligence procedures.

(u) Design methodologies for classifying, identifying, measuring, and controlling ML/TF/FPWMD risk that will form part of the SAGRILAFT.

(v) Assess the ML/TF/FPAM risk to which the company is exposed.

INCOMPATIBILITIES: No person who is disqualified or incompatible from serving as Compliance Officer may hold that position. For this reason, the following shall be grounds for the Compliance Officer not to take office or, having done so, to cease to hold the position:

(i) Belonging to the administration or corporate bodies, internal or external audit or control bodies (statutory auditor or linked to the statutory audit firm that performs this function, if applicable) or anyone who performs similar functions or acts on behalf of the Company.

(ii) Belonging to the company's process exposed to ML/TF/FPWAP risks that may generate a potential conflict of interest in the performance of their duties as Compliance Officer.

(iii) Serving as Compliance Officer in more than ten (10) entities or in another entity that competes with the Company, unless all of them belong to the same business group.

The Compliance Officer shall immediately notify the Legal Representative and the Board of Directors if any of the grounds for incompatibility or disqualification for holding the position arise.

7.4 DUTIES OF THE FISCAL AUDITOR.

As part of the specific duties established for the tax auditor by Article 207 of the Colombian Commercial Code, with respect to ensuring that the operations carried out or performed on behalf of the Company comply with the law, the bylaws, and the decisions of the shareholders' meeting, as well as that the shareholders' meeting is duly informed of any irregularities in the operation of the Company and in the conduct of its business. In this regard, TRIADA's statutory auditor shall:

(a) Report any Suspicious Transactions that come to their attention in the ordinary course of business to the UIAF, and report any suspected crimes against the economic and social order to the competent authorities. They must also bring these facts to the attention of the Company's governing bodies and management.

(b) Verify compliance with current regulations applicable to the Company in matters of self-control and ML/TF/FPWMD risk management, this SAGRILAFT Manual, and the controls established by the Company to protect itself from these risks.

(c) Submit reports, at least annually, on the results of the reviews carried out on the System, as well as recommendations to correct deficiencies, to the Board of Directors or the Shareholders' Meeting, with a copy to the legal representative and the Compliance Officer.

8. RISK FACTORS.

TRIADA has identified the following Risk Factors in its operations, businesses, or contracts.

Risk Factor	Description
With Counterparties	Its employees, customers, suppliers, contractors, and other third parties who may act on behalf of or interact with TRIADA in the course of its business activities.
By Jurisdiction	The geographical location in Colombia or abroad where the company's business operations are carried out and where a higher or lower level of ML/TF risk can be determined.
By Product Type	These are the goods and services that TRIADA sells or purchases in the course of its business.
By Distribution or of Marketing Channels	These are the means through which TRIADA must offer and market its goods and services.

9. STAGES OF SAGRILAFT.

The Company follows these stages for the proper development and implementation of its SAGRILAFT:

9.1 <u>IDENTIFICATION OF ML/TF/ FPWMD RISK – METHODOLOGY</u>.

TRIADA is aware of the economic, reputational, and legal impact that the materialization of ML/TF/FPWMD Risk may have, as well as the risk of contagion that it may face by becoming involved with Counterparties that may be related to or affected by crimes associated with ML/TF/FPWMD.

To identify its Inherent Risk, TRIADA will consider any Risk Factor, internal or external, associated with its activity or entry into new markets. The Company takes into account the context of its business activity, the jurisdictions and regions in which it operates, and the counterparties with which it interacts.

To identify Risk Factors, the Compliance Officer will apply the following model, which suggests a series of steps that help to understand and address the risks present according to the context to be analyzed.

To develop this methodology, an assessment method based on the experience of the Company's various processes is used. Thus, through a compilation of ideas and concepts and an assessment based on the experience of selected personnel, a list of ML/TF/FPWMD Risk Events that may affect TRIADA will be constructed. Managers, leaders, or those responsible for each area will participate: Sales, Marketing, Operations, Finance, Human Resources, Accounting, Portfolio, Systems, with the coordination of the Compliance Officer.

This identification will be an ongoing process, taking into account the LA/FT/FPWMD Risk Factors identified by TRIADA and which can be verified in section 8 above.

As part of this identification stage, not only will the experience-based judgment mentioned above be used, but also the ML/TF/FPT typologies available in documentary sources from the Financial Action Task Force, Latin America Chapter ("**GAFILAT**"), which can be obtained by consulting the WEB.

In the characterization of each Event, the process in which it may occur, its cause, the Risk Source in which it can be categorized, and the Associated Risk will be identified.

This same procedure will be followed when the Company enters new markets to identify the ML/TF/FPWAP Risks of that new market.

9.2 <u>MEASUREMENT OR ASSESSMENT OF ML/TF/ FPWMD RISK</u>.

Initially, TRIADA will take into account the measurement of its ML/TF/FPWMD risks without considering the controls established by it, in order to obtain its inherent risk profile. The Inherent Risk rating is obtained by weighting the probability and impact variables, calculated based on a quantitative and qualitative estimate from the Company's historical data and the analysis of the employees responsible for the ML/TF/FPWMD risk processes. (Page 5)

For the above, in addition to those already existing in the company, the following assessment tables will be used, so that the measurement of risks is as complete as possible:

(a) Probability assessment.

The probability of occurrence refers to the possibility of an identified ML/TF/FPWMD risk event occurring. This can be measured using frequency criteria or by taking into account the presence of internal and external factors that may contribute to the risk, even if it has not materialized.

Score	**Rating**	**Description**
5	Very High	The situation occurs frequently and continuously. The materialization of the risk happens often or on a permanent basis.
4	High	The situation occurs frequently but not continuously. The materialization of the risk may occur several times within a given period.
3	Moderate	The situation occurs at a medium frequency. The risk may materialize occasionally.
2	Low	The situation occurs sporadically. The risk materialization is expected at a minimal level.
1	Very Low	The situation has never occurred or is unlikely to occur. However, the risk is conceivable.

(b) Impact assessment.

The impact is the consequence that the materialization of the risk may have for TRIADA.

Score	Rating	Description
5	Extreme	The materialization of the risk causes significant economic losses and may result in the complete suspension of the Company's operations.
4	Severe	The materialization of the risk causes considerable economic losses and may lead to the temporary suspension of several Company operations.
3	Moderate	The materialization of the risk causes economic losses and may lead to the temporary suspension of certain Company activities.
2	Minor	The materialization of the risk has an impact and may result in indirect economic losses, but it does not cause a suspension of Company activities.
1	Insignificant	The materialization of the risk does not significantly impact the Company's operations.

These probability and impact criteria will be reviewed periodically to further adjust the Risk Matrix in accordance with the nature of TRIADA, a company belonging to the AGROINDUSTRY sector, and the characteristics of its processes and procedures, so that they are aligned with the identified ML/TF/FPTAM risks. As a result of this stage, the company is able to establish its Inherent Risk Profile by multiplying the probability score by the impact score, as follows:

(c) Inherent Risk Assessment:

LOW	
MEDIUM	
HIGH	
EXTREME	

9.3 **ML/TF/FPWMD RISK CONTROL**.

The Company has defined the ML/TF/FPWMD Risk Control mechanisms described in this Section 9 to prevent, control, or mitigate its Inherent Risk. These controls will be applied in accordance with the results of the previous stages, with the purpose of establishing its Residual Risk profile.

The objective is to mitigate risk by taking the necessary measures to reduce the probability of occurrence and/or the impact to which TRIADA is exposed.

The Company has planned the following types of controls, depending on:

(a) The nature of the control:

(i) **Manual:** performed by the employee responsible for the affected process.

(ii) **Mixed:** performed by the employee responsible for the affected process, but involving an automated system for alerting or executing the respective control.

(iii) **Automatic:** performed by an automated alert system and execution of the respective control.

(b) Evidence of execution:

(i) **Evidenced:** documentary evidence of its application is provided.

(ii) **Not evidenced:** its application is not documented.

(c) Application of the control:

(i) **Random:** applied randomly in response to events.

(ii) **Partial:** applied on some occasions when an Event occurs.

(iii) **Total:** applied whenever an Event occurs.

(d) Control documentation:

(i) **Undocumented:** the procedure is not documented.

(ii) **Semi-documented:** the procedure is partially documented or out of date.

(iii) **Documented:** the procedure is documented and up to date.

(e) Type of control:

(i) **Preventive**: applicable before the risk materializes.

(ii) **Detective**: alerts to the presence of failures in a preventive control and allows immediate action to be taken. Used to verify the effectiveness of preventive controls.

(iii) **Corrective**: applicable when the risk has already materialized, therefore allowing actions to be taken to minimize the impact. This control is applied when the previous controls do not work. They usually work hand in hand with detective controls.

The consolidated rating of the above controls provides assessments of the soundness of the control, determining its strength and the need for modification. To this end, the following table of scores assigned to each control based on its characteristics will be taken into account, the sum of which will give the percentage of effectiveness:

Type of control	Score
The control is properly documented	15
The control is semi-documented	10
The person responsible for applying it is fully identified	5
The control is automatic	15
Control is mixed	10
Control is manual	5
Control is preventive	15
Control is corrective	10
Control is detective	5
Control always applies	20
Control applies to some defined cases	10
Control is applied randomly	5
Application is documented (evidenced)	5
The control has proven to be effective in controlling the risk	30

Effectiveness of the control:

(f) **Highly effective:** prevents or mitigates more than 80% of the risk.

(g) **Effective:** prevents or mitigates more than 65% of the risk.

(h) **Moderately effective:** prevents or mitigates more than 50% of the risk.

(i) **Not very effective:** prevents or mitigates more than 25% of the risk.

(j) **Not effective:** prevents or mitigates less than 25% of the risk.

Its effectiveness against a given Event will determine the reduction in the probability and/or impact of the risk and, thus, the Company's Residual Risk Profile (Page 7).

Based on this Residual Risk profile, the Company may define action plans for those risks that exceed its maximum tolerance level, i.e., Residual Risks that exceed an average level. To this end, TRIADA will take into account the following lines of action.

LEVEL	ACTION PLAN
LOW	Risks at this level are a minor threat to the Company and do not require additional measures or controls beyond those already in place. They must be monitored at least twice a year (every two years). This level of residual risk can be accepted, mitigated, or transferred.
MEDIUM	Risks at this level affect the Company and must be addressed by the employee or affected area in the medium term, applying satisfactory measures to mitigate them. They must be monitored at least annually. This level of residual risk must be mitigated or resolved.
HIGH	Risks at this level represent a significant threat to the Company and must be addressed in the short term to ensure a reduction in their level or their causes must be avoided. Likewise, they must be monitored continuously, at least once every six months. This level of residual risk must be mitigated or avoided. This will involve activating alerts, reports, and taking appropriate measures.
EXTREME	Risks at this level represent a high threat to the Company and must be addressed immediately to ensure a reduction in their level or their causes must be avoided. Likewise, they must be monitored continuously, at least quarterly. This level of residual risk must be avoided. This will involve activating alerts, reports, and taking appropriate measures.

NOTE: Periodic adjustments to the Risk Matrix of TRIADA EMA S.A. SUC. COLOMBIA do not constitute a modification of the SAGRILAFT Manual, as they are part of the dynamics of Self-Control and its application.

9.4 ML/TF/FPWMD RISK MONITORING

The Compliance Officer will continuously monitor the System (SAGRILAFT) in order to evaluate the timeliness, effectiveness, and efficiency of the controls, ensuring that they are comprehensive and refer to all identified ML/TF/FPWMD Risk Events. This monitoring must be carried out at least once a year.

Company employees must continuously monitor their activities to ensure that no ML/TF/FPWMD risk situations arise and that the controls applied operate in a timely, effective, and efficient manner. Any deviation must be reported to the Compliance Officer.

Monitoring shall be carried out by the Compliance Officer with the assistance of the process leaders, and its purpose is to apply and suggest the necessary corrective measures and adjustments to ensure effective management of ML/TF/FPWMD risk. After monitoring, the Compliance Officer will evaluate the results and, together with the process leaders, will make proposals for improvement and treatment of the situations detected to the Legal Representative and the Board of Directors.

The statutory auditor also conducts periodic reviews to facilitate the detection and correction of deficiencies in SAGRILAFT, the results of which are communicated to the Board of Directors, the Legal Representative, and the Compliance Officer. The Compliance Officer will then evaluate these and take appropriate action to address the reported deficiencies.

10. SAGRILAFT POLICIES.

10.1 **General ML/TF/ FPWMD Policy**.

The Board of Directors and the Administrators of TRIADA declare and state that the Company:

(a) Puts compliance with ML/TF/ FPWMD prevention rules ahead of achieving commercial goals. The prevention, detection, and monitoring of ML/TF/ FPWMD risk will apply to all TRIADA activities, in pursuit of its corporate purpose, and will maintain self-control and management under the premise of *"the greater the risk, the greater the control*."

(b) Has a duty and commitment to ensure compliance with the law and regulations aimed at preventing and detecting ML/TF/ FPWMD, with a view to protecting TRIADA's image and reputation.

(c) It will refrain from carrying out any operation and will report it to the competent authorities if it can reasonably determine that the funds involved are the proceeds of or intended to finance or support illegal activities.

(d) It declares that its employees and other Counterparties are aware of, apply, and comply with the provisions of the Manual, under penalty of the respective sanctions set forth in section 16 below and the applicable criminal and administrative consequences.

(e) When carrying out capital investment purchase or sale transactions, it will identify the buyer or seller and their economic activity.

(f) It will cooperate with the competent authorities in relation to the prevention and control of ML/TF/ FPWMD, responding promptly to their requests, providing them with all the information it deems relevant, and complying with legal provisions.

(g) TRIADA fully complies with the Self-Regulation and Comprehensive ML/TF/ FPWMD Risk Management Supervision Policy established by the Superintendency of Companies in Circular 100-000008 of June 11, 2021, which is considered to be incorporated into this Manual.

10.2 **Conflict of interest policy**.

No business or transactions that put the Company at risk of ML/TF/FPWMD may be carried out, nor will the omission of ML/TF/FPWMD risk control procedures and measures be authorized.

The following situations are considered conflicts of interest related to ML/TF/FPAM:

(a) **When consulting Restricted or Control Lists, analyzing Unusual Transactions, studying Suspicious Transactions, and filing STRs:** When the consultation, study, analysis, or report has been carried out by an employee on their spouse or permanent partner, relatives within the fourth degree of consanguinity, second degree of affinity, or first degree of civil relationship, or with respect to those transactions or reports in which the person responsible for carrying out the consultation, study, analysis, or report has a personal, direct, or indirect interest in the outcome.

(b) **When reporting to the authorities:** When the decision on whether to file an external report affects the person in charge, directly or indirectly, or when the report or the decision to file it concerns transactions carried out by the spouse or permanent partner, relatives within the fourth degree of consanguinity, second degree of affinity or first degree of civil relationship of the person who must make the decision or file the report.

In any of the above cases, the person in conflict must report it directly to the Compliance Officer. If the person in conflict is the Compliance Officer and it is he or she who becomes aware of the conflict, he or she must immediately withdraw from the situation and delegate all his or her duties in relation to the matter with which he or she has a conflict to the Deputy Compliance Officer. If a third party becomes aware of the Compliance Officer's conflict, they must notify the Board of Directors so that this body may designate another person to carry out these ad hoc tasks.

10.3 **Cash Handling and Payments Policy**

All payments to Counterparties or by Counterparties shall be made through the means provided by the financial system and in favor of the holder of the obligation. They shall be duly legalized and invoiced through the systems regulated by the DIAN, e.g., electronic invoicing or equivalent.

10.4 **Virtual Assets Transaction Policy**

The Company will **not** receive contributions or payments, nor will it make investments or provide services related to Virtual Assets.

10.5 **New Market Entry Policy**.

Prior to entering new markets, the Company will identify the ML/TF/FPWMD Risk Factors and Events specific to that new market and define the relevant ML/TF/FPWMD Risk controls. To do so, it will follow the procedure described in Section 9.

10.6 **Risk Factor Management Policy**.

In cases where the residual risk is high or extreme, TRIADA will restrict the operation or transaction related to or that may be affected by that risk until it is reduced through the application of additional controls. The Company's priority is the management of ML/TF/FPWMD risk over the achievement of commercial or financial goals.

10.7 **Counterparty Due Diligence Policy**.

One of TRIADA's main mechanisms for controlling and preventing ML/TF/FPTD risks is to have adequate knowledge of its Counterparties, from the moment they become involved with TRIADA and throughout their relationship with the Company. The Company does not do business or have commercial relationships with Counterparties whose business nature makes it difficult to verify the transparency of their activities or the origin of their resources, or who refuse to provide the required information and documentation.

Likewise, it will verify that the information provided by Counterparties is updated at least once a year, in order to be aware of any possible changes in their activity and financial information. To this end, it will implement the most appropriate means, such as digital means, to facilitate current knowledge of the respective counterparty.

As some Counterparties may expose the Company to greater ML/TF/FPT risks than others, employees and the Compliance Officer shall take into account the following aspects that represent greater exposure to ML/TF/FPT risks. In the following cases, the Company applies Enhanced Due Diligence procedures:

(a) **With regard to jurisdiction**: Counterparties located in non-cooperative countries and high-risk jurisdictions. For this purpose, TRIADA will take into account the list of non-cooperative countries and high-risk jurisdictions of the Financial Action Task Force (FATF) and the Basel Index (reference instruments available on the website). Regarding the latter, jurisdictions with an overall rating above 6.5 will be considered high risk.

(b) **With regard to PEPs**: due to the higher ML/TF/FPT risk posed by relationships with PEPs, enhanced due diligence procedures and constant monitoring processes will be applied to relationships involving PEPs.

(c) **Linked to Control Lists:** TRIADA will not have contractual links with any natural or legal person linked or related to ML/TF/FPWMD activities, as verified in the restrictive lists Vrg. CLINTON, OFAC

10.8 **Suspicious Transaction Reporting Policy**.

The Company will report to the UIAF any transactions that, due to their amount, characteristics, and other elements, could qualify as Suspicious Transactions. The Company will not require certainty that the activity is criminal, nor will it identify the type of crime or that the resources involved come from such activities. Nor will it be an accusation or imputation against the affected party; the event will be reported and made available to the control body.

10.9 **Document Retention and Handling Policy**.

The Company shall retain documents and records relating to the System in accordance with the provisions of Article 28 of Law 962 of 2005 - Rationalization of Procedures - or any regulation that modifies or replaces it. They shall be kept on paper or any technical medium that guarantees their exact reproduction for a period of ten (10) years from the date of the last entry, document, or receipt. At the end of this period, the documents may be destroyed, provided that the following conditions are met:

(a) There is no request for their delivery by a competent authority.

(b) They are kept in a technical medium that guarantees their subsequent accurate reproduction and the preservation of their probative value, in accordance with the law.

The information and supporting documents sent to the UIAF shall be kept by the Compliance Officer and under no circumstances shall the Counterparties have access to or knowledge of them. Likewise, the information requested by said entity shall be kept confidential.

TRIADA shall keep a special file in which it shall store all SAGRILAFT documents, guaranteeing the integrity, timeliness, reliability, and availability of the information contained therein.

10.10 **Disclosure and training policy**.

TRIADA will promote a culture of ML/TF/FPT risk prevention within the company through training and other available means.

The Company will disclose its policies and procedures for the prevention and control of ML/TF/FPWMD through a training program led by the Compliance Officer. This program will be aimed at all employees. The program will include training at the beginning of the employee's relationship with the company and, thereafter, at least once a year. After the training, a knowledge assessment will be conducted. All of the above may be done in person or virtually, depending on the circumstances.

10.11 **Confidentiality Policy Regarding Authority Information Requests**.

Company employees shall maintain confidentiality regarding judicial requests and inspections carried out by the authorities, as well as reports made to the UIAF.

10.12 **Policy on Non-Compliance with SAGRILAFT**

Any breach of the provisions of this Manual will be verified in accordance with the provisions of the company's internal or contractual rules governing relations with Counterparties.

Any serious breach of the policies and/or procedures set forth in this Manual, whether intentional or caused by carelessness or negligence on the part of any TRIADA employee or contractor, will be punished in accordance with the commitments entered into contractually, labor law, the Internal Work Regulations, and the disciplinary action procedure, without prejudice to the civil, administrative, and criminal consequences that such conduct may entail.

11. DUE DILIGENCE PROCEDURES.

One of the main mechanisms for controlling and preventing ML/TF/FPWAP operations will be adequate knowledge of Counterparties, from the moment the Company becomes genuinely interested in establishing a relationship with them and throughout the relationship.

11.1 **Due Diligence for Suppliers and Contractors**.

The process of getting to know Suppliers and Contractors begins with the initial contact, for their initial engagement, in the context of interaction for the acquisition of goods or services or in the process of updating information.

The Purchasing or Supplier Analyst shall request that Suppliers and Contractors complete the supplier knowledge form provided by TRIADA, including the following documents:

Individual (Natural Person)	**Legal Entity (Juridical Person)**
Legible copy of the national ID card or foreign ID. If not available, a copy of the passport’s main page will be required.	Certificate of existence and legal representation issued no more than 30 days prior, by the Chamber of Commerce of their domicile, or an equivalent document in the case of a foreign legal entity.

Individual (Natural Person)	**Legal Entity (Juridical Person)**
	Shareholding composition.
Tax Identification Number (NIT)	Legible copy of the ID card or foreign ID of the Legal Representative, or an equivalent document in their country.
Additional identification documents that allow clear and precise individualization of the person.	Tax Identification Number (NIT).
Certificates of service to other companies. Proof of experience.	Certificates of service to other companies. Proof of experience.
Public Accountant’s certification of income source.	Financial statements as of December 31 of the previous year.

Once the form has been completed and the required supporting documents have been attached, they will be reviewed by the Purchasing Analyst - Suppliers, and the following procedure will be followed:

(a) Confirmation of information. (b) Consultation of the Control Lists.

(c) Final validation by the Legal Department

This procedure must be documented in order to proceed with the authorization and acceptance of the Supplier or Contractor. The Supplier or Contractor's information will be recorded in TRIADA's database along with the other documents supporting this due diligence process.

The Supplier or Contractor's information must be updated at least once a year, as long as the Supplier or Contractor is active in the Company.

If the Supplier or Contractor, or its Ultimate Beneficiaries, are included in one of the Risk Lists that may pose a risk of contagion for TRIADA, the engagement process will be suspended. If the finding is on a Control List that does not represent a direct risk of Contagion, the Enhanced Due Diligence process described in section 12 below will be followed.

11.2 **Customer Due Diligence (CDD)**.

Before establishing a relationship with Clients, TRIADA must carry out a due diligence process on them. Similarly, this process must be repeated when there is suspicion of an ML/TF/FPWAP act or that the relevant information provided by the Client is not accurate or when the Client's circumstances change substantially (for example, when there is a change of control) or when their representation is modified.

The purpose of this Due Diligence procedure is to fully identify Clients and their Beneficial Owners, obtain information about each of their economic activities, and have objective elements of judgment that allow TRIADA to make informed and responsible decisions about when not to establish relationships with Clients who may represent a ML/TF/CFT Risk to the Company.

TRIADA employees and/or their representatives are not permitted to initiate a relationship with a new Customer without first completing the due diligence process defined below in its entirety.

Depending on whether the potential client is a natural person or a legal entity, the department in charge (Marketing) must ask the potential client to complete the customer information form and attach the following documents:

Natural Person	**Legal Entity**
Legible copy of national ID or foreign ID. Alternatively, a copy of the main page of the passport.	Certificate of existence and legal representation issued no more than 30 days prior by the Chamber of Commerce of the entity's domicile or by a competent authority, or equivalent document for foreign legal entities.
Tax Identification Number (NIT) Public Accountant certification regarding source of income.	Legible copy of the national or foreign ID of the Legal Representative. Alternatively, a copy of the main page of the passport.
Additional identification documents that clearly and precisely individualize the person. --------------------------------------- Data Processing Authorization --------------------------------------- Bank Reference --------------------------------------- Authorization for inquiry with Credit Bureaus and Watchlists	Tax Identification Number (NIT) -- Shareholding Composition -- Data Processing Authorization -- Bank Reference -- Authorization for inquiry with Credit Bureaus and Watchlists

Once the department in charge has the information, it will consult the names of the individuals or legal entities referenced in the form in the Control Lists, recording the result, date, and time of this verification, and verifying the accuracy of the applicant's responses.

If the information cannot be verified or additional information is required, the request must be forwarded to the applicant.

The complete documentation of this process must be included in the respective Client's file for future reference.

If the Client or its Beneficial Owners, or its partner(s) are included in one of the Control Lists that may pose a risk of contagion for TRIADA, the onboarding process will be suspended. If the finding is on a

Control List that does not represent a direct risk of Contagion, the Enhanced Due Diligence process described in section 12 below will be followed.

11.3 **Employee Due Diligence**.

Individuals who aspire to hold a position at TRIADA must be fully identified and must comply with the due diligence procedure outlined below.

For employee knowledge, during the selection and hiring process with TRIADA, the Human Resources Department will review the resume of each candidate with the corresponding supporting documentation.

To this end, candidates will be asked to complete the employee knowledge form and attach their identity document.

The Human Resources Department will verify the suitability of their training in accordance with the job profile, employment references, personal and family references, and any other information provided by the candidate. Similarly, in order to prevent ML/TF/FPWMD risks, the candidate's information must be checked against Control Lists. If the candidate or a current employee is included in one of the Control Lists that may pose a risk of contagion for COSMOAGRO, the hiring process will be suspended or the grounds for justified termination of their relationship with TRIADA will be considered.

For employees who are already affiliated with TRIADA, their data will be updated and verified against the minimum control lists at least once a year.

When warning signs are detected that suggest unusual behavior by one or more employees, this will be reported to the Compliance Officer for investigation. If the risk materializes, the area in charge will analyze and take the appropriate decisions in accordance with the consequences set out in Section 16 below.

11.4 **Shareholder Due Diligence**.

TRIADA shall keep its Shareholder information up to date in accordance with the Shareholder Register.

With regard to its current shareholders, they will be asked to update their information annually and verify it in the Control Lists.

For new shareholders, TRIADA will request the same information and documents in the Customer process defined in Section 11.1 above, depending on whether the shareholder is a legal entity or an individual.

The Compliance Officer will confirm the information and request that it be updated at least once a year. If a risk situation is found, it will be brought to the attention of the Board of Directors so that it can take the appropriate solution and, if necessary, submit it to the Shareholders' Meeting.

The documentation provided by the Shareholders must be filed in an appropriate manner so that it is easily accessible and available to the competent authorities upon request. The same process shall apply to the members of the Board of Directors.

12. ENHANCED DUE DILIGENCE (EDD).

The enhanced due diligence process involves a more in-depth understanding of the Counterparty. This procedure must be applied when a Counterparty identifies itself as part of the groups defined in the due diligence policy set out in section 10.7 above.

Therefore, in cases where a Counterparty must be verified through this enhanced process, its relationship must take into account the following procedure:

(a) The due diligence documents must be submitted to the Board of Directors (JD).

(b) The Board will review the due diligence and decide whether to continue the relationship with the Counterparty.

(c) The person responsible for the process shall execute the BD's decision and, if the relationship is to continue, shall request from the Counterparty a certification, signed by its legal representative and Statutory Auditor or directly by the Counterparty and Certified Public Accountant (if it is a natural person), stating that:

  (i) that all its resources come from lawful activities;

  (ii) that the resources resulting from the relationship with TRIADA will be used for equally lawful purposes;

  (iii) that it has the ML/TF/FPWAP prevention procedures required by law or regulation, or if not required, that it has suitable processes in place to prevent its own ML/TF/FPWAP risks.

(d) The person responsible for the process must update the review of the Counterparty every 6 months, instead of the annual periodic review of the other counterparties.

Enhanced Due Diligence for PEPs shall be extended to (i) the spouses or permanent partners of the PEP; (ii) the relatives of PEPs, up to the second degree of consanguinity, second degree of affinity, and first degree of civil relationship; (iii) associates of a PEP, when the PEP is a partner of, or associated with, a legal entity and, in addition, directly or indirectly owns more than 5% of the legal entity, or exercises control over the legal entity, in accordance with Article 261 of the Commercial Code.

13. DETECTION AND ANALYSIS OF UNUSUAL TRANSACTIONS AND DETERMINATION OF SUSPICIOUS TRANSACTIONS

13.1 <u>Detection and analysis of unusual transactions</u>

The procedure for detecting and analyzing transactions is understood to be the series of activities carried out in order to identify unusual behavior by counterparties for analysis, documentation, and, if determined to be suspicious transactions, reporting such behavior to the UIAF.

The identification of warning signs and unusual transactions is carried out by Company employees or the Compliance Officer during the performance of their duties and, in particular, during the application of controls in the procedures for getting to know counterparties and at all times during the contractual relationship.

Red flags and unusual or suspicious transactions are identified using the following tools:

(a) **Restrictive and Binding Checklists.** These are used to identify possible links with persons or assets related to ML/TF/FPTAD crimes, in accordance with the procedure described in section 11 of this manual.

(b) **Monitoring against the Counterparty profile.** This serves to identify atypical behavior with respect to the characteristics of each Counterparty. It is carried out by comparing the behavior of the Counterparty(ies) to infer the existence of atypical situations, i.e., Unusual Transactions.

13.2 **Red Flags**.

Warning signs are situations that show atypical behavior by counterparties and help identify or detect conduct, activities, methods, or situations that may conceal ML/TF/FPWMD operations.

The fact that a transaction is classified as unusual does not mean that it is linked to illegal activities. For this reason, it is necessary to examine each transaction, business deal, and contract in order to verify its unusual nature.

The following warning signs, among others, may be established and should be brought to the attention of TRIADA employees, who must report them to the Compliance Officer for evaluation.

(a) With regard to commercial transactions or activities with Counterparties related to:

(i) Natural or legal persons who are not fully identified;

(ii) Shareholders or employees with a criminal record of ML/TF/FPTADM; and

(iii) Shareholders or partners who have been accepted or linked without prior verification of the origin of the resources they contribute.

(iv) Counterparty activity that is not consistent with its purpose or contract.

(v) Provision of incorrect, inaccurate, or unverifiable information, or completion of forms without complying with all requirements.

(vi) Matches of the Counterparty, or related to it, in the media on matters related to ML/TF/FPAM.

(vii) Matches involving the Counterparty or related to it in reports from competent national or foreign authorities regarding ML/TF/FPWAP.

(viii) Failure to comply with contract clauses, especially those relating to the prevention and mitigation of ML/TF/FPWAP risks.

(ix) An unjustified increase in assets is detected.

(x) Frequent splitting of financial transactions is detected.

(xi) Requests for payment or money transfers to third parties that are not listed as Clients or Suppliers.

(b) With regard to transactions, businesses, or contracts that represent, have as their object, or involve:

(i) High volume of cash without apparent justification;

(ii) Movable or immovable property at prices significantly different from normal market prices;

(iii) Donations that do not have an apparent final beneficiary, whose origin is unknown or who is domiciled in a high-risk country or jurisdiction;

(iv) Significant transactions, business deals, or contracts that are not in writing;

(v) Transactions with subcontractors that have not been previously identified.

(vi) Commercial transactions or business with persons included in the Control Lists.

(vii) Transactions with counterparties domiciled or located in geographical areas designated by FATF as non-cooperative.

(viii) Transactions involving products derived from illegal activities (including, but not limited to, smuggling);

(ix) Transactions with Products that have not been duly nationalized; and

(x) Transactions involving restricted products that do not have the appropriate authorizations or licenses.

(c) With respect to transactions involving cash originating from or related to:

(i) Countries with a high level of corruption and political instability;

(ii) Unexplained cash deposits in personal or related company bank accounts;

(iii) Amount, value, or currency inconsistent with the circumstances of the bearer;

(iv) Concealed transport of cash;

(v) Transportation with high costs compared to other transportation alternatives;

(vi) Unusual cash invoicing or sales in the sector;

(vii) Large increase in invoicing or cash sales from unidentifiable customers.

13.3 **<u>Internal reporting of red flags and unusual transactions.</u>**

Whenever a Company employee, in the course of their duties, detects a warning sign or an unusual transaction, they must report this to the Compliance Officer so that they can begin the analysis and investigation.

The Compliance Officer shall be notified by email with all supporting documents to the following email address: MAIN: <u>rdaguirreabogado@hotmail.com</u>
DEPUTY: <u>andres.osorio@triada-ema.com</u>

13.4 **<u>Analysis of red flags and unusual transactions.</u>**

The Compliance Officer is responsible for receiving reports from employees and conducting the analysis in conjunction with those responsible for the processes that affect the counterparties analyzed.

Once the analysis of the transaction has been completed and depending on the conclusion, the Compliance Officer will take one of the following actions:

The situation or transaction is NOT unusual.	The reason is documented in writing in the file and the case is closed.
The situation or transaction IS unusual, but was duly justified.	The reason is documented in writing in the file and the case is closed.
The situation or transaction IS unusual and NO reasonable justification could be found.	It is referred for analysis as a potential suspicious transaction.
No conclusion can be drawn about the unusual situation or transaction because there is insufficient information.	The file is kept open. Any additional information required to further investigate the red flag and the counterparty's knowledge is requested. Follow-up is conducted until the appropriate conclusion is reached.

13.5 **Determination of suspicious transactions.**

The Compliance Officer is responsible for analyzing Suspicious Transactions for the purposes of:

- Verify that in-depth activities were carried out on the warning sign and on the knowledge of the Counterparty.
- Request additional information when warranted by the analysis.
- Determine whether the situation is unusual in nature, giving rise to suspicion that cannot be clarified or justified and is likely to be reported to the FIU as a Suspicious Transaction.

The Compliance Officer will determine the Suspicious Transaction and file the corresponding report with the FIU. Suspicious Transactions are determined once the Unusual Transaction has been compared with the Counterparty's information and its normal parameters.

13.6 **Suspicious Transaction Report.**

In accordance with the decision made in the previous step, the Compliance Officer must immediately, that is, from the moment the Company makes the decision to classify the transaction as Suspicious, file a report through the UIAF website, following the guidelines established in the "SIREL *User Manual*" published on the UIAF website.

As the Suspicious Transaction Report (STR) does not constitute a criminal complaint, it does not need to be signed by any official, but is made at the institutional level. The STR shall not give rise to any liability for the Company or for the Administrators or collaborators who participated in its determination and reporting.

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

13.7 **<u>Documentation and filing of cases analyzed</u>.**

Following the completion of the report, the Compliance Officer must keep the supporting documentation (file) that led to the classification of the transaction in one category or another in a file that must be catalogued and archived in accordance with security and confidentiality standards.

These files must be centralized and organized together with the respective report to the UIAF, adopting appropriate security and confidentiality measures for this purpose, so that they can be delivered in a complete and timely manner to the authorities when requested.

Such information shall be managed by the Compliance Officer, who shall regulate the positions authorized to consult this information, and shall be retained for the term established in this Manual.

13.8 **<u>Other external reports</u>.**

(a) **Report of Absence of Suspicious Transactions ("A-ROS") to the UIAF:** In the event that a quarter passes without any STR reports being made, 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 respective quarter, through the UIAF's Online Reporting System (SIREL).

(b) **Report to the UIAF and the Attorney General's Office:** Whenever the Company identifies any property, asset, product, or right owned by or under the administration or control of any country, person, and/or entity designated by the United Nations Security Council Resolutions and those prepared by the various Sanctions Committees of that body, the Compliance Officer shall immediately and in , report it to the UIAF and bring it to the attention of the Attorney General's Office through the secure electronic channels determined by these public authorities and in compliance with the respective legal confidentiality requirements.

14. DISCLOSURE AND TRAINING.

The Compliance Officer, in collaboration and coordination with the person responsible for Human and Organizational Management at TRIADA EMA S.A., shall be responsible for designing and scheduling training and awareness plans related to the content of this SAGRILAFT Manual. This program will be aimed at all employees of the company, following the general training plan for the System.

The Human Resources department of TRIADA shall provide the SAGRILAFT Manual to new employees upon hiring for their review and implementation. In addition, they must carry out the induction process and training on the content of the Manual, the system, and, in general, ML/TF/FPWAP risks, as provided for in the plan. This induction must be carried out within thirty (30) days after each employee's entry.

A record of the above shall be kept in the employee's resume. The Compliance Officer shall be informed of the hiring of new employees so that, if deemed appropriate, the Compliance Officer may provide special support during the induction process due to the sensitivity of the area to which the new employee will be assigned.

Employee attendance at training events is mandatory, and all employees must be allowed the necessary time to participate, depending on the General Plan and coordination with TRIADA's Compliance Officer.

In general terms, the GENERAL PLAN complies with the following conditions:

(a) Ensure that SAGRILAFT becomes part of the culture and corporate values of TRIADA EMA S.A. SUC. COLOMBIA.

(b) Take place at least once a year and keep a record of its implementation, as well as the names of attendees, the date, and the topics covered.

(c) Be disseminated in the form of awareness-raising during the induction process for new employees.

(d) Be given in the form of intensive training to those employees whose duties include carrying out controls on the System, thus ensuring their proper compliance.

(e) As a self-monitoring system, it must be constantly reviewed and updated.

(f) Implement mechanisms for evaluating the results obtained, in order to determine the effectiveness of these programs and the extent to which the proposed objectives have been achieved.

15. RESPONSE TO AUTHORITY REQUESTS.

Any request for information from competent authorities in the area of ML/TF/FPT prevention and control will be handled by the Compliance Officer with the support of the area responsible for the process. The Compliance Officer shall gather the necessary information and draft a response to the request within the established time frame, and shall submit it to the company's General Manager and the Manager or Head of the area responsible for the process for approval. He shall ensure that it is filed in a timely manner and kept in the system's documentation.

16. IMPOSITION OF SANCTIONS.

In the event of non-compliance and depending on its severity, the company will apply the appropriate disciplinary sanctions in accordance with the internal documents established by the Company and the Internal Work Regulations.

In the event of detecting any irregularity or breach of the policies and procedures defined in this Manual, all employees must report the offense immediately, even if it is committed by their immediate superior, to the Compliance Officer at the email address**rdaguirreabogado@hotmail.com** . TRIADA will guarantee that there will be no reprisals against those who report offenses in good faith.

Upon receipt of a report, the Compliance Officer will conduct a preliminary investigation and submit the results and findings to the Legal Representative, who will apply the disciplinary procedure established in the disciplinary action procedure.

If the report is against the Legal Representative, the Compliance Officer shall submit the results of their investigation to the Board of Directors. If the complaint is against the Compliance Officer, the procedure mentioned in section 10.2 above shall be followed.

17. CHANGES, UPDATES, AND PUBLICITY DISCLOSURE

This SAGRILAFT manual and any changes, modifications, or updates made to it, whether by its own decision or by order of a competent authority, shall be approved by the Board of Directors and shall be reported and published in a timely manner at TRIADA's offices and plant located in the PACIFICO FREE ZONE of Palmira, Valle, on the website, the intranet, or by any other means deemed appropriate by management.

The administration of TRIADA shall ensure the current and future dissemination of this SAGRILAFT MANUAL to all its current and new employees, and counterparts in the execution and development of its operation and corporate purpose.

18. CERTIFICATE OF APPROVAL AND IMPLEMENTATION:

This SAGRILAFT MANUAL OF TRIADA EMA S.A. Colombia Branch was discussed, implemented, and approved by the company's Board of Directors at its regular meeting on the twentieth (20th) day of August, two thousand twenty-one (2021), as recorded in MINUTES # 154, and is effective as of that date. It was decided to publish it on the company's website and distribute it to all levels of the organization.

THE CHAIRMAN OF THE BOARD OF DIRECTORS:
(signed) DIEGO FERNANDO PARRA

THE PRINCIPAL LEGAL REPRESENTATIVE
(signed) LUIS ENRIQUE LAVERDE GOMEZ

COMPLIANCE OFFICER:
(signed) RUBÉN DARIO AGUIRRE RAMIREZ

ESTRCT. RDAR. O.C. TRIADA- 08-2021- UNI VERSION