

CIRSA Group Anti-Money Laundering and Terrorism Financing Policy
June/2025



Contents

1. Introduction and Purpose 3

2. Scope of application 3

3. Definitions..... 3

4. Internal regulatory framework 4

5. Corporate Governance Organisation and Structure 5

6. Main operational aspects 6

7. Corporate Training..... 7

8. Approval, effectiveness and dissemination 8

9. Annexes 9

ANNEXE I. Internal structure for money laundering prevention by country 9

1. Introduction and Purpose

The CIRSA Group, aware of the importance that large multinational companies play in anti-money laundering and terrorism financing (hereinafter **AML/TF**), states its highest commitment to compliance with the laws, regulations and recommendations of international institutions in this matter, applying resources and efforts in the fight against all forms of money laundering, terrorism financing and proliferation of weapons of mass destruction.

The corporate policy of the CIRSA Group in this matter aims to establish the internal regulatory framework, the main operational aspects and the governance structure to ensure the effectiveness of its anti-money laundering model, consisting of the following elements:

- An organisational structure with the necessary resources to perform the function of prevention and a clear allocation of the responsibilities attributable to each control body or unit.
- A regulatory framework that sets out the required obligations and preventive measures, with particular emphasis on those related to customer due diligence.
- The implementation of customer due diligence and transaction monitoring measures aimed at identifying potential suspicious activities and reporting them to the relevant authorities.
- The execution of communication and training plans for administrators, directors and employees, with the aim of maintaining an adequate level of information and sensitivity, providing the necessary capabilities to comply with the applicable standards.
- Constant communication between the Central Office and all the subsidiaries of the CIRSA Group in all the countries in which it operates, thus ensuring effective control and supervision.
- Lastly, relying on an independent review to verify and assess the implementation and effectiveness of the other the elements of the model in an independent manner.

2. Scope of application

This document establishes the minimum standards that the Group companies must comply with and applies to all companies and establishments within the CIRSA Group that are subject to anti-money laundering and counter-terrorism financing regulations. It also applies to its administrators, officers and employees, regardless of the geographic location in which they carry out their professional activity, without prejudice to compliance and the applicable laws and regulations of each country.

Therefore, the application of the measures contained in this Policy must ensure due compliance with the applicable regulations in all jurisdictions where the CIRSA Group operates and maintains a presence in the gaming sector.

3. Definitions

• **Money Laundering** is considered to be:

- The conversion, transfer of assets or monetary transactions in gaming operations at establishments of the CIRSA Group, with full knowledge that such assets, capital or money originate from criminal activity, to conceal or disguise their illegal origins, or to assist those involved in evading the legal consequences of their actions.
- The concealment or disguise of the nature, origin, location, disposition, movement or actual ownership of assets or rights over assets, knowing that such assets originate from criminal activity or participation in criminal activity.

- The acquisition, possession or use of goods, knowing, at the time of receipt thereof, that they originate from criminal activity or participation in criminal activity.
 - Participation in any of the activities mentioned in the previous sections, association to undertake these types of actions, attempts to perpetrate them and helping, instigating or advising someone to perform them or facilitate their execution.
- **Terrorism Financing** is considered the deposit, collection, use and delivery of goods, capital or money, by any means, directly or indirectly, with the intention of using them, or with the knowledge that they will be used, in whole or in part, for the commission of any of the crimes of terrorism classified in the different criminal codes of Spain and other countries in which the CIRSA Group operates.

4. Internal regulatory framework

4.1. Global Corporate Policy

This Corporate Policy sets out the guidelines and basic principles of the global prevention model of the CIRSA Group in this matter, which must be supplemented, wherever not regulated therein, by the Laws, Regulations or other rules applicable in Spain and other countries.

Additionally, each of the Divisions or companies of the CIRSA Group that are bound by the provisions of Law 10/2010 on Anti-Money Laundering and Terrorism Financing in Spain and by the applicable laws in each country where they operate have an Anti-Money Laundering Manual of their own, establishing policies, internal controls and procedures intended for compliance with the Corporate Policy and the applicable legislation, inspired by the principles of this Policy.

4.2. Risk Self-Assessment Report

Risk assessment is the element on which the procedures and controls of the AML/TF system are based, identifying the inherent risks of the activity carried out by the Group and establishing the necessary controls to mitigate its residual risk.

This report is reviewed periodically under the parameters of a common methodology, aligned with SEPBLAC recommendations, the different national authorities where the CIRSA Group operates, and with recommendation 1 of the FATF (*Financial Action Task Force*), and which takes as main references the “Supranational Risk Assessment”, published by the European Commission, and the National Risk Analysis/Assessment, published by the Government of each country in which the Group operates.

4.3. Manuals and Regulations for Obligated Entities

The Manuals of the Group entities shall be duly validated by the Corporate Control Body and by their respective Governing Bodies, ensuring that the company:

- Has adequate control measures and internal control and communication bodies, approving in writing effective policies and procedures on due diligence, information, document retention, internal control, risk assessment and management, compliance assurance and communication in order to prevent and hinder the performance of operations related to money laundering and terrorism financing.
- Identifies and knows its customers, has implemented explicit customer acceptance policies based on risk and applies due diligence in the acceptance, identification and knowledge of customers.
- Has staff responsible for compliance with anti-money laundering provisions.
- Complies with the requirements established in the laws for obtaining and maintaining customer identification documents, and the recording and communication of operations.

- Develops and implements appropriate control methods, based on the customer's characteristics and the operations they carry out, to detect the activities of suspicious customers, immediately examining the operations detected and taking any appropriate measures.
- Establishes an internal procedure allowing its employees or managers to anonymously report violations of the law committed within the obliged entity.
- Bases its internal control procedures on a prior risk analysis, which is included in the Risk Self-Assessment Report and reviewed periodically.
- Performs and documents a specific risk analysis prior to the launch of a new product, the provision of a new service or a new distribution channel, or the use of a new technology, and must apply appropriate measures to manage the risk.
- Conducts a risk analysis based on the specific characteristics of the client. These will be classified into risk levels with the objective of designing and implementing measures and controls to mitigate the risk.
- Expressly communicates to internal bodies created for such purpose any fact or operation that presents any of the following characteristics: (i) having evidence or certainty of being related to money laundering and terrorism financing, or (ii) showing an ostensible mismatch with the customer's nature, activity volume or operational history, provided that the previous analysis of the operation does not show economic, business or professional justification for the performance of these operations.
- Refrains from executing suspicious transactions. When abstention is not possible or may hinder the investigation, the operation may be executed, followed by immediate communication detailing the reasons for the execution, in addition to the suspicious sections of the transaction report.
- Collaborates with Financial Intelligence Units or other authorities by providing the information they require in the exercise of their powers; said information may concern any data or knowledge obtained by the obligated subjects with respect to the operations they carry out and the persons involved.
- Conducts training programmes on anti-money laundering and terrorism financing.
- Implements audit systems regarding its anti-money laundering policies and procedures.
- Establishes the duty of confidentiality, so that both the corresponding entity as well as its directors and employees who hold information about the transactions or activities classified as suspicious are totally prohibited from disclosing to the client and third parties the actions they are carrying out, with the exception of the established internal anti-money laundering bodies. Any exception to this confidentiality will be processed, in any of the cases contemplated in the Law, by the appropriate internal body.

5. Corporate Governance Organisation and Structure

5.1. First line

Within the scope of AML/TF, the business units make up the Corporation's first line of defence; they manage the business directly and are able to discern what is normal from what may contain unusual elements. They must know and apply the policies and procedures on the matter, as well as the communication tools whenever they detect and report on a suspicious transaction.

5.2. Second line

The second line is responsible for overseeing compliance with anti-money laundering and counter-terrorism financing regulations. Therefore the second line, in contact with supervisory bodies and/or financial intelligence units, will have to undertake verification that the regulations are being met, as well as examination of anomaly reports and notification of suspicious transactions. The CIRSA Group has organised this line taking into account the local requirements of the countries in which the Group is present, as well as the best international practices in this area.

Annexe I of this Policy includes a description of the main figures and organisational structures in each country where the CIRSA Group is present.

5.3. Third line

The third line is made up of the Group's Internal Audit and Control Department, periodically evaluating compliance with the procedures, as well as the adequacy and effectiveness of the policies and their respective controls, providing an independent assessment and favouring the process of continuous improvement of the AML/TF system.

6. Main operational aspects

6.1. Customer Due Diligence and Risk Segmentation

The customer due diligence procedure establishes a compliance framework at Group level that may vary depending on the risk level of the different gaming activities carried out in each country and the type of customers, in order to implement measures and controls to mitigate said risk level.

This procedure must comply with international standards and the "Know Your Customer" (KYC) principle, with a special focus on ensuring that appropriate knowledge of the customer and their activities is available at all times.

6.2. Operations Detection, Control, and Examination

CIRSA Group companies must have methods in place for detecting, controlling and examining operations. These methods will be applied depending on the risk and will in all cases contain the basic assumptions for the detection of operations:

- a. Internal reporting of suspicious activity by Group employees.
- b. The detection of possible suspicious transactions through established alert systems (at the level of each Group company and/or centralised).
- c. The detection of suspicious transactions will entail carrying out a detailed and comprehensive analysis aimed at determining the actual existence of indications of money laundering or terrorism financing.
- d. Group companies shall report on their own initiative to the supervisory and/or Financial Intelligence authorities any act or transaction — even a mere attempt — that, upon completion of the special review, is determined to involve indications or certainty of a connection with money laundering or terrorism financing. In particular, the supervisory bodies will be informed of operations that show an ostensible mismatch with the nature, activity volume or operational history of the customers.
- e. Group employees shall refrain from executing any transaction where there is an indication or certainty that it is related to money laundering or terrorism financing.

- f. Employees, officers or agents of the Group shall not disclose to the client or third parties that information has been communicated to internal control bodies or the supervisory body, or that any transaction is being or may be examined in case it could be related to money laundering or terrorism financing.

6.3. Communication tool

CIRSA has established an internal communication tool at Group level, allowing its employees, regardless of the country of operation in which they are located, to communicate, even anonymously, any AML/TF non-compliance in accordance with the provisions of the operating policies of this communication channel.

The communication tool is accessible through the CIRSA website and any of its subsidiaries, and the provisions of the personal data protection regulations apply in order to guarantee, to the alerter, protection against any type of retaliation and/or unfair treatment.

6.4. Sanctions List Control

Group companies and their establishments must verify whether their customers are included in the sanctioned lists that are periodically published by the sanctioning bodies of the United Nations, the European Union or OFAC and the local lists of each country that are applicable in the jurisdictions in which the Group companies carry out their activity.

Likewise, they will implement procedures to verify the access of persons with public responsibility to their establishments, for the application of reinforced diligence measures, in accordance with the regulations applicable in each country.

6.5. Document archival and retention

The documentation, information and records generated in compliance with AML/TF measures must be kept for the legally established period in each country, counted from the completion of the corresponding transaction, or from the cancellation of the customer account. In this regard, the following supporting documentation must be kept, among others, for use in any investigation or analysis on the matter of AML/TF:

- A copy of the documents required in application of the due diligence measures.
- Original or copy with evidentiary value of the documents or records that properly certify the transactions, the parties involved, and the business relationships.

6.6. Data protection

The processing of personal data, as well as documentation derived from compliance with AML/TF obligations, will be carried out in compliance with the corresponding data protection legislation of the relevant jurisdiction.

7. Corporate Training

Training and awareness of the risks associated with these crimes is a key element in the fight against money laundering and terrorism.

CIRSA Group companies carry out training programmes for their employees to ensure an adequate level of awareness of all personnel, as required by law, and establish policies that ensure mandatory training in the prevention of money laundering and terrorism financing (including Senior Management and Administrative Bodies) periodically and appropriate to the level of risk exposure of their activities.

The PBC training programmes of all CIRSA Group companies must be validated by the UTPBC (Technical Unit for the Prevention of Money Laundering, for its acronym in Spanish), keeping a record and evidence of the training provided, its contents, and the employees who have received and exceeded it.

8. Approval, effectiveness and dissemination

The Anti-Money Laundering and Terrorism Financing Policy has been approved by the Board of Directors of CIRSA Enterprises, S.A. at its meeting of June 18 2025, and will be communicated to the Management Bodies of the companies integrated in the CIRSA Group in all the countries where they carry out their activity, for their consideration and compliance.

This Policy is effective as of the date it is approved. Its content will be subject to regular review where appropriate in order to adapt it to regulatory changes or incorporate best practices in the matter. The aforementioned Board of Directors will be the competent body to amend it, after supervision, if applicable, by the Audit and Compliance Committee.

The Policy will be available on the Group intranet. It will also be made available to third parties through its publication on the CIRSA website

The Spanish version of this document will prevail in the event of any discrepancy or dispute.

9. Annexes

ANNEXE I. Internal structure for money laundering prevention by country

Spain:

Representative at SEPBLAC:

The CIRSA Group is represented at the Financial Intelligence Unit (SEPBLAC in Spain) by the representative appointed by the Board of Directors of the CIRSA Group in Spain, with the duties assigned by Spanish anti-money laundering regulations.

Internal Control Body:

The Internal Control Body (OCI, for its acronym in Spanish) exercises its functions and is comprised by directors of the various business divisions of the CIRSA Group and corporate management.

Its role is to monitor and verify the effectiveness of the Corporate Policy on money laundering and terrorism financing, without prejudice to the effective implementation of an internal control system with a first level linked to the business divisions themselves, by strengthening regulatory knowledge in the most sensitive areas.

The OCI will meet periodically, with the Representative acting as secretary before the SEPBLAC, who will convenes the meeting; and as chair, one of the members of the body correlatively each year.

The OCI may appoint AML/TF officers from each division or companies that manage operations that are considered to have the greatest risk of money laundering.

The functions of the OCI are those provided for in the regulations applicable in Spain.

Technical Unit:

In addition, the Group has a Corporate Operational Technical Unit (UTPBC), integrated in the Corporate Directorate of Business Compliance and Ethics, which coordinates all policies and actions in this matter, as well as activities related to AML/TF at the CIRSA Group at global level.

The UTPBC may appoint analysts in those companies and establishments that, due to a higher risk or business volume, require greater oversight.

Mexico:

Compliance Officer:

The person responsible for the implementation, strict monitoring and adequate control of the requirements regarding the money laundering prevention efforts in Mexico.

The Compliance Officer will have a hierarchical level according to the responsibilities he/she undertakes, and will have access to all corporate areas and will be empowered to require the collaboration of any officer/employee thereof.

The Compliance Officer is the person appointed as representative before the Secretariat in order to comply with the obligations derived from the Federal Law for the Prevention and Identification of Transactions Involving Illicit Proceeds.

Compliance Body:

The body responsible for the application of AML/TF policies and procedures, approving the Anti-Money Laundering Manual prior to its presentation to the Board of Directors in Mexico. This body, in addition

to AML/TF responsibilities, is also entrusted with overseeing the implementation of the Group's broader crime prevention policies and procedures in the country.

It is composed of:

- Country Director
- Legal Director
- Director of People and Talent
- Compliance Officer

Compliance Analyst:

Performs continuous monitoring of clients, as well as monthly analyses of all charges and prizes at each room or casino, that meet or exceed the notification thresholds defined in the Federal Law for the Prevention and Identification of Transactions Involving Illicit Proceeds.

In addition to the above, prepares the working papers and files in the format established by the authorities for the proper submission of identified transactions to the Financial Intelligence Unit (FIU).

Panama:

Compliance Officer:

The Compliance Officer or Liaison is responsible for institutionalising the culture of prevention and leading the establishment of the prevention programme.

Based on the above, two people have been incorporated into the administrative structure in Panama, having all the necessary authority and independence, and being responsible for ensuring compliance with prevention measures, periodic review of the parameters contained in the Anti-Money Laundering Manual, training all company employees, maintaining ongoing and direct communication with the Compliance Committee and the competent authorities on prevention at national level.

Compliance Committee:

This is the entity responsible for approving the Manual for the prevention of money laundering, terrorism financing, and the financing of the proliferation of weapons of mass destruction (ML/TF/FPWMD), as well as for establishing the policies to be applied in Panama. It consists of:

- Country Director / General Manager
- Chief Operating Officer
- Commercial Director
- Corporate Safety Director
- Chief Financial Officer

The Compliance Officer or liaison serves as secretary of the Committee, participates in meetings, presents reports and recommendations and proposes the changes, adaptations and measures he/she deems necessary to adopt as part of the prevention policies. These proposals are evaluated by the Committee and are only applicable once approved by the Committee itself, either in quarterly meetings or in extraordinary sessions that are convened for this purpose.

The Compliance Committee meets every three months, in order to evaluate the issues presented to it by the Compliance Officer and those proposed by any of its members; approve the changes that are required and dictate the company's policies on the prevention of ML/TF/FPADM.

All Compliance Committee meetings are documented by preparing a minutes that will be drafted by the Compliance Officer or Liaison, and signed by the attendees.

All modifications, procedures and policies related to ML/TF/FPADM that are established in the company must be approved by the Compliance Committee, which has the maximum responsibility and authority in this matter within the company.

Compliance Analyst:

The Compliance Analyst is the person in charge of evaluating and analysing all tickets that are paid at the cashier of each gaming room or casino meeting and/or exceeding the due diligence application threshold, in order to ensure that they have been obtained as a result of a gaming activity.

Dominican Republic:

Compliance Officer:

The person responsible for ensuring the observance and implementation of the procedures and obligations established in the aforementioned Resolution and for making reports and submitting the required information to the UAF (Financial Analysis Unit) or its regulatory entity, with its functions being included in Law 155-17.

Compliance Committee:

It is the body responsible for the application of the AML/TF policies and procedures, approving both the Anti-Money Laundering Manual and the Policy on the subject, prior to its presentation to the Board of Directors. This body, in addition to AML/TF responsibilities, is also entrusted with overseeing the implementation of the Group's broader crime prevention policies and procedures in the country.

This body meets at least once every three months and is chaired by the Country Director, its composition being as follows:

- Compliance Officer
- Chief Financial Officer
- Chief Operating Officer
- Corporate Safety Director
- Cashier Manager

Compliance Assistant:

The person in charge of monitoring customers on an ongoing basis and ensuring compliance with due diligence measures and knowledge of the customer, as well as of supporting the Compliance Officer as required.

Italy:

Liaison:

The representative and main point of contact with the Italian Financial Information Unit, to which suspicious transaction reports are transmitted, which are detected based on specific criteria, defined by the Italian subsidiary of CIRSA, in accordance with the rules and regulations on anti-money laundering.

AML Officer:

The person responsible for verifying that the company's policies and procedures are consistent with the objective of preventing and counteracting anti-money laundering and terrorism financing rules and that they are being applied by employees and managers. (Keep procedures up to date).

Colombia:Compliance Officer:

A senior officer of the company, responsible for verifying the application of the regulations inherent in the management of risk and prevention and money laundering control, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, executing the compliance programme aimed at preventing the obligated operator from being used to commit these crimes, and ensuring the observance and implementation of the policies, procedures, controls, and best practices required for SIPLAFT.

The Compliance Officer must be registered in Coljuegos, which must review and accept such appointment.

SIPLAFT Control Committee:

Responsible for applying policies and procedures, approving/validating the AML Manual and the policy prior to its submission to the Board of Directors, and assessing changes in customer behaviour, based on sound judgement, deciding whether to report them as "unusual or suspicious" to the state surveillance and control authorities using the "REPORTING SUSPECTED OPERATIONS" form found on the UIAF (Financial Information and Analysis Unit) page. This body includes representatives from all business areas and documents its meetings in formal minutes.

It is chaired by the Country Manager, and consists of the following individuals:

- Compliance Officer / Legal Manager
- Commercial Director
- Slot Machines Product Manager
- Table Games Product Manager
- Financial Manager
- Corporate Safety Manager

Compliance Analyst:

Verifies customer due diligence (level of play, economic activity, number of transactions, and characteristics not aligned with normal business practices) and assesses whether the situation or investigation is related to ML/TF in order to determine whether it constitutes a suspicious transaction and should be escalated to the SIPLAFT Committee.

Peru:Compliance Officer:

The person responsible for overseeing the proper implementation and operation of the AML/TF prevention system, as well as proposing strategies to prevent and manage risks on this matter.

They serve as the point of contact between the obligated entity, the FIU-Peru, and the General Directorate of Casino Games and Slot Machines (DGJCMT) of MINCETUR, as the supervisory authority.

The agent on whom the supervisory authority relies to carry out control and oversight of the aforementioned system, with their duties set forth in Article 25 of Resolution SBS-1695-2016.

The appointment of the Compliance Officer must be made by the General Shareholders' Meeting and must be communicated to the UIF-Peru and the DGJCMT, with the identity of the Compliance Officer remaining confidential.

Compliance Body:

The body responsible for the application of AML/TF policies and procedures, approving the AML Manual prior to its presentation to the Board of Directors. This body, in addition to AML/TF responsibilities, is also entrusted with overseeing the implementation of the Group's broader crime prevention policies and procedures in the country.

This body meets at least once every three months and is chaired by the Country Director, its composition being as follows:

- Compliance Officer.
- Chief Financial Officer.
- Director of People and Talent.
- Internal Auditor.

Compliance Analyst:

Responsible for verifying proper compliance with customer knowledge of due diligence and for preparing investigative files on random customers, including: level of play, economic activity, number of operations, Politically Exposed Person (PEP) status, and characteristics that do not align with normal business practices. He/she is also responsible for evaluating any transactions that may be related to AML/TF in order to determine whether it is a suspicious transaction that must be reported to the UIF-Peru in accordance with the established procedures.

Costa Rica:

Compliance Officer:

The person within the company who is responsible for ensuring observance and implementation of the necessary controls and mechanisms within the framework of the AML/TF system, in order to identify the aspects that generate exposure to risk and establish methods and actions for mitigation and prevention.

The Compliance Officer must be appointed by the Board of Directors and reported to both the Superintendency and the UIF, with the functions assigned to the role under Article 27 of SUGEF Agreement 13-19 (AML/TF Regulation).

CIRSA
Ctra. de Castellar, 298
08226 Terrassa. Barcelona. Spain
T. 34 93 728 33 18
info@cirsa.com
www.cirsa.com

