2024

AML/CFT Manual CIRSA Spain

ANTI-MONEY LAUNDERING AND COUNTER FINANCING TERRORISM PROCEDURES MANUAL

ANTI-MONEY LAUNDERING TECHNICAL UNIT

TABLE OF CONTENTS

1. REGULATORY SCOPE, SCOPE, UPDATING AND DISSEMINATION 3

2. INTERNAL STRUCTURE AND CONTROL BODIES 7

3. IDENTIFICATION, ADMISSION AND KNOWLEDGE OF CUSTOMERS 14

4. PRESERVATION OF DOCUMENTATION 20

5. DETECTION OF TRANSACTIONS THAT COULD BE RELATED TO MONEY LAUNDERING 21

6. TRANSACTIONS ANALYSIS 25

7. REPORTING TO THE EXECUTIVE SERVICE OF TRANSACTIONS THAT COULD BE RELATED TO MONEY LAUNDERING 29

8. COMPULSORY MONTHLY DECLARATION OF TRANSACTIONS 30

9. REQUIREMENTS OF THE EXECUTIVE SERVICE AND OTHER AUTHORITIES 31

10. STAFF TRAINING 32

11. INTERNAL VERIFICATION 34

12. CONTROL OF SUBSIDIARIES 36

1. REGULATORY SCOPE, SCOPE, UPDATING AND DISSEMINATION

1.1 Normative scope

CIRSA Group is made up of different companies in the gaming sector, which are considered obliged parties in the prevention of money laundering and the financing of terrorism, with the scope set out in Law 10/2010 on the prevention of money laundering and the financing of terrorism and its implementing regulations.

Among the main obligations of obliged entities in this area are to adopt and implement prevention policies and procedures, to establish adequate internal control bodies responsible for their implementation and to approve a money laundering prevention manual.

Therefore, in order to effectively prevent any money laundering and terrorist financing activity (hereinafter, **AML**), CIRSA ENTERPRISES, S.L.U., the main company of CIRSA Group, has approved this Manual of Procedures for the Prevention of Money Laundering and Terrorist Financing (hereinafter, the **Manual**) by agreement of its Board of Directors, which is mandatory for the Group's companies considered obliged entities, which are under its control, as well as for its employees, managers, directors and team members.

The Manual develops the principles established in CIRSA Group's Corporate AML Policy, with the aim of ensuring the effectiveness of its money laundering prevention model in all the countries in which it carries out its gaming activity, comprising the following elements:

- An organisational structure with the necessary resources to manage and plan the prevention function and a clear allocation of responsibilities attributable to each control body or unit.
- A body of regulations that determines the obligations and preventive measures required; of particular importance are those relating to knowledge of customers.
- The implementation of knowledge and monitoring measures for gaming transactions, with the aim of identifying suspicious activities and ensuring that they are reported to the competent authorities.
- The implementation of communication and training plans for employees, with the aim of maintaining an adequate level of information and sensitivity, providing the necessary skills to comply with applicable standards.
- Permanent communication between the head office and all CIRSA Group's subsidiaries in all the countries in which it is present, thus ensuring effective control and supervision.
- Lastly, the need for an independent periodic review, in order to verify and check the implementation and effectiveness of the other elements of the model in an independent manner.

The recommendations of the supervisory authority in Spain - Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (hereinafter **SEPBLAC**) -, applicable regulations (Law 10/2010, of 28 April, on the prevention of money laundering, Royal Decree 304/2014, of 5 May, approving the Regulations of Law 10/2010 and other national and international implementing regulations), the suggestions contained in the Expert's Report for each financial year, as well as the extensive experience in this area acquired by CIRSA Group in recent years.

1.2 Scope of application

At CIRSA Group we distinguish five lines of business, according to the gaming activities offered in its establishments or through the Internet, grouped into the following business divisions (hereinafter **Divisions**) into which the companies considered obliged entities are integrated.

1.2.1 Casino Division

CIRSA Group's casinos are mainly traditional table games and slot machine establishments and are considered obliged entities in accordance with the provisions of article 2, p) of Law 10/2010, on the prevention of money laundering and the financing of terrorism.

Due to their activity as casinos, they are subject to the general regime, while, due to their currency exchange activity, they are subject to the specific regime; in this respect, Order EHA/2619/2006, of 28 July, which regulates currency exchange activity carried out by obliged entities whose transactions are not debited or credited to the account of the customer who carries them out, is applicable to them.

1.2.2 Bingo Division

The main activity of the companies grouped in CIRSA Group's Bingo Division is the operation, management, and exploitation of Bingo halls.

Law 10/2010 on the prevention of money laundering and terrorist financing, in the version approved by Royal Decree-Law 11/2018, of 31 August, establishes in its article 2, paragraph 2, letter u, that Bingo halls are considered obliged entities of the aforementioned Law, solely with respect to prize payment transactions.

Therefore, the undertakings grouped in this Division are considered obliged entities in relation to prize payment transactions.

1.2.3 Salones Division

The main activity of the companies grouped in the Rooms Division is the operation, management, and exploitation of "B" type amusement machines.

Law 10/2010 on the prevention of money laundering and the financing of terrorism, in the version approved by Royal Decree-Law 11/2018 of 31 August, establishes in its article 2, paragraph 2, letter u, that operators of type "B" machines are considered obliged entities of the aforementioned Law, only with regard to prize payment transactions.

Therefore, the undertakings grouped in this Division are considered obliged entities in relation to prize payment transactions.

1.2.4 Online Sports Betting Division - by electronic, computerised or telematic means

Law 13/2011 of 27 May regulates gaming by electronic, computerised, telematic and interactive means. Those in which any mechanism, facility, equipment, or system is used to produce, store, or transmit documents, data, and information, including any open or restricted communication networks such as television, Internet, fixed and mobile telephony or any others, or interactive communication, whether in real time or deferred.

In relation to the consideration as an obliged entity that forms this Division, the company Sportium Apuestas Digital, in Law 10/2010 on the prevention of money laundering and the financing of terrorism, in the version approved by Royal Decree-Law 11/2018, of 31 August, establishes in its article 2, section 2, letter u, that the persons responsible for the management, operation and marketing of lotteries or other games of chance in person or by electronic, computerised, telematic and interactive means, are considered obliged entities in this area.

1.2.5 Retail Sports Betting Division

Undertakings within this Division carry on the activity of in person counterparty sports betting, in betting areas or betting shops.

Law 10/2010 on the prevention of money laundering and terrorist financing, in the version approved by Royal Decree-Law 11/2018, of 31 August, establishes in Article 2, paragraph 2, letter u, that persons responsible for the management, operation and marketing of lotteries or other games of chance in person or by electronic, computerised, telematic and interactive means are considered obliged entities.

Therefore, this CIRSA Group Control Measures Manual responds to the legal obligation arising from Law 10/2010 and Royal Decree 304/2014, which regulates the obligations, actions and procedures aimed at preventing and impeding the use of the financial system and other sectors of economic activity for money laundering from any type of criminal involvement. Having been adapted to Royal Decree-Law 7/2021, of 27 April, transposing Directive (EU) 2018/843 of the European Parliament and of the Council, of 30 May 2018, amending the Fourth and Fifth European Union Directives on the subject, with the aim of perfecting the mechanisms for the prevention of terrorism and improving the transparency and availability of information on the beneficial owners of legal persons and other entities without legal personality acting in the legal system.

1.3 Updating procedure

This Manual will be reviewed and updated when there are significant legal changes, new recommendations from regulators, changes in internal procedures, new activities carried out by the obliged entities of CIRSA Group or any other circumstance that may require it.

The preparation of the update and corresponding version control will be the responsibility of the Corporate Anti Money Laundering Technical Unit, whose functions are detailed below, which will propose the changes and submit them to the Internal Control Body for prior internal approval and subsequent submission to the Governing Body, which is the body responsible for approving them for all purposes.

The Anti Money Laundering Technical Unit shall be responsible for recording the successive updates of the Manual, with express indication of the modifications made, the reasons for such changes, and the dates on which they were made.

1.4 Dissemination procedure

Once the Manual or its updates are approved, the Anti Money Laundering Technical Unit is responsible for sending the document to each of CIRSA Group's business Divisions and obliged entities, indicated in point 1.1 above, who will be responsible for communicating it to employees by digital means, via email or the Employee Portal, or in person by delivering copies to each of the establishments of the obliged entities; documentary evidence of its effective delivery and dissemination must be kept.

In addition, the Compliance Area will be responsible for publishing it on the Intranet on the Compliance Area website - Procedures Manual, to which CIRSA Group employees have access.

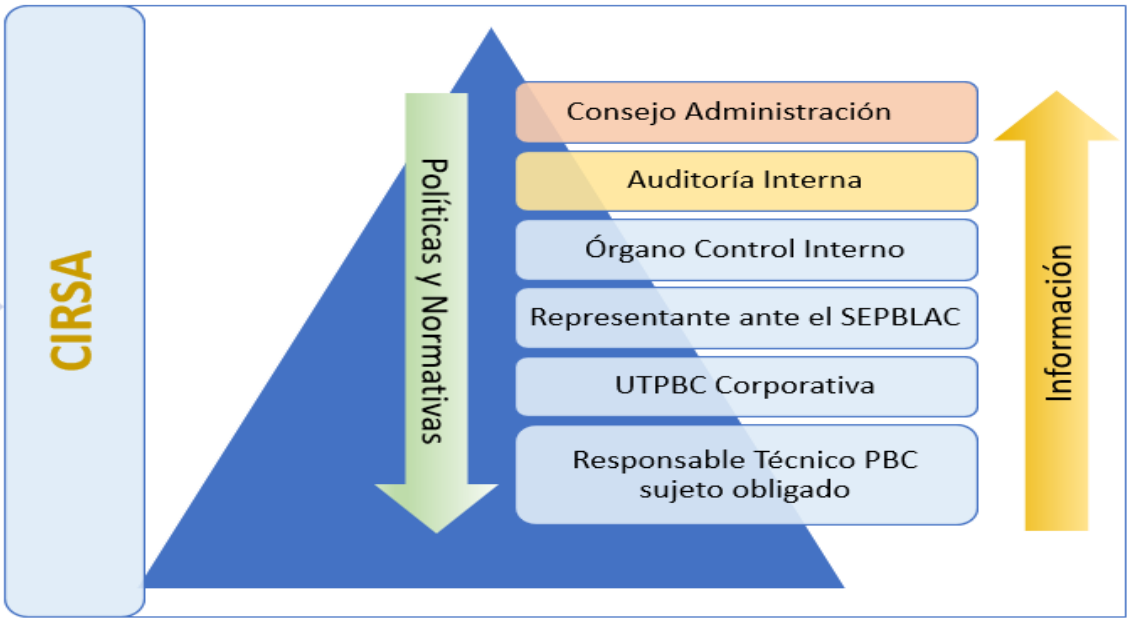
Special attention should be paid to new recruits, who will be given a link to the Manual as part of the welcome documentation provided by CIRSA Group.

2. INTERNAL STRUCTURE AND CONTROL BODIES

CIRSA Group has established a structure at Group level in order to establish and implement control measures to prevent money laundering or terrorist financing activities throughout its organisation.

This structure is made up of the Internal Control Body (hereinafter, **ICB**) and the Anti Money Laundering Technical Unit (hereinafter, **AMLTU**), both with functions at corporate or Group level, in addition to the role exercised by the Board of Directors of the main company of CIRSA Group as the highest authority and responsible for the Prevention of Money Laundering and Financing of Terrorism.

CIRSA Group also has a single representative to SEPBLAC at corporate level, appointed by the Group's Board of Directors.



In addition, each of the Group's Divisions has a person in charge or liaison, integrated in the AMLTU in charge of providing the information required by the ICB and support for coordinating those activities and controls that must be carried out directly in the companies or establishments assigned to each Division.

2.1 Representative to the Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (SEPBLAC)

CIRSA Group has a Corporate Representative to SEPBLAC, having been appointed by the Board of Directors of CIRSA Group's parent company, CIRSA ENTERPRISES, S.L.U.

The Corporate Representative is responsible for the reporting obligations established in the applicable regulations, for responding to any request and for communicating any information required in accordance with the application of the regulations in force; as well as for appearing in any kind of administrative or judicial proceedings in relation to the data collected in the communications addressed to SEPBLAC. They will also be responsible for responding to requests from other authorities (Courts, Police, Civil Guard, Tax Agency, etc.) related to money laundering and terrorist financing.

In order to maintain this responsibility without any interruption due to holidays, illness or other justifiable causes, the Representative may appoint up to two authorised substitutes.

The proposed appointment of the Representative will be communicated to SEPBLAC for acceptance using form F-22 which is published on SEPBLAC's website - www.sepblac.es- and the documentation required in its instructions.

The main functions of the Representative are:

- Receive and respond to requests for information or product tracing sent by SEPBLAC.
- Receive and respond to all requests for assistance in this area (judicial, police, public administrations, agencies and other authorities).
- Report suspicious transactions to SEPBLAC.
- Participate in consultative or informative meetings convened by SEPBLAC.
- Represent the Group in any kind of administrative or legal proceedings that may be related to communications (of any kind) made to SEPBLAC by the entity.
- Participate in meetings and forums convened by other entities and bodies in the field of money laundering.
- Advise senior management on this matter.
- To lead the AMLTU.
- Act as Secretary of the Internal Control Body.
- Appoint the authorised substitutes.

2.2 Internal Control Body

The ICB is made up of those who occupy the following positions in CIRSA Group, and it is not necessary to expressly approve each incorporation, cessation, or nominative appointment, given that the members are established on the basis of the following position they occupy in the organisation:

- Director of the Casinos Division
- Director of the Bingo Division
- Director of the Rooms Division
- Director of the Sports Betting Division
- Corporate Audit Director (with voice but without vote)
- Corporate Economic and Financial Director
- Corporate Director of Inspection and Risk
- Corporate Chief Compliance Officer

The aforementioned Directors may appoint a manager or person responsible for their respective Divisions or Corporate Departments with knowledge of the matter to attend the meetings of this Body on their behalf; they must report to it on the matters dealt with.

The functions of this Body are:

- Verify compliance by the obliged entities with the measures set out in this Manual.
- Supervise and periodically control the operation and application of money laundering procedures, verifying compliance with the obligations established in the regulations in force.
- Ensure adequate coverage of existing money laundering risks.
- Analysing customer transactions involving higher risk.
- Approve risk self-assessment reports.
- Approve changes to the Manual of Procedures on the Prevention and Control of Money Laundering proposed by the AMLTU prior to their submission to the Board of Directors.
- Decide whether to notify SEPBLAC of transactions or events that could be considered money laundering.
- Approve the necessary Training Plan in order to keep the staff constantly informed of the requirements derived from the applicable regulations on the prevention of money laundering. And the review of the monitoring of compliance with the plan.
- Analysing the external expert's report and approving the action plans drawn up by the Prevention Unit to resolve the incidents highlighted in said report.
- Approve the annual report produced by the AMLTU.
- Draw up, approve, and periodically review the Entity's customer admission policy.
- Approve the admission of customers with an above-average risk, in accordance with the risk profile determined in their admission.
- Determine the course of action to be taken on the indexing operation, proposing the cancellation of the relationship and transactions in their establishments and their communication to SEPBLAC; the carrying out of a follow-up; the authorisation of the transaction if the special examination rules out the link with money laundering or terrorist financing.
- Ensure confidentiality throughout the process of analysing suspicious transactions, as well as safeguarding the identity of reporting employees.
- Report to the Board of Directors of CIRSA Group, the most significant deficiencies identified in the external expert's report and its proposals for rectification or improvement. This communication shall be made no later than three months from the date of issue of the report.

The ICB shall meet at least twice a year, once every six months, regardless of the cases in which, due to specific needs or extraordinary situations, it must meet on an ad hoc basis, for the purpose of deciding on the reporting of suspicious transactions to the Executive Service, coordinating programmed activities, organising information to staff on money laundering, resolving doubts, establishing action plans, etc.

Minutes of these meetings shall be taken and kept on file by the AMLTU. The quorum required for the meetings of the ICB to be considered validly constituted shall be half plus one of its members. The minutes shall be signed by those who acted as Chairman and Secretary at each meeting.

One of its members will act as Chairman of the ICB each year, following the above list of members in sequence, starting with the first and so on each year in turn until the list starts again; and the Representative to SEPBLAC will always act as Secretary of the ICB.

One of the points that will form a recurring part of these meetings will be the duty to report any deficiencies detected in each Division and to propose actions aimed at rectifying them, as well as to review the measures proposed in previous sessions.

The members of the ICB will sign a confidentiality agreement in order to reinforce the secrecy and confidentiality of the information and subjects dealt with for the development of their control and monitoring functions.

The ICB reports functionally to the Group's Board of Directors.

2.3 Anti Money Laundering Technical Unit (AMLTU)

In addition to the ICB, CIRSA Group has designated the Anti Money Laundering Technical Unit (hereinafter **AMLTU**), whose head is the Representative to SEPBLAC and which has technicians in the field, knowledgeable about the transactions of the Divisions, as well as the money laundering prevention measures to be applied at Group level, acting as a department of CIRSA Group specialised in this area.

The AMLTU is composed of:

- Corporate Officers: full-time, located at the Group's headquarters and, in general, mainly responsible for risk management, monitoring the model and updating the Group's policy, manual and other internal regulations in this area.
- Division managers: part-time, located at the heart of the business of each of the Group's obliged entities and, in general, mainly responsible for monitoring the model, its effectiveness and improvement.

The functions of the AMLTU Corporate Officers are as follows:

- Supervise and coordinate the Business AML Managers.
- Receipt of any communication and documentation from the ICB or CIRSA Group managers in relation to suspicious money laundering transactions.
- Analyse the reports received by the AML Officers of each business Division and communicate them to the ICB as appropriate.
- Communicate to the AML Officer reporting the transaction the follow-up given to the issue raised.
- Organise and store the documentation from money laundering prevention and control transactions reported to the ICB.
- To ensure compliance with the policies relating to the prevention of money laundering of all CIRSA Group's obliged entities.

- Update and control (version control) the Manual of Procedures for the Prevention and Control of Money Laundering.
- Keep the minutes of the ICB meetings on file.
- Analyse, resolve (prepare documentation and information required to be communicated) and file the requirements of SEPBLAC or other authorities (Courts, Police, Civil Guard, regional police and other public administrations and agencies), related to the prevention of money laundering.
- Draw up the annual Employee Training Plan and submit it to the ICB for consideration. Monitor compliance with the Training Plan.
- Draw up and propose an annual Action Plan with regard to the incidents and recommendations proposed by the Audit Department and in the review carried out by the external expert and follow up to verify and guarantee its implementation.
- Execute periodic tests to verify the degree of compliance with the policies established with regard to the procedure for detecting suspicious transactions.
- Draw up the annual report of actions.
- Update the content of the training courses.
- Verify that the mandatory report of the external AML expert is developed and complies with the requirements of the law.
- Review the risk profile of the Entity's customers in accordance with the corresponding procedures.

Control and record keeping:

a. Proposed amendments to the Manual.

b. Requests from SEPBLAC or other competent authorities.

c. Documents submitted to the Governing Board.

d. Register of suspicious transactions reported to the ICB (HRCs).

e. Other records required by the applicable regulations or for the best effectiveness of CIRSA Group's system for the prevention of money laundering and terrorist financing.

The functions of the AMLTU members responsible for AML in each Business Division are as follows:

- Receipt of any communication and documentation from CIRSA Group employees or Partners in relation to transactions suspected of money laundering.
- Analyse such transactions and communicate them to the Corporate AML Officers if appropriate or in case of doubts.
- Communicate to the sender of the transaction the follow-up given to the issue raised.
- Organise and store documentation from money laundering prevention and control transactions.

- To ensure compliance with the procedures relating to the prevention of money laundering by all CIRSA Group's obliged entities.
- Comply with the requirements of the Corporate AML Officers.
- Store the documentation identifying the customers and accrediting their transactions in accordance with the regulations in force.
- Execute regular tests to verify the degree of compliance with the procedures established with regard to the procedure for detecting suspicious transactions.
- Control and maintenance of records, and generation of quarterly reports:
    a. Transactions analysed.
    b. Customer Registration.
    c. Suspicious transaction register (HRCs).
    d. Other records required by the applicable regulations or to improve the effectiveness of CIRSA Group's system for preventing money laundering and the financing of terrorism: currency exchanges, purchase and sale of chips and tokens, etc.

2.4 Board of Directors

The functions of the Board of Directors in relation to anti-money laundering measures are as follows:

For Cirsa Enterprises:

- Appointment and/or acknowledgement of the Representative to SEPBLAC.
- Acknowledgement of the Internal Control Body and its modifications.
- Acknowledgement of the Corporate AML/CFT Technical Unit and its modifications.
- Approval of the Money Laundering Prevention Manual and its significant amendments.

For the different Business Divisions:

- Be kept adequately informed of efforts to prevent money laundering.
- To know the most relevant cases of suspicious transactions reported to SEPBLAC.
- To be aware of the most significant deficiencies identified in the external expert review, as well as proposals for rectification or improvement.
- Approval of the Money Laundering Prevention Manual and its extraordinary amendments.
- Approval of the Action Plan.
- Approval of the Training Plan.

The topics discussed and decisions taken within the committee relating to the prevention of money laundering shall be documented in the minutes of its meetings.

2.5 Directors' and Officers' Liability

In addition to the Entity's liability, even for simple non-compliance, those who hold administrative or managerial positions in the Entity shall be liable for infringements when these are attributable to their wilful or negligent conduct.

2.6 Recruitment of Employees

Hiring procedures for executives and employees of CIRSA Group companies must guarantee high ethical standards, applying suitability criteria established by the applicable sectorial regulations.

In the absence of specific regulations, in order to determine the concurrence of high ethical standards in managers and employees of the regulated entity, their professional background shall be taken into consideration, assessing their observance of and respect for commercial laws or others that regulate economic activity and business life, as well as good practices in the sector.

In relation to new recruits for the most relevant positions linked to the management of AML files, the absence of a criminal record in offences related to this matter will be confirmed by means of a declaration of responsibility.

3. IDENTIFICATION, ADMISSION AND KNOWLEDGE OF CUSTOMERS

Considering that the different Divisions of CIRSA Group have different obligations in terms of AML, as well as different forms of access by their customers to their varied gaming offer (in person, internet, casinos, bingo halls, rooms), it is necessary to include in this manual, on the one hand (i) the general principles of the customer identification, admission and knowledge policy generally applicable to all the Divisions; and on the other hand (ii) the special principles adapted to the procedures of each of these Divisions, as set out below.

3.1 General Principles of Customer Admissions Policy

The general principles set out below apply to all establishments in all Divisions of CIRSA Group that are considered obliged entities in this area:

- CIRSA Group's establishments or websites that allow access to its in person or online gaming offer must identify all their customers and must apply due diligence measures in their identification and knowledge, as established in the special customer admission policies of each Division.

- Prior to the establishment of any type of business relationship and during the customer identification process, the customer must first accept the Privacy Policy and the specific Terms and Conditions of each Division in compliance with the provisions of EU Regulation 2016/679 of 27 April and LO 3/2018 of 5 December, where they are informed of the collection and processing of their data with regard to money laundering.

- In this regard, obliged entities must have a file, database, register, etc. of their main customers ("**know your customer**" or "**KYC**" files), in which all the information relating to the customer and the type of gaming and transactions established with them is detailed and centralised, as well as that obtained through the application of due diligence measures corresponding to their level of risk.

- In this respect, our customers do not declare their professional activity at the admission stage. For this reason, an investigation and analysis procedure is developed in order to determine the professional activity of those customers who are considered High Risk, using this factor as a risk mitigating element.

- CIRSA Group companies that have establishments open to the public for in person gaming must comply with the rules governing the admission of establishments for public shows and recreational activities and are subject by regulation to the obligation to identify and in some cases also to register all customers to prevent access by minors and banned persons.

- All Divisions check that their customers are not included in blacklists or sanctioned lists published by the European Union, the UN and other entities or institutions, such as OFAC, and have a worldwide database for such verification.

- No gaming activity, relationship or transaction of any kind is permitted with users included in any of the following typologies:

    - Customers who are included in the list of "banned customers" provided by the competent administrations of each demarcation or autonomous community are banned from accessing or participating in gaming.

- In CIRSA Group's establishments, legal entities are not allowed access to the gaming rooms or to the online gaming offering, or to carry out transactions on behalf of third parties or in the interest or on behalf of third parties.
- Persons who refuse to provide the required information or documentation or do so with false information or documentation.
- Persons who have not been properly identified.
- Any other category as determined by the ICB.

- Gaming room staff shall be alerted to conduct by customers who may attempt to act on behalf of a third party, in accordance with the specific training provided; such a case shall be followed up by transactions staff to rule out or confirm such a circumstance and, in such event, warn the customer of their banning or even expulsion from the room.

- The Divisions will decide to classify their customers as High-Risk Customers (hereinafter **HRCs**) when certain circumstances arise, which will be analysed in the Risk Self-Assessment Report. Once a customer has been classified as a HRC, the process of enhanced due diligence on the customer's knowledge must begin, initiating the opening of the HRC Folder, which AMLTU will be responsible for completing, if necessary, by providing further information (commercial or financial reports, internet searches or other methods it deems appropriate, depending on the customer's characteristics), as well as archiving it.

- In accordance with the provisions of Law 10/2010 of 28 April, Politically Exposed Persons (hereinafter PEPs) shall be considered to be those natural persons who perform or have performed important public functions, both in Spain and in other States, as well as their next of kin and persons recognised as close relatives.

  For these purposes, the following definitions shall apply:

  a) By natural persons who perform or have performed important public functions: heads of state, heads of government, ministers or other members of government, secretaries of state or under-secretaries; members of parliament; judges of supreme courts, constitutional courts or other high judicial bodies whose decisions are not normally subject to appeal, save in exceptional circumstances, including the equivalent members of the Public Prosecutor's Office; members of courts of auditors or boards of central banks; ambassadors and chargés d'affaires; senior military personnel of the armed forces; members of the administrative, management or supervisory bodies of publicly owned enterprises; directors, deputy directors and members of the board of directors, or equivalent function, of an international organisation; and senior officials of political parties with parliamentary representation.

  b) Likewise, persons other than those listed in the previous section, who are considered senior officials in accordance with the provisions of article 1 of the Law regulating the exercise of senior positions in the General State Administration, shall also be considered PEPs; persons who hold or have held important public functions in the Spanish autonomous community, such as Presidents and Councillors and other members of the Governing Councils, as well as persons who hold positions equivalent to those listed in point a), and autonomous community deputies and senior management positions in political parties with autonomous community representation.

c) In the Spanish local sphere, mayors, councillors and persons holding positions equivalent to those listed in point a) of the municipalities of provincial capitals, or of Autonomous Communities and Local Entities with more than 50,000 inhabitants, as well as senior management positions in political parties with representation in those districts.

d) Also senior management positions in Spanish trade union or employers' organisations will be considered as PEPs.

e) And lastly, persons who perform important public functions in international organisations accredited in Spain.

f) None of these categories shall include public employees at intermediate or lower levels.

In relation to customers listed as Politically Exposed Persons, in addition to the normal due diligence measures, the enhanced due diligence measures foreseen in each of the Group's Divisions shall be applied.

3.2 General principles of the Customer Admissions Policy specific to the On-Premises Business Divisions - Casinos, Rooms, Bingo halls and Sports Betting

These are public establishments and must therefore comply with the rules governing the admission of establishments for public shows and recreational activities of each Autonomous Community with jurisdiction in this area. Consequently, they are subject by regulation to the obligation to identify all customers accessing the gaming room, in order to prevent access by minors and self-excluded or banned customers.

In the specific case of Sportium Apuestas Retail, it offers its in person sports betting via telematic means, controlled and supervised internally at all times, in establishments with public access, both its own and in its own betting corners, but within the gaming offer of third parties in its bingo halls, rooms and casinos, which means that it must comply with the rules governing the admission of establishments for public shows and recreational gaming activities.

3.2.1 Access to the Gaming Room

Customers wishing to access the Gaming Room must first identify themselves at Reception, proving their identity by means of one of the current documents accepted.

When checking the identity of the Customer at reception, the System checks against: (i) the lists of self-excluded or banned persons provided by the different Autonomous Communities, (ii) the blacklists of sanctioned persons and, (iii) the lists of PEPs available to CIRSA Group, with the support of the AMLTU if necessary. Exceptions to the consultation of the blacklists of sanctioned and PEPs are the Bingo Division and the Rooms Division, where, on a bimonthly basis, the list of winners of prizes subject to Law 10/2010 will be consulted on these lists.

3.3 Special Principles of Customer Admissions Policy

Each of the business divisions of CIRSA Group's gaming companies has a specific customer admission policy, depending on its obligations in terms of AML and the different types of customer access to its leisure and gaming offer.

Divisions shall take into account and apply the General Principles in 3.1 and 3.2 above in all matters not defined or regulated in the Special Principles.

3.4 Checking in databases and official lists

3.4.1 Checking blacklists of those sanctioned or convicted of money laundering, terrorism, drug trafficking and other crimes

In general, CIRSA Group checks, by means of a double check, whether its users are included in one of the most comprehensive international databases on the market, which includes the lists of suspects, sanctioned persons and terrorists issued by the various official bodies (UN, OFAC, EU, etc.). A first time during the customer admission process via direct match with the National Identity Card (with the exception of the Rooms and Bingo Divisions), and a second time, every six months, by means of a computer routine that automatically allows a complete check of the database of registered Customers or Customers with an Account, depending on each specific case according to the specificities of each Division (with the exception of the Rooms and Bingo Divisions, where, on a bimonthly basis, the AMLTU will check the list of prize winners against the aforementioned database of sanctioned customers).

In this first manual match against the DNI, in the event of an exact match (100%), access will be momentarily blocked, and the Head of the Business Division belonging to the AMLTU will be notified for analysis and assessment, and depending on the result:

a) True positive: access will be denied and reported to the AMLTU, the ICB and SEPBLAC. A person shall be considered true positive if they have been positively convicted of money laundering and terrorist financing offences within the last two years.

b) De-contextualised positive: access will be granted; the customer will be marked as belonging to a special category and appropriate enhanced due diligence measures will be applied for ongoing monitoring to determine the source of wealth and funds. A decontextualised positive shall be understood as all those not considered as true positives.

During the second check, in case of a high match (≥ 97%) based on a matching matrix for the identification of PEPs and suspects, these users are included in a specific report:

From which the Head of the Business Division of the AMLTU analyses and evaluates them in order to rule out false positives:

a) In the event of a real match, they will be barred from future entry, any pending trades will be cancelled, their deposits will be blocked, and they will be reported to the AMLTU, the ICB and SEPBLAC.

b) In the case of a decontextualised positive, the Customer will be marked as belonging to a special category and the appropriate enhanced due diligence measures will be applied for ongoing monitoring to determine the origin of the assets and funds.

c) And if it is a false positive, no additional due diligence will be applied.

The Group's AMLTU shall be informed.

3.4.2 Checking the lists of Politically Exposed Persons (PEPs)

In the same sense as in the previous subsection, CIRSA Group also generally checks with a double check whether its users are included in one of the most comprehensive international databases of Politically Exposed Persons (PEPs). A first time during the customer admission process via direct match with the National Identity Card, and a second time, every month, by means of a computer routine that automatically allows a complete check of the database of registered Customers or Customers with an Account, depending on each specific case according to the specificities of each Division. As in the preceding section, the Bingo and Rooms Divisions shall carry out a bimonthly check of the list of customers who have won a prize exceeding the reference threshold in terms of amount.

In this first direct match against the DNI, in case of an exact match (100%), the customer will be marked as belonging to a special category, the Head of the Business Division belonging to AMLTU will be notified for authorisation, and in case of establishing or maintaining business relationships, the relevant enhanced due diligence measures will be applied in order to perform ongoing monitoring to determine the origin of the assets and funds.

During the second check, in the case of a high degree of coincidence (≥ 97%) based on a coincidence matrix for the identification of PEPs and suspects, these users are included in a specific report from which the Head of the Business Division belonging to the AMLTU analyses them in order to rule out false positives. In the event of a real match, the Customer will be marked as belonging to a special category, business relationships will be analysed and, if authorised, the necessary enhanced due diligence measures will be applied in order to carry out ongoing monitoring to determine the origin of the assets and funds.

The Group's AMLTU shall be informed.

3.5 Identification documents

All customers wishing to access the Group's establishments must first identify themselves at the Reception desk, proving their identity by means of one of the following documents:

Reliable documents for identification purposes:

-Spanish nationals: ID

Exceptionally, in accordance with article 6.1 a) of RD 304/2014, obliged entities may accept other personal identity documents issued by a government authority provided that they enjoy adequate guarantees of authenticity and include a photograph of the holder, for example, a driving licence.

In addition, their exceptional admission through other documents is supported by:

FATF Recommendation 11 on record keeping states that:

"Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity. Financial institutions should be required to keep all records obtained through CDD measures (e.g. copies or records of official identification documents like passports, identity cards, driving licences or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g. inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction."

And on the other hand, the European Commission, in its information note of 18 January 2013, in relation to the third EU directive (Directive 2006/126/EC), regarding the European driving licence, points out that:

"A driving licence not only gives access to all kinds of vehicles in many EU countries it can also be used as an identification document. Therefore, anti-fraud protection is a major cause for concern. The new licence is almost impossible to falsify. It is backed up by a European electronic data exchange system, which will facilitate the management of driving licences by administrations and contribute to better detection of driving licence fraud."

- Foreigners:

For foreign nationals, the Residence Permit, Foreigners' Identity Card, Passport or, in case of citizens of the European Union or of the European Economic Area, the official personal identity document or card issued by the authorities of origin. The identity document issued by the Ministry of Foreign Affairs and Cooperation for the staff of diplomatic and consular missions of third countries in Spain shall also be valid for the identification of foreigners.

Exceptionally, obliged entities may accept other personal identity documents issued by a governmental authority provided that they have adequate guarantees of authenticity and include a photograph of the holder.

Staff of diplomatic missions: Identity card issued by the Ministry of Foreign Affairs and Cooperation.

All identification documents of any person must be in force on the date on which the transactions are carried out.

4. PRESERVATION OF DOCUMENTATION

4.1 Gaming Activity

The documentation derived from the activity of the obliged entities formalising compliance with CIRSA Group's regulatory obligations in the area of AML shall be kept for a period of ten years, starting from the execution of the transaction carried out or the termination of the business relationship, and shall be anonymised or eliminated after this period of time has elapsed.

Five years after the termination of the relationship, transaction or the execution of the occasional gaming transaction, the retained documentation shall be accessible only to the members of the ICB and the AMLTU and, where appropriate, to those charged with their legal defence.

Documentation shall be retained for use in any investigation or analysis of possible money laundering or terrorist financing by SEPBLAC or any other legally competent authority:

- Copy of the documents required under the due diligence measures.
- Original or a copy with evidentiary force of the documents or records that adequately prove the transactions, the parties to the transactions and the business relationships.

4.2 File

In general, due to the nature of the information contained in the documents related to the prevention of money laundering, the documents shall be stored on electronic media in digital format, in such a way as to guarantee their integrity, their confidentiality, the correct reading of the data, the impossibility of manipulation and their adequate storage and location.

The electronic filing mode will be carried out through a cloud service with the maximum guarantees in terms of Information Security and compliance with the applicable regulations on Data Protection:

- Access management and profiling of actions.
- Servers with automatic back up process.
- Archived in folders, grouped by Country or Business Division, chronologically ordered, easily identifiable and locatable.
- Five years after the termination of the business relationship or the execution of the occasional transaction, the retained documentation shall only and exclusively be accessible via permissions by the members of the AMLTU and the ICB.
- After a period of ten years from the termination of the business relationship or the execution of the occasional transaction, the documentation will be anonymised or deleted depending on its typology.

5. DETECTION OF TRANSACTIONS THAT COULD BE RELATED TO MONEY LAUNDERING

5.1 Detection of transactions

CIRSA Group has developed an exemplary list of events and transactions that are particularly likely to be linked to money laundering in the gaming sector.

This list contains the transactions, indicators, activities, and situations that may represent a potential risk of being linked to money laundering activities.

However, any other transaction which does not appear in the above-mentioned list, but which is suspected or certain to be related to money laundering may be considered as suspicious.

In addition, and for guidance purposes, the Exemplary Catalogue of money laundering risk transactions in the gaming sector and the Exemplary Catalogue of money laundering risk transactions for currency exchange establishments, published by the Secretary of State for the Economy, which can be consulted before carrying out any CIRSA Group transaction on the website www.sepblac.es, will be taken into account.

The detection of suspicious transactions is a joint responsibility of all those involved in CIRSA Group's transactions, from reception, security, cashier, transactions, gaming and management where the gaming is in person, and of the managers and those responsible for procedures in online or internet gaming.

The alert system in CIRSA Group's establishments is based mainly on the observation of the employees in the gaming room, given that gaming transactions are immediate and, therefore, the most effective way of detecting suspicious behaviour must be at the very moment when the customer participates in the game. The alerts are transmitted by the employee who detects a suspicious transaction to their hierarchical superior, who will then inform the most senior manager present in the gaming room, in order to coordinate the monitoring of the customer's transactions, both in the gaming room and in cash transactions; special attention shall be paid to requests for the issuing of cheques and/or winnings certificates, only and exclusively accepted by the Casino Division, always verifying that they are real winnings from the customer's participation in the game. In any case, prior authorisation must be sought from the head of the AMLTU in such cases, who will in turn communicate this to the members of the ICB at the next meeting for the record. All of this taking into account that in the gaming sector it is necessary for procedures to be agile for the treatment and detection of those transactions on which it is necessary to apply due diligence measures urgently given the immediacy with which they are produced or executed.

For this reason, the training plans stress the importance of these employees being aware of and knowing how to detect this type of transactions, with a catalogue or register of types of transactions related to AML and types of customers according to risk, which is reviewed periodically in accordance with the activities carried out and experience acquired by the Group's companies.

This is different in the case of online or internet gaming, where a warning system has been established by the relevant Division.

On a semi-annual basis, AMLTU shall execute periodic tests to verify the degree of compliance with the established policies regarding the procedure for the detection of suspicious transactions. The tests shall consist of carrying out queries of the database used by CIRSA Group to detect transactions that may be related to money laundering according to the list of suspicious transactions mentioned in the first paragraph and to verify, where appropriate, the treatment given to the conduct and transactions detected.

In the event that the AMLTU detects the frequent execution of a specific transaction included in the catalogue or register of types of risk transactions, the channels or procedures for communication with the Business Divisions set out in this Manual must be reviewed to verify whether they are functioning correctly, and to clarify why the business units continue to accept and execute that specific transaction.

5.2 Abstention Procedure

Employees, officers, room managers or those responsible for managing customer relationships and transactions shall refrain from executing any transaction where there is any indication or certainty that it is related to money laundering of proceeds of any kind of criminal involvement.

When an employee or manager observes any of these transactions, the following procedure shall be followed:

1. The employee or manager shall, as far as possible, refrain from carrying out the transaction.

2. The employee, in case of doubt, shall immediately contact their line manager, who may decide to refrain from carrying out the gaming transaction or contact the establishment's AML manager or liaison or the head of the AMLTU reporting the transaction or the observed event.

3. In the latter case, the head of the establishment's AML liaison or, where appropriate, the head of the AMLTU shall analyse the transaction as quickly as possible and if, after analysing the information available, they determine that there is an indication or certainty that the transaction is related to money laundering, they shall give instructions to refrain from executing the transaction.

4. Notwithstanding the above, the person in charge of AML of the establishment or of the AMLTU may authorise the transaction to be carried out if they consider that abstention is not possible or if it would hinder the prosecution of the beneficiaries of the transaction.

5. These circumstances shall be communicated to the members of the ICB by the head of the AMLTU and shall be recorded in the minutes of the next meeting to be held.

5.3 Procedure for reporting suspicious transactions to AMLTU

When an employee or manager observes any of the transactions compiled in the list of events and transactions particularly likely to be related to money laundering, or has a suspicion that a transaction or event may be likely to be related to money laundering because it does not correspond to the nature, volume of activity or operational background of the customer, and there is no economic, professional or business justification; such transaction may be reported to the AMLTU for analysis. The following procedure shall be followed:

1. The employee or manager who has observed the transaction in question shall complete the suspicious transaction report form and send it by e-mail to the AMLTU.

2. The AMLTU shall analyse the observed event or situation according to the procedure described in section 6 below of this Manual.

3. The head of the AMLTU shall inform the ICB of the suspicious transaction together with the result of the analysis performed.

4. The ICB, after reviewing the analysis performed, will decide whether to report it to SEPBLAC. The communication shall be made in accordance with the procedure described in section 7 of this Manual.

5. In any case, the person in charge of the AMLTU will inform the employee or manager about the follow-up given to their communication by filling in and sending the corresponding form.

In the event of any communication made by employees or managers about facts or situations that could be related to money laundering, CIRSA Group undertakes to guarantee absolute confidentiality regarding the identity of the communicators and the content of the communication, and exempts them from any liability that may arise from the act of communication.

The status of dispatch and receipt of the form shall be recorded at all times by both the person sending the form and the sender.

Executives or employees may report directly to SEPBLAC any transactions of which they become aware in the course of their duties and with respect to which there are indications or certainty that they are related to money laundering, in cases where the AMLTU has not been informed by the reporting officer or employee in accordance with Article 18 of Law 10/2010 within a maximum period of 10 working days.

The reporting employee or manager will be informed of the decision taken by the ICB to report the suspicious transaction to SEPBLAC through the same channel.

5.4 Internal procedure for reporting transactions

In addition to the above communication procedure, employees and directors also have at their disposal a series of communication channels through which they can communicate, even anonymously, any relevant information on possible breaches of the regulations on the prevention of money laundering or the policies and procedures implemented to comply with them, committed internally or externally in CIRSA Group's activities.

- The link to the EthicsLine Channel platform is (link located on the Intranet):

  https://www.bkms-system.com/COMPLIANCE-CIRSA

- The e-mail address is: compliance@cirsa.com

- The postal address is:

  Corporate Compliance Area

  Anti Money Laundering Technical Unit

  Ctra. Castellar, 338, 08226 Terrassa (Barcelona)

All these communication channels are those implemented by CIRSA Group in application of its Code of Conduct, Anti-Corruption Policy and Ethics Line Channel Operation Policy, and their recipients are the members of the Corporate Compliance Body, including the Group's Representative to SEPBLAC in their capacity as Chief Compliance Officer of the Group, and this body has an internal protocol for investigating complaints received through these channels.

The provisions of the regulations on personal data protection for internal complaint information systems are applicable to this internal communication system and procedure.

CIRSA Group ensures that employees or managers who report wrongdoing in the organisation are protected against retaliation, discrimination, and any other type of unfair treatment.

5.5 Duty of confidentiality

CIRSA Group will not disclose to the customer or to third parties the actions it is carrying out in relation to its obligations under article 24 of Law 10/2010 in the manner regulated by the aforementioned regulation.

Employees are warned of the confidential nature of the documentation they handle and the knowledge they acquire in the course of their work in CIRSA Group, both of the clientele, and of the systems, methods and organisation of money laundering prevention.

6. TRANSACTIONS ANALYSIS

The AMLTU's activities include obtaining information from the Group's various establishments/operators in order to analyse transactions that may be related to money laundering reported by employees or managers.

The AMLTU will not only apply due diligence measures to all new customers but also to existing customers on the basis of a risk analysis. In any case, they shall apply to existing customers when new products are contracted, the circumstances of the customer change or when there is a significant transaction due to its volume or complexity.

The ex-ante analysis shall be carried out on a monthly basis within a maximum of one month from the start of the analysis and shall be formally documented for submission to the ICB.

In addition to the due diligence measures indicated above, the following additional procedures shall be applied for those customers who, due to their nature, their characteristics, or their own transactions observed in ongoing monitoring, are categorised as having a higher-than-average-risk, in accordance with the customer admission policy. A detailed study of the customer, which must be recorded in a report created for this purpose by the AMLTU, containing all the information gathered during the ordinary procedure, the documentation requested, the measures taken to verify each of the information provided. It is important to consult external databases and to carry out research on the customer.

These categories include most notably Politically Exposed Persons (PEPs) or customers domiciled or resident in countries considered high risk or with a higher than average level of risk.

The ICB will review the information provided, discuss it, and decide whether to report it to SEPBLAC. The decision to disclose shall be taken when, after careful examination of the additional information and documentation, it is concluded that it shows a clear mismatch with the nature, volume of activity or transaction history of the customers and that there is no economic, professional, or business justification for the conduct of the transactions. And in any case provided that, after special examination, it is known, suspected or has reasonable grounds to suspect that it is related to money laundering, or its predicate offences or the financing of terrorism.

For those alerts that are classified as "under review", the AMLTU will analyse, over the next 3 months, the transactions of those customers that fall into this category in order to determine the pretext that gave rise to the alert or, on the contrary, to clarify the evidence for study and communication to the ICB.

The purpose of the report is to ensure that all the information available on the customer allows us to consider that the business relationship that they intend to establish is in line with their economic capacity, ruling out any type of relationship with money laundering or the financing of terrorism.

Whatever the case may be, the communication decision taken shall be recorded in writing with the documentary support. In a record which will subsequently be reflected in the official minutes of the ICB, and in case of a decision not to communicate, the reasons for such a decision shall also be documented. This information will subsequently be submitted to the Governing Body of the relevant business Division.

6.1 Risk Mitigation

Users of CIRSA Group's different business units do not declare their professional activity when they are admitted as customers. On the other hand, the Group has established guidelines for searching for and investigating the professional activities of those customers who, due to their volume of gaming, may pose a risk in terms of money laundering prevention in the event that the volume of gaming does not match the economic profile of the user.

For this purpose, a distinction is made between the sources of consultation to be used, both for domestic and foreign users, with a view to obtaining the possible origin of the funds.

For Spanish users:

- Central Commercial Register.
- Registradores.org.
- Axesor.

For foreign users:

- United Kingdom: companycheck.co.uk.
- France: verif.com and societe.com.
- Switzerland: dnb.com/business-directory.
- European: e-justice.europa.eu (Business registers).
- Opencorporates.com

The proposed list is not exhaustive and may be expanded as other reliable company information sites become available.

For those cases where no information can be found through the registers and reliable company information pages, Google searches will be carried out in Spanish, English and the customer's native language in order to cover a possible larger number of results.

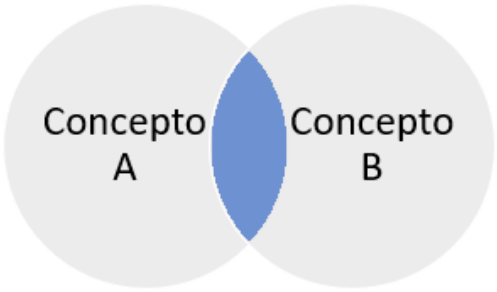
In order to obtain results that are closer to the search we want to carry out, scientific search methods can be used in a meta-search engine.

Meta-search engine: https://www.etools.ch/

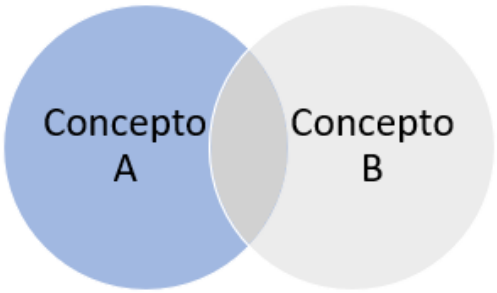
Scientific search methods:

- Exact match search: "word/phrase". By entering the word or phrase to be searched for in inverted commas (" "), the meta-search engine will return results that exactly match your search.
- Search by truncation: wor*. Replacing the part of the term that we do not know, or want to leave open, with the symbol (*), will give us results for each word that could be formed with the truncation base. In the case of the example, we would get results for word, little word, strange word...
- Substitution search: mexic?. By substituting the character that can vary by the symbol (?), we will obtain all the word results that can be formed from that missing character. In the case of the example, we would obtain results for Mexico, Mexican, etc.

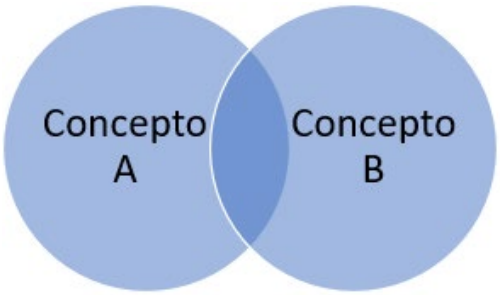
- Boolean logic criteria:
    - AND: Logical operator AND. The search will return results that include ALL the different concepts that are "tied" with this logical operator.



    - NOT: Logical operator NOT. The search we carry out will return results that do not include the concepts joined with this logical operator.



    - OR: Logical operator OR. The search we carry out will return results that include one or more of the concepts that are linked to this logical operator.



- For those cases in which, after the investigation and analysis work, no information is found regarding the user's economic activity or the possible origin of their funds, three hypothetical situations are differentiated for the purpose of assessing the action to be taken in such cases: Occasional user, meaning a user who accesses the gaming offer on one occasion, or for a limited period of time, and who does not return within two years. In these cases, enhanced due diligence measures will be applied to determine, through the transactions carried out by the customer, whether there are indications of money laundering for the purposes of reporting to SEPBLAC. If no evidence is found, the cases will be closed.
- Temporary users, understood as those who access the gaming offer on a recurring basis, focusing their activity on specific times of the year. In these cases, enhanced due diligence measures will be applied in order to determine, through the transactions carried out by the customer, whether there are indications of money laundering for the purposes of notifying SEPBLAC and an alert will be established in the management application in order to monitor their activity on their next visit.

- Frequent/recurrent user, where frequent/recurrent user is defined as a user who has continuous activity throughout the year. In such cases, the customer will be asked to provide a document justifying their economic activity and/or the origin of the funds.

7. REPORTING TO THE EXECUTIVE SERVICE OF TRANSACTIONS THAT COULD BE RELATED TO MONEY LAUNDERING

7.1 Communication procedure

Notification to the Executive Service shall be made directly by the Representative or their authorised deputies to SEPBLAC, and by electronic means on the website of the Bank of Spain through the Virtual Office https://sedeelectronica.bde.es/sede/es/ or by any other means provided for this purpose.

In any case, communications shall always include the following information:

- List and identify the natural persons involved in the transaction and the concept of their participation in the transaction.
- The known activity of the natural persons involved in the transactions and the correspondence between the activity and the transactions carried out.
- A list of the transactions and dates to which they relate, indicating their nature, currency, amount, place(s) of execution, purpose and payment or collection instruments used.
- The steps taken by CIRSA Group to investigate the reported transactions.
- A statement of the circumstances of any kind from which it may be inferred that there is an indication or certainty of a link to money laundering or that there is no economic, professional or business justification for the activities.
- Other information relevant to the prevention of money laundering as determined by the Executive Service.

To report suspicious transactions to SEPBLAC, the F-19 form available on the website www.sepblac.es or any other form that may be determined for this purpose in the future shall be used.

Copies of the communications sent to SEPBLAC, as well as proof of receipt, shall be kept for the annual report.

7.2 Exemption from liability

Information provided to SEPBLAC in communications made in compliance with this Manual by its officers or employees shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any law or regulation and shall not involve its officers or employees in any liability of any kind, provided that it is not a false complaint.

7.3 File

For each suspicious transaction report that has been made, an electronic file will be created in a database, where the steps followed in the analysis of the customer's transaction will be recorded. Likewise, an electronic folder will also be opened, as a repository, where, given the sensitive nature of the information contained, its integrity, limited access, confidentiality and adequate conservation and location will be guaranteed, based on the highest standards in Information Security Management Systems, and where all the documentation consulted and used to prepare the communication and/or response will be kept, and which will be archived in the AMLTU for 10 years in chronological order of the same.

8. COMPULSORY MONTHLY DECLARATION OF TRANSACTIONS

The only CIRSA Group entities in Spain that are obliged to submit monthly declarations of transactions, as established in Art.27.1.a of RD 304/2014 of 9 June, are Casinos and only for their currency exchange activity.

9. REQUIREMENTS OF THE EXECUTIVE SERVICE AND OTHER AUTHORITIES

9.1 Persons in charge and means used

CIRSA Group's Representative to SEPBLAC or, failing that, the authorised deputies, are responsible for responding to the requests sent by SEPBLAC or by other authorities (Courts, Police, Civil Guard, Tax Agency, and other competent administrations) related to the prevention of money laundering.

Beforehand, the AMLTU shall study the request and collect information on customers, if any, and the transactions carried out in order to analyse the transaction in depth and respond to the request in as much detail as possible, when the information requested relates to customer transactions.

All requests from SEPBLAC or other authorities (Courts, Police, Civil Guard, etc.) related to the prevention of money laundering will be dealt with as quickly as possible and within the established deadlines. In case the request does not indicate a maximum response date, this should not exceed 30 calendar days.

9.2 Filing procedure of the requested requirements

For each request from SEPBLAC or other authorities (Courts, Police, Civil Guard, etc.) related to the prevention of money laundering, an electronic file will be created in a database, where the steps followed in the analysis of the customer's transactions will be recorded.

Likewise, an electronic folder will also be opened where all the documentation consulted and used to prepare the communication and/or reply will be kept, and which once replied to will be archived at the AMLTU for a period of 10 years.

At the same time, an electronic register will be created where the AMLTU will note the date of receipt, the content of the request and the date of response.

10. STAFF TRAINING

10.1 Scope

The AMLTU is responsible for promoting the necessary communication and training actions in order to keep the staff constantly informed about the requirements of the applicable anti-money laundering regulations and to ensure that they know how to detect suspicious transactions and how to proceed in each case.

The annual training plan shall take into account the risks in the gaming sector and shall contain:

- The basic content of the courses and material used, which, in any case, shall include the presentation of cases relating to transactions with indications that have occurred in the entity or that may be specific to the sector in which the regulated entity operates.
- Duration and periodicity of these.
- Form of delivery, in person or distance learning, and profile of trainers.
- Employees, departments, and lines of business at which it is aimed, developing suitable courses according to the profile of each group of employees.
- An initial training course on AML for new employees.
- Implementation of a system of evaluation of the knowledge acquired after the courses given.

Training in the Prevention of Money Laundering will be aimed at those employees who are in a position of responsibility and close to the development of transactions that may be susceptible to being related to money laundering, as well as members of the ICB, AMLTU and directors.

AMLTU will support the ICB in training matters; the content and level of detail of the training plan will be proposed by AMLTU to the ICB.

As a general rule, training for a new employee in money laundering prevention will be the responsibility of their immediate superior and will be integrated into their induction (welcome) programme.

In addition, specific training actions will be implemented when there are significant changes in the legislation in force and/or in the internal regulations for the prevention and detection of money laundering and, if there are no substantial changes within a period of two years, reinforcement training actions.

Both specific and reinforcement training actions may be carried out by trainers from CIRSA Group itself, as well as by external service companies with demonstrable experience in the field.

The annual training plan should be monitored, so that at the end of the year an assessment is made of how many of the employees who were planned to be trained have actually been trained to a sufficient level of proficiency.

10.2 Documentary support for training actions

The AMLTU is responsible for implementing the appropriate procedures for the purpose of accrediting to SEPBLAC and/or third parties the effective delivery of all specific training actions foreseen in the prevention of money laundering.

These procedures will allow the following aspects to be evidenced in relation to each of the training actions:

- Subjects taught.
- Effective attendance of the members of the Organisation to whom the training actions are addressed.
- Evaluation of the knowledge acquired by the participants.

11. INTERNAL VERIFICATION

11.1 Internal Audit

The Corporate Internal Audit Department will verify CIRSA Group's compliance with its AML obligations and the effectiveness of the prevention system.

The Annual Audit Plan will include the review of the prevention function, covering the functioning of the ICB and AMLTU and the overall effectiveness of the prevention system.

The internal audit shall be conducted annually and may be conducted in person or remotely at the discretion of the Corporate Audit Department.

The functioning of control measures and key aspects of the effectiveness of the system such as employee and management training, customer admission policy, transaction recording and the overall functioning of the system will be reviewed.

In order to carry out such a review, samples will be taken in order to give an opinion on the effectiveness of the prevention system.

The management of each Division shall be informed of the outcome of the audits carried out and the procedure established to ensure that any weaknesses or deficiencies detected are rectified within a reasonable period of time.

The report shall state the opinion on the degree of compliance with the recommendations document issued by SEPBLAC.

11.2 External expert

In addition, CIRSA Group's internal control procedures and bodies will be subject to an annual review by an external expert.

The results of the examination shall be set out in a confidential written report describing in detail the internal control measures in place, assessing their operational effectiveness and proposing, where appropriate, any corrections or improvements. The report, which shall include a detailed description of the professional background of the expert drafting it as an annex, shall in any case be available to the Executive Service for six years after it has been drawn up.

11.3 Annual report

Each year, the AMLTU shall draw up a specific report on all internal activities carried out in relation to the prevention of money laundering, which shall be submitted to the ICB for analysis and approval. This annual report shall include (where appropriate) documentation relating to:

- Communications to SEPBLAC.
- SEPBLAC requirements.

The following documents shall also be filed together in a folder intended for this purpose:

- Copy of the Minutes of the meetings held by the ICB.
- Copy of review reports of the Prevention Manual, issued by External Experts and/or Internal Audit.
- Changes in the structure and organisation of the ICB and AMLTU.

- Statistical data on the number of alerts, transactions subject to special analysis, implementation of improvements indicated by the external expert.

12. CONTROL OF SUBSIDIARIES

The Corporate AML Policy applies to all Group companies that are considered obliged entities, including subsidiaries located in third countries, without prejudice to the adaptations necessary to comply with the specific rules that must be provided for in the regulations of each country.

The principles that inspire this Manual are based on the aforementioned Corporate Policy, as are the Manuals that must be approved in each country following these same principles, adapted in each case to the rules that apply to them.

CIRSA Group has established a procedure to ensure that its majority-owned subsidiaries abroad have established and apply AML procedures and measures aligned with those established by the parent company, with the main measures:

- Appointment of an AML compliance officer in each country who will report to the AMLTU.
- Approval of a specific manual for each country, adapted to the applicable regulations and which includes the principles of the Corporate AML Policy.
- Preparation of a checklist detailing the main obligations in each country to be reviewed quarterly by the AMLTU.
- Delivery of the guide to AML functions to the country operational officers.
- The AMLTU will have a responsible technician who will ensure that each country complies with internal AML regulations and procedures.

The AMLTU coordinates the Compliance Officers in each country, who are responsible for the application of the money laundering prevention measures applicable to their jurisdiction, enforcing the principles set out in the Corporate Policy, as well as being in charge of direct control in this area, adapted to the regulations of each country and the manuals of each area.

The communication procedure with foreign entities is channelled through the quarterly report that compliance officers must send to the AMLTU, as established in the Guide to AML functions.