I. GENERAL PROVISIONS

MINISTRY OF FINANCE AND PUBLIC ADMINISTRATIONS

9659 *Resolution of 12 July 2012 by the Directorate General for the Regulation of Gambling, approving the provision establishing the model and content of the final certification report of the technical systems used by gaming operators and developing the change management procedure.*

Law 13/2011 of 27 May on the regulation of gaming establishes the framework regulations for state-wide gaming activities, in their different modes, in order to ensure public order is protected, combat fraud, prevent addictive behaviour, protect the rights of minors and safeguard the rights of participants in games.

Article 16 of this Law establishes that "entities that organise, operate and develop the games regulated within the scope of Law 13/2011 of 27 May on the regulation of gaming, must have the software, equipment, systems, terminals and instruments in general needed to carry out gaming activities, which must be properly approved", and makes the National Gaming Commission responsible for approving technical gaming systems, establishing the functional specifications needed and the procedure for certifying them.

Meanwhile, Article 6.1 of Royal Decree 1613/2011, of 14 November, implementing Law 13/2011 of 27 May on the regulation of gaming, regarding the technical requirements of gaming activities, establishes in fine that the National Gaming Commission approvals "may be based on reports certifying that the operator's technical gaming systems are suitable, issued by appropriate bodies designated for this purpose". Also, Article 8.1 of the same Royal Decree 1613/2011 rules that the National Gaming Commission will establish the minimum content of the reports issued by the entities appointed to certify the technical gaming systems.

Furthermore, final provision one of Royal Decree 1613/2011 makes the National Gaming Commission responsible for developing certain technical aspects specific to the marketing of the gaming activities governed by Law 13/2011 of 27 May on the regulation of gaming.

This Resolution, issued in compliance with the mandate of Article 8 of Royal Decree 1613/2011, is intended to establish the minimum content of the final certification reports issued by the designated bodies, and the forms to be used by them.

In accordance with temporary provision one of Law 13/2011 of 27 May on the regulation of gaming, the Directorate General for the Regulation of Gambling, part of the Ministry of Finance and Public Administrations, is responsible for developing and specifying the technical requirements established in Law 13/2011 and Royal Decree 1613/2011, of 14 November, which implements it.

This provision was subjected to a hearing on 22 May 2012, in which arguments were heard from the companies GLI Europe B.V.; Quinel, Quality in Electronics; Epoche and Espri, SL; Spread your Wings Spain, PLC; Bet365 Group Limited; Remote Gambling Association; PT Entretenimiento Online EAD; Betfair International PLC; and Electraworks España PLC.

Also, on 29 May 2012, a report was requested from the State Attorney's Office in the Secretary of State for Finance, and a favourable report was received on 4 July 2012.

In view of the above, the Directorate General for the Regulation of Gambling of the Ministry of Finance and Public Administrations agrees:
One.

To approve the provision establishing the form and content of the final report certifying the technical gaming systems of operators authorised in Spain, which is attached to this Resolution as Appendix I.

Two.

To approve Appendices II, III, IV, V, VI and VII, attached to this Resolution.

Three.

The references to the National Gaming Commission in the provision approved by this Resolution will be understood to refer to the Directorate General for the Regulation of Gambling of the Ministry of Finance and Public Administrations. Any references to the Chairman of the National Gaming Commission will be understood to have been made to the Director General for the Regulation of Gambling.

Four.

This Resolution will take effect the day after its publication in the Official State Gazette.

The interested party may present an appeal for review against this resolution before the Secretary of State for Finance, in accordance with Articles 114 and 115 of Law 30/1992 of 26 November on the Legal System for Public Administrations and Common Administrative Procedure, within one month from the day after its publication.

Madrid, 12 July 2012. The Director General for the Regulation of Gambling, Enrique
Alejo González.

CONTENTS

APPENDIX I

Provision establishing the form and content of the final report certifying the technical systems of gaming operators and specifying the change management procedure

One. *Purpose and scope.*

This provision is intended to establish the form and minimum content of the final report certifying compliance with regulatory requirements by the technical gaming systems used for developing and operating the games governed by the corresponding general or specific licence.

The final certification report will be issued by one or more of the entities appointed for this purpose by the National Gaming Commission, and will lead to obtaining approval for the operators' technical gaming systems. A report must be presented for each general or specific licence awarded to the operator in question.

The final certification report, with the form and minimum content established in this provision, covers the certification of the technical gaming systems of operators holding a general licence for operating and commercialising the game modes referred to in Article 3 (c), (e) and (f) of Law 13/2011 of 27 May on the regulation of gaming, and the types of games regulated until its publication date.

This provision is not intended to cover the approval of physical auxiliary terminals.

This provision also sets out the change management procedure referred to in Article 8.4 of Royal Decree 1613/2011, of 14 November, implementing Law 13/2011 of 27 May on the regulation of gaming, regarding the technical requirements of gaming activities, complementing the existing stipulations of section 4.13 of the Resolution of 16 November 2011 by the Directorate General for the Regulation of Gambling, which approves the provision establishing the technical specifications to be met by technical gaming systems.

Two. *Definitions.*

For the purposes of this provision, the terms used herein will have the meaning established in Section 1.2 of the provision establishing the technical specifications to be met by the technical gaming systems for which licences are awarded under Law 13/2011 of 27 May on the regulation of gaming, approved by a Resolution by the Directorate General for the Regulation of Gambling on 16 November 2011 (BOE of 18 November 2011).

Three. *Procedure and deadline for the approval of technical gaming systems.*

The initial approval procedure for technical gaming systems will take place within the framework of the procedure for issuing general and specific licences.

The final certification report or reports on operators' technical gaming systems must be presented by the interested party within the non-extendable period of four months from the date of notification of the resolution to award the general licence or provisional specific licence.

The final certification report consists of the following documents:

a) Description of the licensed technical system, filled in by the operator.
b) Final report certifying functionality.
c) Final report certifying security.
d) Report on the operator's compliance with regulations on the protection of personal data.

The approval procedure will begin when the final certification report is received by the General Register of the Ministry of Finance and Public Administrations as established in Article 38.4 of Law 30/1992 of 26 November on the Legal System for Public Administrations and Common Administrative Procedure. The procedures will begin in the order in which the reports are received.

The final certification report and the additional documentation and reports must be presented in electronic format. Only the identification, purpose and executive summary of the certification must be presented as a hard copy, duly signed by the person or persons authorised by the certifying entity.

If the operator should present the certification report electronically, it must ensure that the certification report is signed using a certificate issued within the scope of the General State Administration, in accordance with Law 11/2007, of 22 June, on electronic access by the public to public services, and the regulations implementing it.

The National Gaming Commission may require the interested parties to submit the documentation and information it deems necessary for the resolution of the approval procedure.

After receiving the final certification report and giving it a favourable assessment, the National Gaming Commission will approve the technical gaming systems in accordance with Article 16 of Law 13/2011 of 27 May on the regulation of gaming, in a maximum of six months from the date of notification of the licence award, without prejudice to an extension to this period for the time the interested party spent responding to any requirements issued by the National Gaming Commission after the presentation of the final certification report.

Four. *Description of the technical system to be licensed.*

For the description of the technical system to be licensed, the following documentation must be provided:

– Updated description of the technical system.
– In the case of specific licences, the specific rules.
– The descriptive questionnaire of the licence, which will state the scope of the technical gaming system to be certified.

The questionnaire will refer to all the technical elements used in the technical system to operate and market the game to be licensed, describe the technical infrastructure and identify the software elements used, specifying the manufacturer, product name and version.

In the cases where the certifying bodies must use the questionnaire in the certification reports, they must include the digital fingerprints of the elements classified as critical components.

The content of the questionnaire filled in by the operator must match the final certification reports presented. If not, the operator must provide reasons for any differences.

Five. *Certification reports.*

The operator must present a final certification report on the functionality of the technical gaming system and a final certification report on the security of the technical gaming system used to operate and execute the licensed game.

The final certification report on the functionality of the technical gaming system must be issued by one of the entities appointed by the National Gaming Commission to certify gaming software.

The final certification report on the security of the technical gaming system must be issued by one of the entities appointed by the National Gaming Commission to certify the security of the computer systems.

The final certification reports must accredit that the technical system actually used by the operator to develop and operate the licensed game meets the technical requirements required by gaming regulations, and report on the technical gaming system in use at the date of presentation.

The final certification reports which must be provided by the operator after a general licence is awarded must cover the user account, the gaming account, collection and payout management, the internal control system and the different terminals and/or applications which allow access by participants.

The final certification reports which must be provided by the operator after a provisional specific licence is awarded must cover the gaming software and, where relevant, the random number generator, the internal control system and the different terminals and/or applications which allow access by participants.

The operator in question may present each certification report only once, whether or not it is applicable to the approval process of one or more licences awarded to it. If this should be the case, after the first presentation of the certification report, it will be sufficient to refer to it and identify the procedure for which it was submitted.

The report will be written entirely in Spanish. The Appendices and supporting documentation for the report may be in Spanish or in their original language, in which case the National Gaming Commission may require the operator to provide a translation into Spanish, within ten days, of any of the Appendices or documents initially provided in another language.

Six. *Providers of gaming services.*

The technical gaming system actually used by the operator to operate and market the licensed game will include the systems of all gaming service providers participating in the overall system.
The applicant operator must take responsibility for standardising the entire technical gaming system and presenting final certification reports which must include the technical systems of all gaming service providers.

Seven. *Report certifying functionality.*

The final functionality certification report will assess how the technical gaming system actually used by the operator to develop and operate the licensed game complies with the technical requirements.

In general licences, a single report will be presented which covers all areas.
In specific licences, various reports may be submitted when the software of the games or modes included in the report is completely separate from the software of the games or modes in other reports. In all cases, each report must provide evidence of compliance with all the technical requirements for the games and modes included and the internal control system and integration with the gaming platform.
The form and minimum content of the final functionality certification report are shown in Appendix III of the Resolution approving this provision.
The final functionality certification report will include at least three sets of tests or analyses:

a) Tests to evaluate compliance with the technical requirements:

To evaluate compliance with the technical requirements, the certifying entity may choose the test or tests it considers most suitable. The list of technical requirements is given in Appendix V of the Resolution approving this provision.
The certifying entity issuing the report may carry out any of the tests referred to in an environment other than that actually used by the operator to develop and operate the licensed game, but in all cases the certification issued must refer to the technical gaming system actually used by the operator. In cases where environments are used other than that actually used by the operator, the certifying entity must certify, accepting liability, that the results obtained in the testing environment can be extrapolated to show the results which would have been obtained if they had been carried out in the technical system actually used by the operator to develop and operate the licensed game, having assessed that any differences between the testing environment and the technical gaming system actually used do not affect the quality of the test results.

b) Specific analyses of important functionalities:

The certifying entity must carry out a specific analysis of certain especially important functionalities.
For general licences, procedures to check identity and causes for individual bans will be analysed, and measures to combat fraud and money laundering will be evaluated. For specific licences, the logic of the game will be analysed and, where applicable, the return to player percentage and the random number generator.

c) Integration tests:

The certifying entity must design and carry out the integration tests needed to accredit compliance with the requirements of the technical gaming system actually in use.
The integration tests must always be carried out on the technical gaming system actually used by the operator to develop and operate the licensed game. A different environment cannot be used for this purpose.
The integration tests must include at least those described in Appendix VI of the Resolution approving this provision.
The integration tests are intended to analyse real data generated during the development and operation of the gaming activity by the operator. These integration tests with real data require the

technical gaming system to have at least one month's worth of data, and cannot be carried out in test environments or simulations. In cases where, at the time of presenting the final certification report, the operator has not begun operating the gaming activity, the report may be presented without providing the results of these tests, although the approval will remain conditional on these results being presented and then favourably assessed by the National Gaming Commission. The result of the tests which analyse real data generated during the development and operation of the gaming activity, if not presented with the final certification report, must be presented within three months from the start date of the corresponding gaming activity.

The final functionality certification report will include a copy of the binary file of the certified software and a digital fingerprint of the components classified as critical.

Eight. *Reports certifying security.*

Security certification tests may only be carried out on the technical gaming system actually used by the operator to develop and operate the licensed game, and the security procedures, processes, plans and measures actually implemented.
The operator may request a single security certification report from the certification authority, which covers the entire technical gaming system. This certification can then be used in the authorisation processes for each of the licences awarded to them.
In the event that one or a number of gaming service providers form part of the technical system used by the operator to develop and operate the game which is the object of the corresponding licence, the applicant must submit a final certification report on the security of the technical infrastructure for each of the providers.
The form and minimum content of this final certification report on security are shown in Appendix IV of the Resolution approving this provision.
The final report certifying security will consist of two parts. In the first, the certifying entity will accredit compliance with the security requirements listed in Appendix VII of the Resolution approving this provision. It will be possible to partly validate compliance with the technical security requirements when the security management system to be certified holds an ISO 27001 certificate with an identical scope, current at the date of applying for approval. The security requirements that can benefit from this certificate are listed in Appendix VII. The certifying entity must attach a copy of the ISO 27001 certificate, which clearly states the recipient, the scope of the certificate, and the period for which it is valid.
In the second part, the certifying entity must carry out specific audits of the list of critical components, change management, business continuity management and the prevention of data loss.

Nine. *Compliance with regulations on the protection of personal data.*

Together with the final certification report, the operator will present a report describing its compliance with the regulations on the protection of personal data.
This will be a single report per operator and will be applicable across the different general and specific licences it holds.
The National Gaming Commission, in compliance with Article 16.4 of Law 13/2011 of 27 May on the regulation of gaming, will request a report from the Spanish Data Protection Agency.

Ten. *Procedure for managing changes in the technical gaming system.*

Operators must have a documented change management procedure for monitoring changes in the equipment and components of the technical gaming system effectively used.

a) There will be a formal process for internally approving all changes, which must involve a request to make the change and its approval by the corresponding management figures.
b) In the case of changes to critical components, these must be evaluated to decide whether the change is significant.
c) Requests for changes and the decisions made will be recorded and may later be audited.
d) Copies must be kept of the binary files of the software elements of all versions of the software used in the technical system actually in use over the last four years. The National Gaming Commission may establish the obligation for the binary file archiving procedure to

include a digital fingerprint of the files.

Any significant change to a critical component will require prior approval from the National Gaming Commission, following the presentation of the corresponding certification report. The National Gaming Commission will rule on the authorisation of significant changes to critical components within one month from the date of reception of the operator's application.

The National Gaming Commission may classify as critical other components in addition to those listed in the final certification reports or classified as such by the operator.

In the case of special emergencies affecting security, duly accredited and reported to the National Gaming Commission, the operator may make significant changes to critical components and request their authorisation later. In such cases, to obtain approval, the operator will present a report accrediting the exceptional circumstances and the risk to the security of the technical gaming system, together with the certification report, to the National Gaming Commission.

From the awarding of the licence to the operator presenting the final certification reports, any changes to the technical gaming system will not need prior authorisation, although the National Gaming Commission must be notified of any significant changes from the technical project originally evaluated for awarding the licence 15 days before they are implemented. If the National Gaming Commission considers any of the changes made to be in breach of gaming regulations, it may require their immediate reversal.

After obtaining approval, the operator will draw up a quarterly report describing all the changes made to the technical gaming system and send this to the National Gaming Commission. This will include the following documentation:

– An executive summary in Spanish explaining the changes made in qualitative terms.
– A description of the updated technical system for which the licence was awarded, with the content described in Article 4 of Appendix I to the Resolution approving this provision.

The National Gaming Commission may establish an obligation for the quarterly report describing all the changes made to the technical gaming system to include the digital fingerprint of the binary files.

The National Gaming Commission will request any information it deems necessary from the operator regarding the changes made.

If the National Gaming Commission considers any changes made to critical components to be significant, it will require the operator to seek approval for the changes, without prejudice to the possibility of requiring the operator to roll back the change until the relevant approval is obtained.

Eleven. *Digital fingerprints.*

The following guidelines should be followed for obtaining the digital fingerprint of the software referred to in this Resolution:

a) The SHA-1 algorithm will be used, unless there are technical reasons making it advisable to use another algorithm, which must be previously authorised by the National Gaming Commission.
b) The digital fingerprints must be accompanied by the tool or procedure used to obtain them, and the tool or procedure used to validate them. The necessary tools must be attached on a digital medium, or a location given where they are available publicly and free of charge.
c) In the case of tools protected by a patent or intellectual property rights, details must be provided as to how the National Gaming Commission and any other certifying entity can have free access and rights to use the tools.

APPENDIX II

Descriptive licence questionnaire

The questionnaire will gather information on the technical elements used in the technical system to develop and operate the game specified in the corresponding licence.

The questionnaire may include, among others, the following information:

- Identification of the operator and the licence.
- Description of the gaming offer.
- Description of the communication channels used.
- Description of the means of payment accepted.
- Description of the means used to check identity and individual bans.
- Description of the providers of gaming services.
- Description of the providers of gaming software.
- Description of the technical infrastructure.
- Description of the software elements used.
- Description of the associated data.
- Description of the applications for access by the participant.
- Description of the physical auxiliary terminals.

The questionnaire may also include any other information on the technical gaming system of relevance for its approval.
To make it easier to fill in, it will be published in electronic format on the National Gaming Commission website.
The National Gaming Commission may update the content and format of the questionnaire. The questionnaire to be used in all cases will be the most recently published.

APPENDIX III

Form and minimum content of the report certifying functionality

The final functionality certification report will be structured in sections with the minimum content listed below:

1. Identification of the certificate.
2. Description of the certification subject.
3. Executive summary of the functionality certificate.
4. Details on compliance with the technical requirements.
5. Details of specific analyses.
6. Details of the integration tests.
7. Description of the location, equipment and dates of the certification tests.
8. Description of the environments used for the test if different to the environment actually used by the operator for the gaming activity.
9. Description of the digital format to accompany the certification report.

1. *Identification of the certificate*

The first page of the report will include the following information:

a) Type of certification report: It will be marked "final certification report on functionality".
b) Code identifying the report: The report will be identified by a unique code, clearly differentiating it from any other report issued by the certifying entity. Each time the certifying entity modifies a report, a new identification code must be created for it.
c) Identification of the certifying entity.
d) Identification of the person signing the report on behalf of the certifying entity. e) Dates of the certification tests.
f) Issue date of the certification report.

2. *Description of the certification subject*

The certification subject will explain the scope of the technical gaming system being certified and refer to the technical elements used in the technical system to develop and operate the licensed game, describing the technical infrastructure and identifying the software elements used, specifying the manufacturer, product name and version, and identifying the element of the technical infrastructure in which they are installed.
For this purpose, the certifying entity will fill in the descriptive questionnaire for the licence referred

to in Appendix II of the Resolution approving this provision. The questionnaire must also be attached on an electronic medium.

3. *Executive summary of the functionality certificate*

3.1 Overall functionality classification.

The report will include an overall classification of compliance with the technical requirements by the technical gaming system actually used by the operator for the licensed activity. The classification may be "Compliant" or "Non-compliant".
The classification may be "Compliant" only when the certifying entity considers the technical gaming system actually used by the operator for the licensed activity to meet all the applicable requirements.

Overall functionality classification.	The overall result of the analysis will be classified as "Compliant" or "Non-compliant".

3.2 Table summarising compliance with the technical requirements.

The areas of requirements where compliance must be certified for each licence are described in Appendix V of the Resolution approving this provision.
For each requirement a classification must have been obtained, which can be "Compliant", "Non-compliant", or "Not applicable".
The technical requirements have been grouped into areas.
The executive summary will present a summarised table with the number of requirements for classification in each area.
The classifications will be detailed as follows:

	Number requirements	Number requirements compliant	Number requirements non-compliant	Number requirements not applicable
Area XXX	7	6	0	1
Area YYY	4	4	0	0

3.3 Table summarising the specific analyses.

The certifying entity must carry out specific analyses of certain especially important functionalities. In some cases, the analyses carried out will need to be listed in a later section.

3.3.1 Analysis of methods used to check identity and gambling bans.

This analysis will be applicable for general licences only.

Classification.	The overall result of the analysis will be classified "Compliant" or "Non-compliant" with the technical requirements for this area.

General data

Accepts non-resident participants.	Yes/No.

Play is allowed without a user account.	Yes/No. If so, list the games in which this is allowed.
Channels used for proof of identity.	Give a list of the channels: internet, telephone, text message, in-person,

Checks before activating the user account

Uses the identity verification service provided by the National Gaming Commission for residents.	Yes/No. If this service is used but not for all the cases, indicate when.
Other methods of checking identity.	List of other methods used to verify identity
Identification documents accepted for non-residents.	List of documents accepted as proof of identity for non-residents
Check of legal age.	Yes/No.

Uses the service checking inclusion in the RGIAJ.
Yes/No.

Checks for associated individuals.	Yes/No.

Checks before prize payouts

Uses the service to check for changes in the RGIAJ list hourly and updates the operator's banned list.	Yes/No.

3.3.2 Analysis of the random number generator.

This analysis will be applicable only to specific licences where a random number generator, or RNG, is used.

Classification.	The overall result of the analysis will be classified as "Compliant" or "Non-compliant" with the technical requirements of this area.
Manufacturer.	Information on the manufacturer of the RNG.
Product and version.	Name and version of the software element.
Digital fingerprint.	Digital footprint of the binary.
Type of RNG.	This will indicate: – hardware RNG. – software RNG.
Random/Pseudorandom.	This will indicate: – Random. – Pseudorandom. If random, this will indicate the name of the phenomenon on which it is based.

Shared RNG.	This will indicate one of the following values: – RNG instance not shared with other games. – RNG instance shared with other games. Indicate which. – RNG integrated in the gaming software. – Others. Describe.
Algorithm.	In the case of hardware RNG, this will indicate the name of the phenomenon on which it is based. In the case of software RNG, give the name of the algorithm and of the libraries or calls to the operating system on which it is based. If based on a proprietary algorithm, indicate this.
Reseeding.	Yes/No to indicate if a reseeding procedure is included.
Length of the space.	Length in bits of the space of different random numbers.
List of statistical tests.	List of names of the statistical tests carried out.

3.3.3 Analysis of the return to player percentage.

This analysis will be applicable only to specific licences in games with a return to player percentage.

Published return to player percentage for the game	Indicates the return to player percentage published by the operator for each game.
	This will also indicate the place where the return to player percentage is published.

.

3.3.4 Analysis of the logic of the game and random events.

This analysis will be applicable for specific licences only.

Compliance with specific game rules.	Yes/No.
Risk management system for fixed odds bets.	Indication of custom development or the name of the product or service used.
Auditing changes in the configuration through parameters of the fixed odds betting risk management system.	Yes/No.
Auditing changes made by the operator's personnel to bets.	Yes/No.
List of random events.	List of events in which the random number generator is involved, indicating whether they are pre-drawn.
Auditing changes in the configuration through game logic parameters.	Yes/No.

3.3.5 Measures to combat fraud and money laundering.

This analysis will be applicable for general licences only.

Existence of technical measures against fraud and money laundering.	Yes/No.

3.4 Table summarising the integration tests.

This table will include the classification of the integration tests carried out, classified by areas, which must include at least those described in Appendix VI.
The names of tests in addition to those described in Appendix VI will start with "X".
The results will be listed as follows:

Area and reference of the requirement	Classification

Area of requirements A

A.1 Name of the test.	. Compliant.
A.2 Name of the test	Not applicable.
A.3 Name of the test.	Non-compliant.
X.1 Name of the additional test.	Compliant.
X.2 Name of the additional test	Compliant.

Area and reference of the requirement	Classification

Area of requirements B

B.1 Name of the test.	Compliant.
B.2 Name of the test.	Not applicable.
X.3 Name of the additional test.	Compliant.

4. *Details on compliance with the technical requirements*

The technical requirements where compliance must be certified for each licence are described in Appendix V of the Resolution approving this provision.
For each requirement a classification must have been obtained, which can be "Compliant", "Non-compliant", or "Not applicable".
This section will list the compliance of each technical requirement. The requirements are grouped by areas.
The following must also be noted in the comments space:

– When the requirement could be classified as "Not applicable", and why.
– When there are incidents, even if these are later corrected.
– When the tests were carried out in an environment other than that actually used by the operator for the gaming activity.

The classifications will be detailed as follows:

Area and reference of the requirement	Classification	Comments
Area of requirements X:		
Reference A	Compliant.	
Reference B	Non-compliant.	The requirement was not met
Reference C	Not applicable.	The requirement is not applicable because...

The certifying entity must submit an Appendix documenting proof of the tests carried out and results obtained for each technical requirement.

5. *Details of specific analyses*

For certain particularly important functionalities, the certifying entity must carry out various specific analyses, described in this section.

5.1 Analysis of methods used to check identity and gambling bans.

The certifying entity will analyse the checks of identity and gambling bans.
The analysis must describe at least the following:

– General data:

o Whether the system accepts non-resident participants.
o Whether the system allows play without a user account. The certifying entity will describe the game or games in which this circumstance may arise.
o The list of channels which can be used to accredit identity: internet, telephone, text message, in-person, or others.

– Checks made before activating the user account:

- o Whether the identity verification service provided by the National Gaming Commission for residents is used.
- o List of other methods used to verify identity.
- o Checking legal age.
- o Use of the service to check inclusion in the RGIAJ.
- o Checking for associated individuals.

- Checks made before prize payouts:

- o Uses the service to check for changes in the RGIAJ list hourly and updates the operator's list of people banned from gambling and the status of the affected participants.

5.2 Analysis of the random number generator.

This analysis will be applicable only to specific licences where a random number generator, or RNG, is used.

The certifying entity will describe the analyses and tests carried out to prove the random behaviour of the RNG and compliance with the technical requirements. This will include the supporting summaries or graphs, the number of simulations carried out, the parameters used, and the confidence interval.

The certifying entity will indicate whether there are reseeding procedures and if they comply with the technical requirements.

If the RNG functionality may depend on configuration parameters, these will be described and the configuration values for which the certification was carried out will be indicated.

5.3 Analysis of the return to player in the games.

The certifying entity must describe the return to player percentage published by the operator for each game. It must also verify the place where the percentage was published.

The certifying entity must describe all the configuration parameters which may affect the return to player percentage, and whether the technical gaming system permits the recording of audits of the changes in these parameters.

5.4 Analysis of the logic of the game and random events.

The certifying entity must accredit that the game operates according to its specific rules in each of its variants.

The certifying entity must analyse certain aspects of the game logic, the random events in the game, the parameterisable configurations, the game accounting and, in general, the capacity to audit any change introduced in the bets or winners manually.

This analysis will be applicable for specific licences only.

In the case of bets:

– Risk management system.

For fixed odds bets, the risk management system will be described, indicating whether a commercial application or custom development has been installed for this purpose.

It must be indicated whether the system used is parameterisable. If it is, the most important configuration parameters and the values configured at the time of certification must be described.

Also, the certifying entity will include in this report whether the application saves a record of the changes to the system affecting risk management. If so, the files or tables in the database where this information is stored will be indicated.

– Auditing bets.

The certifying entity must explain the application to manage bets, and to record and track any modifications which can be made through back office applications by the operator's personnel, including an analysis of at least:

- o Changes in the data of a bet.
- o Insertion of new bets.
- o Deletion of bets.
- o Changes in the result of the event.
- o Changes in the adjudication of prizes.

Change audits, and how manipulation of audits is prevented, will be described.
The files or tables in the database where auditing information is stored must be described.

– Management of funds.

In parimutuel betting, the application which manages the accounts of funds must be analysed.
The application will explain the records and auditing of gaming funds, the distribution of prizes, cases when there are no winners in a category, or any other movement.

In casino games, poker and complementary games:

– It will describe each of the random events implemented in the game involving the random number generator. For example, if there is an initial shuffling of cards, drawing cards from the deck if there is no initial shuffle, the production of bingo cards, the sale of bingo cards, the pre-drawing of bingo balls, the drawing of a bingo ball if not pre-drawn, the spin of the roulette wheel, etc.
– It must analyse the accounting management of the individual games or rounds, and the rollover prizes in games which allow them. The amounts wagered, the prizes won, the commissions calculated and the rollover prizes set up or applied must be auditable.
– Auditing individual games or rounds.
The certifying entity must explain the recording and tracking of any modifications made through the back office applications by the operator's personnel.
Change audits, and how manipulation of audits is prevented, will be described.
The files or tables in the database where auditing information is stored must be described.
– If the software used to implement the game logic is configurable, the certifying entity must describe and indicate the value of the configuration parameters relating to the following aspects:

- Game modes.
- Game strategy of the bank or level of risk assumed.
- Maximum amounts.
- Game rules.

The certifying entity must also accredit that there is a record of the auditing of any modifications of these parameters.

5.5 Measures to combat fraud and money laundering.

This analysis will be applicable for general licences only.
The certifying entity will describe and assess the measures implemented in the technical gaming system to combat fraud and money laundering.

6. *Details of the integration tests*

This section will detail the integration tests carried out, classified by areas, which will include at least those described in Appendix VI of the Resolution approving this provision.
The names of these tests, which are in addition to those described in Appendix VI,
will start with "X".
The result of each test will be classified as "Compliant", "Non-compliant", or
"Not applicable", according to the expected result and compliance with regulations.
Each test will be detailed as follows:

Area.	Of Appendix VI.
Test reference.	Of Appendix VI or "X***" for additional tests.
Test name.	
Test description.	
Expected result.	
Type of test.	According to the classification of types of test in
Date/time the test was carried out.	
Result obtained.	
Classification.	
Comments.	

As the result obtained, the certifying entity must deliver an Appendix that includes and documents proof of the result of the integration tests. The proof to be included will depend on the type of test to be carried out, as described in Appendix VI of the Resolution approving this provision.

7. *Description of the location, equipment and dates of the certification tests*

This section will describe the equipment used for the certification tests, and when and where they were performed.

8. *Description of the environments used for the test if different to the environment actually used by the operator for the gaming activity.*

If some of the tests of the technical gaming system were carried out in an environment other than that actually used by the operator to develop and operate the licensed game, in this section the certifying entity must describe the different environments used.
There must be a list of the tests carried out in each environment.

9. *Description of the digital format to accompany the certification report.*

This section will describe the content of the digital medium which will accompany the certification report.

The certification report will be accompanied by information on a digital medium, structured as follows:

– Complete certification report in digital format.
– Descriptive questionnaire of the subject of the certification in digital format.
– Proof of the assessment of the technical requirements. This will be grouped in a folder titled "Technical requirements".
– Proof of the integration tests. This will be grouped in a folder titled "Integration".
– Copy of the software elements of the technical gaming system, containing a copy of the binary files of the software elements of the certified technical gaming system. These should be grouped in a folder titled "Binary files" structured with sub-folders with the name of each of the software elements indicated on the questionnaire.

APPENDIX IV

Form and minimum content of the report certifying security.

The final security certification report will be structured in sections with the minimum content listed below:

1. Identification of the certificate.
2. Description of the certification subject.
3. Executive summary of the security certificate.
4. Details on compliance with the security requirements.
5. Details of the specific audit analyses.
6. Description of the location, equipment and dates of the certification tests.
7. Description of the digital format to accompany the certification report.

1. *Identification of the certificate*

The first page of the report will include the following information:

a) Type of certification report: It will be marked "final certification report on security".
b) Code identifying the report: The report will be identified by a unique code, clearly differentiating it from any other report issued by the certifying entity. Each time the certifying entity modifies a report, a new identification code must be created for it.
c) Identification of the certifying entity.
d) Identification of the person signing the report on behalf of the certifying entity. e) Dates of the certification tests.
f) Issue date of the certification report.

2. *Description of the certification subject*

The security certification will be carried out on the technical gaming system actually used by the operator to develop and operate the licensed game, and the security procedures, processes, plans and measures actually implemented.

For the purposes of describing the scope of the security certification, there will be a list of the data processing centres (DPC) where the technical gaming system is hosted and where the security procedures, processes, plans and measures are implemented.

DPC	Street, number	City	Country	Type	Name of the hosting provider
DPC 1					
DPC 2					
……..					

The fields "street", "number", "city" and "country" refer to the physical location of the DPC. The field "type" indicates the form of housing of the DPC and must match one of the following values: "hosting", "housing" or "own".
The field "name of the hosting provider" need be filled in only if "type" contains one of these values: "hosting" or "housing".

3. *Executive summary of the security certificate*

3.1 Overall security classification.

The report will include an overall classification of compliance with the technical security requirements by the technical gaming system actually used by the operator for the licensed activity. The classification may be "Compliant" or "Non-compliant".
The classification may be "Compliant" only when the certifying entity considers the technical gaming system actually used by the operator for the licensed activity to meet all the applicable requirements.

Overall functionality classification.	The overall result of the analysis will be classified

as

"Compliant" or "Non-compliant".	ISO 27001 validation. This will indicate whether the report uses the option of validating certain requirements based on ISO 27001 certification.

3.2 Table summarising compliance with the security requirements.

The security requirements where compliance must be certified for each licence are described in Appendix VII of the Resolution approving this provision.
For each requirement a classification must have been obtained, which can be "Compliant", "Validated", "Non-compliant" or "Not applicable".
The technical requirements have been grouped into areas.
The executive summary will present a summarised table with the number of requirements for classification in each area.
The classifications will be detailed as follows:

	Number of requirements	Number of requirements complied with	Number of requirements validated (ISO 27000)	Number of requirements not complied with	Number of non-applicable requirements
Area XXX	7	6	0	0	1
Area YYY	4	3	1	0	0

3.3 Table summarising the specific audit analyses.

For certain particularly important security areas, the certifying entity must carry out various specific analyses of audits, described in another section below.
This section will provide an executive summary of these analyses:

3.3.1 Analysis of audits of critical components.

Classification.	The overall result of the analysis will be classified as “Compliant" or "Non-compliant" regarding the correct identification of critical components.

3.3.2 Analysis of audits of change management.

Classification.	The overall result of the analysis will be classified as "Compliant" or "Non-compliant" with the technical requirements of this area.

3.3.3 Analysis of audits of business continuity management and the prevention of information loss.

Classification.	The overall result of the analysis will be classified as "Compliant" or "Non-compliant" with the technical requirements of this area. A "Compliant" result means the certifying entity is satisfied that the operator's technical system can achieve the recovery times or data loss figures specified in this section.
Maximum recovery time objective.	This will indicate the worst of the disaster recovery time objectives (RTO) provided by the operator.
Maximum recovery point objective.	This will indicate the worst disaster recovery point objectives (RPO) provided by the operator.

4. *Details of compliance with the security requirements*

The security requirements where compliance must be certified for each licence are described in Appendix VII of the Resolution approving this provision.
For each requirement a classification must have been obtained, which can be "Compliant", "Non-compliant", or "Not applicable".
This section will list the compliance of each technical requirement. The requirements are grouped by areas.
The following must also be noted in the comments space:

– When the requirement could be classified as "Not applicable", and why.
– When there are incidents, even if these are later corrected.

If the report uses the option of validating certain requirements based on ISO 27001 certification, the classification "Validated" will be used, and "ISO 27001" noted in the comments field.

The classifications will be detailed as follows:

Area and	Classifi	Comments	Documentary
Area of requirements X:			
Requirement	Satisfa		Document XXXXX
Requirement	Non-	The requirement was not	
Requirement YY.	Not	The requirement is not	
Requirement	Validat	ISO 27001	

The certifying entity must deliver an Appendix attaching the security documentation, and all evidence confirming compliance with the requirements.
In cases where there is documentation supporting the policy or procedure, the documentary reference and the section supporting compliance must be noted in the comments field.
The certifying body must accredit the effective application of security controls in the technical gaming system actually in use. For this purpose, the tests carried out in addition to documentary checks will be described.

5. *Details of the specific audit analyses.*

For certain particularly important security areas, the certifying entity must carry out the specific analyses of audits described in this section.

5.1 Analysis of audits of critical components.

The certifying entity will issue an analysis of the correct identification by the operator of the critical components of the technical gaming system.
The certifying entity will include the list of critical components of the technical gaming system, indicating whether their security has been reinforced. It must indicate what software element or elements in the questionnaire presented by the operator correspond to each component on the list.

5.2 Analysis of audits of change management.

The certifying entity will issue an analysis of the correct implementation of the change management procedure.
The certifying entity will attach the proof and documentation, if any, associated with the last three change management procedures carried out by the operator before the time of this analysis.
If a software tool is available for change management, indicate which. The certifying entity must also accredit that any action (introduction, modification or withdrawal of changes) can be audited.

5.3 Analysis of audits of business continuity management and the prevention of information loss.

The certifying entity must analyse the maximum recovery time objective (RTO) given by the operator and assess whether the technical measures available are sufficient to achieve it. The analysis must describe the technical measures and the use of redundancy, security backup plans, backup centres and other measures.

The certifying entity must analyse the maximum recovery point objective (RPO) given by the operator and assess whether the technical measures available are sufficient to achieve it. The analysis must describe the technical measures and the use of redundancy, security backup plans, backup centres and other measures. The certifying entity must make sure that the available measures protect all the operator's data, both for users and for the games.
As a disaster case, it must evaluate the possibility of an incident which makes a physical location totally unusable in the case of an unforeseen contingency.

6. *Description of the location, equipment and dates of the certification tests*

This section will describe the equipment used for the certification tests, and when and where they were performed.

7. *Description of the digital format to accompany the certification report.*

This section will describe the content of the digital medium which will accompany the certification report.
The certification report will be accompanied by an appendix in digital, structured as follows:

– Complete certification report in digital format.
– The complete security documentation used for evaluating security, gathered in a folder titled "Documentation".
– Proof of the evaluation of technical requirements regarding security. This will be grouped in a folder titled "Technical requirements".

ISO 27001 certification, if provided for validation.

APPENDIX V

List of technical requirements for functionality.

The different requirements to be subject of certification are established by gaming regulations: Law, Royal Decrees, Ministerial Orders and Resolutions.
Only the obligations established in the regulations which are directly related with the technical evaluation of equipment, software or instruments will be subject to technical gaming system certification.
This section aims to offer a guide to all the different regulatory texts that need to be taken into consideration for certifying functionality.
The requirements are grouped into areas and include the terms to be used in the final report on functionality certification.

Areas:

General licences:

– Area: Responsible gaming.
– Area: Contract. Acceptance, backup copy and modifications.
– Area: User account and checking bans.
– Area: Gaming account, charges and payouts.
– Area: Limits on deposits.
– Area: Register and traceability.
– Area: Terminals and session.
– Area: Communication channels.

– Area: Free gaming applications.
– Area: Internal control system.

Specific licences:

– Area: Return percentage and tables of prizes.
– Area: Random number generator.
– Area: Game logic.
– Area: Register and traceability.
– Area: Terminals and session.
– Area: Communication channels.
– Area: Free gaming applications.
– Area: Graphic interface.
– Area: Behaviour in response to technical errors.
– Area: Automated gaming.
– Area: Repetition of the bet.
– Area: Live gaming.
– Area: Various functionalities.
– Area: Rollover prizes.
– Area: Internal control system.
– Area: Game operation.
– Area: Financial limits on participation.
– Area: Obligations with regard to sharing information with participants
– Area: Promoting games

APPENDIX VI

List of minimum integration tests

This Appendix describes the mandatory tests to certify the integration of operators' technical gaming systems.
The integration tests must always be run on the environment actually used by the operator to develop and operate the licensed game.
For integration tests requiring the personal information of residents in Spain, the certifying entity may use the test games to be provided for this purpose by the National Gaming Commission for the production environment of the online verification services.
The tests are classified according to the type of licence.
The following types of test are defined, with the minimum proof to be provided for each one:

a) Functional.

Functional tests will consist of the evaluation of the external characteristics of an application or system using the same means available to a participant, or the management applications available to the operator's personnel.
The minimum proof to be provided is:

- o Compliance or non-compliance of the test
- o Screen captures of the interaction between the participant or operator personnel performing the test and the gaming platform.

b) Traceability.

Traceability tests will consist of the analysis and testing of the records and the traces generated in the system when the described test is performed. The records and traces of this type of test will be those of the information system of the Central Gaming Unit, not the internal control system.
The minimum proof to be provided is:

- Compliance or non-compliance of the test
- Screen captures showing the information of the recorded or tracked subject.
- Description of the information source (file, table, etc.) where the record or trace is obtained.

c) Real data.

The real data analysis will consist of checking for the correct accounting, format and integrity of the data generated by the interaction between participants and the technical gaming system.
These integration tests with real data will require the technical gaming system to have at least one month's worth of data, and cannot be carried out in test environments or simulations.
The minimum proof to be provided is:

- Compliance or non-compliance of the test
- The source (file, tables, etc.) where the information was obtained.
- The representative data required for each test.

The minimum integration tests, according to the type of licence, and classified by areas are:

A. General licences

A.1. User account and checking bans.

Test reference	A.1.1
Test name	Creation of the user account
Type of test	Functional, traceability
Test description	From the point of view of a participant, the registering of: - A participant resident in Spain with correct identity information, of legal age and not registered with the RGIAJ. - A non-resident participant. This test must be performed by all operators, whether or not a user account is required to participate in the game or to record the winners.
Expected result	The result will include the DNI/NIE (personal identification numbers), date and time of each user account created, so that the National Gaming Commission can verify a posteriori whether the CNJ verification services were consulted. The registration of the non-resident will include the code used to identify the client, and the date and time of the tests. Functional This must check whether the user has been registered in the system. The system must record all the information fields of the participant described in RES_TEC Appendix I section 2.1.1. In the case of a non-resident participant, the system must request a copy of an identification document. Traceability The records and traces of the system used to collect the data from new user accounts will be analysed. The traceability of the acceptance of the gaming contract signed by the player must be verified.

Test reference	A.1.2
Test name	Checking individual gambling bans
Type of test	Functional, traceability
Test description	From the point of view of a participant, the registering of: - A participant resident in Spain who provides incorrect identity information. - A participant resident in Spain, with correct identity data, who is registered with the RGIAJ. - A participant resident in Spain, with correct identity data, who is under the legal age. - A non-resident participant under the legal age. The test must use the operational verification services of the National Gaming Commission.
Expected result	The result will include the DNI/NIE (personal identification numbers), date and time of each user account created, so that the National Gaming Commission can verify a posteriori whether the CNJ verification services were consulted. Functional The system must not permit the registration of participants who are underage, registered with the RGIAJ or whose identification data are found to be incorrect. Traceability The records and traces of the system used to collect the data from new user accounts will be analysed.

A.2. Gaming account, charges and payouts.

Test reference	A.2.1
Test name	Correct recording of operations in the gaming account
Type of test	Functional, traceability
Test description	From the point of view of the participant, operations will be performed to deposit and withdraw money in the gaming account. The existence of other operations available in the gaming account will be noted.
Expected result	The result will include the DNI, date and time, and a description of each operation, so that the National Gaming Commission can verify a posteriori whether the data are received correctly in the internal control system. Functional The correct accounting of deposits and withdrawals in the gaming account will be checked. If other operations are available in the gaming account, they will be listed in the result. It will be checked that none of the operations permit credit to be received from the operator or transferred between participants. Traceability The records and traces of the system used to collect the accounting data for deposits and withdrawals will be analysed.

A.3. Limits on deposits.

Test reference	A.3.1
Test name	Deposit over the limits.
Type of test	Functional, traceability
Test description	The system will be accessed from an account with a daily, weekly or monthly limit on deposits by default. The limits will be lowered to 10, 15 and 20 euros respectively. Deposits will be made below the limit. Deposits will be made above the limit. Each limit must be tested, whether daily, weekly or monthly, at different times of day.
Expected result	Functional The system lets limits be reduced. The system allows deposits below the limit and not above it. Traceability The records and traces in the system showing changes to the limits will be analysed.

Test reference	A.3.2
Test name	Data on deposit limits
Type of test	Real data
Test description	Real data in the system will be consulted to check how many participants have amounts higher than those initially established. If there are participants whose limits are higher than those initially established, it must be checked that the necessary requests to increase the limits have been made and evaluated correctly. For the purposes of this test, it is enough to check a sample of 5 participants, if available.
Expected result	The results will include the "PlayerId" identification codes of the participants analysed, indicating the dates of the requests to increase the limits, and the dates they were authorised. It will be checked that the system saves records and traces of limit increase requests, analyses and authorisations.

A.4. Internet. Redirection to an ".es" domain.

Test reference	A.4.1
Test name	Redirection to an ".es" domain.
Type of test	Functional
Test description	The operator will provide the certifying entity with the list of domain names, other than ".es" domains, where it, its parent company or its subsidiary companies offer the games. The certifying entity will access each site from an IP address associated with Spanish territory and check the redirection.
Expected result	It will be checked that the sites redirect to an ".es" domain. The certifying entity will list the different ".es" domain names used in the test.

A.5. Internal control system.

Test reference	A.5.1.
Test name	Integrity of the ICS data.
Type of test	Real data
Test description	This test will compare the data in the ICS (internal control system) with the data in the operator's computer system, in order to evaluate the integrity of the ICS data. The following monthly data will be obtained for each month: Based on the monthly RUT records: o Number of accounts created o Number of participants per status. Based on the monthly CJT records: o Initial balance o Deposits o Withdrawals o Stake o Repayment of the stake o Prizes o Final balance o Prizes in kind o Other movements. This test requires the certifying entity to access unencrypted real data. The operator must provide unencrypted monthly RUT and CJT files to the certifying entity, which must check that these match the data actually stored in the operator's computer system. The certifying entity is not required to access RUD or CJD files or have access to personal data. In no case is the certifying entity required to know the encryption key.

Expected result	The certifying entity will check what certificate is used to sign the data and will accredit that this certificate is valid and has not been revoked. The certifying entity will indicate in the result the public part of the certificate used to sign the stored data. For the monthly RUT: - The data in the RUT file will be compared with lists obtained from the technical gaming system back office. The certifying entity must confirm the veracity of these lists, as they are the source for checking the integrity of the real data in the ICS. For the monthly CJT: - The data in the CJT file will be compared with lists obtained from the technical gaming system back office. The certifying entity must confirm the veracity of these lists, as they are the source for checking the integrity of the real data in the ICS. - It will be checked that the initial balance for a month is the same as the final balance for the month immediately preceding it. - It will be checked that the final balance equals the initial balance plus the other movements. As a result of this test, the certifying entity must include: - The compliance of the checks made. - The following data, calculated from the monthly data, for each month: o For RUT, the quotient between the total number of new accounts in the month and the number of user accounts (to 4 decimals). o For CJT, the quotient between the total amounts withdrawn and the total amounts deposited throughout the month (to 4 decimals). NOTE: The result will not directly include player or turnover figures. NOTE: The checks and calculations will be performed separately, both in monetary units (EUR) and in any other unit, which may be bonus points or others.

Executive summary form for the integration tests for general licences.

Area and requirement	Classification
A.1. User account and checking bans.	
A.1.1. Creating a new user account	
A.1.2 Checking for individual bans	
A.2 Gaming account, charges and payouts	
A.2.1. Correct recording of operations in the gaming	
A.3 Limits on deposits	
A.3.1 Deposits over the limits	
A.3.2 Data on deposit limits	
A.4 Internet. Redirection to an".es" domain.	
A.4.1 Redirection to an ".es" domain.	
A.5 Internal Control System	
A.5.1 Integrity of the data in the ICS	

B. SPECIFIC LICENCES

B.1. Gaming offer.

Test reference	B.1.1
Test name	Gaming offer and game variants.
Type of test	Functional
Test description	The system will be accessed from the player interface to test the gaming offer corresponding to the specific licence. The gaming offer available from each of the different participation applications or terminals will be analysed. Each of the games and variants offered will be analysed, checking that they correspond to the games and variants allowed by the basic regulations. This test does not require playing the game, but rather, analyses the information published by the operator, which may be informational or the rules of the games.
Expected result	The result will give a list with the following information: - the commercial name of the games and variants found - the applications or terminals where they are available. - their correspondence with the variants of the basic regulations. - the version of the specific rules evaluated. This information will be compared with the descriptive questionnaire on the licence filled in by the operator.

Test	B.1.2
Test name	Operation of the game and correct accounting.
Type of test	Functional, traceability

Test description	The player interface will be used to participate in the game, checking: - correct accounting of bets, prizes, commissions and other transactions. - in the case of games with an operator's commission, it must be checked whether the commissions are calculated as established in the specific rules. - the tester will attempt to participate with a higher amount than the available balance in the gaming account. In the case of certain games, there will be checks: - For betting, that no bets can be made at times not established in the specific rules, and particularly after the close of the marketing period, the start of the event for conventional betting, or the end of the event for live betting. - For bingo, that cards cannot be purchased outside the marketing period, or when the game has already begun. - For poker or casino games, that bets cannot be made outside the times designated in the specific rules. Note: This test will be repeated for each of the different participation applications or terminals and for each game, variant or mode.
Expected result	Functional Compliance of the checks described above, broken down by each variant analysed. It will be checked that it is not possible to participate for a higher amount than the available balance in the gaming account. The version of the specific rules will also be indicated. Traceability The result will describe the tables, files or other sources containing the information. An opinion will be given as to whether the recording system of the technical gaming system allows information to be recovered to explain each situation and to reconstruct the entire series of events in each game session.

Test reference	B.1.3
Test name	Tracking participation for channels other than internet
Type of test	Traceability
Test description	If there are other channels than internet, testers will participate several times in each one, for example, text message and telephone.
Expected result	TRACEABILITY The records and traces of the system will be analysed in each participation channel used, checking, in the case of text messages and phone calls, that the system saves the details of: - date/time of each message or call - telephone number the message or call came from - content of the message or call

B.2. Financial limits on participation.

Test reference	B.2.1
Test name	Financial limits on participation.
Type of test	Functional
Test description	The system will be checked for compliance with financial limits: maximum amounts for stakes and prizes. For this, the certifying entity will participate in the game, attempting to exceed each of the limits described in the ministerial orders on gaming, in part 2 of Appendix III.
Expected result	Proof will be established of the tests performed and the results obtained.

B.3. Behaviour in response to technical errors.

Test reference	B.3.1
Test name	Loss of communication with the client.
Type of test	Functional
Test description	Tests will be conducted in which a game or session is begun and then communication with the Central Gaming Unit is deliberately interrupted. The connection will be re-established after 1 minute, 5 minutes or 15 minutes (different time intervals). The reaction of the system for finalising the session and its compliance with the specific rules will be verified. This test must be performed for each of the terminals, applications or clients and for each game or mode offered.
Expected result	Compliance with the specific rules will be indicated. The result will state the behaviour obtained for each terminal, application and client, and for each game or mode. It will also include the version of the specific rules analysed.

Test reference	B.3.2
Test name	Client error.
Type of test	Functional
Test description	A session will begin and the client terminal will deliberately be turned off without warning. The terminal will be restarted after 1 minute, 5 minutes or 15 minutes (different time intervals). The reaction of the system for finalising the session and its compliance with the specific rules will be verified. This test must be performed for each of the terminals, applications or clients and for each game or mode offered.
Expected result	Compliance with the specific rules will be indicated. The result will state the behaviour obtained for each terminal, application and client, and for each game or mode. It will also include the version of the specific rules analysed.

B.4. Internal control system.

Test reference	B.4.1
Test name	Integrity of the ICS data.
Type of test	Real data
Test description	This test will compare the data of the ICS with the data in the operator's computer system in order to assess the integrity of the ICS data. The following monthly data will be obtained for each month: Based on the monthly OPT/ORT register: o Stake o Repayment of the stake o Prizes o Prizes in kind The following daily data will be obtained for the 5 days before running the test: Based on the JUT/JUD registers: o Number of games or rounds in each mode o A random sample of 5 sessions will be taken and their data will be compared with the operator's computer system. For example, the participants, the prizes, the event in the case of betting or the number of text messages in the case of a contest. This test requires the certifying entity to access unencrypted real data. The operator must provide unencrypted OPT/ORT and JUT/JUD files to the certifying entity, which must check that these match the data actually stored in the operator's computer system. The certifying entity is not required to have access to personal data. In no case is the certifying entity required to know the encryption key.

Expected result	The certifying entity will check the certificate used to sign the data and accredit that it is valid and has not been revoked. The certifying entity will indicate in the result the public part of the certificate used to sign the stored data. The data in the OPT/ORT and JUT/JUD files will be compared with lists obtained from the technical gaming system back office. The certifying entity must confirm the veracity of these lists, as they are the source for checking the integrity of the real data in the ICS. As a result of this test, the certifying entity must include: - The compliance of the checks made. - The following OPT/ORT data, calculated from the monthly data, for each month: o The quotient between the value of the prizes and the value of the stake. (to 4 decimals). Note: The result will not directly include turnover figures. Note: The checks and calculations will be performed separately, both in monetary units (EUR) and in any other unit, which may be bonus points or others.

Executive summary form for the predefined tests for specific licences.

Area and requirement	Classification
B.1 Gaming offer	
B.1.1. Gaming offer and game variants.	
B.1.2 Operation of the game and correct accounting.	
B.1.6 Tracking participation for channels other than internet.	
B.2 Financial limits on participation.	
B.2.1 Financial limits on participation.	
B.3. Behaviour in response to technical errors.	
B.3.1 Loss of communication with the client.	
B.3.2 Client error.	
B.4. Internal control system.	
B.4.1 Integrity of the ICS data.	

APPENDIX VII

List of technical requirements for security.

This Appendix is intended to establish the list of requirements which, in accordance with the provision setting out the technical specifications to be met by the technical gaming systems governed by the licences awarded under Law 13/2011 of 27 May on the regulation of gaming, approved by the Directorate General for the Regulation of Gambling Resolution of 16 November 2011 ("BOE" 18 November), must be met by the technical systems of the gaming operators and must be verified by the certifying bodies in their final certification reports.
The areas which must be checked by the certifying bodies and the order in which they must be presented in the corresponding report is as follows:

a) Security policy.

In accordance with section 4.4 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. The operator has security procedures.
2. The security procedures have been communicated in their entirety to its employees, and where applicable, to its partner companies.

Organisations which have obtained current ISO 27001 certification may already be in compliance with requirements 1 and 2. "ISO 27001" must be noted in the comments field.

b) Risk analysis and management.

In accordance with sections 4.1, 4.2 and 4.3 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. The operator has a risk analysis and management plan
2. The risk analysis is regularly reviewed.
3. The organisation has identified the critical components of its technical gaming system.
4. The list of critical components includes:

a) The user account.
b) The gaming account.
c) Processing of means of payment.
d) In the random number generator: the components of the technical gaming system which transmit or process random numbers which will be the subject of game output, and the integration of the random number generator output in the game logic.
e) Components which store, handle or transmit sensitive client information such as personal data, authentication, etc.
f) Components which store the status of the games at any given time.
g) Connections to the National Gaming Commission.
h) The internal control system: the capture system and data storage.
i) Access points and communications with the previous critical components.
j) The communications networks which transmit participants' sensitive information.

5. The operator has reinforced security in all critical components.

Relating to requirements 4 and 5, the certifying entity will note the documentary references in the comments field, and sections where the documents confirm compliance with these requirements.

c) Organisation of information security.

In accordance with section 4.5 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that the organisation has defined a management framework for information security, indicating the duties and responsibilities of its personnel.
Organisations which have obtained current ISO 27001 certification may already be in compliance with requirements in this area. "ISO 27001" must be noted in the comments field.

d) Security in communications with participants.

In accordance with sections 2.1.12 and 4.6 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. The operator has adopted authentication mechanisms which let the gaming system identify the participant, and in turn let the participant identify the gaming system.
2. Communications are encrypted if transmitting personal data (user account) or financial data (gaming account).
3. In relation with communications, the operator has adopted the necessary measures to ensure integrity and non-repudiation when transmitting personal or financial data, and in game participation transactions.
4. An initial user password will be set by default or by the participant.
5. During the process of defining the user password, the participant is given recommendations on choosing secure passwords
6. The minimum length of the password is 4 characters or digits
7. If the password is established by the user and is shorter than 6 characters, one of which is a letter and at least one is a digit, the user will receive a message recommending best practices in the choice of secure passwords.
8. The password cannot contain any of the following data: the username, alias, first name, surname or date of birth of the participant.
9. The user will receive a password change reminder at least once a year, although the change is not obligatory.
10. The mechanism of identification by username and password will be locked if more than 5 failed access attempts are made the same day. The operator may establish a lower limit for this requirement.
Relating to requirements 1, 2, 3, 4, 5, 6, 7, 8 and 9 above, the certifying entity will note the documentary references in the comments field, and the sections where the documents confirm compliance with these requirements.

e) Security of human resources and third parties.

In accordance with section 4.7 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. The operator has a Personnel Security plan
2. The programme includes training for all employees in the organisation, with special attention to critical component and information access permits
3. If the operator needs third party services which involve accessing, processing, communicating or handling information, or access to facilities, products or services relating to the game, these third parties must meet all the security requirements demanded of other personnel.

Organisations which have obtained current ISO 27001 certification may already be in compliance with requirements in this area. "ISO 27001" must be noted in the comments field.

f) Physical and environmental security.

In accordance with section 4.8 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. There is a plan for the physical security of the components of the technical gaming system.
2. Perimeter security is defined for areas containing critical components and sensitive information.
3. There are physical access control points to the facilities housing the equipment, both for employees and for external personnel, including physical elements, authorisation procedures, access records and surveillance services.
4. Protection is provided against environmental risks: water, fire, intentionally provoked, etc.
5. The critical equipment is protected from power failures and other interruptions caused by failures in the supporting facilities, and the power supply cables are protected from damage.
6. Control mechanisms are defined for access to communications cables if they transport critical unencrypted information.
7. Suitable maintenance is provided and planned for the facilities and equipment.
8. The devices containing information are securely wiped or destroyed before being reused or removed.
9. Equipment containing information cannot be taken out of the secure facility without the corresponding authorisation.

Relating to requirements 2, 3, 4, 5, 7, 8 and 9 above, the certifying entity will note the documentary references in the comments field, and the sections where the documents confirm compliance with these requirements.
Organisations which have obtained current ISO 27001 certification may already be in compliance with requirements in this area. "ISO 27001" must be noted in the comments field.

g) Communications and Operations Management.

In accordance with section 4.9 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. The critical components are monitored to avoid versions other than the approved version being used.
2. Communications between the components of the technical gaming systems guarantee integrity and confidentiality.

3. Tasks are segregated among different areas of responsibility to minimise the possibility of unauthorised access and potential damage.
4. Development, testing and production tasks are separated.
5. Third party services include security controls and metrics in contracts, and are regularly audited and monitored.
6. Measures have been adopted to protect against malware.
7. Backup copies are made regularly at a suitable frequency, and are stored as set out in the backup plan.
8. Security measures have been adopted in the communications network.
9. Security measures have been adopted for handling removable media and secure wiping or destruction of such media, in the form of a documented procedure.
10. The clocks of all the components, especially critical ones, are synchronised with a reliable time source, and the operator has established measures and controls to avoid the manipulation or later alteration of timestamps, especially in auditing records.
11. Auditing records are generated and saved for the activities of all users, exceptions and information security events for a minimum period of 2 years.
12. The auditing records are protected from alteration and unauthorised access.
13. The activities of the System Administrator and System Operator are being recorded.
14. Auditing records are regularly analysed and actions taken according to the incidents found.

Relating to requirements 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 14 above, the certifying entity will note the documentary references in the comments field, and the sections where the documents confirm compliance with these requirements.
Organisations which have obtained current ISO 27001 certification may already be in compliance with requirements in this area. "ISO 27001" must be noted in the comments field.

h) Access Control

In accordance with section 4.10 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. The information access policy is documented.
2. Authorised access is ensured and unauthorised access is prevented by controls in the creation of user accounts, management of login privileges, regular reviews of login privileges and a password management policy.
3. Users follow best practices in the use of passwords and protect the documentation and media at their workstation adequately.
4. Users have access only to the services they have been authorised to use.
5. There are no generic users, and all users log in with their own unique username.
6. The system checks all access, whether by its own personnel, maintenance or other personnel, including from other systems and components. Gaming Commission personnel or other personnel acting in its name will also be authenticated.
7. The networks will be segregated by area and responsibility for the task or duty.
8. Access to the operating systems requires a secure authentication mechanism.

This text of this site is unofficial English translation of the official texts in Spanish. The later will prevail in case of discrepancies

9. The use of programmes which enable access and security controls to be avoided will be restricted and controlled.
10. Sessions will have a maximum connection time and a time-out period if inactive.
11. Computer support personnel have restricted access to the real data of applications. Sensitive real data is stored in isolated environments.
12. The risks associated with mobile devices are managed.
13. If there are remote workers, check that the associated risk is managed as part of the security plan.

Relating to requirements 1, 2, 3, 4, 6, 7, 8, 9, 10, 11 and 12 above, the certifying entity will note the documentary references in the comments field, and the sections where the documents confirm compliance with these requirements.
Organisations which have obtained current ISO 27001 certification may already be in compliance with requirements in this area. "ISO 27001" must be noted in the comments field.

i) Purchase, development and maintenance of the systems.

In accordance with section 4.11 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that there is a security plan for making decisions on purchasing, developing and maintaining computer systems.
Organisations which have obtained current ISO 27001 certification may already be in compliance with requirements in this area. "ISO 27001" must be noted in the comments field.

j) Management of security incidents.

In accordance with section 4.12 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. There is a documented security incident management procedure.
2. There is a record of security incidents (with events, impacts and measures adopted).

Organisations which have obtained current ISO 27001 certification may already be in compliance with requirements in this area. "ISO 27001" must be noted in the comments field.

k) Change management.

In accordance with section 4.13 of the provision setting out the technical specifications to be met by technical gaming systems and Article 10 of this Provision, the certifying entity must verify that:

1. There is a change management procedure for the equipment and components of the technical gaming system in the production environment.
2. There is an internal process for approving changes (change request, approval by managers).
3. A record is kept of changes (requests, decisions made) which can later be audited.
4. In the case of changes to critical components, these must be evaluated to decide whether the change is significant.
5. Copies must be kept of the binary files of the software elements of all software versions used in the technical system actually in use.

The National Gaming Commission may establish the obligation for the binary file archiving procedure to include a digital fingerprint of the files.

Relating to requirements 1, 2, 3, 4 and 5 above, the certifying entity will note the documentary references in the comments field, and the sections where the documents confirm compliance with these requirements.

l) Information loss prevention plan.

In accordance with section 4.15 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. There is a plan to prevent the loss of data or transactions affecting the progress of the games, the rights of participants or public interest.
2. There is a plan with measures to prevent information loss, which will include the following aspects:

a) Location where backup copies of the information are stored.
b) Security measures to protect the backup from unauthorised access.

3. There is a procedure for action in case of information loss, which will include the following aspects:

a) Mechanisms to attend to claims.
b) Mechanisms for continuing interrupted games.

Relating to requirements 1, 2 and 3 above, the certifying entity will note the documentary references in the comments field, and the sections where the documents confirm compliance with these requirements.

m) Business continuity management.

In accordance with sections 4.14 and 4.16 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. There is a business continuity management plan in case of disasters which will include the following aspects:

a) The technical, human and organisational measures necessary to ensure the continuity of the service.
b) Replica of the Central Gaming Unit which permits activities to go on as normal.

2. The continuity plan covers the following scenarios:

a) User account and gaming account, with the possibility of consulting the balance and movements of the associated gaming accounts. The maximum time for providing these services again will be one week.
b) Withdrawal of funds. The maximum time for providing these services again will be one week.
c) Continuation of unfinished games or pending bets and payment of validly won prizes. The maximum time for providing these services again will be one month.
d) Complete restoration of all services.

3. In all scenarios the following information is included:

a) Services recovered.
b) Maximum recovery time.

Relating to requirements 1, 2 and 3 above, the certifying entity will note the documentary references in the comments field, and the sections where the documents confirm compliance with these requirements.
Organisations which have obtained current ISO 27001 certification may already be in compliance with requirements in this area. "ISO 27001" must be noted in the comments field.

n) Penetration test and vulnerability analysis

In accordance with section 4.17 of the provision setting out the technical specifications to be met by the technical gaming systems, the certifying entity must verify that:

1. In the last six months the technical gaming system has passed a penetration test and vulnerability analysis.
2. There is a plan to analyse vulnerability at least twice a year.

Relating to requirement 1 above, the certifying entity will note the documentary references in the comments field, and the sections where the documents confirm compliance with these requirements.