

PROYECTO DE DISPOSICIÓN QUE ESTABLECE EL MODELO Y CONTENIDO DEL INFORME DE CERTIFICACIÓN DEFINITIVA DE LOS SISTEMAS TÉCNICOS DE LOS OPERADORES DE JUEGO Y SE DESARROLLA EL PROCEDIMIENTO DE GESTIÓN DE CAMBIOS.

ÍNDICE

Anexo I. Disposición por la que se establece el modelo y contenido del informe de certificación definitivo de los sistemas técnicos de los operadores de juego y se desarrolla el procedimiento de gestión de cambios.

Primero. Objeto y alcance.

Segundo. Definiciones.

Tercero. Procedimiento y plazo para la homologación de los sistemas técnicos de juego.

Cuarto. Descripción del sistema técnico objeto de licencia.

Quinto. Informes de certificación.

Sexto. Proveedores de servicios de juego.

Séptimo. Informe de certificación de la funcionalidad.

Octavo. Informes de certificación de la seguridad.

Noveno. Cumplimiento de la normativa de protección de datos de carácter personal.

Décimo. Procedimiento de gestión de cambios en el sistema técnico de juego.

Undécimo. Huellas digitales.

Anexo II. Cuestionario descriptivo de la licencia.

Anexo III. Modelo y contenido mínimo del informe de certificación de la funcionalidad. **Anexo IV.** Modelo y contenido del informe de certificación de la seguridad.

Anexo V. Relación de requisitos técnicos de funcionalidad.

Anexo VI. Relación mínima de pruebas de integración.

Anexo VII. Relación de requisitos técnicos de seguridad.

ANEXO I

Disposición por la que se establece el modelo y contenido del informe de certificación definitivo de los sistemas técnicos de los operadores de juego y se desarrolla el procedimiento de gestión de cambios

Primero. *Objeto y alcance.*

Esta disposición tiene por objeto el establecimiento del modelo y contenido mínimo del informe definitivo de certificación del cumplimiento de los requisitos establecidos en la vigente normativa por los sistemas técnicos de juego empleados para el desarrollo y explotación de los juegos objeto de la correspondiente licencia general o singular.

El informe definitivo de certificación será emitido por una o varias de las entidades designadas a estos efectos por la Dirección General de Ordenación del Juego y tendrá como objeto la obtención de la homologación de los sistemas técnicos de juego de los operadores. Deberá presentarse un informe por cada licencia general o singular que hubiera sido otorgada al operador interesado.

El informe definitivo de certificación, cuyo modelo y contenido mínimo se establece en esta disposición, alcanza a la certificación de los sistemas técnicos de juego de los operadores con licencia general para el desarrollo y explotación de las modalidades de juego a las que se refieren las letras c), e) y f) del artículo 3 de la Ley 13/2011, de 27 de mayo, de regulación del juego, y respecto de los tipos de juego regulados hasta la fecha de publicación de la misma.

Asimismo, esta disposición desarrolla el procedimiento de gestión de cambios a que se refiere el artículo 8.4 del Real Decreto 1613/2011, de 14 de noviembre, por el que se desarrolla la Ley 13/2011, de 27 de mayo, de regulación del juego, en lo relativo a los requisitos técnicos de las actividades de juego, complementando a lo ya dispuesto en el apartado 4.13 de la Resolución de 16 de noviembre de 2011, de la Dirección General de Ordenación del Juego, por la que se aprueba la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego.

Segundo. *Definiciones.*

A los efectos de esta disposición, los términos que en ella se emplean tendrán el sentido que se establece en el apartado 1.2 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego objeto de licencias otorgadas al amparo de la Ley 13/2011, de 27 de mayo, de regulación del juego, aprobada por Resolución de la

Dirección General del Juego de 16 de noviembre de 2011 («BOE» de 18 de noviembre de 2011).

Tercero. *Procedimiento y plazo para la homologación de los sistemas técnicos de juego.*

La homologación inicial de los sistemas técnicos de juego se realizará en el marco del procedimiento de otorgamiento de licencias generales y singulares.

El informe o informes definitivos de certificación de los sistemas técnicos de juego de los operadores deberán presentarse por el interesado en el plazo improrrogable de cuatro meses contados desde que le hubiera sido notificada la resolución de otorgamiento de la licencia general o de la licencia singular provisional.

El informe definitivo de certificación se compone de los siguientes documentos:

- a) Descripción del sistema técnico objeto de licencia, cumplimentado por el operador.
- b) Informe definitivo de certificación de la funcionalidad.
- c) Informe definitivo de certificación de la seguridad.
- d) Informe de cumplimiento de la normativa de protección de datos de carácter personal por parte del operador.

El procedimiento de homologación se iniciará en el momento en que el informe definitivo de certificación tenga entrada en el Registro General del Ministerio de Hacienda y Administraciones Públicas en la forma establecida en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Los procedimientos se iniciaran en función del orden de entrada de los informes.

El informe definitivo de certificación y la documentación e informes adicionales deberán presentarse en formato electrónico. Únicamente deberá presentarse en papel, y debidamente firmados por la persona o personas autorizadas en la entidad de certificación, la identificación de la certificación, el objeto de la misma y su resumen ejecutivo.

Si el operador realizara la presentación telemática del informe de certificación, deberá asegurarse de que el informe de certificación esté firmado mediante un certificado admitido en el ámbito de la Administración General del Estado, de acuerdo con la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y su desarrollo reglamentario.

La Dirección General de Ordenación del Juego podrá requerir a los interesados cuanta documentación e información considere precisa para la resolución del procedimiento de homologación.

Recibido el informe definitivo de certificación y previa la valoración favorable del mismo, la Dirección General de Ordenación del Juego homologará los sistemas técnicos de juego de acuerdo con lo establecido en el artículo 16 de la Ley 13/2011, de 27 de mayo, de regulación del juego, en un plazo máximo de seis meses contados desde la notificación del otorgamiento de la licencia, sin perjuicio de la ampliación del plazo citado por el tiempo que el interesado hubiera empleado para atender a los requerimientos que, tras la presentación del informe definitivo de certificación, practicara la Dirección General de Ordenación del Juego.

Cuarto. *Descripción del sistema técnico objeto de licencia.*

Para la descripción del sistema técnico objeto de licencia se deberá aportar la siguiente documentación:

- Descripción actualizada del sistema técnico.
- En el caso de licencias singulares, las reglas particulares.
- El cuestionario descriptivo del operador.

El cuestionario descriptivo del operador es un documento elaborado por este, que incluye información estructurada en relación al ejercicio de su actividad, su oferta de juego, sus proveedores y sus contactos.

El contenido del cuestionario cumplimentado por el operador debe coincidir con el de los informes definitivos de certificación presentados en aquellos aspectos que son comunes. En caso contrario, el operador deberá justificar las diferencias existentes.

Quinto. *Informes de certificación.*

El operador deberá presentar un informe definitivo de certificación de la funcionalidad del sistema técnico de juego y un informe definitivo de certificación de la seguridad del sistema técnico de juego empleado para el desarrollo y ejecución del juego objeto de la correspondiente licencia.

El informe definitivo de certificación de la funcionalidad del sistema técnico de juego deberá ser emitido por una de las entidades designadas por la Dirección General de Ordenación del Juego para la certificación de software de juego.

El informe definitivo de certificación de seguridad deberá ser emitido por una de las entidades designadas por la Dirección General de Ordenación del Juego para la certificación de seguridad de los sistemas de información.

Los informes definitivos de certificación deberán acreditar que el sistema técnico efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la correspondiente licencia cumple los requisitos técnicos exigidos por la vigente normativa de juego, pronunciándose sobre el estado del sistema técnico de juego empleado a la fecha de su presentación.

Los informes definitivos de certificación que han de ser aportados por el operador tras el otorgamiento de una licencia general deberán alcanzar al registro de usuario, la cuenta de juego, la gestión de los cobros y pagos, el sistema de control interno y los diferentes terminales o aplicaciones que permitan el acceso del participante.

Los informes definitivos de certificación que han de ser aportados por el operador tras el otorgamiento provisional de una licencia singular deberán alcanzar al software de juego y, en su caso, el generador de números aleatorios, al sistema de control interno y a los diferentes terminales o aplicaciones que permitan el acceso del participante.

El operador interesado podrá presentar una única vez un mismo informe de certificación, con independencia de que éste sea de aplicación en los procesos de homologación de una o varias de las licencias que le hubieren sido otorgadas. En este supuesto, y tras la primera presentación del informe de certificación, bastará con la referencia a su aportación y la identificación del procedimiento en que ésta se hubiera realizado.

El informe se realizará íntegramente en castellano. Los anexos, las evidencias o la documentación de soporte del informe podrán recogerse en castellano o en el idioma original en que estuvieran redactados, en cuyo caso, la Dirección General de Ordenación del Juego podrá requerir al operador para que, en el plazo de diez días, aporte la traducción al castellano de cualquiera de los anexos o documentos inicialmente aportados en otro idioma.

Sexto. *Proveedores de servicios de juego.*

El sistema técnico de juego efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la licencia comprenderá a los sistemas de todos los proveedores de servicios de juego que participen en la solución completa.

El operador solicitante deberá responsabilizarse de homologar el sistema técnico de juego completo y de presentar informes definitivos de certificación que deberán comprender los sistemas técnicos de todos los proveedores de servicios de juego.

Séptimo. *Informe de certificación de la funcionalidad.*

El informe definitivo de certificación de la funcionalidad evaluará el cumplimiento de los requisitos técnicos del sistema técnico de juego efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la licencia.

En las licencias generales se presentará un único informe que cubra el alcance completo.

En las licencias singulares se podrán presentar varios informes cuando el software de los juegos o modalidades incluidos en un informe, sea completamente independiente del software de los juegos o modalidades de otros informes. En todo caso cada informe deberá acreditar el cumplimiento de todos los requisitos técnicos para los juegos y modalidades incluidas así como el sistema de control interno y la integración con la plataforma de juego.

El modelo y contenido mínimo del informe definitivo de certificación de la funcionalidad es el que figura en el anexo III a la Resolución por la que se aprueba esta disposición.

El informe definitivo de certificación de la funcionalidad constará como mínimo de tres conjuntos de pruebas o análisis:

a) Pruebas de evaluación del cumplimiento de los requisitos técnicos:

Para la evaluación del cumplimiento de los requisitos técnicos, la entidad de certificación podrá escoger la prueba o pruebas que considere más adecuadas. La relación de requisitos técnicos se describe en el anexo V a la Resolución por la que se aprueba esta disposición.

La entidad de certificación que emita el informe podrá realizar alguna de las pruebas referidas en un entorno distinto del efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la licencia, pero la certificación emitida deberá de referirse en todo caso al sistema técnico de juego que sea efectivamente empleado por el operador. En los casos en que se utilicen entornos diferentes del efectivamente empleado por el operador, la entidad de certificación deberá certificar bajo su responsabilidad que los resultados obtenidos en el entorno de prueba son extrapolables a los que

hubieran sido obtenidos de haberse realizado en el sistema técnico efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la licencia, habiendo analizado que las eventuales diferencias entre el entorno de pruebas y el sistema técnico de juego efectivamente empleado no afectan a la calidad del resultado de las pruebas realizadas.

b) Análisis específicos de funcionalidades relevantes:

La entidad de certificación deberá realizar un análisis específico de determinadas funcionalidades de especial relevancia.

En los supuestos de licencia general se analizarán las comprobaciones de la identidad y de las causas de prohibición subjetiva y se evaluarán las medidas de lucha contra el fraude y el blanqueo de capitales. En los supuestos de licencia singular se analizará la lógica del juego, y, cuando resulten de aplicación, el porcentaje de retorno al jugador y el generador de números aleatorio.

c) Pruebas de integración:

La entidad de certificación deberá diseñar y realizar las pruebas de integración necesarias para acreditar el cumplimiento de los requisitos en el sistema técnico de juego efectivamente empleado.

En el caso de la homologación inicial, las pruebas de integración deberán realizarse en el sistema técnico de juego efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la licencia, no pudiendo utilizarse a estos efectos un entorno distinto.

En el caso de certificaciones posteriores, en el contexto de una gestión de un cambio sustancial, las pruebas de integración podrán realizarse en un entorno distinto del efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la licencia. En los casos en que se utilicen entornos diferentes del efectivamente empleado por el operador, la entidad de certificación deberá certificar bajo su responsabilidad que los resultados obtenidos en el entorno de prueba son extrapolables a los que hubieran sido obtenidos de haberse realizado en el sistema técnico efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la licencia, habiendo analizado que las eventuales diferencias entre el entorno de pruebas y el sistema técnico de juego efectivamente empleado no afectan a la calidad del resultado de las pruebas realizadas.

El conjunto de pruebas de integración deberá comprender como mínimo las que se describen en el anexo VI de la Resolución por la que se aprueba esta disposición.

Las pruebas de integración tienen por objeto el análisis de datos reales generados durante el desarrollo y comercialización de la actividad de juego por parte del operador. Estas pruebas de integración con datos reales requieren que el sistema técnico de juego disponga al menos de un mes de datos, y no pueden ser completados mediante pruebas o simulaciones. En los casos en los que, en el momento de presentación del informe definitivo de certificación, el operador no hubiera iniciado el desarrollo de la actividad de juego, el informe podrá ser presentado sin aportar el resultado de las pruebas citadas, si bien la homologación quedará condicionada a la presentación del resultado de las mismas y su valoración favorable por parte de la Dirección General de Ordenación del Juego. El resultado de las pruebas que tienen por objeto el análisis de datos reales generados durante el desarrollo y comercialización de la actividad de juego, si no se presentara junto al informe definitivo de certificación, deberán ser presentados en el plazo de tres meses contados desde la fecha de inicio de la actividad de juego correspondiente.

El informe definitivo de certificación de la funcionalidad incluirá una copia de los binarios del software certificado y una huella digital de aquellos componentes calificados como críticos.

Octavo. *Informes de certificación de la seguridad.*

La certificación de la seguridad únicamente podrá realizarse sobre el sistema técnico de juego efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la correspondiente licencia, en relación con los procedimientos, procesos, planes y medidas de seguridad efectivamente implementados.

El operador podrá solicitar a la entidad de certificación un único informe de certificación de la seguridad que alcance a la totalidad del sistema técnico de juego, al objeto de poder emplearlo en los procesos de homologación de cada una de las licencias que le hubieran sido otorgadas.

En los casos en que uno o varios proveedores de servicios de juego formen parte del sistema técnico de juego efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la correspondiente licencia, el operador solicitante deberá presentar un informe definitivo de certificación de la seguridad de la infraestructura técnica de cada uno de los proveedores.

El modelo y contenido mínimo del referido informe definitivo de certificación de la seguridad es el que figura en el anexo IV a la Resolución por la que se aprueba esta disposición.

El informe definitivo de certificación de la seguridad constará de dos partes. En la primera, la entidad de certificación acreditará el cumplimiento de los requisitos de seguridad, cuyo listado figura en el anexo VII a la Resolución por la que se aprueba esta disposición. Será posible la convalidación parcial del cumplimiento de los requisitos técnicos de seguridad cuando el sistema de gestión de la seguridad objeto de certificación disponga de una certificación ISO 27001 con idéntico alcance vigente a la fecha de la solicitud de homologación. Los requisitos de seguridad que podrán beneficiarse de este reconocimiento se indican en el referido anexo VII. La entidad de certificación deberá adjuntar copia de la certificación ISO 27001 en la que conste claramente el destinatario, el alcance de la misma y su vigencia temporal.

En la segunda parte, la entidad de certificación deberá realizar análisis de auditoría específicos respecto de la relación de componentes críticos, gestión de cambios, gestión de continuidad de negocio y prevención de la pérdida de información.

Noveno. Cumplimiento de la normativa de protección de datos de carácter personal.

El operador presentará junto con el informe definitivo de certificación un informe descriptivo del cumplimiento de la normativa de protección de datos de carácter personal.

Este informe será único por operador y resultará de aplicación a las diferentes licencias generales y singulares de las que sea titular.

La Dirección General de Ordenación del Juego, en cumplimiento del artículo 16 apartado 4 de la Ley 13/2011, de 27 de mayo, de regulación del juego, solicitará informe a la Agencia Española de Protección de Datos.

Décimo. Procedimiento de gestión de cambios sustanciales en el sistema técnico de juego.

La puesta en producción de cualquier modificación sustancial que afecte a un componente crítico necesitará la previa autorización de la Dirección General de Ordenación del Juego tras la presentación del correspondiente informe de certificación. La Dirección General de Ordenación del Juego se pronunciará

sobre la autorización de los cambios sustanciales de componentes críticos, en el plazo de un mes contados desde la fecha de recepción de la solicitud del operador.

La Dirección General de Ordenación del Juego podrá calificar como críticos otros componentes adicionales a los que consten en los informes definitivos de certificación o a los que el operador haya calificado como tales.

Ante situaciones de emergencia extraordinaria que afecten a la seguridad, debidamente acreditadas y comunicadas a la Dirección General de Ordenación del Juego, el operador podrá introducir cambios sustanciales en los componentes críticos y solicitar posteriormente su autorización. En estos supuestos, para la obtención de la homologación el operador presentará a la Dirección General de Ordenación del Juego, junto al informe de certificación, un informe en el que queden acreditadas las circunstancias excepcionales y el riesgo para la seguridad del sistema técnico de juego.

Desde el otorgamiento de licencia hasta que el operador realice la presentación de los informes de certificación definitivos, los cambios que se realicen sobre el sistema técnico de juego no necesitarán autorización previa para su puesta en marcha, si bien, los cambios sustanciales respecto al proyecto técnico evaluado para el otorgamiento de la licencia deberán ser comunicados a la Dirección General de Ordenación del Juego con 15 días de antelación a su puesta en marcha. Si la Dirección General de Ordenación del Juego estimara que alguno de los cambios efectuados incumple con lo establecido en la normativa de juego, podrá requerir su retirada inmediata.

Tras la obtención de la homologación, el operador elaborará trimestralmente un informe descriptivo de todos los cambios realizados en el sistema técnico de juego y lo notificará a la Dirección General de Ordenación del Juego. Se incluirá la siguiente documentación:

- Un resumen ejecutivo, en castellano, que explique de manera cualitativa los cambios realizados.
- La descripción del sistema técnico objeto de licencia actualizado, con el contenido descrito en el artículo cuarto del anexo I a la Resolución por la que se aprueba esta disposición.

La Dirección General de Ordenación del Juego podrá establecer la obligación de que el informe trimestral descriptivo de todos los cambios realizados en el sistema técnico de juego incluya una huella digital de los binarios.

La Dirección General de Ordenación del Juego solicitará al operador cuanta información considere precisa en relación con los cambios realizados.

Si la Dirección General de Ordenación del Juego estimara sustancial alguno de los cambios realizados en componentes críticos, requerirá al operador para que proceda a la homologación de los cambios, sin perjuicio de la posibilidad de requerir al operador para que proceda a la retirada del cambio hasta que obtenga la homologación pertinente.

Undécimo. *Huellas digitales.*

Respecto al procedimiento de obtención de la huella digital del software a que hace referencia esta Resolución, se deberá observar lo siguiente:

a) Se utilizará el algoritmo SHA-1, salvo justificación técnica de la conveniencia de la utilización de otro algoritmo, que deberá ser autorizada previamente por la Dirección General de Ordenación del Juego.

b) Deberá adjuntarse junto con las huellas digitales la herramienta o procedimiento utilizado para obtener las huellas digitales, así como la herramienta o procedimiento que permita validar las huellas digitales obtenidas. Deberá adjuntarse en soporte digital las herramientas necesarias o indicar la ubicación desde la que son públicamente disponibles y de acceso gratuito.

c) En el caso de tratarse de herramientas bajo patente o propiedad intelectual, deberá justificarse la manera en que la Dirección General de Ordenación del Juego y cualquier otra entidad de certificación pueden tener acceso gratuito y derechos de uso de las mismas.

ANEXO II

Cuestionario descriptivo del operador

El cuestionario recogerá información sobre el operador, su actividad y su sistema técnico de juego para el desarrollo y explotación de los juegos objeto de las licencias de las que es titular.

El cuestionario incluirá, entre otras, la siguiente información:

– Datos identificativos del operador y de las licencias de las que es titular, así como del inicio de su actividad.

- Información sobre sus contactos.
- Descripción los proveedores de software.
- Relación de sus dominios.
- Relación de los dominios diferentes al “.es” que sean propiedad o estén controlados por el operador de juego, su matriz o sus filiales.
- Tipos de medios utilizados para la verificación de identidad de los jugadores.
- Relación de los medios de pago utilizados y fecha de comienzo de su comercialización. Los tipos de medios de pago deberán ajustarse a la clasificación establecida en la Resolución por la que se aprueba el modelo de datos del sistema de monitorización de la información correspondiente a los registros de operaciones de juego.
- Información relativa a las redes coorganizadas de juego.
- Descripción de la oferta de juego.
- Descripción de las aplicaciones para el acceso del participante.
- Descripción de los canales de comunicación utilizados y las tecnologías de acceso.

El cuestionario podrá incluir también cualquier otro dato del sistema técnico de juego que sea relevante para la actividad de homologación.

Para facilitar su cumplimentación, se publicará en formato electrónico en el sitio web de la Dirección General de Ordenación del Juego.

La Dirección General de Ordenación del Juego podrá actualizar el contenido y formato del cuestionario. El cuestionario que deberá emplearse será en todo caso el último publicado.

ANEXO III

Modelo y contenido mínimo del informe de certificación de la funcionalidad

El informe definitivo de certificación de la funcionalidad se estructura en los apartados y presentará el contenido mínimo que a continuación se relaciona:

1. Identificación de la certificación.
2. Descripción del objeto de certificación.
3. Resumen ejecutivo de la certificación de la funcionalidad.
4. Detalle del cumplimiento de los requisitos técnicos.

5. Detalle de los análisis específicos.
6. Detalle de las pruebas de integración.
7. Descripción del lugar, equipo y fechas de realización de la certificación.
8. Descripción de los entornos utilizados en las pruebas diferentes al efectivamente empleado por el operador para el desarrollo de la actividad de juego.
9. Descripción del soporte digital que acompañará al informe de certificación.

1. *Identificación de la certificación*

En la primera página del informe se detallará lo siguiente:

- a) Tipo de informe de certificación: Se consignará «informe definitivo de certificación de la funcionalidad».
- b) Código de identificación del informe: El código de identificación del informe será único y permitirá referirse al mismo de manera unívoca y su diferenciación de cualquier otro informe emitido por la entidad de certificación. Cada vez que la entidad de certificación realice cualquier modificación en un informe deberá generar un nuevo código de identificación para el mismo.
- c) Datos identificativos de la entidad certificadora.
- d) Datos identificativos de quien firma el informe por parte de la entidad certificadora.
- e) Fechas de realización de los trabajos de certificación.
- f) Fecha de emisión del informe de certificación.

2. *Descripción del objeto de certificación*

El objeto de certificación expondrá el alcance del sistema técnico de juego objeto de certificación, e incluirá al menos la siguiente información:

- La identificación de los elementos de software empleados en el sistema técnico para el desarrollo y explotación del juego objeto de la licencia correspondiente, con mención expresa del fabricante, nombre del producto y versión. En esta relación de elementos deberá constar en todo caso el capturador y el almacén.
- Relación de los componentes calificados como críticos y huella de los mismos. Esta relación podrá adjuntarse en un apartado diferenciado, como anexo, respondiendo a criterios de orden.

- La identificación de los centros de procesos de datos en que están instalados,
- Canales de acceso certificados (Internet, SMS, IVR, presencial...).

Para las licencias generales:

- Sitios web certificados y nombres comerciales,
- Versión del servicio web de verificación de identidad de jugadores contra el que el sistema consulta,
- Medios de pago utilizados durante la certificación,

Para las licencias singulares:

- Rol del operador: deberá indicarse si el operador actúa como B2C, B2B o ambos. En el caso de que se trate de un operador B2B, deberá indicarse si actúa como coorganizador de juego, es decir, si gestiona plataformas de juego en la que sean miembros o se adhieran otros operadores de juego que pongan en común cantidades jugadas por sus respectivos usuarios.
- La oferta de juego bajo el alcance de la certificación, indicando variantes de juego certificadas. Para cada uno de los juegos y variantes certificadas, se indicará el nombre definido por el fabricante, el nombre comercial y, en su caso, la correspondencia con los juegos y variantes permitidas por la reglamentación básica.
- Tecnologías de acceso al sistema técnico de juego certificadas, como por ejemplo:
 - Acceso web
 - Cliente descargable en tecnología Flash
 - Clientes descargables para PC (indicando para qué sistemas operativos)
 - Aplicaciones nativas para Smartphone, tabletas u otros dispositivos móviles (indicando para qué sistemas operativos)
 - Clientes de móvil de acceso web, por ejemplo, basados en HTML.

Para el caso de las apuestas deportivas de contrapartida y las apuestas cruzadas deberá indicarse si se han certificado si se incluyen apuestas en directo.

Cuando el alcance del informe de certificación incluya varias variantes de juego, deberá indicarse a lo largo del informe, para cada prueba, análisis o

requisito técnico, si la valoración emitida o cualquier otra información que se incluya hacen referencia a todas las variantes, o en su caso, solo a las que corresponda.

3. Resumen ejecutivo de la certificación de la funcionalidad

3.1 Calificación global de la funcionalidad.

Se incluirá una calificación global del cumplimiento de los requisitos técnicos por el sistema técnico de juego efectivamente utilizado por el operador para la licencia. La calificación podrá ser «Conforme» o «No conforme».

Esta calificación solamente podrá ser «Conforme» cuando la entidad de certificación estime que el sistema técnico de juego efectivamente utilizado por el operador para la licencia es conforme con todos los requisitos que resulten de aplicación.

Calificación global de la funcionalidad	Se Calificará globalmente el resultado del análisis como «Conforme» o «No conforme».
---	--

3.2 Cuadro resumen del cumplimiento de los requisitos técnicos.

Las áreas de requisitos cuyo cumplimiento deben certificarse para cada licencia se describen en el anexo V a la Resolución por la que se aprueba esta disposición.

Para cada requisito se habrá obtenido una calificación que podrá ser «Conforme», «No conforme», o «No aplica».

Los requisitos técnicos han sido agrupados por áreas.

En el resumen ejecutivo se presentará una tabla resumen con el número de requisitos que reciben cada calificación para cada área.

Las calificaciones se detallarán del siguiente modo:

	Número de requisitos	Número de requisitos conformes	Número de requisitos no conformes	Número de requisitos no aplica
Área XXX.....	7	6	0	1
Área YYY.....	4	4	0	0

3.3 Cuadro resumen de los análisis específicos.

Para determinadas funcionalidades de especial relevancia, la entidad de certificación deberá realizar varios análisis específicos. En algunos casos será necesario detallar el análisis llevado a cabo en un apartado posterior.

3.3.1 Análisis de las comprobaciones de identidad y prohibiciones.

Este análisis será de aplicación únicamente para licencias generales.

Calificación	Se calificará globalmente el resultado del análisis como «Conforme» o «No conforme» respecto a los requisitos técnicos en esta materia
--------------	--

Datos generales

Acepta participantes no residentes.	Sí/No.
Permite jugar sin registro de usuario.	Sí/No. En caso afirmativo, listar los juegos en que lo permite.
Canales para acreditar la identidad.	Indicar relación de canales: internet, telefónico, SMS, presencial, otros

Comprobaciones antes de activar el registro de usuario

Utiliza el servicio de verificación de la identidad proporcionado por la Dirección General del Juego para residentes.	Sí/No. En caso de que se utilice pero no en todos los casos, indicar cuándo.
Otros medios de comprobación de identidad.	Relación de otros medios de comprobación de la identidad utilizados.
Documentos de identificación admitidos para no residentes.	Relación de documentos admitidos para acreditar la identidad de no residentes.
Comprobación de la mayoría de edad.	Sí/No.
Utiliza el servicio de verificación de inclusión el RGIAJ.	Sí/No.
Realiza comprobación de vinculados.	Sí/No.

Comprobaciones antes del abono de premios

Utiliza el servicio de variaciones del RGIAJ cada hora y actualiza la lista de prohibidos del operador.	Sí/No
---	-------

3.3.2 Análisis del generador de números aleatorios.

Este análisis será de aplicación únicamente para licencias singulares donde se utilice un generador de números aleatorios, o GNA.

Calificación.	Se calificará globalmente el resultado del análisis como «Conforme», o «No conforme» respecto a los requisitos técnicos en esta materia.
Fabricante.	Datos del fabricante del GNA.
Producto y versión.	Nombre del elemento software y versión.
Huella digital.	Huella digital del binario.
Tipo de GNA.	Se indicará: - GNA hardware. - GNA software.
Aleatorio/Pseudoaleatorio.	Se indicará: - Aleatorio. - Pseudoaleatorio. En caso de ser aleatorio, se indicará el nombre del fenómeno en que se basa.
GNA compartido.	Se indicará uno de los siguientes valores: - Instancia de GNA no compartida con otros juegos. - Instancia de GNA compartida con otros juegos. Indicar cuáles. - GNA integrado en el propio software de juego. - Otros. Describir.
Algoritmo.	En el caso de GNA hardware se indicará el nombre del fenómeno en que se basa. En el caso de GNA software se indicará el nombre del algoritmo, así como el nombre de las librerías o llamadas del sistema operativo en que se basa. En el caso de que se base en un algoritmo propio, indicarlo.
Resemillado.	Indicar Sí/No incluye procedimiento de resemeado.
Longitud del espacio	Longitud en bits del espacio de diferentes números aleatorios.
Relación de tests estadísticos.	Relación de los nombres de los tests estadísticos que se han realizado.

3.3.3 Análisis del porcentaje de retorno al jugador.

Este análisis será de aplicación únicamente para licencias singulares, en aquellos juegos con porcentaje de retorno.

Porcentaje de retorno al jugador publicado para el juego.	Se indicará el porcentaje de retorno publicado por el operador para cada juego.
---	---

	Se indicará adicionalmente el sitio donde esté publicado el porcentaje de retorno.
--	--

3.3.4 Análisis de la lógica del juego y los sucesos aleatorios.

Este análisis será de aplicación únicamente para licencias singulares.

Cumplimiento de reglas particulares del juego.	Sí/No
Sistema de gestión de riesgos para apuestas de contrapartida.	Indicación de desarrollo a medida o nombre del producto o servicio utilizado.
Auditoría de cambios en la configuración mediante parámetros del sistema de gestión de riesgos de las apuestas de contrapartida.	Sí/No.
Auditoría de cambios realizados por el personal del operador sobre las apuestas.	Sí/No.
Relación de sucesos aleatorios.	Relación de sucesos en los que intervenga el generador de números aleatorios, indicando si son presorteados.
Auditoría de cambios en la configuración mediante parámetros de la lógica del juego.	Sí/No.

3.3.5 Medidas contra el fraude y el blanqueo de capitales.

Este análisis será de aplicación únicamente para licencias generales y deberá describir las medidas implementadas por el operador para el control de los comportamientos fraudulentos o colusorios por parte del jugador.

Existencia de medidas técnicas contra el fraude y el blanqueo de capitales	Sí/No.
--	--------

3.4 Cuadro resumen de las pruebas de integración.

Este cuadro incluirá la calificación de las pruebas de integración practicadas clasificadas por áreas, que como mínimo deberá incluir a las descritas en el anexo VI.

La nomenclatura para las pruebas adicionales a las descritas en el anexo VI comenzará por «X».

Los resultados se detallarán del siguiente modo:

Área de requisitos A

A.1	Nombre de la prueba.....	Conforme.
A.2	Nombre de la prueba.....	No aplica.

A.3	Nombre de la prueba.....	No conforme.
X.1	Nombre de la prueba adicional.....	Conforme.
X.2	Nombre de la prueba adicional.....	Conforme.

Área y referencia del requisito.	Calificación.
----------------------------------	---------------

Área de requisitos B

B.1	Nombre de la prueba.....	Conforme.
B.2	Nombre de la prueba.....	No aplica.
X.3	Nombre de la prueba adicional.....	Conforme.

4. *Detalle del cumplimiento de los requisitos técnicos*

Los requisitos técnicos cuyo cumplimiento debe certificarse para cada licencia se describen en el anexo V a la Resolución por la que se aprueba esta disposición.

Para cada requisito se habrá obtenido una calificación que podrá ser «Conforme», «No conforme», o «No aplica».

En este apartado se detallará el cumplimiento de cada uno de los requisitos técnicos. Los requisitos se han agrupado por áreas.

Adicionalmente será necesario documentar en el espacio de observaciones las siguientes situaciones:

- Cuando el motivo por el que el requisito pudiera calificarse como «No aplica».
- Cuando haya habido incidencias, aunque posteriormente se hayan subsanado.
- Cuando las pruebas se hayan realizado en un entorno distinto al efectivamente empleado por el operador para el desarrollo de la actividad de juego.

Las calificaciones se detallarán del siguiente modo:

Área y referencia del requisito	Calificación	Observaciones
Área de requisitos X:		
Referencia A	Conforme.	
Referencia B	No conforme.	No es conforme al requisito debido a...
Referencia C	No aplica.	El requisito no es de aplicación debido a...

La entidad de certificación deberá entregar un anexo en el que para cada requisito técnico se documenten las evidencias de las pruebas realizadas y los resultados obtenidos.

5. *Detalle de los análisis específicos*

Para determinadas funcionalidades de especial relevancia, la entidad de certificación deberá realizar varios análisis específicos que se describen en este apartado.

5.1 Análisis de las comprobaciones de identidad y prohibiciones subjetivas.

La entidad de certificación analizará las comprobaciones de identidad y de las prohibiciones subjetivas.

El análisis deberá describir como mínimo los siguientes aspectos:

- Datos generales:
 - Si el sistema acepta participantes no residentes.
 - Si el sistema permite jugar sin registro de usuario. La entidad de certificación describirá el juego o juegos en los que puede darse esta circunstancia.
 - La relación de canales que pueden utilizarse para acreditar la identidad: internet, telefónico, SMS, presencial u otros.
- Las comprobaciones realizadas antes de activar el registro de usuario:
 - Si se utiliza el servicio de verificación de la identidad proporcionado por la Comisión Nacional del Juego para residentes.
 - Relación de otros medios de comprobación de la identidad utilizados.
 - La comprobación de la mayoría de edad.
 - La utilización del servicio de verificación de inclusión en el RGIAJ.
 - La realización de la comprobación de vinculados.
- Comprobaciones realizadas antes del abono de premios:
 - La utilización del servicio de variaciones del RGIAJ cada hora y la consiguiente actualización de la lista de prohibidos del operador y los estados de los participantes afectados.

5.2 Análisis del generador de números aleatorios.

Este análisis será de aplicación únicamente para licencias singulares donde se utilice un generador de números aleatorios, o GNA.

La entidad de certificación describirá los análisis, pruebas o tests realizados para justificar el comportamiento aleatorio del GNA y el cumplimiento de los requisitos técnicos. Se incluirán los resúmenes o gráficos justificativos, el número de simulaciones realizadas, los parámetros utilizados, así como el intervalo de confianza.

La entidad de certificación indicará si existen procedimientos de resemillado y si cumplen los requisitos técnicos.

En el caso de que existan parámetros de configuración de los que pudiera depender el funcionamiento del GNA, se describirán y se indicarán los valores de configuración para los que se ha realizado la certificación.

5.3 Análisis del retorno al jugador en los juegos.

La entidad de certificación deberá describir el porcentaje de retorno al jugador publicado por el operador para cada juego. También deberá verificar el sitio de publicación del referido porcentaje.

La entidad de certificación deberá describir todos los parámetros de configuración que puedan afectar al porcentaje de retorno al jugador, así como si el sistema técnico de juego permite registrar la auditoría de los cambios en dichos parámetros.

5.4 Análisis de la lógica del juego y los sucesos aleatorios.

La entidad de certificación, para cada una de las variantes de juego, deberá acreditar que el desarrollo del juego es conforme a las reglas particulares.

La entidad de certificación deberá analizar ciertos aspectos de la lógica del juego, los sucesos aleatorios en el juego, las configuraciones parametrizables, la contabilidad del juego y en general la capacidad de auditoría de cualquier cambio que se introduzca en las apuestas o los ganadores de forma manual.

Este análisis será de aplicación únicamente para licencias singulares.

En el caso de apuestas:

- Sistema de gestión de riesgos.

Para las apuestas de contrapartida, se describirá el sistema de gestión de riesgos, indicándose si para este fin se ha instalado alguna aplicación comercial o un desarrollo a medida.

Deberá indicarse si el sistema usado es parametrizable o no. En caso afirmativo, deberán describirse los parámetros de configuración más importantes así como los valores configurados en el momento de la certificación.

Asimismo, la entidad de certificación incluirá en este informe si la aplicación guarda un registro de los cambios llevados a cabo en el sistema referidos a la gestión de riesgos. En caso de que así sea, se indicará los ficheros o tablas de base de datos donde se almacena esta información.

Adicionalmente, para los operadores que ofrezcan apuestas en directo, deberán describirse las medidas implementadas por el operador para evitar que el jugador pueda realizar apuestas sobre acontecimientos que ya hayan tenido lugar o cuyo resultado sea conocido (“late betting”).

– Auditoría de las apuestas.

La entidad de certificación deberá explicar la aplicación de gestión de apuestas, y el registro y traza de las modificaciones que pudieran realizarse desde las aplicaciones de backoffice por el personal del operador, entre las cuáles se analizarán al menos las siguientes:

- Cambio de los datos de una apuesta.
- Inserción de nuevas apuestas.
- Borrado de apuestas.
- Cambio en el resultado del evento.
- Cambio en la adjudicación de los premios.

Se describirá la auditoría de los cambios, así como la manera en que se impide la manipulación de la auditoría.

Se deberá describir los ficheros o tablas de base de datos donde se almacena esta información de auditoría.

– Gestión de los fondos.

En las apuestas mutuas se deberá analizar la aplicación que gestiona la contabilidad de los fondos.

La aplicación explicará el registro y auditoría del fondo de juego, del reparto de premios, de los supuestos en que no hubiese acertantes de una categoría, o de cualquier otro movimiento.

En los juegos de casino, póquer, juegos complementarios y máquinas de azar:

– Se describirá cada uno de los sucesos aleatorios implementados en el juego en los que intervenga el generador de números aleatorios. Por ejemplo si existe mezcla inicial de cartas, el sorteo de la carta del mazo si no existe una mezcla inicial, la fabricación de los cartones de bingo, venta de cartones de bingo, el presorteo de las bolas del bingo, el sorteo de una bola de bingo si no es

presorteado, el giro de la ruleta, el giro de los rodillos en las máquinas de azar, etcétera.

– Se deberá analizar la gestión contable de las partidas y, de los botes progresivos, en aquellos juegos en los que se permita su utilización. Los importes apostados, los premios obtenidos, las comisiones calculadas o los botes progresivos constituidos o aplicados deberán poder ser auditados.

– Auditoría de las partidas.

La entidad de certificación deberá explicar el registro y traza de las modificaciones que pudieran realizarse desde las aplicaciones de backoffice por el personal del operador.

Se describirá la auditoría de los cambios, así como la manera en que se impide la manipulación de la auditoría.

Se deberá describir los ficheros o tablas de base de datos donde se almacena esta información de auditoría.

– En el caso de que el software utilizado para implementar la lógica de juego sea configurable, la entidad de certificación deberá describir e indicar el valor de los parámetros de configuración que estén relacionados con los siguientes aspectos:

- Modalidades de juego.
- Estrategia de juego de la banca o nivel de riesgo asumido.
- Importes máximos.
- Reglas de juego.

La entidad de certificación deberá acreditar asimismo que existe registro de auditoría de cualquier modificación de estos parámetros.

5.5 Medidas contra el fraude y el blanqueo de capitales.

Este análisis será de aplicación únicamente para licencias generales.

La entidad de certificación describirá y evaluará las medidas implementadas en el sistema técnico de juego contra el fraude y el blanqueo de capitales. Asimismo, se adjuntarán aquellos documentos o evidencias recabadas durante la certificación.

6. *Detalle de las pruebas de integración*

En este apartado se detallarán las pruebas de integración realizadas, clasificadas por áreas, que como mínimo comprenderán a las que se describen en el anexo VI a la Resolución por la que se aprueba esta disposición.

La nomenclatura para estas pruebas adicionales a las descritas en el anexo VI comenzará por «X».

El resultado de cada prueba recibirá la calificación de «Conforme», «No conforme», o «No aplica», en función del resultado esperado y el cumplimiento de la reglamentación.

Cada prueba se detallará del siguiente modo:

Área.	Del anexo VI.
Referencia de la prueba.	Del anexo VI o «X***» para las pruebas adicionales.
Nombre de la prueba.	
Descripción de la prueba.	
Resultado esperado.	
Tipo de prueba.	Según la clasificación de tipos de prueba del anexo VI.
Fecha/hora de realización de la prueba.	
Resultado obtenido.	
Calificación.	
Observaciones.	

Como resultado obtenido, la entidad de certificación deberá entregar un anexo en el que recogerá y documentará las evidencias del resultado de la realización de las pruebas de integración. Las evidencias que se deben recoger dependen del tipo de prueba a realizar y están descritas en el referido anexo VI a la Resolución por la que se aprueba esta disposición.

7. Descripción del lugar, equipo y fechas de realización de la certificación

En este apartado se describirá el equipo de trabajo que ha realizado la certificación, así como el lugar o lugares y la fecha o fechas en que se ha realizado.

8. Descripción de los entornos utilizados en las pruebas diferentes al efectivamente empleado por el operador para el desarrollo de la actividad de juego

En el caso de que determinadas pruebas del sistema técnico de juego se hayan realizado en un entorno diferente al efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la licencia, la

entidad de certificación deberá describir en este apartado los diferentes entornos empleados.

Para cada uno de estos entornos, se indicará la relación de pruebas para las que se ha utilizado cada entorno.

9. *Descripción del soporte digital que acompañará al informe de certificación*

Este apartado describirá el contenido del soporte digital que acompañará al informe de certificación.

El informe de certificación se acompañará de un soporte digital, y estará estructurado de la siguiente manera:

- Informe de certificación completo en formato digital.
- Cuestionario descriptivo del objeto de certificación en formato digital.
- Evidencias de la evaluación de los requisitos técnicos. Se agruparán dentro de una carpeta denominada «Requisitos técnicos».
- Evidencias de las pruebas de integración. Se agruparán dentro de una carpeta denominada «Integración».
- Copia de los elementos software del sistema técnico de juego, que contendrá copia de los binarios de los elementos software del sistema técnico de juego certificado. Deberán agruparse en una carpeta que se denominará «Binarios» y se estructurarán en subcarpetas con el nombre de cada uno de los elementos software indicados en el cuestionario.

ANEXO IV

Modelo y contenido del informe de certificación de la seguridad.

El informe de certificación de la seguridad se estructura en los apartados y presentará el contenido mínimo que a continuación se relaciona:

1. Identificación de la certificación.
2. Descripción del objeto de certificación.
3. Resumen ejecutivo de la certificación de la seguridad.
4. Detalle del cumplimiento de los requisitos de seguridad.
5. Detalle de los análisis de auditoría específicos.
6. Descripción del lugar, equipo y fechas de realización de la certificación.
7. Descripción del soporte digital que acompañará al informe de certificación.

1. Identificación de la certificación

En la primera página del informe se detallará lo siguiente:

- a) Tipo de informe de certificación: Se consignará «informe definitivo de certificación de la seguridad».
- b) Código de identificación del informe: El código de identificación del informe será único y permitirá referirse al mismo de manera unívoca y su diferenciación de cualquier otro informe emitido por la entidad de certificación. Cada vez que la entidad de certificación realice cualquier modificación en un informe deberá generar un nuevo código de identificación para el mismo.
- c) Datos identificativos de la entidad certificadora.
- d) Datos identificativos de quien firma el informe por parte de la entidad certificadora.
- e) Fechas de realización de los trabajos de certificación.
- f) Fecha de emisión del informe de certificación.

2. Descripción del objeto de certificación

El objeto de certificación de la seguridad será el sistema técnico de juego efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la correspondiente licencia, en relación con los procedimientos, procesos, planes y medidas de seguridad efectivamente implementados

A los efectos de describir el alcance del objeto de certificación de la seguridad se enumerarán tanto los centros de procesos de datos donde se albergue el sistema técnico de juego, como el software instalado en ellos, como las organizaciones donde estén implementados los procedimientos, procesos, planes y medidas de seguridad.

Para describir los centros de procesos de datos objeto que han sido objeto de certificación, se incluirá la siguiente relación:

CPD	Calle, número	Ciudad	País	Tipo	Razón social del proveedor de alojamiento
CPD 1					
CPD 2					
.....					

Los campos «calle», «número», «ciudad» y «país», se refieren a la localización física del CPD. El campo «tipo» indica la modalidad de alojamiento del CPD y

deberá coincidir con uno de los siguientes valores: «hosting», «housing» o «propio».

El campo de «razón social del proveedor de alojamiento», solo habrá de completarse en el caso de que «tipo» contenga uno de estos valores: «hosting» o «housing».

Para cada uno de los centros de procesos de datos, deberán identificarse los elementos de software empleados en el sistema técnico instalados en ellos, con mención expresa del fabricante, nombre de producto y versión.

Así mismo, deberá indicarse la relación de entidades responsables de la gestión de seguridad, es decir, de aplicar las políticas, procedimientos y medidas de seguridad certificadas en el informe.

3. Resumen ejecutivo de la certificación de la seguridad

3.1 Calificación global de la seguridad.

Se incluirá una calificación global del cumplimiento de los requisitos técnicos en materia de seguridad por el sistema técnico de juego efectivamente utilizado por el operador para la licencia. La calificación podrá ser «Conforme» o «No conforme».

Esta calificación solamente podrá ser «Conforme» cuando la entidad de certificación estime que el sistema técnico de juego efectivamente utilizado por el operador para la licencia es conforme con todos los requisitos que resulten de aplicación.

Calificación global de la funcionalidad	Se calificará globalmente el resultado del análisis como «Conforme» o «No conforme».
Convalidación ISO 27001	Se indicará si se utiliza en el informe la posibilidad de convalidación de ciertos requisitos a partir de una certificación ISO 27001.

3.2 Cuadro resumen del cumplimiento de los requisitos de seguridad.

Los requisitos técnicos en materia de seguridad cuyo cumplimiento debe certificarse para cada licencia se describen en el Anexo VII a la Resolución por la que se aprueba esta Disposición.

Para cada requisito se habrá obtenido una calificación que podrá ser «Conforme», «Convalidado», «No conforme», o «No aplica».

Los requisitos técnicos han sido agrupados por áreas.

En el resumen ejecutivo se presentará una tabla resumen con el número de requisitos que reciben cada calificación para cada área.

Las calificaciones se detallarán del siguiente modo:

	Número de requisitos	Número de requisitos conformes	Número de requisitos convalidados (ISO 27000)	Número de requisitos no conformes	Número de requisitos no aplica
Área XXX	7	6	0	0	1
Área YYY	4	3	1	0	0

3.3 Cuadro resumen de los análisis de auditoría específicos.

Para determinadas áreas de seguridad de especial relevancia, la entidad de certificación deberá realizar varios análisis de auditoría específicos que se describen en un apartado posterior.

En este apartado se señalará un resumen ejecutivo de los mismos:

3.3.1 Análisis de auditoría de los componentes críticos.

Calificación.	Se calificará globalmente el resultado del análisis como «Conforme» o «No conforme» respecto a la correcta identificación de los componentes críticos
---------------	---

3.3.2 Análisis de auditoría de la gestión de cambios

Calificación.	Se calificará globalmente el resultado del análisis como «Conforme» o «No conforme» respecto a los requisitos técnicos en esta materia.
---------------	---

3.3.3 Análisis de auditoría de la gestión de continuidad de negocio y prevención de la pérdida de información.

Calificación.	Se calificará globalmente el resultado del análisis como «Conforme» o «No conforme» respecto a los requisitos técnicos en esta materia. El resultado «Conforme» representa la conformidad de la entidad de certificación con que el sistema técnico del operador permite alcanzar los tiempos de recuperación o de pérdida de datos analizados en este apartado.
Tiempo máximo de recuperación ante un desastre.	Se indicará el peor de los tiempos máximo de recuperación ante un desastre, o RTO del inglés «recovery time objective» de entre los proporcionados por el operador.
Tiempo máximo de	Se indicará el peor de los tiempos máximos de

pérdida de información ante un desastre.	pérdida de información ante un desastre, o RPO del inglés «recovery point objective» de entre los proporcionados por el operador.
--	---

4. Detalle del cumplimiento de los requisitos de seguridad

Los requisitos técnicos en materia de seguridad cuyo cumplimiento debe certificarse para cada licencia se describen en el Anexo VII a la Resolución por la que se aprueba esta Disposición.

Para cada requisito se habrá obtenido una calificación que podrá ser «Conforme», «No conforme», o «No aplica».

En este apartado se detallará el cumplimiento de cada uno de los requisitos técnicos. Los requisitos se han agrupado por áreas.

Adicionalmente será necesario documentar en el espacio de observaciones las siguientes situaciones:

- El motivo por el que el requisito pudiera calificarse como «No aplica».
- Cuando haya habido incidencias, aunque posteriormente se hayan subsanado.

En el caso de que se haga uso de la posibilidad de convalidación de ciertos requisitos a partir de una certificación ISO 27001, se utilizará la calificación de «Convalidado» y en el campo de observaciones se indicará «ISO 27001».

Las calificaciones se detallarán del siguiente modo:

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
Área de requisitos X:			
Requisito AA.	Conforme		Documento XXXXX apartado YY
Requisito XX.	No conforme	No es conforme al requisito debido a....	
Requisito YY.	No aplica	El requisito no es de aplicación debido a...	
Requisito ZZ.	Convalidado	ISO 27001	

La entidad de certificación deberá entregar un anexo en el que adjuntará la documentación de seguridad, así como todas aquellas evidencias que permitan constatar el cumplimiento de los requisitos.

En aquellos casos donde exista soporte documental de la política o procedimiento, deberá hacerse constar en el campo de observaciones, la referencia documental así como el epígrafe donde se apoya el cumplimiento. La entidad de certificación deberá acreditar la efectiva aplicación de los controles de seguridad en el sistema técnico de juego efectivamente empleado. A tal efecto, se describirán las pruebas adicionales a la comprobación documental que se hayan realizado.

5. *Detalle de los análisis de auditoría específicos*

Para determinadas áreas de seguridad de especial relevancia, la entidad de certificación deberá realizar varios análisis de auditoría específicos que se describen en este apartado.

5.1 Análisis de auditoría de los componentes críticos.

La entidad de certificación emitirá un análisis sobre la correcta identificación por parte del operador de los componentes críticos del sistema técnico de juego. La entidad de certificación incluirá la relación de componentes críticos del sistema técnico de juego, indicando si la seguridad de los mismos ha sido reforzada. Para cada componente de esta relación deberá indicarse con qué elemento o elementos software del cuestionario presentado por el operador se corresponde.

5.2 Análisis de auditoría de la gestión de cambios.

La entidad de certificación emitirá un análisis sobre la correcta llevanza del procedimiento de gestión de cambios.

La entidad de certificación adjuntará, en caso de haberlas, las evidencias y documentación asociada de las tres últimas gestiones de cambio, respecto al momento de realizarse este análisis, realizadas por el operador.

En caso de disponer de una herramienta software para la gestión de cambios deberá indicarse cuál. Asimismo la entidad de certificación deberá acreditar que cualquier actuación (alta, modificación o baja de cambios) puede ser auditada.

5.3 Análisis de auditoría de la gestión de continuidad de negocio y prevención de la pérdida de información.

La entidad de certificación deberá analizar el tiempo máximo de recuperación ante un desastre, o RTO del inglés «recovery time objective», que indique el

operador, y valorar si las medidas técnicas disponibles son suficientes para lograrlo. El análisis deberá describir las medidas técnicas y la utilización de redundancia, planes de copias de seguridad, centros de respaldo u otras medidas.

La entidad de certificación deberá analizar el tiempo máximo de pérdida de información ante un desastre, o RPO del inglés «recovery point objective».que indique el operador, y valorar si las medidas técnicas disponibles son suficientes para lograrlo. El análisis deberá describir las medidas técnicas y la utilización de redundancia, planes de copias de seguridad, centros de respaldo u otras medidas. La entidad de certificación deberá cerciorarse de que las medidas dispuestas protegen todos los datos del operador, tanto los de usuario como los de juego.

Como desastre deberá evaluarse la posibilidad de un incidente que inutilice totalmente una ubicación física ante una contingencia imprevista.

6. Descripción del lugar, equipo y fechas de realización de la certificación

En este apartado se describirá el equipo de trabajo que ha realizado la certificación, así como el lugar o lugares y la fecha o fechas en que se ha realizado.

7. Descripción del soporte digital que acompañará al informe de certificación

Este apartado describirá el contenido del soporte digital que acompañará al informe de certificación.

El informe de certificación se acompañará de un anexo en soporte digital, que estará estructurado de la siguiente manera:

- Informe de certificación completo en formato digital.
- Documentación de seguridad completa utilizada para la evaluación de la seguridad, que se recogerá dentro de una carpeta con la denominación «Documentación».
- Evidencias de la evaluación de los requisitos técnicos en materia de seguridad. Se agruparán dentro de una carpeta denominada «Requisitos técnicos».

Certificación ISO 27001, en el caso de que sean aportadas para su convalidación.

ANEXO V

Relación de requisitos técnicos de funcionalidad.

Los diferentes requisitos que deben ser objeto de certificación se establecen en las normas reguladoras del juego: Ley, Reales Decretos, Órdenes Ministeriales y Resoluciones.

Sólo serán objeto de certificación del sistema técnico de juego las obligaciones establecidas en la normativa que estén directamente relacionadas con la evaluación técnica de equipos, software o instrumentos.

En este apartado se pretende mantener una guía que recopila los requisitos técnicos de los diferentes textos normativos que deben tener en consideración para la certificación de la funcionalidad.

Los requisitos se agrupan clasificados por áreas y se incluye la nomenclatura a utilizar en los informes definitivos de certificación de la funcionalidad.

Áreas:

Licencias generales:

- Área: Juego Responsable.
- Área: Contrato. Aceptación, copia y modificaciones.
- Área: Registro de usuario y comprobación de las prohibiciones.
- Área: Cuenta de juego, cobros y pagos.
- Área: Límites a los depósitos.
- Área: Registro y trazabilidad.
- Área: Terminales y sesión.
- Área: Canales de comunicación
- Área: Aplicaciones de juego gratuito.
- Área: Sistema de control interno.

Licencias singulares:

- Área: Porcentaje de retorno y tablas de premios.
- Área: Generador de números aleatorios.
- Área: Lógica del juego.
- Área: Registro y trazabilidad.
- Área: Terminales y sesión.
- Área: Canales de comunicación.
- Área: Aplicaciones de juego gratuito.
- Área: Interfaz gráfica.

- Área: Comportamiento ante errores técnicos.
- Área: Juego automático.
- Área: Repetición de la jugada.
- Área: Juegos «en vivo».
- Área: Funcionalidades varias.
- Área: Botes progresivos.
- Área: Sistema de control interno.
- Área: Desarrollo del juego.
- Área: Límites económicos a la participación.
- Área: Obligaciones de información a los participantes.
- Área: Promoción de los juegos.

ANEXO VI

Relación mínima de pruebas de integración

Este Anexo tiene por objeto la descripción de las pruebas que obligatoriamente han de ser realizadas para la certificación de la integración de los sistemas técnicos de juego de los operadores.

Las pruebas de integración deberán realizarse siempre en el entorno efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la licencia.

En las pruebas de integración que requieran datos personales de residentes en España, las entidades de certificación podrán hacer uso de los juegos de ensayo que facilitará a tal efecto la Dirección General de Ordenación del Juego para el entorno de producción de los servicios web de verificación.

Las pruebas se clasifican en función del tipo de licencia.

Se definen los siguientes tipos de pruebas junto con las evidencias mínimas que deberán recogerse en cada uno de ellos:

a) Funcional.

Las pruebas funcionales consistirán en la evaluación de características externas de una aplicación o sistema, utilizando los mismos medios que están a disposición de un participante o las aplicaciones de gestión que están a disposición del personal del operador.

Como evidencia deberá recogerse como mínimo:

- La conformidad o disconformidad de la prueba.

- Las capturas de pantalla resultado de la interacción entre el participante o personal del operador que realiza la prueba y la plataforma de juego.

b) Trazabilidad.

Las pruebas de trazabilidad consistirán en el análisis y contraste de los registros y trazas que se generan en el sistema cuando se realiza la prueba descrita. Los registros y trazas de este tipo de prueba serán los del sistema de información de la unidad central de juegos, no los del sistema de control interno.

Como evidencia deberá recogerse como mínimo:

- La conformidad o disconformidad de la prueba.
- Las capturas de pantalla que muestren la información del objeto de registro o traza.
- La descripción de la fuente de información (fichero, tabla...) donde se ha obtenido el registro o traza.

c) Datos reales.

El análisis de datos reales consistirá en verificar la correcta contabilidad, formato e integridad de los datos generados por la interacción entre participantes y el sistema técnico de juego.

Estas pruebas de integración con datos reales necesitarán que el sistema técnico de juego disponga al menos de un mes de datos, que no podrán ser completados mediante pruebas o simulaciones.

Como evidencia deberá recogerse como mínimo:

- La conformidad o disconformidad de la prueba.
- La fuente (fichero, tablas, etc.) de la que ha sido obtenida la información.
- Aquellos datos representativos que en cada prueba se requieran.

Las pruebas mínimas de integración en función del tipo de licencia y clasificadas por áreas son las siguientes:

A. Licencias Generales

A.1. Registro de usuario y comprobación de las prohibiciones.

Referencia de la prueba	A.1.1
Nombre de la prueba	Alta de registro de usuario
Tipo de prueba	Funcional, Trazabilidad
Descripción de la prueba	Desde el punto de vista de un participante, se procederá a realizar el registro de:

	<ul style="list-style-type: none"> - Un participante residente en España, con datos de identidad correctos, mayor de edad y no inscrito en el RGIAJ. - Un participante no residente. <p>Esta prueba deberá realizarse por parte de todos los operadores, independientemente de que el registro de usuario se requiera para la participación en el juego o para el registro de los ganadores.</p>
Resultado Esperado	<p>Se incluirá en el resultado el DNI/NIE, fecha y hora en la que se ha realizado cada alta, de forma que la Comisión Nacional del Juego pueda verificar a posteriori que los servicios de verificación de la DGOJ han sido consultados.</p> <p>En el registro del no residente, se incluirá el código utilizado para identificar al cliente, fecha y hora en la que se ha realizado las pruebas.</p> <p>Funcional</p> <p>Deberá validarse que el usuario ha sido dado de alta en el sistema.</p> <p>El sistema deberá recoger del participante todos los campos de información del participante descritos en la RES_TEC Anexo I apartado 2.1.1.</p> <p>En el caso de participante no residente, el sistema deberá solicitar una copia de un documento identificativo.</p> <p>Trazabilidad</p> <p>Se analizarán los registros y trazas del sistema que recogen los datos del registro de usuario realizado.</p> <p>Deberá verificarse la trazabilidad de la aceptación del contrato de juego firmado por el jugador.</p>

Referencia de la prueba	A.1.2
Nombre de la prueba	Comprobación de las prohibiciones subjetivas.
Tipo de prueba	Funcional, trazabilidad
Descripción de la prueba	<p>Desde el punto de vista de un participante, se procederá a realizar el registro de:</p> <ul style="list-style-type: none"> - Un participante residente en España que aporta datos incorrectos de identidad. - Un participante residente en España, con datos correctos de identidad, que figura inscrito en el RGIAJ. - Un participante residente en España, con datos correctos de identidad, menor de edad. - Un participante no residente en España, menor de edad. <p>La prueba se deberá realizar con los servicios de verificación operativos de la Dirección General de Ordenación del Juego</p>
Resultado Esperado	<p>Se incluirá en el resultado el DNI, fecha y hora en la que se ha realizado cada alta, de forma que la Dirección General de Ordenación del Juego pueda verificar a posteriori que los servicios de verificación de la DGOJ han sido consultados.</p> <p>Funcional</p> <p>El sistema no debe permitir el registro de los participantes menores, inscritos en el RGIAJ o cuyos datos de verificación resulten ser incorrectos.</p> <p>Trazabilidad</p> <p>Se analizarán los registros y trazas del sistema que recogen los datos del registro de usuario.</p>

A.2. Cuenta de juego, cobros y pagos.

Referencia de la prueba	A.2.1
Nombre de la prueba	Registro correcto de operaciones en la cuenta de juego
Tipo de prueba	Funcional, trazabilidad
Descripción de la prueba	Desde el punto de vista del participante, se realizarán operaciones de depósito y retirada en la cuenta de juego. Se analizará si existen otras operaciones disponibles en la cuenta de juego.
Resultado Esperado	Se incluirá en el resultado el DNI, fecha y hora, y descripción de cada operación realizada, de forma que la Comisión Nacional del Juego pueda verificar a posteriori que los datos llegan correctamente al sistema de control interno. Funcional Se verificará la correcta contabilización en la cuenta de juego de los depósitos y retiradas. En el caso de existir otras operaciones disponibles en la cuenta de juego, se incluirá en el resultado la relación de las mismas. Se verificará que entre las operaciones no existe ninguna que permita recibir crédito del operador o realizar transferencias entre participantes. Trazabilidad Se analizarán los registros y trazas del sistema que recogen los datos de la contabilización de depósitos y retiradas.

A.3. Límites a los depósitos.

Referencia de la prueba	A.3.1
Nombre de la prueba	Depositar por encima de los límites.
Tipo de prueba	Funcional, trazabilidad
Descripción de la prueba	Se accederá con una cuenta que tenga límites de depósito diario, semanal o mensual por defecto. Se bajarán los límites a 10, 15 y 20 euros respectivamente. Se realizarán depósitos por debajo del límite. Se realizarán depósitos por encima del límite. Se deberá probar cada límite, ya sea diario, semanal o mensual, utilizando diversas combinaciones de rangos horarios.
Resultado Esperado	Funcional El sistema permite reducir los límites. El sistema permite depósitos por debajo del límite y no los permite por encima. Trazabilidad Se analizarán los registros y trazas del sistema que muestren los cambios de los límites.

Referencia de la prueba	A.3.2
Nombre de la prueba	Datos de límites de depósito
Tipo de prueba	Datos reales
Descripción de la prueba	Se consultarán los datos reales del sistema para averiguar cuántos participantes tienen importes superiores a los preestablecidos. En caso de que existan participantes cuyos límites sean

	superiores a los preestablecidos, se verificará que se han realizado y evaluado correctamente las necesarias solicitudes de incremento de límites. A los efectos de esta prueba, bastará con realizar la comprobación de una muestra de 5 participantes, en caso de haberlos.
Resultado Esperado	Se incluirá en el resultado los códigos de identificación "JugadorId" de los participantes analizados, indicando las fechas en que realizaron las peticiones de incremento de límites y las fechas en que fueron autorizadas. Se verificará que el sistema conserva registros y trazas de las solicitudes, análisis realizados y autorización de incremento de límites.

A.4. Internet. Redirección a dominio «.es».

Referencia de la prueba	A.4.1
Nombre de la prueba	Redirección a dominio «.es»
Tipo de prueba	Funcional
Descripción de la prueba	El operador proporcionará a la entidad de certificación la lista de dominios diferentes a «.es» en los que él mismo, su matriz o sus filiales ofrecen juego. La entidad de certificación accederá a cada uno de los sitios desde una dirección IP asociada al territorio español y verificará la redirección.
Resultado Esperado	Se verificará que se efectúa la redirección a dominio «.es». La entidad de certificación listará los dominios diferentes de «.es» que se han utilizado en la prueba.

A.5. Sistema de Control Interno.

Referencia de la prueba	A.5.1
Nombre de la prueba	Estructura de directorios y ficheros reportados en el SCI.
Tipo de prueba	Datos reales
Descripción de la prueba	En esta prueba se verificará que la estructura de ficheros del almacén se ajusta a la establecida en el modelo de datos. Se revisará que para cada uno de los directorios se están reportando los registros oportunos. En concreto, se deberá revisar: <ul style="list-style-type: none"> • La estructura de directorios. • Que se reportan los registros correspondientes a las áreas RU y CJ. • Que se reportan los registros correspondientes a las áreas OP y JU para todas aquellas licencias singulares cuya actividad ha dado comienzo. • Que no se reportan registros correspondientes a las áreas OP y JU para licencias singulares de las que el operador no es titular.
Resultado Esperado	La entidad de certificación deberá indicar: <ul style="list-style-type: none"> • La estructura de directorios. • Si esta se ajusta al modelo de datos, indicando en su caso,

	<p>cualquier particularidad de éste, (existencia de varios almacenes, sinergias con otros operadores, etc.)</p> <ul style="list-style-type: none">• Cada uno de los tipos de registro correspondientes a las áreas RU y CJ que se reportan.• Relación de licencias singulares cuya actividad haya comenzado a operar. El rol del operador (B2C, B2B, ambos, y en caso de B2B, si actúa como coorganizador de juego) para cada uno de los juegos que haya comenzado a ofrecer en el momento de la certificación.• En relación al anterior punto, cada uno de los tipos de registro correspondientes a las áreas OP y JU que se reportan, que además, deberán ser consecuentes con el rol del operador para cada tipo de licencia indicado anteriormente.• Que no se reportan registros correspondientes a las áreas OP y JU para licencias singulares de las que el operador no es titular.
--	---

PROYECTO

Referencia de la prueba	A.5.2
Nombre de la prueba	XSD del SCI.
Tipo de prueba	Datos reales
Descripción de la prueba	En esta prueba se verificará que cada uno de los registros correspondientes a las áreas RU y CJ que se están reportando se ajustan al XSD del modelo de datos de monitorización.
Resultado Esperado	<p>La entidad de certificación deberá indicar:</p> <ul style="list-style-type: none"> • Cada uno de los registros correspondientes a las áreas RU y CJ que se reportan. • Si cada uno de los registros anteriores se ajustan al XSD. • Para cada uno de los registros, la versión de XSD utilizada.

PROYECTO

Referencia de la prueba	A.5.3
Nombre de la prueba	Integridad de los registros RUT y CJT.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se contrastarán los datos del SCI respecto a los datos del sistema de información del operador, con objeto de evaluar la integridad de los datos del SCI.</p> <p>Se obtendrán los siguientes datos mensuales para cada uno de los meses:</p> <p>A partir del registro RUT mensual:</p> <ul style="list-style-type: none"> • Número de altas • Número de participantes por estado. <p>A partir del registro CJT mensual:</p> <ul style="list-style-type: none"> • Saldo inicial • Depósitos • Retiradas • Participación • Devolución de la participación, • Premios • Saldo final • Premios en especie • Otros movimientos. <p>Esta prueba requiere que la entidad de certificación acceda a datos reales en claro. El operador deberá proporcionar en claro los ficheros RUT y CJT mensuales a la entidad de certificación y ésta deberá validar que éstos coinciden con los almacenados realmente en el sistema de información del operador.</p> <p>En ningún caso se requiere que la entidad de certificación conozca la clave de cifrado.</p>
Resultado Esperado	<p>Para el RUT mensual:</p> <ul style="list-style-type: none"> - Se contrastarán los datos del fichero RUT con listados obtenidos del backoffice del sistema técnico de juego. Es necesario que la entidad de certificación se cerciore de la veracidad de estos listados, dado que son la fuente para contrastar la integridad de los datos reales del SCI. <p>Para el CJT mensual:</p> <ul style="list-style-type: none"> - Se contrastarán los datos del fichero CJT con listados obtenidos del backoffice del sistema técnico de juego. Es necesario que la entidad de certificación se cerciore de la veracidad de estos listados, dado que son la fuente para contrastar la integridad de los datos reales del SCI. - Se verificará que el saldo inicial de un mes es igual al saldo final del mes inmediatamente anterior. - Se verificará que el saldo final equivale al saldo inicial y la suma del resto de movimientos. <p>Como resultado de esta prueba, la entidad de certificación</p>

	<p>deberá incluir:</p> <ul style="list-style-type: none">- La conformidad de las comprobaciones realizadas y evidencias de las mismas. <p>NOTA: Las comprobaciones y los cálculos se realizarán por separado, tanto en unidades monetarias "EUR", como en cualquier otra unidad, ya sean puntos de bonificación u otros.</p>
--	--

PROYECTO

Referencia de la prueba	A.5.4
Nombre de la prueba	Integridad de los registros RUD.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se contrastarán los datos del SCI respecto a los datos del sistema de información del operador, con objeto de evaluar la integridad de los datos del SCI.</p> <p>Se obtendrán los siguientes datos:</p> <p>A partir de los registros RUD se obtendrán:</p> <ul style="list-style-type: none"> • Diez altas de usuario escogidos de manera aleatoria. <p>Esta prueba requiere que la entidad de certificación acceda a datos reales en claro. El operador deberá proporcionar en claro los ficheros RUD mensuales a la entidad de certificación y esta deberá validar que éstos coinciden con los almacenados realmente en el sistema de información del operador.</p> <p>En ningún caso se requiere que la entidad de certificación conozca la clave de cifrado.</p>
Resultado Esperado	<p>Para el RUD mensual:</p> <ul style="list-style-type: none"> - Se contrastarán los datos del fichero RUD con listados obtenidos del backoffice del sistema técnico de juego. Se contrastará el estado de los usuarios, sus datos de identificación y su límite de depósitos. Es necesario que la entidad de certificación se cerciore de la veracidad de estos listados, dado que son la fuente para contrastar la integridad de los datos reales del SCI. <p>Como resultado de esta prueba, la entidad de certificación deberá incluir:</p> <ul style="list-style-type: none"> - La lista de identificadores de usuarios (campo ID) sobre los que se ha realizado la prueba. - La conformidad de las comprobaciones realizadas.

Referencia de la prueba	A.5.5
Nombre de la prueba	Integridad de los registros CJD.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se contrastarán los datos del SCI respecto a los datos del sistema de información del operador, con objeto de evaluar la integridad de los datos del SCI.</p> <p>Se obtendrán los siguientes datos:</p> <p>A partir de los registros CJD correspondientes a 10 usuarios elegidos aleatoriamente cuya participación sea distinta de cero euros, se obtendrá la siguiente información:</p> <ul style="list-style-type: none"> • Saldo inicial • Depósitos • Retiradas • Participación • Devolución de la participación, • Premios • Saldo final • Premios en especie • Otros movimientos. <p>Esta prueba requiere que la entidad de certificación acceda a datos reales en claro. El operador deberá proporcionar en claro los ficheros CJD mensuales a la entidad de certificación y ésta deberá validar que éstos coinciden con los almacenados realmente en el sistema de información del operador.</p>
Resultado Esperado	<p>Para el CJD mensual:</p> <ul style="list-style-type: none"> - Se contrastarán los datos del fichero CJD con listados obtenidos del backoffice del sistema técnico de juego. Es necesario que la entidad de certificación se cerciore de la veracidad de estos listados, dado que son la fuente para contrastar la integridad de los datos reales del SCI. <p>Como resultado de esta prueba, la entidad de certificación deberá incluir:</p> <ul style="list-style-type: none"> - La lista de identificadores de usuarios (campo ID) sobre los que se ha realizado la prueba. - La conformidad de las comprobaciones realizadas. <p>NOTA: Las comprobaciones y los cálculos se realizarán por separado, tanto en unidades monetarias "EUR", como en cualquier otra unidad, ya sean puntos de bonificación u otros.</p>

Referencia de la prueba	A.5.6
Nombre de la prueba	Consistencia entre los registros correspondientes al área RU.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se verificará la consistencia entre los registros correspondientes al área RU.</p> <p>En concreto, se deberá revisar:</p> <ul style="list-style-type: none"> • Número de jugadores totales en el RUD y de manera desagregada para cada uno de los estados. • Número de jugadores totales en el RUT y de manera desagregada para cada uno de los estados. • Se deberá verificar la correspondencia entre ambos.
Resultado Esperado	Se deberá indicar el número de jugadores obtenidos para cada estado a partir de cada registro y una valoración sobre la congruencia entre ellos.

PROYECTO

Referencia de la prueba	A.5.7
Nombre de la prueba	Consistencia entre los registros correspondientes al área CJ.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se verificará la consistencia entre los registros correspondientes al área CJ.</p> <p>En concreto, se deberá revisar:</p> <ul style="list-style-type: none"> • Saldo inicial • Depósitos • Retiradas • Participación • Devolución de la participación, • Premios • Saldo final • Premios en especie • Otros movimientos. <p>Se deberá verificar, para cada uno de los conceptos indicados, la correspondencia entre lo reflejado en el fichero CJT y la suma de cada uno de los valores reflejados en los ficheros CJD.</p>
Resultado Esperado	Se deberá indicar la suma total obtenida para cada uno de los conceptos y una valoración sobre la correspondencia entre los diferentes registros.

Referencia de la prueba	A.5.8
Nombre de la prueba	Consistencia del contenido del registro CJT.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se verificará la consistencia del contenido de los ficheros CJT, comparando los importes totales con los desglosados.</p> <p>Se obtendrán los siguientes datos mensuales a partir del registro CJT mensual:</p> <ul style="list-style-type: none"> • Saldo inicial • Depósitos • Retiradas • Participación • Devolución de la participación, • Premios • Saldo final • Premios en especie • Otros movimientos. <p>Esta prueba requiere que la entidad de certificación acceda a datos reales en claro.</p>
Resultado Esperado	<p>Se contrastarán para cada uno de los conceptos anteriormente señalados, que el valor del campo "Total" coincide con la suma de cada uno de los apuntes que figuran en el desglose (por tipo de juego o por tipo de medio de pago, según corresponda).</p> <p>Como resultado de esta prueba, la entidad de certificación deberá incluir:</p> <ul style="list-style-type: none"> - La lista de identificadores de usuarios (campo ID) sobre los que se ha realizado la prueba. - La conformidad de las comprobaciones realizadas. <p>NOTA: Las comprobaciones y los cálculos se realizarán por separado, tanto en unidades monetarias "EUR", como en cualquier otra unidad, ya sean puntos de bonificación u otros.</p>

Referencia de la prueba	A.5.9
Nombre de la prueba	Consistencia del contenido del registro CJD.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se verificará la consistencia del contenido de los ficheros CJD, comparando los importes totales con los desglosados.</p> <p>Se obtendrán los siguientes datos:</p> <p>A partir de los registros CJD correspondientes a 10 usuarios elegidos aleatoriamente cuya participación sea distinta de cero euros, se obtendrá la siguiente información:</p> <ul style="list-style-type: none"> • Saldo inicial • Depósitos • Retiradas • Participación • Devolución de la participación, • Premios • Saldo final • Premios en especie • Otros movimientos. <p>Esta prueba requiere que la entidad de certificación acceda a datos reales en claro.</p>
Resultado Esperado	<p>Se contrastarán para cada uno de los conceptos anteriormente señalados, que el valor del campo "Total" coincide con la suma de cada uno de los apuntes que figuran en el desglose (por tipo de juego o por tipo de medio de pago, según corresponda).</p> <p>Como resultado de esta prueba, la entidad de certificación deberá incluir:</p> <ul style="list-style-type: none"> - La lista de identificadores de usuarios (campo ID) sobre los que se ha realizado la prueba. - La conformidad de las comprobaciones realizadas. <p>NOTA: Las comprobaciones y los cálculos se realizarán por separado, tanto en unidades monetarias "EUR", como en cualquier otra unidad, ya sean puntos de bonificación u otros.</p>

Referencia de la prueba	A.5.10
Nombre de la prueba	Consistencia entre los registros CJD y RUD.
Tipo de prueba	Datos reales
Descripción de la prueba	En esta prueba se verificará que no existen jugadores para los cuales se esté reportando su registro CJD y, sin embargo, no conste su correspondiente registro RUD.
Resultado Esperado	Se deberán indicar los jugadores obtenidos en su caso, y una valoración sobre la correspondencia entre los registros.

Referencia de la prueba	A.5.11
Nombre de la prueba	Consistencia entre los registros CJ y las licencias de las que el operador es titular.
Tipo de prueba	Datos reales
Descripción de la prueba	En esta prueba se verificará que no existen registros correspondientes al área CJ en cuyo contenido se haga referencia a un juego para cuya actividad el operador no es titular de la correspondiente licencia. Asimismo, se verificará que se reportan registros CJ correspondientes a todos los juegos cuya actividad haya sido iniciada por el operador en el momento de la certificación.
Resultado Esperado	Se deberán indicar los juegos detectados durante la revisión del contenido de los registros CJ y una valoración sobre la correspondencia de estos con las licencias de las que el operador es titular y/o de las que ha iniciado actividad.

Referencia de la prueba	A.5.12
Nombre de la prueba	Certificado válido.
Tipo de prueba	Datos reales
Descripción de la prueba	En esta prueba se verificará con qué certificado se están firmando los datos y acreditará que se trata de un certificado válido y que no ha sido objeto de revocación. En ningún caso se requiere que la entidad de certificación conozca la clave de cifrado.
Resultado Esperado	La entidad de certificación verificará con qué certificado se están firmando los datos y acreditará que se trata de un certificado válido y que no ha sido objeto de revocación. La entidad de certificación indicará en el resultado la parte pública del certificado con que se están firmando los datos del almacén.

Referencia de la prueba	A.5.13
Nombre de la prueba	Validación del campo DNI/NIE.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se verificará que el sistema de control interno dispone de mecanismos para evitar los siguientes escenarios:</p> <ul style="list-style-type: none"> - Introducir valores erróneos en el DNI o NIE, como por ejemplo, errores de formato o letras incongruentes con el número. - Pasar a estado activo un registro de usuario cuyo DNI o NIE incluye errores. - Confundir el campo NIE con el campo DNI y viceversa.
Resultado Esperado	Se deberá describir el comportamiento del sistema para cada uno de los escenarios anteriormente expuestos, y una valoración sobre éste.

Referencia de la prueba	A.5.14
Nombre de la prueba	Validación del campo Tipo de medio de pago.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se verificará que los valores del campo "tipo de medio de pago se ajustan a la relación propuesta por la DGOJ en el momento de la certificación:</p> <p>Se deberá revisar para el registro CJT y para tres registros CJD elegidos de manera aleatoria que hayan registrados depósitos o retiradas por valor distinto de 0 €</p>
Resultado Esperado	<ul style="list-style-type: none"> - Se deberá indicar el registro CJT y los registros CJD sobre los que se ha hecho la prueba. - Se deberá indicar la versión de la relación de tipos de medios de pago con la que se ha realizado la valoración. - Se deberá indicar la conformidad de la prueba.

Modelo de resumen ejecutivo de las pruebas de integración para licencias generales.

Área y requisito	Calificación
A.1 Registro de usuario y comprobación de las prohibiciones	
A.1.1. Alta de registro de usuario	
A.1.2 Comprobaciones de las prohibiciones subjetivas	
A.2 Cuenta de juego, cobros y pagos	
A.2.1. Registro correcto de operaciones en la cuenta de juego	
A.3 Límites a los depósitos	
A.3.1 Depositar por encima de los límites	
A.3.2 Datos de límites de depósito	
A.4 Internet. Redirección a dominio “.es”	
A.4.1 Redirección a dominio “.es”	
A.5 Sistema de Control Interno	
A.5.1 Estructura de directorios y ficheros reportados en el SCI.	
A.5.2 XSD del SCI.	
A.5.3 Integridad de los registros RUT y CJT.	
A.5.4 Integridad de los registros RUD.	
A.5.5 Integridad de los registros CJD.	
A.5.6 Consistencia entre los registros correspondientes al área	
A.5.7 Consistencia entre los registros correspondientes al área	
A.5.8 Consistencia del contenido del registro CJT.	
A.5.9 Consistencia del contenido del registro CJD.	
A.5.10 Consistencia entre los registros CJD y RUD.	
A.5.11 Consistencia entre los registros CJ y las licencias de las	
A.5.12 Certificado válido.	
A.5.13 Validación del campo DNI/NIE.	
A.5.14 Validación del campo Tipo de medio de pago.	

B. Licencias Singulares.

B.1. Oferta de juego.

Referencia de la prueba	B.1.1
Nombre de la prueba	Oferta de juego y variantes de juego.
Tipo de prueba	Funcional
Descripción de la prueba	<p>Desde el interfaz del jugador, se accederá a comprobar la oferta de juego correspondiente a la licencia singular.</p> <p>Se analizará la oferta disponible de juego desde cada una de las diferentes aplicaciones o terminales de participación.</p> <p>Se analizará cada uno de los juegos y variantes ofrecidas, y se buscará la correspondencia con los juegos y variantes permitidas por la reglamentación básica.</p>

	Para realizar esta prueba no se requiere jugar, sino analizar la información publicada por el operador, ya sea informativa o reglas de los juegos.
Resultado Esperado	<p>Se indicará en el resultado una relación con la siguiente información:</p> <ul style="list-style-type: none"> - el nombre comercial de los juegos y variantes encontrados - las aplicaciones o terminales desde los que están disponibles. - la correspondencia con las variantes de la reglamentación básica. - la versión de las reglas particulares evaluadas. <p>Se contrastará esta información con el cuestionario descriptivo de la licencia cumplimentado por el operador.</p>

Referencia de la prueba	B.1.2
Nombre de la prueba	Desarrollo del juego y correcta contabilización.
Tipo de prueba	Funcional, trazabilidad
Descripción de la prueba	<p>Desde el interfaz del jugador se realizará participación en el juego, verificándose:</p> <ul style="list-style-type: none"> - la correcta contabilización de apuestas, premios, comisiones u otros. - en el caso de juegos en los que exista comisión del operador, se deberá verificar que el cálculo de comisiones se corresponde con lo establecido en las reglas particulares. - se intentará realizar una participación por importe superior al saldo disponible en la cuenta de juego. En el caso de determinados juegos, se verificará: <ul style="list-style-type: none"> - Para apuestas, que no se pueden realizar apuestas en momentos no previstos por las reglas particulares, y en particular con posterioridad al cierre de la comercialización, del inicio del evento para apuestas convencionales, o del final del evento para apuestas en directo. - Para bingo, que no permite comprar cartones fuera del periodo de comercialización, o cuando la partida hubiera comenzado. - Para póquer o casino, que no se pueden realizar apuestas fuera de los momentos designados para ello en las reglas particulares. - Para máquinas de azar, se comprobará que cuando la sesión destinada al juego de máquinas de azar finalice automáticamente por alcanzar el tiempo predeterminado o la cantidad fijada al configurar dicha sesión, la partida en curso finaliza ordenadamente, y la contabilización es correcta. <p>Nota: Esta prueba se repetirá para cada una de las diferentes aplicaciones o terminales de participación, y para cada uno de los juegos, variantes o modalidades.</p>
Resultado Esperado	<p>Funcional</p> <p>La conformidad de las verificaciones descritas anteriormente, desglosadas para cada variante analizada.</p> <p>Se verificará que no es posible realizar participación por importe</p>

	<p>superior al saldo disponible en la cuenta de juego. Asimismo se indicará la versión de las reglas particulares.</p> <p>Trazabilidad Se describirá en el resultado las tablas, ficheros u otros que contienen la información.</p> <p>Se emitirá juicio sobre si el sistema de registro del sistema técnico de juego permite recuperar información para explicar cada una de las situaciones, así como reconstruir totalmente lo acontecido en cada una de las partidas.</p>
--	---

Referencia de la prueba	B.1.3
Nombre de la prueba	Traza de la participación para canales diferentes a internet
Tipo de prueba	Trazabilidad
Descripción de la prueba	En el caso de que existan, se realizarán varias participaciones de cada uno de los canales diferentes de internet, por ejemplo, SMS y teléfono.
Resultado Esperado	<p>Trazabilidad</p> <p>Se analizarán los registros y trazas del sistema de cada una de los canales de participación utilizados, verificando que en el caso de SMS y teléfono el sistema conserva detalle de:</p> <ul style="list-style-type: none"> - fecha/hora de cada mensaje o llamada realizada - número de teléfono que ha originado el mensaje o llamada - contenido del mensaje o de la llamada

B.2. Límites a la participación.

Referencia de la	B.2.1
Nombre de la prueba	Límites a la participación.
Tipo de prueba	Funcional
Descripción de la prueba	<p>Se verificará que el sistema es conforme a los límites económicos: importes máximos de participación y de premio.</p> <p>Para ello la entidad de certificación participará en el juego intentando superar cada uno de los límites descritos en las órdenes ministeriales de los juegos, en el anexo III apartado segundo.</p> <p>Para las máquinas de azar se verificará que el sistema es conforme a los límites establecidos al iniciar la sesión destinada al juego de máquinas de azar, tanto el límite económico como el límite temporal. Asimismo, se verificará que la cantidad de dinero que un mismo participante puede dedicar a la participación en la máquina de azar no podrá exceder del importe del saldo que el participante tenga en su cuenta de juego en el momento en que se inicie la sesión de destinada al juego de máquinas de azar de las máquinas de azar, incrementado en el importe de los premios obtenidos en dicha sesión.</p>
Resultado Esperado	Se dejará constancia de las pruebas realizadas y el resultado obtenido.

B.3. Comportamiento ante errores técnicos.

Referencia de la	B.3.1
------------------	-------

Nombre de la prueba	Pérdida de la comunicación con el cliente.
Tipo de prueba	Funcional
Descripción de la prueba	<p>Se realizarán pruebas de iniciar una partida y se provocará la pérdida de comunicación con la unidad central de juegos.</p> <p>Se restablecerá la conexión al transcurrir 1 minuto, 5 minutos o 15 minutos (diferentes intervalos de tiempo).</p> <p>Se verificará la reacción del sistema para finalizar la partida y su conformidad con lo descrito en las reglas particulares. Esta prueba se deberá realizar para cada uno de los terminales, aplicaciones o clientes y cada uno de los juegos o modalidades ofrecidas.</p>
Resultado Esperado	<p>Se indicará la conformidad con las reglas particulares.</p> <p>Se indicará en el resultado el comportamiento obtenido para cada terminal, aplicación o cliente, y para cada juego o modalidad.</p> <p>Se incluirá también la versión de reglas particulares analizadas.</p>

Referencia de la prueba	B.3.2
Nombre de la prueba	Error en el cliente.
Tipo de prueba	Funcional
Descripción de la prueba	<p>Se iniciará una partida y se provocará el apagado inesperado del terminal cliente.</p> <p>Se iniciará de nuevo el terminal al transcurrir 1 minuto, 5 minutos o 15 minutos (diferentes intervalos de tiempo).</p> <p>Se verificará la reacción del sistema para finalizar la partida, y su conformidad con lo descrito en las reglas particulares. Esta prueba se deberá realizar para cada uno de los terminales, aplicaciones o clientes y cada uno de los juegos o modalidades ofrecidas.</p>
Resultado Esperado	<p>Se indicará la conformidad con las reglas particulares.</p> <p>Se indicará en el resultado el comportamiento obtenido para cada terminal, aplicación o cliente, y para cada juego o modalidad.</p> <p>Se incluirá también la versión de las reglas particulares analizadas.</p>

B.4. Sistema de control interno.

Referencia de la prueba	B.4.1
Nombre de la prueba	Estructura de directorios y ficheros reportados en el SCI.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se verificará que la estructura de ficheros del almacén se ajusta a la establecida en el modelo de datos. Se revisará que para cada uno de los directorios se están reportando los registros oportunos.</p> <p>En concreto, se deberá revisar:</p> <ul style="list-style-type: none">• La estructura de directorios.• Que se reportan los registros correspondientes a las áreas OP y JU para la licencias singular objeto del informe de certificación.
Resultado Esperado	<p>La entidad de certificación deberá indicar:</p> <ul style="list-style-type: none">• Si la estructura de directorios se ajusta al modelo de datos, indicando en su caso, cualquier particularidad de éste, (existencia de varios almacenes, sinergias con otros operadores, etc.)• El rol del operador (B2C, B2B, ambos, y en caso de B2B, si actúa como coorganizador de juego)• En relación al anterior punto, cada uno de los registros correspondientes a las áreas OP y JU que se reportan, que además, deberán ser consecuentes con el rol del operador.

Referencia de la prueba	B.4.2
Nombre de la prueba	XSD del SCI.
Tipo de prueba	Datos reales
Descripción de la prueba	En esta prueba se verificará que cada uno de los registros correspondientes a las áreas OP y JU que se están reportando se ajustan al XSD del modelo de datos de monitorización.
Resultado Esperado	<p>La entidad de certificación deberá indicar:</p> <ul style="list-style-type: none"> • Cada uno de los registros correspondientes a las áreas OP y JU que se reportan. • Si cada uno de los registros anteriores se ajustan al XSD. • Para cada uno de los registros, la versión de XSD utilizada.

PROYECTO

Referencia de la prueba	B.4.3
Nombre de la prueba	Integridad de los datos del SCI.
Tipo de prueba	Datos reales
Descripción de la prueba	<p>En esta prueba se contrastarán los datos del SCI respecto a los datos del sistema de información del operador, con objeto de evaluar la integridad de los datos del SCI.</p> <p>Se obtendrán los siguientes datos mensuales para cada uno de los meses:</p> <p>A partir del registro OPT/ORT mensual:</p> <ul style="list-style-type: none"> • Participación • Devolución de la participación • Premios • Premios en especie <p>Se obtendrán los siguientes datos diarios de los 5 días previos a la realización de la prueba:</p> <p>A partir de los registros JUT/JUD:</p> <ul style="list-style-type: none"> • Número de partidas de cada modalidad • Se tomará una muestra aleatoria de 5 partidas y se contrastarán sus datos con el sistema de información del operador. Por ejemplo, los participantes, los premios, el evento en el caso de una apuesta o el número de SMS's en el caso de un concurso. <p>Esta prueba requiere que la entidad de certificación acceda a datos reales en claro. El operador deberá proporcionar en claro los ficheros OPT/ORT y JUT/JUD a la entidad de certificación y ésta deberá validar que éstos coinciden con los almacenados realmente en el sistema de información del operador. No se requiere que la entidad de certificación tenga acceso a datos personales.</p> <p>En ningún caso se requiere que la entidad de certificación conozca la clave de cifrado.</p>

<p>Resultado Esperado</p>	<p>La entidad de certificación verificará con qué certificado se están firmando los datos y acreditará que se trata de un certificado válido y que no ha sido objeto de revocación. La entidad de certificación indicará en el resultado la parte pública del certificado con que se están firmando los datos del almacén.</p> <p>Se contrastarán los datos de los ficheros OPT/ORT y JUT/JUD con listados obtenidos del backoffice del sistema técnico de juego. Es necesario que la entidad de certificación se cerciore de la veracidad de estos listados, dado que son la fuente para contrastar la integridad de los datos reales del SCI.</p> <p>Como resultado de esta prueba, la entidad de certificación deberá incluir:</p> <ul style="list-style-type: none"> - La conformidad de las comprobaciones realizadas. - Los siguientes datos de OPT/ORT, calculados a partir de los datos mensuales, para cada mes: <ul style="list-style-type: none"> El cociente entre el importe de premios y el importe de participación (expresado con 4 decimales). <p>Nota: No se incluirá en el resultado cifras de facturación directamente.</p> <p>Nota: Las comprobaciones y los cálculos se realizarán por separado, tanto en unidades monetarias "EUR", como en cualquier otra unidad, ya sean puntos de bonificación u otros.</p>
---------------------------	---

Modelo de resumen ejecutivo de las pruebas predefinidas para licencias singulares

Área y requisito	Calificación
B.1 Oferta de Juego	
B.1.1. Oferta de juego y variantes de juego.	
B.1.2 Desarrollo del juego y correcta contabilización.	
B.1.6 Traza de la participación para canales diferentes a internet	
B.2 Límites económicos a la participación	
B.2.1 Límites económicos a la participación.	
B.3. Comportamiento ante errores técnicos.	
B.3.1 Pérdida de la comunicación con el cliente.	
B.3.2 Error en el cliente.	
B.4. Sistema de control interno.	
B.4.1 Estructura de directorios y ficheros reportados en el SCI.	
B.4.2 XSD del SCI.	
B.4.3 Integridad de los datos del SCI.	

ANEXO VII

Relación de requisitos técnicos de seguridad

Este Anexo tiene por objeto establecer la relación de los requisitos que, de conformidad con lo dispuesto en la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego objeto de las licencias otorgadas al amparo de la Ley 13/2011, de 27 de mayo, de regulación del juego, aprobada por Resolución de la Dirección General de Ordenación del Juego, de 16 de noviembre de 2011 («BOE» de 18 de noviembre), han de ser cumplidos por los sistemas técnicos de los operadores de juego y que deben ser verificados por las entidades de certificación en sus informes definitivos de certificación.

Las áreas que han de ser verificadas por las entidades de certificación y el orden en que habrán de presentarse en el informe correspondiente es el que sigue:

- a) Política de Seguridad.

De conformidad con el apartado 4.4 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. El operador dispone de procedimientos de seguridad.
2. Los procedimientos de seguridad han sido comunicados a la totalidad de sus empleados y, en su caso, a las entidades colaboradoras.

Aquellas organizaciones que hayan obtenido la certificación ISO 27001 vigente, podrán dar conformidad a los requisitos 1 y 2. En el apartado de observaciones se indicará «ISO 27001»

b) Análisis y Gestión de Riesgos.

De conformidad con los apartados 4.1, 4.2 y 4.3 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. El operador dispone de un plan de análisis y gestión de riesgos
2. Se realiza una revisión periódica del análisis de riesgos.
3. La organización tiene identificados los componentes críticos del Sistema Técnico de Juego.
4. En la relación de componentes críticos están incluidos:
 - a) El registro de usuario.
 - b) La cuenta de juego.
 - c) El procesamiento de los medios de pago.
 - d) En el generador de números aleatorios: los componentes del sistema técnico de juego que transmiten o procesan números aleatorios que serán objeto del resultado de los juegos y la integración de los resultados del generador de números aleatorios en la lógica del juego.
 - e) Aquellos componentes que almacenan, manipulan o transmiten información sensible de los clientes, como datos personales, de autenticación, etc.
 - f) Aquellos componentes que almacenan el estado puntual de los juegos. g) Las conexiones con la Dirección General de Ordenación del Juego.
 - h) El sistema de control interno: el capturador y el almacén.
 - i) Los puntos de acceso y las comunicaciones de y hacia los componentes críticos anteriores.
 - j) Las redes de comunicación que transmiten información sensible de participantes.
5. El operador tiene reforzada la seguridad de todos los componentes críticos.

En relación con los requisitos 4 y 5, la entidad de certificación en el campo de observaciones anotará las referencias documentales así como los epígrafes dentro de éstas en los que se constate el cumplimiento de dichos requisitos.

c) Organización de la Seguridad de la Información.

De conformidad con el apartado 4.5 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que la organización ha definido un marco de gestión para la seguridad de la información, indicando las funciones y responsabilidad de su personal.

Aquellas organizaciones que hayan obtenido la certificación ISO 27001 vigente, podrán dar conformidad a los requisitos de este área. En el apartado de observaciones se indicará «ISO 27001»

d) Seguridad en la comunicación con los participantes.

De conformidad con los apartados 2.1.12 y 4.6 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. El operador ha adoptado mecanismos de autenticación que permiten al sistema de juego identificar al participante, y que, a su vez, permiten al participante identificar al sistema de juego.
2. Las comunicaciones son cifradas en los casos de transmisión de datos personales (registro de usuario) o económicos (cuenta de juego).
3. En relación con las comunicaciones, el operador ha adoptado las medidas que resultan necesarias para garantizar la integridad y el no repudio en los casos de transmisión de datos personales o económicos, y en las transacciones de participación en el juego.
4. Se establece, por defecto o por el participante, una contraseña inicial de usuario.
5. Durante el proceso de definición de la contraseña de usuario, el participante es informado sobre buenas prácticas en la elección de contraseñas seguras
6. La longitud mínima de la contraseña es de 8 caracteres o dígitos, e incluye al menos elementos de tres de los siguientes grupos: números, letras minúsculas, letras mayúsculas y otros símbolos.

7. La contraseña no puede contener ninguno de los siguientes datos: el nombre del usuario, el seudónimo, el nombre o apellidos o la fecha de nacimiento del participante.
8. Se ofrece al usuario un recordatorio de cambio de contraseña con una frecuencia mínima anual, aunque no es obligatorio que el usuario realice el cambio.
9. El mecanismo de identificación mediante usuario y contraseña se bloquea si se producen en un mismo día más de 5 intentos de acceso erróneos. El operador puede establecer un límite inferior a este requisito.
10. El sistema del operador está diseñado para requerir la autenticación del participante ante cada inicio de sesión, y en el caso de uso de contraseñas, la introducción de la contraseña. El sistema no utiliza cookies u otros mecanismos para evitar la autenticación del usuario o la introducción de la contraseña.
11. El operador dispone de un procedimiento para detectar las cuentas inactivas durante un tiempo razonablemente prolongado y requiere un nivel de autenticación superior al normal o verificaciones adicionales a través del servicio de atención al cliente, antes de permitir reanudar la actividad de juego, especialmente las retiradas de fondos.
12. El operador dispone de un procedimiento para detectar dentro de lo razonable accesos no autorizados a la cuenta de los participantes, intentos de suplantación de identidad o acceso a sus datos personales.
13. El operador dispondrá de un procedimiento para detectar cambios bruscos en el comportamiento de un participante, y en particular del importe de los depósitos o retiradas, e iniciará alguna acción para prevenir que la cuenta de juego pueda estar siendo accedida por un tercero.

En relación con los requisitos anteriores, la entidad de certificación, en el campo de observaciones anotará las referencias documentales así como los epígrafes dentro de estas en las que se constata el cumplimiento de dichos requisitos.

e) Seguridad de recursos humanos y terceros.

De conformidad con el apartado 4.7 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. El operador dispone de un plan de Seguridad del Personal.

2. El plan incluye acciones formativas para todos los empleados de la organización, prestando especial atención a los permisos de acceso a información y componentes críticos.

3. En los casos en los que el operador necesite servicios de terceros que impliquen acceso, procesamiento, comunicación o tratamiento de la información, o bien el acceso a instalaciones, productos o servicios relacionados con el juego, éstos terceros deben cumplir la totalidad de los requisitos de seguridad exigibles al resto del personal.

Aquellas organizaciones que hayan obtenido la certificación ISO 27001 vigente, podrán dar conformidad a los requisitos de este área. En el apartado de observaciones se indicará «ISO 27001».

f) Seguridad física y medioambiental.

De conformidad con el apartado 4.8 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. Existe un plan de seguridad física de los componentes del sistema técnico de juego.

2. La seguridad perimetral para las áreas que contienen componentes críticos e información sensible está definida.

3. Existe un Control de acceso físico a las instalaciones en las cuales se encuentren los equipos, tanto para empleados como para personal externo, y que este control incluye elementos físicos, procedimientos de autorización, registros de acceso y servicios de vigilancia.

4. Está contemplada la protección frente a riesgos ambientales: agua, fuego, provocados por personas, etc.

5. Los equipos críticos están protegidos frente a cortes del suministro eléctrico y otras interrupciones causadas por fallos en instalaciones de soporte y que el cableado de suministro eléctrico está protegido de daños.

6. Están definidos los mecanismos de control de acceso al cableado de comunicaciones si transporta información crítica sin cifrar.

7. Se proporciona y está previsto el adecuado mantenimiento de las instalaciones y equipos.

8. Los dispositivos que contienen información son borrados de manera segura o destruidos antes de ser reutilizados o retirados.

9. Los equipos que contienen información no pueden ser trasladados fuera de las instalaciones seguras sin la correspondiente autorización.

En relación con los requisitos 2, 3, 4, 5, 7, 8, 9 anteriores, la entidad de certificación, en el campo de observaciones anotará las referencias documentales así como los epígrafes dentro de estas en las que se constata el cumplimiento de dichos requisitos.

Aquellas organizaciones que hayan obtenido la certificación ISO 27001 vigente, podrán dar conformidad a los requisitos de este área. En el apartado de observaciones se indicará «ISO 27001».

g) Gestión de Comunicaciones y Operaciones.

De conformidad con el apartado 4.9 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. Los componentes críticos son monitorizados para evitar que puedan utilizarse versiones diferentes de la homologada.
2. La comunicación entre los componentes de los sistemas técnicos de juego garantizan la integridad y la confidencialidad.
3. Las tareas se segregan entre las diferentes áreas de responsabilidad, para minimizar la posibilidad de acceso no autorizado y potenciales daños.
4. Se han separado las tareas de desarrollo, pruebas y producción.
5. Los servicios proporcionados por terceras partes incluyen controles y métricas de seguridad en los contratos y son periódicamente auditados y monitorizados.
6. Se han adoptado medidas de protección contra código malicioso.
7. Se hacen regularmente copias de seguridad con la frecuencia adecuada y se conservan custodiadas según quede recogido en el plan de copias de seguridad.
8. Se han adoptado medidas de seguridad en la red de comunicaciones.
9. Se han adoptado medidas de seguridad en la manipulación de soportes portátiles así como de borrado seguro o de destrucción de los mismos y que se plasma en un procedimiento documentado.
10. Los relojes de todos los componentes, especialmente de los críticos, están sincronizados con una fuente de tiempo fiable y el operador ha establecido

medidas y controles para evitar la manipulación de las marcas de tiempo o su alteración posterior, especialmente en los registros de auditoría.

11. Se genera y guarda registro de auditoría de actividad de todos los usuarios, excepciones y eventos de seguridad de la información durante un periodo mínimo de 2 años.

12. Los registros de auditoría están protegidos frente a la alteración y el acceso indebido.

13. Las actividades del Administrador del Sistema y del operador del Sistema están siendo registradas.

14. Se realiza un análisis periódico de los registros de auditoría y se toman acciones en función de las incidencias detectadas.

En relación con los requisitos 2, 4, 5, 6, 7, 8, 9,10, 11, 12, 13 y 14 anteriores, la entidad de certificación en el campo de observaciones anotará las referencias documentales así como los epígrafes dentro de éstas en las que se constata el cumplimiento de dichos requisitos.

Aquellas organizaciones que hayan obtenido la certificación ISO 27001 vigente, podrán dar conformidad a los requisitos de este área. En el apartado de observaciones se indicará «ISO 27001».

h) Control de Acceso.

De conformidad con el apartado 4.10 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. La política de acceso a información está documentada.
2. Se asegura el acceso autorizado y se impide el no autorizado mediante controles en el alta de usuarios, gestión de privilegios de acceso, revisión periódica de los privilegios de acceso y política de gestión de las contraseñas.
3. Los usuarios siguen buenas prácticas en el uso de contraseñas y protegen adecuadamente la documentación y soportes en su puesto de trabajo.
4. Los usuarios únicamente tienen acceso a los servicios que han sido autorizados a usar.
5. No existen usuarios genéricos y todos los usuarios acceden con su usuario propio único.
6. El sistema autentica todos los accesos, ya sea personal propio, de mantenimiento u otros, ya sea de otros sistemas y componentes. También será

autenticado el personal de inspección de la Comisión del Juego u otro personal que actúe en su nombre.

7. Las redes están segregadas en función del área y responsabilidad de la tarea o función.

8. El acceso a los sistemas operativos requiere un mecanismo de autenticación seguro.

9. Se restringe y se controla el uso de programas que permiten evitar los controles de acceso y de seguridad.

10. Las sesiones tienen un tiempo máximo de duración de la conexión y un tiempo de desconexión por inactividad.

11. El personal de soporte informático tiene restringido el acceso a los datos reales de las aplicaciones. Los datos reales sensibles están ubicados en entornos aislados.

12. Se gestionan los riesgos asociados a dispositivos móviles.

13. Si existe teletrabajo, se comprueba que el riesgo asociado está gestionado en el marco del plan de seguridad.

En relación con los requisitos 1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12 anteriores, la entidad de certificación en el campo de observaciones anotará las referencias documentales así como los epígrafes dentro de éstas en las que se constata el cumplimiento de dichos requisitos.

Aquellas organizaciones que hayan obtenido la certificación ISO 27001 vigente, podrán dar conformidad a los requisitos de este área. En el apartado de observaciones se indicará «ISO 27001».

i) Compra, desarrollo y mantenimiento de los sistemas.

De conformidad con el apartado 4.11 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que existe un plan de seguridad en la toma de decisiones de compra, desarrollo y mantenimiento de los sistemas de información.

Aquellas organizaciones que hayan obtenido la certificación ISO 27001 vigente, podrán dar conformidad a los requisitos de este área. En el apartado de observaciones se indicarán que «ISO 27001».

j) Gestión de incidentes de seguridad.

De conformidad con el apartado 4.12 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. Existe un procedimiento documentado de gestión de incidentes de seguridad.
2. Existe un registro de incidentes de seguridad (con hechos, impactos y medidas adoptadas).

Aquellas organizaciones que hayan obtenido la certificación ISO 27001 vigente, podrán dar conformidad a los requisitos de este área. En el apartado de observaciones se indicará «ISO 27001»

k) Gestión de cambios.

De conformidad con el apartado 4.13 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego y a lo establecido en el artículo décimo de esta Disposición, la entidad de certificación deberá verificar que:

1. Existe un procedimiento de gestión de cambios en equipos y componentes del sistema técnico de juego en el entorno de producción.
2. Existe un proceso de aprobación interna de cambios (petición de cambio, aprobación de los responsables).
3. Se conserva un registro de cambios (peticiones, decisiones adoptadas) y podrán ser objeto de posterior auditoría.
4. En el caso de cambios en componentes críticos, deberá evaluarse si se trata de un cambio sustancial.
5. Se conservarán copias de los binarios de los elementos de software de todas las versiones software que se hayan utilizado en el sistema técnico efectivamente empleado.

La Dirección General de Ordenación del Juego podrá establecer la obligación de que el procedimiento de conservación de las copias de los binarios incluya una huella digital de los mismos.

En relación con los requisitos 1, 2, 3, 4 y 5 anteriores, la entidad de certificación en el campo de observaciones anotará las referencias documentales así como

los epígrafes dentro de éstas en las que se constata el cumplimiento de dichos requisitos.

l) Plan de prevención de pérdida de información.

De conformidad con el apartado 4.15 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. Existe un plan de prevención de pérdida de datos o transacciones que afecten al desarrollo de los juegos, a los derechos de los participantes o al interés público.

2. Existe un plan de medidas para cumplir con el plan de prevención de pérdida de información y que incluirá los siguientes aspectos:

a) Ubicación donde se conservarán las copias de la información.

b) Medidas de seguridad de protección de la copia frente accesos no autorizados.

3. Existe un procedimiento de actuación en caso de pérdida de información que incluirá los siguientes aspectos:

a) Mecanismos de atención de reclamaciones.

b) Mecanismos de continuación de juegos interrumpidos.

En relación con los requisitos 1, 2 y 3 anteriores, la entidad de certificación en el campo de observaciones anotará las referencias documentales así como los epígrafes dentro de éstas en las que se constata el cumplimiento de dichos requisitos.

m) Gestión de continuidad de negocio.

De conformidad con los apartados 4.14 y 4.16 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. Existe una gestión de continuidad del negocio ante desastres que incluirá los siguientes aspectos:

- a) Medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio.
- b) Replica de la Unidad Central de Juegos que permita el normal desarrollo de la actividad.

2. El plan de continuidad considera los siguientes escenarios:

- a) Registro de usuario y cuenta de juego, con posibilidad de consultar el saldo y los movimientos de sus cuentas de juego asociadas. El tiempo máximo para prestar de nuevo estos servicios será de una semana.
- b) Retirada de fondos. El tiempo máximo para prestar de nuevo estos servicios será de una semana.
- c) Continuación de juegos incompletos o apuestas pendientes y pago de los premios válidamente conseguidos. El tiempo máximo para prestar de nuevo estos servicios será de un mes.
- d) Restablecimiento completo de todos los servicios.

3. En todos los escenarios se incluyen la siguiente información:

- a) Servicios recuperados.
- b) Tiempo máximo de recuperación.

En relación con los requisitos 1, 2 y 3 anteriores, la entidad de certificación en el campo de observaciones anotará las referencias documentales así como los epígrafes dentro de éstas en las que se constata el cumplimiento de dichos requisitos.

Aquellas organizaciones que hayan obtenido la certificación ISO 27001 vigente, podrán dar conformidad a los requisitos de este área. En el apartado de observaciones se indicarán que «ISO 27001».

- n) Penetración y análisis de vulnerabilidades.

De conformidad con el apartado 4.17 de la disposición por la que se desarrollan las especificaciones técnicas que deben cumplir los sistemas técnicos de juego, la entidad de certificación deberá verificar que:

1. En los últimos seis meses el sistema técnico de juego ha pasado un test de penetración y un análisis de vulnerabilidades.
2. Existe un plan de análisis, al menos bianual, de vulnerabilidades.

En relación con el requisito 1 anterior, la entidad de certificación en el campo de observaciones anotará las referencias documentales así como los epígrafes dentro de éstas en las que se constata el cumplimiento de dichos requisitos.

PROYECTO