PREGUNTAS FRECUENTES SOBRE LOS PROCEDIMIENTOS DE CERTIFICACIÓN, HOMOLOGACIÓN Y AUDITORÍA DE LOS SISTEMAS TÉCNICOS DE JUEGO.

1. Objetivo del documento

Habiéndose recibido en esta Dirección General de Ordenación del Juego (DGOJ) numerosas consultas en relación con los procedimientos de certificación, homologación y auditoría, se ha elaborado esta relación de preguntas frecuentes. El documento está sujeto a evolución y cambios.

2. Control de cambios

Versión	Fecha	Descripción de los cambios
1.0	12 de julio de 2012	Creación del documento: Preguntas frecuentes de carácter general.
1.0	30 de octubre de 2014	Creación del documento: Guía complementaria a la publicada en 2012.
2.0	15 de junio de 2016	• Se unifica en un único documento la Guía básica de preguntas frecuentes publicada en 2012 y la publicada en 2014. • Se eliminan las referencias al periodo transitorio. • Se amplían los supuestos en los que es posible presentar “informe de proveedor”. • Se hace referencia a la gestión telemática de los procedimientos.
3.0	11 de julio de 2017	Nuevo apartado: 13) Se incluyen aclaraciones en relación a los métodos de autenticación en la comunicación con los participantes.
4.0	22 de agosto de 2018	Nuevo apartado: 14) Se incluyen aclaraciones en relación a las auditorías bienales.
5.0	1 de abril de 2019	Nuevo apartado: 15) Se incluyen aclaraciones en relación a los generadores de números aleatorios criptográficamente fuertes.
6.0	15 de noviembre de	Se elimina el último párrafo del apartado 9.a.2, sección “Informe definitivo de certificación de la funcionalidad” de

	2019	acuerdo con los cambios introducidos en la nota sobre gestión de cambios sobre comercialización de juegos y cambios de CPD de proveedores sin licencia y que hayan sido previamente homologados por la DGOJ. Se modifica el apartado 7.a) en relación al contenido del informe de cumplimiento de la normativa de protección de datos de carácter personal. En el apartado 7.b, se actualiza la normativa del pliego de bases de solicitud de licencia, en la que se desarrolla el contenido del proyecto técnico.

3. Índice

4. Abreviaturas utilizadas

RES_TEC: *Resolución de 6 de octubre de 2014, de la Dirección General de Ordenación del Juego, por la que se aprueba la disposición por la que se desarrollan las especificaciones técnicas de juego, trazabilidad y seguridad que deben cumplir los sistemas técnicos de juego de carácter no reservado objeto de licencias otorgadas al amparo de la ley 13/2011, de 27 de mayo, de regulación del juego*.

RES_PRE_SCI: *Resolución de 6 de octubre de 2014, de la Dirección General de Ordenación del Juego, por la que se aprueba la disposición por la que se establecen los modelos de informes preliminares de las certificaciones de los proyectos técnicos y el modelo de informe de certificación de sistema de control interno, presentados por los solicitantes de licencias generales.*

RES_CERT: *Resolución de 6 de octubre de 2014, de la Dirección General de Ordenación del Juego, por la que se aprueba la disposición por la que se 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.*

OM_AZA: *Orden HAP/1370/2014, de 25 de julio, por la que se aprueba la reglamentación básica del juego de máquinas de azar.*

5. Procedimiento y plazo para solicitar la homologación

a) Plazos para la presentación de los informes definitivos de certificación

El plazo para la presentación de los informes de certificación será de cuatro meses improrrogable contado desde que le hubiera sido notificada la resolución de otorgamiento de la licencia general o de la licencia singular provisional.

La Dirección General de Ordenación del Juego dispondrá de un plazo de seis meses para la valoración de la homologación, contados también desde que le hubiera sido notificada la resolución de otorgamiento de la licencia general o de la licencia singular provisional.

b) Efectos de la no presentación de los informes de certificación en plazo

Los efectos de la no presentación del informe de certificación son los siguientes:

Licencias Generales

De acuerdo con la Orden por la que se aprueba el pliego de bases que regirán la convocatoria de licencias generales para el desarrollo y explotación de actividades de juego de la Ley 13/2011, el otorgamiento de la licencia general quedará condicionado a la presentación, en el plazo improrrogable de cuatro meses contados desde la notificación al interesado de la concesión de la citada licencia, del informe o informes definitivos de certificación de los sistemas técnicos de juego y su posterior homologación por parte de la Dirección General de Ordenación del Juego.

Licencias Singulares

De acuerdo con la Resolución de la Dirección General de Ordenación del Juego, por la que se establece el procedimiento de solicitud y otorgamiento de las Licencias Singulares para el desarrollo y explotación de los distintos tipos de actividades de juego, el otorgamiento provisional de la licencia singular quedará condicionado a la obtención, en el plazo improrrogable de seis meses contados desde su notificación al interesado, de la homologación definitiva a la que se refiere el número tercero del artículo 11 del Real Decreto 1613/2011, de 14 de noviembre, por el que se desarrolla la Ley 13/2011, de regulación del juego, en lo relativo a los requisitos técnicos de las actividades de juego. La licencia provisional se extinguirá en todo caso transcurrido el plazo referido en el párrafo anterior sin necesidad de pronunciamiento expreso por parte de la Dirección General de Ordenación del Juego.

c) Plazo para la presentación de las pruebas con datos reales

Determinadas pruebas obligatorias para la certificación requieren disponer de datos reales con al menos un mes de datos.

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 las mismas.

Los resultados de estas pruebas deberán ser presentados en el plazo de tres meses contados desde la fecha de inicio de la actividad de juego correspondiente.

d) Informes de certificación del operador que no ha iniciado la operación

El operador que no haya iniciado la operación de una determinada licencia debe presentar también el informe definitivo de certificación del sistema técnico de juego. Los informes de certificación del sistema técnico de juego deben ser presentados en plazo, independientemente de que el operador no haya iniciado la operación.

Para ello, aunque el operador no haya iniciado la operación deberá disponer de un sistema técnico, aunque no se esté utilizando efectivamente en la comercialización de juego, del que se realizará la certificación. Cuando el operador decida comenzar a comercializar juego deberá valorar necesita realizar cambios sustanciales de componentes críticos y por lo tanto el sistema debe ser homologado antes de su puesta en producción.

6. Alcance de la certificación

a) Alcance de los sistemas técnicos de juego

El 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, establece en su artículo 2 la definición del sistema técnico de juego y sus partes.

A los efectos de la homologación, el sistema técnico de juego es "*el conjunto de equipos, sistemas, terminales, instrumentos y material software empleado por el operador para la organización, explotación y desarrollo de la actividad de juego. El sistema técnico de juego soporta todas las operaciones necesarias para la organización, explotación y desarrollo de la actividad de juego, así como la detección y el registro de las transacciones correspondientes entre los jugadores y el operador*".

La organización, explotación y desarrollo de la actividad de juego puede abarcar en sentido amplio muchos elementos y servicios, como por ejemplo las redes de telecomunicaciones o los medios de pago.

De cara a la homologación de los sistemas técnicos de juego debemos hacer una interpretación más restrictiva atendiendo a los elementos que pueden condicionar el desarrollo del juego, el acceso de los participantes o el sistema de control interno.

Ejemplos de elementos que deben ser homologados (la lista no es exhaustiva):

- El registro de usuario y la comprobación de las prohibiciones subjetivas.
- La integración con servicios de verificación de la identidad.
- La cuenta de juego y la gestión de los fondos de los participantes.
- La integración de la plataforma de juego con la pasarela de pagos.
- El software de juego y el generador de números aleatorios.
- La integración con servicios de información sobre eventos, probabilidades, riesgos, precios o resultados de los mismos.
- Las aplicaciones de back-office que puedan alterar la configuración, el desarrollo y el resultado de los juegos. Por ejemplo, la aplicación de back-office que permita rectificar el ganador de una apuesta.
- El registro y la trazabilidad de los datos.
- El sistema de control interno: el capturador y el almacén.
- La interfaz de usuario:
    - Páginas web, scripts, objetos flash, etc.
    - Las aplicaciones descargables o las apps para terminales móviles.
- Los terminales físicos de carácter accesorio.
- Los elementos de juego físicos utilizados en el juego, como por ejemplo las mesas de ruleta para la versión «en vivo».
- El «call center» cuando se utilice para realizar juego.

Ejemplos de elementos que no deben ser homologados (la lista no es exhaustiva):

- El ordenador personal del participante.
- Las redes públicas de telecomunicaciones.
- Los proveedores de medios de pago, las redes de medios de pago o las pasarelas de pago.
- Los proveedores de servicios de verificación de la identidad.
- Los proveedores de servicios de información sobre eventos, probabilidades, riesgos, precios o resultados de los mismos.

- Los sistemas de información del operador que no puedan alterar la configuración, el resultado o el desarrollo de los juegos, o participen en el registro y la trazabilidad de los datos. Por ejemplo:
    - Las aplicaciones de back-office que únicamente consulten datos.
    - El sistema de contabilidad general del operador,
    - El datawarehouse del operador, si no forma parte del registro y trazabilidad del juego.
- El «call center» cuando no se utilice para realizar juego, sino para dar soporte a consultas, quejas y reclamaciones.

b) Requisitos que no sean de aplicación

En función de la oferta, desarrollo y comercialización de juego de un operador, determinados requisitos pueden no ser de aplicación. En este caso, los informes de certificación deben cumplimentarse con un «N/A».

En cualquier caso, debe entregarse un informe con todos los apartados cumplimentados.

La entidad de certificación debe juzgar qué requisitos y apartados del informe de certificación serán de aplicación en el caso de cada operador concreto.

c) Objeto de la certificación

El objeto de la certificación es el sistema técnico de juego efectivamente empleado por el operador para el desarrollo y explotación del juego objeto de la correspondiente licencia.

Esto es así tanto en los informes de certificación de la funcionalidad como de la seguridad.

Por ejemplo, para determinados requisitos de seguridad puede ser necesario evaluar la existencia y el contenido de procedimientos documentados de seguridad. La certificación no se realiza sobre la documentación, sino sobre el sistema real, de manera que se debe certificar que los procedimientos están operativos y que los controles y medidas que describen existen efectivamente.

d) Gestión electrónica de los procedimientos.

Las solicitudes de homologación y de cambio sustancial deben realizarse a través de la sede electrónica de la DGOJ. A tal efecto, se ha habilitado un formulario en la sección:

Procedimientos y Servicios electrónicos/ Para el operador/ Licencias

La tramitación de los procedimientos se hará íntegramente por medios electrónicos y no será necesario el uso del registro presencial para ningún trámite. Los resúmenes ejecutivos en papel firmados por la persona autorizada en la entidad de certificación podrán ser custodiados por el operador a disposición de la DGOJ que podrá requerirlos en caso necesario.

7. Documentación a presentar

a) Informe de cumplimiento de la normativa de protección de datos de carácter personal

En la solicitud de homologación del sistema técnico de juego, 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 según el *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (RGPD) y la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (LOPDGDD).

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.

El informe de la AEPD podrá ser tenido en cuenta por la Dirección General de Ordenación del Juego para la homologación del sistema técnico de juego.

En la Nota técnica que desarrolla el procedimiento de solicitud de cambios sustanciales en sistemas técnicos de juego se describen los supuestos de cambio en los que es necesario presentar una nueva versión del informe.

Dicho informe de valoración de cumplimiento ha de estar firmado por el delegado de protección de datos (DPO) del operador y debe contener la siguiente documentación:

- Registro de actividades de tratamiento (RAT) efectuadas bajo la responsabilidad del operador como responsable del tratamiento.
- Evaluación del impacto relativo a la protección de datos por los tratamientos de datos realizados por el operador.
- Política de privacidad evaluada por el DPO.

b) Descripción del sistema técnico de juego

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

1. Descripción actualizada del sistema técnico.
2. En el caso de licencias singulares, las reglas particulares.
3. El cuestionario descriptivo de la licencia.

<u>Descripción actualizada del sistema técnico</u>

Los operadores que certifiquen un sistema que haya sufrido variaciones respecto al descrito en el Proyecto Técnico deben actualizar la documentación aportada para que describa el sistema realmente utilizado que es objeto de certificación.

Para elaborar la documentación de la descripción actualizada del sistema técnico se puede tomar como referencia la siguiente:

- Para licencias generales, la requerida en el Anexo III de la Orden HFP/1227/2017, de 5 de diciembre, por la que se aprueba el pliego de bases que regirán la convocatoria de licencias generales para el desarrollo y explotación de actividades de juego de la Ley 13/2011, de 27 de mayo, de regulación del juego.
- Para licencias singulares, la requerida en el Anexo II de la Resolución de 1 de diciembre de 2017, de la Dirección General de Ordenación del Juego, por la que, de conformidad con lo dispuesto en el artículo 17 del Real Decreto 1614/2011, 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 licencias, autorizaciones y registros del juego, se establece el procedimiento de solicitud y otorgamiento de las Licencias Singulares para el desarrollo y explotación de los distintos tipos de actividades de juego.

Reglas particulares

Se deberán adjuntar las reglas particulares de todos los juegos, modalidades y variantes de la licencia correspondiente.

Cuestionario descriptivo del operador

Se deberán adjuntar en soporte electrónico el cuestionario descriptivo del operador.

Es fundamental que en la pestaña “LS Otros Juegos” (o en su caso, “LS Apuestas” o “LS Concursos”) del Cuestionario descriptivo del operador se describa claramente la oferta de juego del operador B2C. Para ello se deberá incluir el nombre del juego, el nombre del proveedor, la tecnología de acceso disponible y la fecha de inicio de la comercialización del juego.

c) Formato para la documentación a aportar

Es conveniente que la documentación aportada en formato electrónico esté organizada, para lo cual se sugiere una estructura de carpetas similar a la siguiente (subrayadas las carpetas):

- Licencia General/Singular XXXX
  - Resumen: relación de informes de certificación aportados para la licencia.
  - Descripción del Sistema Técnico de Juego
    - Descripción del Sistema Técnico.
    - Descripción de las Reglas Particulares, en el caso de licencias singulares.
    - Cuestionario descriptivo del operador.
  - Informe definitivo de certificación de la funcionalidad 01
  - Informe definitivo de certificación de la funcionalidad 02
  - Informe definitivo de certificación de la funcionalidad 03
  - Informe definitivo de certificación de la seguridad 01
  - Informe definitivo de certificación de la seguridad 02

Cada informe definitivo de certificación de la funcionalidad debería tener una estructura similar a la siguiente:

- Informe definitivo de certificación de la funcionalidad 01
  - Informe definitivo de certificación de la funcionalidad, completo.
  - Requisitos técnicos (evidencias)
    - Anexo RQ1…
    - Anexo RQ2…
    - ...
  - Análisis específicos (evidencias)
    - Anexo AE1…
    - Anexo AE2…
    - ...
  - Integración (evidencias)
    - Anexo PI1…
    - Anexo PI2…
    - ...
  - Binarios (copia de binarios del sistema técnico de juego)

Cada informe definitivo de certificación de la seguridad debería tener una estructura similar a la siguiente:

- Informe definitivo de certificación de la seguridad 01
  - Informe definitivo de certificación de la seguridad, completo.
  - Documentación (documentación de seguridad evaluada)
    - Documento de seguridad 01
    - Documento de seguridad 02
    - …
  - Requisitos técnicos (evidencias)
    - Anexo RQ1…
    - Anexo RQ2…
    - ...
  - ISO27001
    - Certificación ISO 27001, en caso de haber sido utilizada.

8. Aspectos a considerar en las pruebas de certificación

a) Juegos de ensayo para las pruebas de los sistemas de verificación de la identidad y RGIAJ

La Dirección General de Ordenación del Juego proporcionará a las entidades de certificación un conjunto de juegos de ensayo para la realización de las pruebas de integración de las comprobaciones de las prohibiciones subjetivas en el registro de usuario.

Estos juegos de ensayo están definidos para los siguientes servicios que proporciona la Dirección General de Ordenación del Juego:

- Consultas del servicio de verificación de la identidad.
- Consultas del registro general de interdicciones de acceso al juego (RGIAJ).

Estos juegos de ensayo solo cubren pruebas de usuarios con DNI o NIE, no de personas no residentes y no son de utilidad para otros servicios de verificación.

La DGOJ enviará la relación de juegos de ensayo al representante de cada una de las entidades de certificación por correo electrónico. Si alguna entidad de certificación experimenta alguna incidencia con la recepción o el uso de los juegos de ensayo, puede ponerse en contacto con el buzón dgoj.control@hacienda.gob.es.

b) Detalle de las evidencias del cumplimiento de requisitos técnicos

Los informes de certificación deben recoger el detalle que permita verificar que la prueba ha sido llevada a cabo y disponer de información suficiente para contrastar el resultado. El detalle necesario dependerá del mecanismo utilizado para la acreditación de los requisitos. A este respecto se puede tomar como referencia lo definido para los tipos de pruebas FUNCIONAL, TRAZABILIDAD, DATOS REALES, descritas en el ANEXO VI de la Resolución de la DGOJ por la que se aprueba la 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.

En el caso de que se utilicen otros métodos de acreditación, las siguientes observaciones pueden servir como guía:

- DOCUMENTALES: se debe aportar el documento en el que se sustenta la acreditación, así como la referencia dentro del documento que permite acreditar el requisito en cuestión.
- ANÁLISIS DE CÓDIGO: se deberá hacer una breve descripción del proceso de selección de los casos de prueba, de los criterios de cobertura utilizados (sentencias, decisiones, estructurales, funcionales, estadísticos, etc.) así como de los resultados obtenidos.
- SIMULACIÓN: se deberá describir brevemente el método de simulación utilizado, el número de iteraciones realizadas, el análisis de los resultados obtenidos y el grado de confianza estadístico de los resultados obtenidos.

c) Pruebas de integración con datos reales del sistema de control interno (SCI)

Determinadas pruebas de integración tratan sobre la integridad de los datos reales del sistema de control interno. Estas pruebas se han diseñado de manera que se garantice la seguridad y se evite el acceso a datos personales en la medida de lo posible. Las entidades de certificación no tendrán acceso a las claves de cifrado de los datos en el almacén:

- Para ello se requiere que el operador proporcione determinados ficheros del SCI en claro a la entidad de certificación.
- La entidad de certificación incluirá en el informe ciertos cálculos, por ejemplo, el cociente entre el importe de premios y el importe de participación, de manera que la DGOJ podrá auditar posteriormente que los datos evaluados por la entidad de certificación coinciden con los que han sido aportados por el operador al SCI.
- Los ficheros a comprobar serán RUT, CJT, OPT/ORT, JUT y JUD, que no contienen datos personales de participantes.

La entidad de certificación deberá contrastar los datos del SCI con listados obtenidos del backoffice del sistema técnico de juego. Es necesario que la entidad de certificación se cerciore de la veracidad estos listados, dado que son la fuente para contrastar la integridad de los datos reales del SCI.

d) Tiempo necesario para las pruebas de integración con datos reales

Pruebas con datos reales en el contexto de la solicitud de homologación del sistema técnico de juego:

Las 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.

Para las pruebas del SCI con ficheros mensuales, pruebas A.5.1 y B.4.1, deberá utilizarse al menos un fichero mensual en el que el operador haya comercializado el juego durante el mes completo. Ejemplos:

- Para los operadores que hayan iniciado la comercialización el 5 de junio, el informe de certificación deberá evaluar como mínimo los datos mensuales de junio y julio, siendo julio el primer mensual completo.
- Para los operadores que hayan iniciado la comercialización el 10 de julio, el informe de certificación deberá evaluar como mínimo los datos mensuales de julio y agosto, siendo agosto el primer mensual completo.

Las pruebas sobre datos reales del backoffice del operador distintos de los contenidos en el SCI, prueba A.3.2, se requerirá que el sistema disponga de un mes de datos. Ejemplo:

- Para un operador que haya iniciado la comercialización el 5 de junio, la primera fecha en la que se podría realizar esta prueba sería el 5 de julio.

Pruebas con datos reales en el contexto de certificación de cambio sustancial:

En la certificación con carácter previo al cambio, no es requisito indispensable realizar pruebas en el entorno empleado efectivamente para la comercialización. Al exigirse que la certificación se realice con anterioridad a la puesta en producción las pruebas pueden realizarse en un entorno de preproducción.

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.

Las pruebas de integración sobre el sistema de control interno, pruebas A.5.1, B.4.1 y B.4.2, deberán realizarse con datos ficticios de la forma más aproximada posible tomando las consideraciones que se consideren oportunas. No será necesario realizar las pruebas con datos reales.

e) Pruebas de todos los juegos, variantes y modalidades

Determinadas pruebas incluyen la siguiente aclaración o un comentario similar:

NOTA: Esta prueba se repetirá para cada una de las diferentes aplicaciones o terminales de participación y para cada una de los juegos, variantes o modalidades.

Ello significa que se deben probar todas las aplicaciones, terminales, juegos, variantes o modalidades que puedan tener alguna influencia en la prueba realizada. Ejemplos:

- Al probar las reglas del juego de los juegos complementarios será necesario probar cada uno de los juegos, por ejemplo, mus, tute y brisca, ya que cada uno de ellos tendrá una implementación y una lógica del juego distinta.
- Al probar las reglas de las apuestas deportivas no será necesario probar apuestas en cada uno de los deportes si el motor de las apuestas es común en todos ellos. Es posible que el motor implemente una lógica diferente para las apuestas en vivo o las convencionales por lo que tendría sentido que se realicen pruebas de cada uno de estos tipos.
- El operador puede ofrecer tres tipos de Black Jack por lo que será necesario probar cada uno de ellos ya que cada variante tiene su propia lógica del juego.

f) Huellas digitales de los componentes críticos en los informes de certificación

El apartado séptimo del anexo I de la RES_CERT establece en su último párrafo que: *"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."*

Los informes definitivos de certificación de la funcionalidad incluirán las huellas digitales de los componentes calificados como críticos. Se incluirán las huellas digitales de estos componentes críticos dentro del apartado "2. Descripción del objeto de certificación" del Anexo III por el que se describe el modelo y contenido del informe de certificación de funcionalidad.

Los informes definitivos de certificación de la seguridad incluirán un análisis de auditoría específico de los componentes críticos, si bien en este informe no se requiere incluir las huellas digitales de los mismos.

9. Notas aclaratorias de diferentes supuestos en la presentación de informes de certificación

a) ¿En qué casos se acepta un "informe de proveedor"?

La certificación y homologación de un sistema técnico de juego se realiza por Licencia y Operador. El operador es el responsable último del cumplimiento de los requisitos técnicos y los informes de certificación deben ser realizados para el operador y sobre su sistema técnico de juego. No obstante, en determinados supuestos, es posible acreditar el cumplimiento en los procedimientos de homologación mediante informes de certificación del proveedor.

a.1) Certificación preliminar en el marco de la solicitud de licencia

Apartados b) y c) del Proyecto técnico e Informes preliminares de licencias generales (LG) y licencias singulares (LS):

Los apartados b) y c) del proyecto técnico de LG y LS podrán dividirse y presentarse organizados por proveedores por lo que los informes preliminares de certificación de LG y LS podrán estar realizados a nombre del proveedor y no del operador final.

El informe de certificación preliminar podrá realizarse sobre el proyecto técnico propuesto por un proveedor que por tanto podrá ser reutilizado por varios operadores en el caso de que no varíe la solución técnica que describe el proyecto técnico.

En todo caso:

- La información contenida en el proyecto técnico y en el informe preliminar, elaborados por un proveedor y su entidad de certificación y presentados por un operador en la solicitud de una licencia, debe ser de aplicación íntegramente en la solución del operador. Por ejemplo, no sería válido presentar un proyecto técnico de un proveedor que incluyera 10 variantes de juego y 2 canales de participación y adicionalmente un proyecto técnico del operador que modifique la información anterior para indicar que solo se tiene intención de ofrecer 5 variantes y 1 canal de participación.
- El operador es responsable de toda la información contenida en los documentos que presenta en el procedimiento incluido el proyecto técnico del proveedor por lo que aquellas cuestiones que no le apliquen no deberán ser incluidas en el proyecto.
- La información aportada debe ser consistente y no deben existir contradicciones entre diferentes documentos del operador y de su proveedor.

Informes de certificación del SCI:

El informe de certificación definitiva del SCI en el marco de la solicitud de licencia podrá realizarse sobre la solución de sistema de control interno implementada por un proveedor y podrá ser reutilizado por varios operadores en el caso de que no varíe la solución técnica implementada.

a.2) Certificación definitiva en el marco de la solicitud de homologación inicial o cambio sustancial:

Informe definitivo de certificación de la seguridad:

El operador podrá solicitar a la entidad de certificación un único informe de certificación de la seguridad que alcance a todo su sistema técnico de juego y 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.

Algunos ejemplos podrían ser los siguientes:

- Un operador presenta un informe de certificación de la seguridad de toda su infraestructura técnica, y reutiliza el mismo informe en todas las licencias generales y singulares.
- Un operador utiliza varios CPD's. En unos se aloja el Black Jack y en otros la ruleta. Podría decidir presentar un único informe de seguridad que cubra todos los CPD's, o bien podría decidir presentar un informe de seguridad de los CPD's del Black Jack y otro de los CPD's de la ruleta.
- Un operador tiene infraestructura técnica propia, pero para el juego del póquer se apoya adicionalmente en un proveedor de servicios de juego. Para el póquer deberá presentar:
    - El informe de certificación de seguridad de su propia infraestructura.
    - El informe de certificación de seguridad de su proveedor de póquer.
- Un operador con un proveedor de almacén. Deberá presentar:
    - El informe de certificación de seguridad de su propia infraestructura.
    - El informe de certificación de seguridad de su proveedor de almacén.

Informe definitivo de certificación de la funcionalidad:

La primera vez que un operador se integre con un proveedor de software para la explotación de una determinada licencia, ya sea en la homologación inicial o a través de una gestión de cambios posterior, es necesario presentar un informe definitivo de certificación de la funcionalidad realizado al operador que acredite la correcta integración de la plataforma del operador[1] con el nuevo proveedor de software de juego.

En caso de que existan varios tipos de integraciones deberá acreditarse la certificación de todas ellas. Por ejemplo, si existe una integración con la plataforma para PC y una integración con la plataforma para móvil será necesario certificar la correcta integración del operador con su proveedor en ambas.

Si con posterioridad se producen cambios sustanciales en los servicios del proveedor tales como la introducción de nuevos juegos, un cambio mayor en una versión de software de juego o cambios que

[1] A estos efectos forma parte de la plataforma del operador, en su caso, la de sus proveedores de registro de usuario, cuenta de juego, software de sesión destinada al juego de máquinas de azar o sistema de control interno.

modifiquen la generación de los números aleatorios y el tratamiento de esta información, si los cambios no afectan a la integración el operador podrá presentar un informe definitivo de certificación de la funcionalidad de proveedor.

b) Certificación de la sesión destinada al juego de máquinas de azar.

En función del modelo de negocio del operador, los componentes software correspondientes a la sesión de juego destinada a las máquinas de azar pueden estar implementados en la capa de software de juego o bien en la capa de plataforma de juego. En este último caso, para certificar el sistema técnico de juego correspondiente a la licencia singular de máquinas de azar se podrá presentar:

- Un informe de certificación de funcionalidad independiente para cada uno de los proveedores de software de juego que certifique el software de juego.

- Un informe de certificación de funcionalidad que certifique la sesión de juego de las máquinas de azar y su integración con cada uno de los proveedores de juegos y con la plataforma de juego del operador. En el alcance de este informe se describirá la solución implementada y el conjunto de proveedores de juegos de máquinas de azar integrados. En caso de que existan varios tipos de integraciones (por ejemplo, PC, móvil, etc.), deberán certificarse todas.

  Los requisitos técnicos que deberán certificarse son, al menos, los relativos a las siguientes áreas:

  - ✓ Área: Configuración y desarrollo de la sesión de juego destinada a máquinas de azar.
  - ✓ Área: Obligaciones de información a los participantes en relación a la sesión de juego destinada a máquinas de azar.

  En cuanto a las pruebas de integración, deberá certificarse el desarrollo, la correcta contabilización y los límites en la participación definidos en el marco de la sesión de juego destinada a máquinas de azar y la integridad de los registros del sistema de control interno. Es decir, deberán realizarse las pruebas de integración B.1.2, B.2.1, B.4.1 B.4.2 en lo que concierne a la sesión de juego destinada a máquinas de azar.

c) Informes definitivos de certificación de funcionalidad por oferta de juego

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

En las licencias singulares, si se desea certificar la funcionalidad de un conjunto de variantes de juego se podrá emitir un único informe por cada variante o bien incluir en un único informe todas las variantes. En este último caso es fundamental que el alcance describa claramente el conjunto de variantes certificadas y sus tecnologías de acceso y que a lo largo del informe se indique, para cada prueba, análisis o requisito técnico, las variantes a las que se refiere la valoración emitida o cualquier otra información que se incluya en el proyecto.

d) Informes de certificación y proveedores de servicios / proveedores de software de juego

A los efectos de la certificación del sistema técnico de juego se deben diferenciar los proveedores de servicios de juego y los proveedores del software de juego. Los proveedores de servicios de juego participan con su infraestructura técnica en el sistema técnico de juego completo ("Software As A Service"), mientras que los proveedores de software de juego proporcionan el software pero no gestionan la infraestructura técnica ("Adquisición de Software"). El sistema técnico de juego incluye los sistemas de todos los proveedores de servicios de juego que participen en la solución completa y el software suministrado por los proveedores de software de juego.

El operador solicitante deberá responsabilizarse de homologar el sistema técnico de juego completo y de presentar informes definitivos de certificación. Esto es independiente de que el proveedor de servicios de juego o de software de juego pueda tener la condición o no de operador de juego en España.

Dicho esto, un proveedor de servicios de juego puede certificar la seguridad de su sistema, y dicho informe de certificación de la seguridad podrá ser presentado y reutilizado por cada uno de los operadores a los que preste servicio.

e) Informes de certificación de operadores coorganizadores de red

En el procedimiento de homologación de una licencia singular de un operador que es coorganizador de una red, el operador coorganizador deberá presentar:

- El informe de certificación de la funcionalidad con las siguientes características:
  - El alcance de la certificación deberá incluir únicamente los elementos del sistema técnico del operador de red dedicados a la licencia singular.
  - En cada caso concreto y según sea la solución técnica adoptada serán o no de aplicación algunos requisitos tales como las obligaciones de información a los participantes, la promoción de los juegos, o la publicación de las reglas del juego.
  - El operador de red deberá disponer de un Sistema de Control Interno en el que constarán los registros ORT, BOT, JUT y JUD.
- El informe de certificación de la seguridad

f) Informes de certificación de operadores que se conectan a un operador coorganizador de red

En el procedimiento de homologación de una licencia singular de un operador cuyos participantes acceden al juego de un operador coorganizador de una red, el operador deberá presentar:

- El informe de certificación de la funcionalidad con las siguientes características:
  - El alcance de la certificación incluirá tanto los sistemas del operador como los sistemas del operador coorganizador.
  - El operador certificará todos los requisitos en el sistema objeto de certificación. En las pruebas de integración también participarán los sistemas del operador coorganizador.
  - El operador deberá disponer de un sistema de control interno en el que probablemente constará únicamente el registro OPT.
- El informe de certificación de la seguridad.
  - El operador puede presentar dos informes, el informe de seguridad de su propia infraestructura técnica y el informe de seguridad del operador coorganizador.

g) Informes de certificación de operadores sin relación directa con participantes

Para aquellos operadores que no tengan relación directa con los participantes (registro de usuario, cuenta de juego, depósitos, retiradas, contrato de juego), la mayor parte de los requisitos de una licencia general no son aplicables.

En los informes de certificación de la funcionalidad de la licencia general, pueden ser de aplicación los apartados 3.3.5 y 5.5 en el caso de que el sistema técnico implemente medidas contra el fraude y el blanqueo de capitales. En caso de que las medidas contra el fraude y blanqueo de capitales no formen parte del sistema técnico de juego, sino que se realice mediante procedimientos u otras actividades, podría considerarse que no existe un sistema técnico de juego asociado a la licencia general. En este caso, no sería necesario presentar informe de certificación de la funcionalidad ni de seguridad, si bien, en su lugar deberá presentarse un escrito del operador que justifique esta circunstancia.

h) Informes de certificación de operadores de concursos

Para la certificación de licencias generales de aquellos operadores de concursos que dispongan de autorización para la participación en el juego sin la previa identificación de los participantes la entidad de certificación deberá evaluar qué requisitos son de aplicación.

Ejemplo: requisitos de registro de usuario:

- Los requisitos orientados a verificar la comprobación de identidad previa al juego no son aplicables.
- Los requisitos de disponer de un registro de usuario seguirán siendo de aplicación, únicamente para los ganadores.

10. Aclaraciones en relación a la sesión destinada al juego de máquinas de azar

a) Definición de sesión de máquinas de azar

"Conjunto de partidas realizadas por el participante, ya sea en una o en varias máquinas de azar, durante el periodo de tiempo delimitado por cada una de sus conexiones al juego de máquinas de azar del operador de juego". (Artículo 2.3 de la OM_AZA).

La sesión de máquinas de azar es un concepto creado en el marco del juego responsable. El objetivo es poner a disposición del jugador un entorno de control del juego (límites económicos, límites de tiempo, obligaciones de información, etc.). El concepto de "Sesión destinada al juego de máquinas de azar" tiene varias implicaciones técnicas, que se desarrollan a continuación.

b) Inicio y finalización de la sesión destinada al juego de máquinas de azar

En el contexto de una sesión de usuario solo es posible tener iniciada simultáneamente una única sesión destinada al juego de máquinas de azar. La sesión destinada al juego de máquinas de azar iniciada por un jugador en la página web de un operador deberá ser en todo momento única, independientemente de otras cuestiones técnicas o comerciales como el número de sesiones de usuario abiertas, el número de conexiones a diferentes terminales de usuario, o la oferta de juego de máquinas de azar disponible en la página web del operador (de uno o varios proveedores).

El "log out" de un jugador en el sistema del operador (a través del cierre del conjunto de sesiones de usuario que estuviesen iniciadas) implica la finalización de la sesión destinada al juego de máquinas de azar que, en su caso, pudiera estar iniciada. Si, a posteriori, el jugador vuelve a iniciar sesión de usuario en el sistema del operador y desea jugar a las máquinas de azar deberá configurar una nueva sesión destinada al juego de máquinas de azar.

c) Convivencia de máquinas de azar con otros juegos (ruleta, black jack, etc.)

- ¿Puede un jugador durante el transcurso de una sesión destinada al juego de máquinas de azar jugar a otros juegos?

  Sí, pero mientras que la sesión destinada al juego de máquinas de azar permanezca abierta deberán respetarse los requisitos establecidos en la Orden: obligaciones de información relativa al tiempo y dinero dedicado al juego de máquinas de azar, límites establecidos para las máquinas de azar, aviso periódico, etc.

- ¿Puede interrumpirse una sesión destinada al juego de máquinas de azar para jugar a otros juegos (ruleta, black jack, etc.) y reanudarse la misma sesión destinada al juego de máquinas de azar cuando el jugador vuelva a las máquinas de azar?

  No. Una misma sesión destinada al juego de máquinas de azar nunca puede ser interrumpida y reanudada posteriormente por el hecho de dejar de jugar a máquinas de azar y hacerlo a otros juegos. Los hechos por los que la sesión destinada al juego de máquinas de azar finaliza son:

- ✓ Cumplimiento de los límites fijados por el usuario al configurar la sesión.
- ✓ Cierre voluntario de la sesión por parte del usuario, ya sea expreso (finalización de la sesión específica de máquinas de azar) ya sea por cierre de la sesión de usuario o, en su caso, por cierre del navegador.
- ✓ Cierre involuntario o interrupción sobrevenida de la sesión por incidencias ajenas al usuario o al operador, por ejemplo, como consecuencia de la interrupción inesperada de la comunicación entre cliente y servidor.

Si atendiendo a criterios técnicos, el operador decide interrumpir la sesión destinada al juego de máquinas de azar cuando un jugador desea jugar a otros juegos, el operador debe forzar el cierre de la sesión destinada al juego de máquinas de azar y cumplir con las correspondientes obligaciones previstas y, posteriormente, solicitar al jugador configurar una nueva sesión destinada al juego de máquinas de azar (distinta a la anterior) para que el jugador pueda volver a jugar a máquinas de azar.

d) Convivencia de proveedores software de juegos de máquinas de azar en la página web de un mismo operador

La sesión destinada al juego de máquinas de azar iniciada por un jugador en la página web de un operador deberá ser en todo momento única, independientemente de la oferta de juego de máquinas de azar disponible en la página web del operador, de uno o varios proveedores.

Podemos encontrar múltiples implementaciones técnicas de la sesión de máquinas de azar:

- ✓ La sesión puede implementarse en la plataforma general, controlando desde la plataforma general el tiempo y dinero empleado en todos los juegos de máquinas de azar integrados con la plataforma general.

- ✓ La sesión puede implementarse a nivel de proveedor de software de juego, y, en consecuencia, obligar al jugador a cerrar una sesión destinada al juego de máquinas de azar e iniciar una nueva sesión destinada al juego de máquinas de azar para cambiar de proveedor, además de incorporar los mecanismos que fueran necesarios para evitar que el jugador abra simultáneamente más de una sesión destinada al juego de máquinas de azar.

En resumen, cualquier implementación técnica podría ser válida siempre que la sesión destinada al juego de máquinas de azar, una vez iniciada y hasta su cierre, sea única por jugador y operador independientemente del número de proveedores.

e) Configuración de la sesión destinada a máquinas de azar y obligaciones de información

Se procede a aclarar y concretar algunos de los aspectos relacionados con la configuración de las máquinas de azar y las obligaciones de información al participante.

- "*Artículo 14.1. El participante, antes de iniciar la sesión destinada al juego de máquinas de azar, deberá establecer el tiempo máximo que está dispuesto a emplear y la cantidad máxima en que está dispuesto a minorar su cuenta de juego a lo largo de dicha sesión. Esta determinación deberá realizarse expresamente, cada vez que se acceda a la sesión destinada al juego de máquinas de*

azar, sin que se puedan predeterminar por defecto estos valores ni guardar los establecidos en sesiones anteriores."

Una posible implementación técnica para que el jugador establezca el tiempo máximo que está dispuesto a emplear y la cantidad máxima en que está dispuesto a minorar su cuenta de juego, es ofrecer un conjunto de valores predeterminados, con las siguientes salvedades:

- ✓ El rango de valores debe ser suficientemente amplio.
- ✓ Los valores para establecer el tiempo máximo, deben ser cifras concretas.
- ✓ Entre los valores para establecer la cantidad máxima en que el jugador está dispuesto a minorar su cuenta de juego, sí podría incluirse un valor máximo que haga referencia al saldo del jugador, sin necesidad de incluir explícitamente el valor del saldo (ya que el valor del saldo de la cuenta de juego debe aparecer en todo momento en la interfaz de usuario (Art. 3.9.2 de la RES_TEC)).
- ✓ Ni los valores mínimos ofrecidos, ni la propia distribución de los rangos, deben desnaturalizar el propósito de las medidas de autolimitación, en particular induciendo al jugador a seleccionar valores elevados.
- ✓ No es aceptable incluir un botón específico para que se despliegue el menú de valores con la opción del máximo saldo/tiempo pre-marcado.

➢ *Artículo 14.1): "En todo caso, el operador de juego deberá anticipar al participante la proximidad del cumplimiento de los límites predeterminados en la configuración previa de la sesión, a fin de que dicho participante pueda realizar, si así lo desea, un cierre ordenado."*

El espíritu de la norma es que cada vez que el jugador se acerque al umbral de proximidad del cierre de la sesión por cumplimiento del límite de gasto debe aparecer el aviso. Para el aviso de proximidad temporal la solución es única. Sin embargo, con el aviso de proximidad del gasto la casuística que puede darse es amplia pudiendo existir repetidos acercamientos e incluso franqueos del umbral en corto espacio de tiempo o más espaciados. En este sentido, no se considera necesario que el aviso inicial se reactive hasta pasados 15 minutos de su primera generación (15 minutos es coincidente con la duración máxima del aviso de juego reiterativo que en paralelo debe generarse a lo largo de la sesión de juego). Una vez se ha generado el aviso de límite de gasto no será necesario activar nuevamente el mismo aviso al bordear el umbral determinado en los siguientes 15 minutos.

➢ *"Artículo 14.2. En la configuración de la sesión destinada al juego de máquinas de azar, el participante podrá restringir temporalmente su acceso a una sesión futura, para el supuesto de que la actual finalice automáticamente como consecuencia del agotamiento de alguno de los límites establecidos en el apartado 1 de este artículo."*

Una posible implementación técnica para que el jugador establezca el tiempo de autoexclusión es ofrecer un conjunto de valores predeterminados, con las siguientes salvedades:

- ✓ El rango de valores debe ser suficientemente amplio, estableciendo al menos los valores de "1 día", "1 semana" y "1 mes".
- ✓ Se considera aceptable incluir en el rango de valores un valor mínimo de 1 hora.

- ✓ Una vez que el jugador ha configurado y confirmado un periodo de autoexclusión, en los términos establecidos en el artículo 14.2, no es posible revisar o modificar la configuración establecida.

➢ *Artículo 14.3. "El participante, antes de iniciar la sesión, determinará la frecuencia del aviso referido en el apartado 2 del artículo 8 de esta orden ministerial, siendo el intervalo mínimo de quince minutos a contar desde el inicio de la sesión destinada al juego de máquinas de azar o desde el último aviso."*

El intervalo máximo de tiempo en que debe aparecer el aviso es de 15 minutos. Es decir, el jugador podrá configurar la sesión para que el aviso aparezca cada 5, 10, o cualquier otro valor igual o inferior a 15 minutos.

➢ *Artículo 8.1.2.i) "Durante el transcurso de cada sesión, saldo de la sesión destinada al juego de máquinas de azar con desglose de los importes de participación y premios en su caso obtenidos. Esta información estará visible en la interfaz del juego desde el inicio de la sesión destinada al juego de máquinas de azar."*

En todo momento, durante el transcurso de la sesión destinada a máquinas de azar, deben aparecer en la interfaz de usuario (incluido en la interfaz de los terminales móviles) las siguientes cifras:

- ✓ Balance de la sesión (calculado como suma de premios menos suma de participaciones).
- ✓ Suma de participaciones.
- ✓ Suma de premios.

Este requisito es de aplicación para cualquier interfaz de usuario, incluida la de los dispositivos móviles. No está permitido implementar este requisito a través de un enlace que redirija al jugador a otra sección.

No se exige poner a disposición del jugador un historial que incluya información de cada spin, round, saldos parciales durante la sesión, etc.

➢ *Artículo 8.1.2.j): "Histórico de los importes jugados y premios obtenidos en cada sesión destinada al juego de máquinas de azar, así como el saldo resultante de los anteriores."*

Se exige poner a disposición del jugador un historial que incluya información de todas y cada una de las sesiones destinadas a máquinas de azar finalizadas, y en concreto, para cada una:

- ✓ Balance final de la sesión (calculado como suma de premios menos suma de participaciones).
- ✓ Suma de participaciones.
- ✓ Suma de premios.

➢ *Art. 13.2 "Los operadores emitirán un documento acreditativo al final de cada sesión destinada al juego de máquinas de azar, que deberá facilitarse a cada participante por el mismo medio por el que participó en la sesión, con el resumen de las cantidades apostadas y de los resultados obtenidos."*

El documento acreditativo al que hace referencia el artículo 13.2 debe incluir, al menos:

- ✓ Suma de participaciones.
- ✓ Suma de premios.

En caso de que la sesión destinada al juego de máquinas de azar no se cierre ordenadamente, entendiendo por tal, por ejemplo, que el jugador cierra directamente el navegador, o que se interrumpe inesperadamente la comunicación entre cliente y servidor, es aceptable que, por imposibilidad técnica, no se dé cumplimiento a las obligaciones de información en los términos del art. 13.2. No obstante, los datos de la sesión cerrada de forma involuntaria se incorporarán al histórico de sesiones de juego en máquinas de azar.

➢ *Artículo 8.1.2.e): "Expectativa matemática de retorno del juego, calculada sobre el plazo de un año, así como el porcentaje real de devolución de premios sobre cantidades jugadas de cada uno de los juegos en cada uno de los seis meses precedentes. Se excluirán del cálculo de dicho porcentaje los premios derivados de botes, sin perjuicio de la información que adicionalmente el operador considere proporcionar en relación con éstos."*

Para las máquinas de azar se establece la obligación de publicar el RTP teórico y el RTP real mensual de los últimos seis meses (excluyendo el importe destinado a botes y los botes eventualmente repartidos). El operador podrá incluir otros valores adicionales, entre los cuales se encuentra el RTP incluyendo información relacionada con los botes.

f) Extensión de determinados elementos aplicables a la sesión de máquinas de azar al resto de juegos

Los operadores podrían optar por realizar la configuración de la autolimitación de cantidades y tiempo de sesión, así como el resto de elementos que comporta el inicio de la sesión específica para máquinas de azar (aviso de proximidad de límites, aviso de juego reiterativo), al iniciar la sesión de usuario, y haciendo extensiva la aplicación de los mencionados elementos al conjunto de los juegos ofrecidos.

Esta es una opción viable y aceptable, con las siguientes salvaguardas, relacionadas con elementos exclusivamente aplicables al juego de máquinas de azar:

- ✓ La información sobre el transcurso de cada sesión (artículo 8.1.2 de la OM_AZA) debe estar referida a la sesión específica de máquinas de azar. En particular los apartados:
  - o Saldo de la sesión destinada al juego de máquinas de azar con desglose de los importes de participación y premios en su caso obtenidos. Esta información estará visible en la interfaz del juego desde el inicio de la sesión destinada al juego de máquinas de azar.
  - o Histórico de los importes jugados y premios obtenidos en cada sesión destinada al juego de máquinas de azar, así como el saldo resultante de los anteriores.
- ✓ La posibilidad de reinvertir las ganancias una vez iniciada la sesión específica de las máquinas de azar. Esta posibilidad solo se refiere a ganancias derivadas del juego de máquinas de azar y no de otros juegos (Artículo 12.2 OM_AZA).

g) Otros conceptos de sesión

En la normativa reguladora de los juegos se utiliza el término "sesión" en diferentes contextos: en el contexto técnico como "*sesión de usuario*", en el contexto del juego responsable en el juego de máquinas de azar como *"sesión destinada al juego de máquinas de azar*" y por último, en el contexto de la monitorización para el modelo de datos del sistema de control interno. Se procede a aclarar los diferentes conceptos:

➢ Sesión destinada al juego de máquinas de azar

El término de "sesión destinada al juego de máquinas de azar" es un concepto creado en el marco del juego responsable y en el que ya se ha incidido anteriormente.

➢ Sesión de usuario

Definición: *Se denomina sesión de usuario al período de tiempo que un usuario permanece conectado al sitio web del operador, y que comprende desde la autenticación válida del usuario en el sistema hasta la desconexión del mismo* (3.8 del RES_TEC).

Aclaración: Se trata de un concepto técnico, delimitado habitualmente por un intercambio de claves y un cierre de la sesión, que puede producirse, entre otros, por solicitud del jugador, por pérdida de conexión entre el cliente y el servidor o por inactividad del jugador.

Obligaciones de información:

En el contexto de la sesión de usuario, existen un conjunto de obligaciones, entre las que se destacan las siguientes:

- *La interfaz mostrará un reloj con la hora actual visible o el tiempo de sesión transcurrido. Cuando el usuario inicia sesión, se le mostrará el momento en que se conectó por última vez.* (Orden de convocatoria de Licencias Generales, Anexo II: Contenido del plan operativo, 3.1.c).
  Este requisito es de aplicación para cualquier interfaz de usuario, incluida la de los dispositivos móviles. No está permitido implementar este requisito a través de un enlace que redirija al jugador a otra sección.

- Nombre del juego y saldo del participante (3.9.1 y 3.9.2 de la RES_TEC):
  El nombre del juego que el participante está jugando debe ser claramente visible en todas las pantallas asociadas.
  La pantalla debe mostrar el saldo actual del participante al menos en euros y las apuestas realizadas, unitarias y totales.

➢ Sesión en el contexto de la monitorización

En el marco del modelo de datos del sistema de control interno, se han publicado una serie de directrices sobre cómo reportar información relativa a juegos de sesión: en concreto sobre los juegos de Ruleta, Black Jack, Juegos complementarios y Máquinas de azar.

Se recomienda al lector dirigirse a la guía específica del modelo de datos para una mayor concreción. A continuación, se transcriben los aspectos más relevantes:

Ruleta, Black Jack y Juegos complementarios:

Los datos correspondientes a los juegos de Ruleta, Black Jack y Juegos complementarios pueden reportarse, a elección del operador, usando cualquiera de las tres opciones siguientes:

- Reporte por sesión de juego: El reporte por sesión de juego agrupa todas las partidas de una misma sesión para un mismo juego.

- Reporte por sesión de usuario: El reporte de sesión de usuario, agrupa todas las partidas de una misma sesión de usuario, es decir, desde que el usuario se valida en la plataforma hasta que se desconecta.

- Reporte por mano o partida: Cada partida o mano se reporta de forma independiente.

Máquinas de azar

Los datos de máquinas de azar siempre se referirán a la sesión de máquinas de azar. El reporte de las sesiones de máquinas de azar, debe especificar la fecha y hora de inicio y finalización de la sesión destinada al juego de máquinas de azar, y la duración y cantidad máxima configurada previamente por el participante.

11. Aclaraciones en relación a la redirección al dominio «.es».

Art. 3.2 del Anexo de la RES_TEC.

Este requisito está dirigido fundamentalmente a operadores con presencia en el "punto com" con el fin de evitar, entre otras cosas, comportamientos fraudulentos por parte de jugadores que bajo el ámbito de la Ley 13/2011, de 27 de mayo, de Regulación del Juego, estén intentando acceder y jugar en páginas fuera del ámbito de la Ley, mediante técnicas de ocultación de IP.

No se pretende prohibir el uso de VPNs en entornos controlados (trabajos de certificación, acceso remoto de los administradores de sistemas, etc.).

Por otra parte, en relación a las medidas, la propia evolución tecnológica hace que desde un punto de vista puramente técnico no existan mecanismos 100% eficaces a la hora de evitar que el jugador enmascare su IP para jugar en el "punto com" desde territorio español. En todo caso, se solicita que, en la medida de lo posible, se implementen mecanismos para mitigar este riesgo. Los controles técnicos deberán complementarse con medidas organizativas que permitan contrastar el lugar de residencia de los jugadores.

12. Aclaraciones en relación al test de penetración y análisis de vulnerabilidades.

Art. 4.17 del Anexo de la RES_TEC.

La nueva redacción responde a unos criterios de flexibilidad, pero en ningún caso pretende conllevar una merma en la eficacia de las pruebas. Un operador que cuente con medios técnicos y humanos suficientes podrá realizar sus propios test de penetración y análisis de vulnerabilidades.

En todo caso, el hecho de que una entidad de certificación designada por la DGOJ deba valorar estos trabajos y emitir una conformidad al respecto, da garantías de que los trabajos se han realizado adecuadamente. Es decir, la entidad de certificación es responsable de emitir la conformidad del test y del análisis. Un laboratorio no debe acreditar la conformidad de un test si existen dudas sobre la eficacia de éste. Ante la detección de un fallo grave, el sistema no podrá acreditarse como conforme. Ante la detección de fallos de seguridad leves o medios, podrá acreditarse como conforme en tanto que exista un plan de acción con las medidas correctivas.

13. Aclaraciones en relación a los métodos de autenticación en la comunicación con los participantes.

El apartado D) del Anexo VII de la *Resolución de 6 de octubre de 2014, de la Dirección General de Ordenación del Juego, por la que se aprueba la 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* (RES_CERT) establece los requisitos de autenticación en la comunicación con los participantes.

La DGOJ ha analizado las mejores prácticas del mercado en materia de autenticación y el estado actual de la tecnología con el objeto de adaptar los requisitos de autenticación a la evolución de la tecnología. Los estándares analizados han sido los siguientes:

1. Norma de seguridad de las TIC (CCN - Esquema Nacional de Seguridad), en la que se definen tres niveles de seguridad (bajo, medio y alto).
2. PCI DSS Versión 3, en la que se establece la autenticación por dos factores (en adelante, 2FA) o por multifactor (en adelante, MFA).
3. NIST 800-63-2, en la que se aportan directrices para la elección de factores de autenticación.
4. OWASP Mobile Top 10 2016, y concretamente en su categoría M4–Insecure Authentication, donde se aportan nociones sobre cómo evitar la autenticación insegura de usuarios.

El estándar de PCI define los siguientes factores de autenticación:

1. Algo que el usuario sepa (contraseña, PIN, etc.).
2. Algo que el usuario tenga (tarjeta inteligente, dispositivo físico, etc.).
3. Algo que el usuario sea (rasgo biométrico, como por ejemplo la huella dactilar).

Teniendo en cuenta estas directivas técnicas y los requisitos establecidos en la normativa, se ha definido el siguiente esquema de autenticación de sistemas técnicos de juego:

1. Autenticación de nivel bajo: No se considera conforme a la normativa.
2. Autenticación de nivel medio. Se considera conforme con los requisitos establecidos en la normativa bajo alguno de los siguientes criterios:
   a. Contraseña de al menos 8 caracteres de longitud y tres tipos de caracteres con políticas de bloqueo asociadas (en adelante, 8C-PB); o
   b. Medios de nivel bajo asociados en esquemas de autenticación de dos factores (2FA) con políticas de bloqueo asociadas (en adelante, PB).
3. Autenticación de nivel alto. Se considera conforme con los requisitos establecidos en la normativa bajo alguno de los siguientes criterios:
   a. Patrones biométricos con un segundo factor de autenticación como puede ser un dispositivo físico; o
   b. Medios de nivel bajo asociados en esquemas de autenticación multifactor (MFA) con PB.

A continuación, se exponen casos prácticos a modo de ejemplo de acuerdo con el esquema definido:

Caso	Conforme	Seguridad	Observaciones
Aplicación móvil	NO	Bajo	Debe asociarse un esquema multifactor de autenticación.
Patrón lineal	NO	Bajo	Debe asociarse un esquema multifactor de autenticación.
PIN	NO	Bajo	Debe asociarse un esquema multifactor de autenticación.
Tarjeta de proximidad NFC	NO	Bajo	Debe asociarse un esquema multifactor de autenticación.
Aplicación móvil con PIN	NO	Bajo	Una aplicación en dispositivo físico con un único factor de grado bajo asociado se considera un nivel bajo de seguridad, debido al riesgo de robo del terminal.
Aplicación móvil con patrón	NO	Bajo	Una aplicación en dispositivo físico con un único factor de grado bajo asociado se considera un nivel bajo de seguridad, debido al riesgo de robo del terminal.
Aplicación móvil con SMS	NO	Bajo	Una aplicación en dispositivo físico con un único factor de grado bajo asociado basado en envío de SMS, se considera un nivel bajo de seguridad, debido a la vulnerabilidad asociada a

			protocolos SMS.
Tarjeta de proximidad NFC con SMS	NO	Bajo	Se considera un nivel bajo de seguridad debido a la vulnerabilidad asociada a protocolos SMS.
Contraseña (8C-PB)	SÍ	Medio	Contemplado en el Anexo VII. D de la RES_CERT.
Aplicación móvil con PIN (PB)	SÍ	Medio	Se considera un nivel medio de seguridad, debido a que el riesgo de robo del terminal se mitiga con una política de bloqueo con límite de intentos para que no se pueda hackear el terminal por fuerza bruta (2FA).
Aplicación móvil con patrón (PB)	SÍ	Medio	Se considera un nivel medio de seguridad, debido a que el riesgo de robo del terminal se mitiga con una política de bloqueo con límite de intentos para que no se pueda hackear el terminal por fuerza bruta (2FA).
Aplicación móvil con correo electrónico	SÍ	Medio	Se considera un nivel medio de seguridad, debido a que el riesgo de robo del terminal se mitiga con una política de envío de un correo electrónico con cada autenticación en el sistema (2FA).
Tarjeta de proximidad NFC con PIN (PB)	SÍ	Medio	Se considera un nivel medio de seguridad, debido a que el riesgo de robo de la tarjeta se mitiga con una política de bloqueo con límite de intentos para que no se pueda hackear la tarjeta por fuerza bruta (2FA)
Tarjeta de proximidad NFC con correo electrónico	SÍ	Medio	Se considera un nivel medio de seguridad, debido a que el riesgo de robo de la tarjeta se mitiga con una política de envío de un correo electrónico con cada autenticación en el sistema (2FA).
Aplicación móvil con contraseña (8C-PB)	SÍ	Alto	Se considera un nivel alto de seguridad, debido a que se utiliza un esquema de dos factores en el que uno de ellos tiene un grado de seguridad medio (2FA).
Aplicación móvil con huella	SÍ	Alto	Se considera un nivel alto de seguridad, debido a que se utiliza un esquema de dos factores en el que uno de ellos tiene un grado de seguridad medio (2FA).
Aplicación móvil con patrón (PB) y correo electrónico	SÍ	Alto	Se considera un nivel alto de seguridad, debido a que se utiliza un esquema multifactor (MFA).
Aplicación móvil con PIN (PB) y correo electrónico	SÍ	Alto	Se considera un nivel alto de seguridad, debido a que se utiliza un esquema multifactor (MFA).

Los factores aplicados sobre “aplicaciones móviles” podrían aplicarse como funcionalidad nativa en el dispositivo siempre y cuando el sistema operativo lo permita de forma segura.

Por otra parte, los operadores deben contemplar la posible pérdida del token y/u olvido de la contraseña por parte del jugador, por lo que debe existir un proceso de "recuperación de contraseña” que contemple un nivel de seguridad similar a los métodos de autenticación utilizados. Por ejemplo, un método de autenticación basado en contestar varias preguntas secretas se considera un nivel medio de seguridad análogo al caso “Contraseña (8C-PB)”.

La puesta en producción de nuevos métodos de autenticación en la comunicación con los participantes tiene carácter de cambio sustancial en el sistema técnico de juego y por consiguiente es objeto de certificación y autorización previa a su puesta en producción. Con la solicitud de autorización de cambio sustancial, deberá adjuntarse la siguiente documentación:

- Análisis técnico y normativo con el estudio de impacto y análisis de riesgos de la solución implementada.
- Informe de la certificación de la seguridad actualizado. Se deben certificar las siguientes áreas:
    - Seguridad en la comunicación con los participantes.
    - Penetración y análisis de vulnerabilidades.
- Proyecto técnico actualizado. Se debe actualizar el apartado c) 7 para el proyecto técnico correspondiente a la Licencia General: “Descripción de las medidas para garantizar la seguridad, confidencialidad e integridad de las comunicaciones con el participante.”

A modo de ejemplo en relación al análisis técnico y normativo, se presentan a continuación las principales consideraciones a tener en cuenta en el caso de implementar un método de autenticación basado en aplicación móvil con reconocimiento de huella dactilar:

1. Análisis técnico: Se deberá utilizar hardware estándar de reconocimiento de huella, TouchID en el caso de iOS y hardware con encriptación similar al estipulado en las normas de Google en el caso de Android. Se podría considerar errónea por tanto a nivel técnico, la siguiente implementación de este tipo de soluciones: obtener la huella mediante un software de reconocimiento no homologado o distinto a lo estipulado por los principales sistemas operativos móviles.

2. Análisis normativo: Con la entrada en vigor del Reglamento General de Protección de Datos[2], a los ya considerados como datos especialmente protegidos (ideología, religión, afiliación sindical, creencias, salud, origen racial y vida sexual) se añaden los datos biométricos dirigidos a identificar de forma inequívoca a una persona. Si se plantease almacenar estos datos en el sistema técnico de juego del operador, implicaría la realización de una “Evaluación de Impacto Previo” (EIP) según dicho reglamento.

3. Conclusiones y recomendaciones sobre la implementación:

2 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

a. Obtención de la huella mediante dispositivo hardware homologado por SO o que cumpla sus especificaciones.
b. Guardar una asociación matemática de la huella con usuario/contraseña en un lugar seguro en el propio dispositivo y de forma encriptada, produciéndose la conexión al sistema técnico de juego con la dupla usuario/contraseña asociada en la aplicación.

Si un operador tiene intención de implementar otra solución equivalente y no contemplada en el anterior listado de casos prácticos, puede presentar una consulta ante el buzón dgoj.control@hacienda.gob.es, incluyendo el análisis y control de riesgos, e incorporando además los "controles de compensación" implementados, entendiendo que este tipo de controles deben cumplir con el mismo rigor que el esquema definido anteriormente, proporcionando un nivel similar de defensa.

14. Aclaraciones en relación a la auditoría bienal de los sistemas técnicos juegos.

El siguiente apartado tiene por objeto aclarar las dudas planteadas por los operadores en relación al plazo de presentación y al alcance de la auditoría técnica que los operadores deben realizar sobre su sistema técnico de juego.

a) Alcance de la auditoría cuando el sistema técnico de juego se compone de diferentes proveedores de software de juego.

Desde el punto de vista administrativo, el plazo de realización y presentación de la auditoría del sistema técnico de juego viene determinado por la fecha de homologación de cada licencia de la que dispone cada operador. No obstante, la realidad del mercado es que los sistemas técnicos de juego son sistemas en constante evolución y uno de los indicadores más evidentes en este sentido es la continua incorporación de nuevos proveedores de máquinas de azar en los sistemas de los operadores.

El presente apartado tiene por objeto clarificar el plazo de presentación y el alcance de la auditoría en estos casos. Para ello, será necesario distinguir fundamentalmente entre el plano técnico y el plano administrativo.

Desde el punto de vista administrativo, de forma análoga al proceso de certificación y homologación, la auditoría del sistema técnico de juego se realiza por Licencia y Operador. El operador es el responsable último de la presentación de los informes de auditoría que incluyan su sistema técnico de juego completo.

Sin embargo, como viene sucediendo con el proceso de certificación, la propia industria se ha organizado de tal forma que cada proveedor trabaja con una única entidad de certificación para cada uno de los trabajos requeridos. En este sentido, el operador puede acreditar el cumplimiento de la auditoría de su sistema técnico de juego, mediante el informe de auditoría de su(s) proveedor(es).

Desde un punto de vista técnico, los proveedores de software de juego deben someterse a la auditoría de sus operadores, ya que forman parte del sistema técnico de juego de estos. No obstante, los proveedores pueden optar por realizar su propia auditoría con su propia entidad de certificación, al menos en lo que respecta a aquellos requisitos que no puedan o quieran ser cubiertos a través de la auditoría realizada por cada uno de los operadores con los que está integrado. En estos casos, la primera auditoría deberá realizarse en los seis meses posteriores a los dos años desde la fecha de la primera Resolución por la que se homologa su integración con un operador con licencia en el ámbito

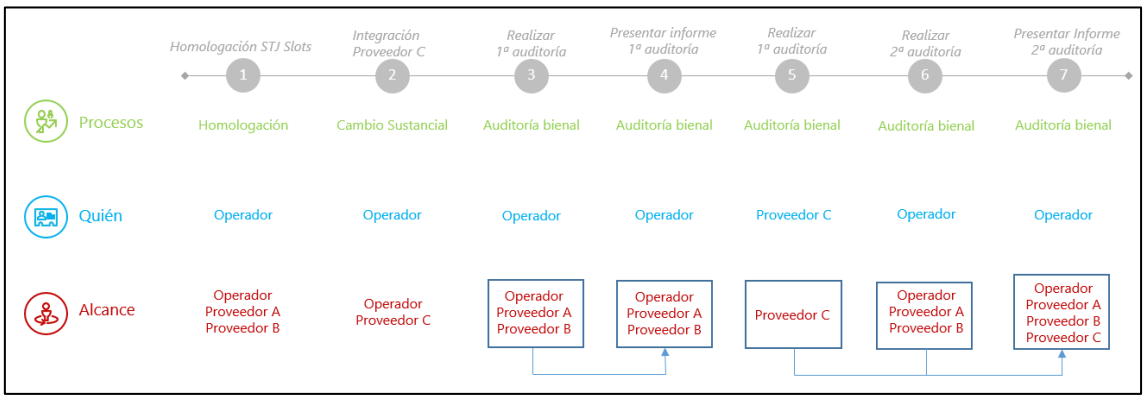
de la Ley 13/2011. Es decir, un proveedor puede estar integrado con varios operadores. No obstante, el primer operador con el que se integra, y en concreto, la fecha en la que este operador obtiene la resolución por la que se homologa la integración, es la que marca el calendario de realización de auditorías del proveedor. Téngase en cuenta que la primera homologación puede producirse a través de una Resolución de homologación o de una Resolución de cambio sustancial. Las sucesivas auditorías deberán realizarse en los seis meses siguientes a los cuatro, seis y ochos años desde la fecha indicada.

Los operadores, en el momento de presentar el informe de auditoría, deberán incluir bajo el alcance de esta aquellos proveedores de juego que lleven al menos dos años comercializando.

Como ejemplo práctico, analicemos el siguiente escenario:

Escenario:

1. Un operador obtiene la homologación de su sistema técnico juego, que incluye los proveedores A y B.
2. Un año después, el operador incorpora un tercer proveedor de juego C a través de un procedimiento de gestión de cambio.
3. A los dos años de la homologación, el operador realiza la primera auditoría de su sistema, que incluye los proveedores A y B.
4. A los dos años y 6 meses de la homologación, el operador presenta un informe de auditoría que incluye los proveedores A y B.
5. Dos años después de la resolución de cambio sustancial por la que se homologa la integración del proveedor C con el operador, el proveedor C (que ha decidido realizar su propia auditoría con su propia entidad de certificación) realiza su primera auditoría.
6. A los cuatro años de la homologación, el operador realiza la segunda auditoría de su sistema, que incluye los proveedores A, B y C. En relación al proveedor C, los aspectos que únicamente dependen del proveedor ya han sido auditados y no deben de volver a ser auditados.
7. A los cuatro años y 6 meses de la homologación, el operador presenta los informes de auditoría que acreditan la auditoría completa del operador y de los proveedores A, B y C (es decir, presenta su informe de operador y el informe del proveedor C).



b) ¿Es estrictamente necesario un informe de auditoría de proveedor?

No. Como se ha indicado anteriormente, la propia industria se ha organizado de tal forma que cada entidad de juego (operador o proveedor) trabaja con una única entidad de certificación para cada uno

de los trabajos requeridos. En este sentido, el operador podría acreditar el cumplimiento de la auditoría de su sistema técnico de juego, mediante el informe de auditoría de su(s) proveedor(es). Pero sería igualmente aceptable que el operador presente un único informe de auditoría realizado por una única entidad de certificación y que incluya bajo su alcance el conjunto de requisitos técnicos aplicables tanto al sistema técnico del operador, como al de sus proveedores.

c) ¿Cuál es el alcance de un informe de auditoría de proveedor?

El informe de auditoría de proveedor debe incluir todos los aspectos que no hayan sido auditados en la auditoría realizada directamente por el operador.

Desde el punto de vista de seguridad, de forma análoga a la certificación inicial a la que se sometió el proveedor, el alcance de la auditoría ha de cubrir el total de áreas de seguridad definidas.

d) ¿Debe auditarse un sistema que no está en producción?

No. Una plataforma que no está en producción a la fecha del cumplimiento del plazo de presentación del informe de auditoría está exenta de someterse a la auditoría. Esta circunstancia deberá comunicarse formalmente a la DGOJ. No obstante, la reactivación de dicha plataforma requerirá la previa presentación del informe de auditoría.

e) Auditoría y cambios de plataforma.

La primera auditoría se realizará en los seis meses siguientes al vencimiento del plazo de dos años contados desde la primera homologación inicial de una licencia singular o desde la fecha de resolución de homologación de gestión de cambio cuyo alcance contemple el sistema técnico de juego completo del operador. A partir de ahí, las sucesivas auditorías se realizarán cada dos años, siempre en el plazo máximo de seis meses.

Es decir, cuando un operador se somete a un cambio íntegro de plataforma se reinician las fechas y se volverá a pasar una “primera” auditoría de la nueva plataforma, cuando esta lleve dos años en funcionamiento.

f) Incompatibilidad de la entidad de certificación para la certificación y auditoría.

La entidad de certificación que realiza las auditorías no puede haber participado en los procesos de certificación inicial o de certificación de cambios sustanciales del sistema auditado.

Una única entidad de certificación puede realizar todas las auditorías, siempre y cuando este no haya participado en los procesos de certificación del sistema auditado.

Por ejemplo, en un escenario en el que un operador realiza un cambio íntegro de plataforma, las entidades de certificación que participaron en las certificaciones y auditorías de la anterior plataforma son irrelevantes, en tanto que se trata de dos plataformas diferentes.

15. Aclaraciones en relación a los generadores de números aleatorios criptográficamente fuertes.

La *Resolución de 6 de octubre de 2014, de la Dirección General de Ordenación del Juego, por la que se aprueba la disposición por la que se desarrollan las especificaciones técnicas de juego, trazabilidad y seguridad que deben cumplir los sistemas técnicos de juego de carácter no reservado objeto de licencias otorgadas al amparo de la Ley 13/2011, de 27 de mayo, de regulación del juego* establece en su apartado "*3.5 Generador de números aleatorios (GNA). 3.5.1 Funcionamiento del GNA."* del Anexo I:

"El generador de números aleatorios será criptográficamente fuerte".

Esta modificación normativa viene a dar respuesta a la necesidad de actualizar los requisitos técnicos del generador de números aleatorios desde el punto de vista de su diseño y su seguridad ante nuevas amenazas que podrían poner en riesgo el correcto funcionamiento del azar en el juego y, por consiguiente, el juego justo. Con esta modificación se consigue, por una parte, establecer un requisito que de facto ya incluyen la mayoría de los generadores, por el propio estado del arte de la industria en esta materia y, por otra parte, equiparar los requisitos de los generadores a la mayoría de las jurisdicciones de nuestro entorno.

Un generador de números aleatorios es criptográficamente fuerte cuando sus resultados son impredecibles incluso cuando el atacante tiene información sobre el algoritmo, la semilla o los resultados anteriormente generados. Es decir, para que un generador de números aleatorios se considere criptográficamente fuerte, no solo debe pasar satisfactoriamente pruebas estadísticas de aleatoriedad, sino que, además, debe superar ataques severos, incluso si parte de su estado está disponible a un atacante.

En la anterior versión de la Resolución se establecía que *"Los datos aleatorios generados deben ser impredecibles (su predicción debe ser irrealizable por computación sin conocer el algoritmo y la semilla)."* Un generador de números aleatorios criptográficamente fuerte incrementa su entropía en su propio diseño, evitando la predicción de sus resultados ante un posible atacante. Por ejemplo, en un generador de números aleatorios software, es necesario que la fuente que genera la semilla sea criptográficamente impredecible para poder afirmar que el generador es criptográficamente fuerte.

Los cambios que se deban realizar en los sistemas de generación de números aleatorios de los operadores de juego (en los suyos propios y en los de sus proveedores) para hacerlos criptográficamente fuertes tienen consideración de cambio sustancial en el sistema técnico de juego por lo que su puesta en producción necesita la previa autorización de la Dirección General de Ordenación del Juego tras la presentación del correspondiente informe de certificación. Los operadores de juego disponen de plazo hasta el 1 de enero de 2020 para adaptar sus sistemas.

Aquellos operadores que ya dispusieran de un generador de números aleatorios criptográficamente fuerte, deberán presentar un escrito emitido por su entidad de certificación de funcionalidad en el que quede acreditada tal circunstancia. La presentación de dicho escrito debe realizarse por vía telemática, a través del trámite denominado "Comunicaciones Genéricas a la DGOJ" disponible en la sección de la sede electrónica de la DGOJ "Procedimientos y Servicios / De utilidad general", con los siguientes datos:

Unidad: S.G. de Inspección del Juego

Asunto: Generador de números aleatorios