INFORME DE AUDITORÍA BIENAL

DE LOS SISTEMAS TÉCNICOS DEL JUEGO

EYECON ALDERNEY LIMITED

Solicitante:	**Eyecon Alderney Limited**
Auditoria:	**Informe bienal de auditoría del sistema técnico de juego**
ATF Informe número:	**ESP.EYE-OL.1005.01.01**
Documento número:	**01**
Fecha:	**2 de noviembre de 2023**
Número de páginas:	**51**

BMM Spain Testlabs s.l.u.

DATOS GENERALES

Nombre y datos del operador:	Robert Black Operations Director Eyecon Alderney Limited Inchalla, Le Val Alderney GY9 3UL
Nombre y datos de la entidad operadora:	Eyecon Alderney Limited Inchalla, Le Val Alderney GY9 3UL
Fecha de inicio de la auditoria:	28 de septiembre de 2023
Fecha de finalización de la auditoria:	26 de octubre de 2023
Categoría del Ensayo	Categoría 0
Nombre y datos del laboratorio:	BMM Spain Testlabs, s.l.u. Edificio Vinson del Parque Empresarial Vallsolana Camí de Can Camps, 17-19 08174 Sant Cugat del Vallés – Barcelona (Spain)
Lugar de realización del ensayo:	BMM Spain Testlabs, s.l.u. Edificio Vinson del Parque Empresarial Vallsolana Camí de Can Camps, 17-19 08174 Sant Cugat del Vallés – Barcelona (Spain)
Tipo de auditoria:	Informe bienal de auditoría de los sistemas técnicos del juego
Modelo, tipo y otra identificación:	Plataforma online
Número de referencia del solicitante:	Petición de ensayo de 25 de mayo de 2023.
Jurisdicciones recomendadas:	España
Versión del estándar utilizado para el ensayo:	EURSAM-SPA-MO-04 v6.0
Conclusión:	Conforme
Número de referencia de BMM:	EYE-OL.1005
Dimensión de la auditoria	20 jornadas
Ingeniero de test:	Imanol del Rio Crespo, Adrià Brau

1. ALCANCE DE LA AUDITORÍA DEFINITIVA.

Eyecon Alderney Limited solicita a BMM la realización del informe bienal de auditoría de los sistemas técnicos de juego con el fin de evaluar la correcta implementación de estos en aplicación de las siguientes jurisdicciones:

- NOTA TÉCNICA Y OPERATIVA SOBRE AUDITORÍAS BIENALES DE LOS SISTEMAS TÉCNICOS DE JUEGO (versión 3).
- Anexo I. Lista de requisitos de funcionalidad bajo el alcance de la auditoría bienal (versión 3).

2. DESCRIPCIÓN DEL OBJETO DE LA AUDITORÍA.

2.1. LICENCIAS DE JUEGO BAJO ALCANCE.

No aplica. El alcance de la presente evaluación corresponde a la auditoría bienal de los sistemas técnicos del proveedor de juegos Eyecon Alderney Limited.

2.2. PROVEEDORES DE SOFTWARE BAJO EL ALCANCE.

En la siguiente tabla se detalla la oferta de juego bajo el alcance de la auditoría así como las variantes de juego certificadas.

Licencia	Proveedor de software
No aplica. La presente evaluación corresponde a la de un proveedor de juegos	Eyecon Alderney Limited

2.3. CENTROS DE PROCESOS DE DATOS.

Los centros de procesos de datos donde se alberga el sistema técnico de juego son los listados a continuación.

CPD	Calle, número	Ciudad	País	Tipo	Razón social del proveedor del alojamiento	Código de Informe de certificación	Fecha de homologación
Malta Data Centre	MAR Building, Cannon Road	Qormi, QRM9039	Malta	Hosting	Continent 8 Technologies PLC	No aplica	No aplica
Gibraltar Data Centre	Admiralty Tunnel 77, Queensway	Gibraltar, GX11 1AA	Gibraltar	Hosting	Continent 8 Technologies PLC	No aplica	No aplica
Dublin Data Centre	Unit B10, Ballycoolin Business & Technology Park, Blanchardstown	Dublin	Irlanda	Hosting	Continent 8 Technologies PLC	No aplica	No aplica

CPD	Calle, número	Ciudad	País	Tipo	Razón social del proveedor del alojamiento	Código de Informe de certificación	Fecha de homologación
Guernsey Data Centre	Centenary House La Vrangue Saint Peter Port GY1 2EY Guernsey	Saint Peter Port	Guernsey	Hosting	Sure (Jersey) Ltd Incorporating Foreshore Limited	No aplica	No aplica

2.4. ELEMENTOS DE SOFTWARE.

Los elementos de software empleados en el sistema técnico para el desarrollo y explotación de los juegos objetos de la licencia correspondiente son los siguientes:

Nombre del archivo	Versión	Ubicación lógica	Ubicación física	Huella Digital	Fabricante	Nombre del producto
game-server-web	3.12.2	Game Server	Gibraltar, Malta y Guernsey	24777dce0622371ac04f9ec43e4d786ebf025882	Eyecon Alderney Limited	Game Server
carbine-game-engine	5.12.2	Game Server	Gibraltar, Malta y Guernsey	49a784673d32bb1ad71e5bc013a1f6c72d7375b5	Eyecon Alderney Limited	Carbine
eyecon-rng	1.0.1	Game Server, Pool Server	Gibraltar, Malta y Guernsey	d2bfe8ef8fb4f0c33d2988f9a2a030fd66a295f9	Eyecon Alderney Limited	RNG
pool-server-web	1.4.1	Standalone	Gibraltar, Malta y Guernsey	5b91a26e1f13099917baa8652b7c5478456b62b3	Eyecon Alderney Limited	Pool Server

3. RESUMEN EJECUTIVO DE LA AUDITORÍA.

3.1. CALIFICACIÓN GLOBAL DE LA FUNCIONALIDAD.

En la siguiente tabla se muestra la calificación global del cumplimiento por cada uno de los bloques de requisitos auditados.

Bloque	Calificación Global
Requisitos de seguridad	Conforme
Requisitos de funcionalidad para Licencias Generales	No aplica
Requisitos de funcionalidad para Licencias Singulares	Conforme

3.2. COMENTARIO EJECUTIVO.

En lo relativo a la evaluación de los requisitos funcionales y de seguridad, Eyecon Alderney Limited ha demostrado un cumplimiento suficiente de los requisitos.

4. MEJORA CONTÍNUA.

4.1. PLAN DE ACCIONES DE MEJORA.

En este apartado se incluye un análisis de las causas de cada uno de los puntos de mejora identificados durante la auditoría, así como la propuesta de las acciones de mejora que se llevarán a cabo por parte del operador.

Nº de punto de mejora	No aplica, no se ha encontrado ningún punto de mejora
Requisito	No aplica, no se ha encontrado ningún punto de mejora
Punto de mejora	No aplica, no se ha encontrado ningún punto de mejora
Causa de raíz	No aplica, no se ha encontrado ningún punto de mejora
Acción/es de mejora propuestas	No aplica, no se ha encontrado ningún punto de mejora

4.2. REVISIÓN DE PLAN DE ACCIONES DE MEJORA.

Este título no es de aplicación debido a que no hay puntos de acciones de mejora en el informe de auditoría anterior.

5. DESCRIPCIÓN DE LOS ENTORNOS UTILIZADOS EN LA AUDITORÍA DIFERENTES AL EFECTIVAMENTE EMPLEADO POR EL OPERADOR PARA EL DESARROLLO DE LA ACTIVIDAD DE JUEGO.

No es de aplicación debido a que la auditoría se ha realizado en el entorno de operación.

6. DETALLE DEL CUMPLIMIENTO DE LOS REQUISITOS AUDITADOS.

6.1. CUADRO RESUMEN DEL GRADO DE CUMPLIMINETO POR ÁREA.

Bloque	Área	Auditado	Calificación Global
SEGURIDAD	Política de seguridad	No	No aplica
	Análisis y Gestión de riesgos	Sí	Conforme
	Organización de la seguridad de la información	Sí	Conforme
	Seguridad en las comunicaciones con los participantes	No	No aplica
	Seguridad de recursos humanos y terceros	Sí	Conforme
	Seguridad física y medioambiental	Sí	Conforme
	Gestión de comunicaciones y operaciones	Sí	Conforme
	Control de acceso	No	No aplica

Bloque	Área	Auditado	Calificación Global
	Compra, desarrollo y mantenimiento de los sistemas	Sí	Conforme
	Gestión de incidentes de seguridad	Sí	Conforme
	Gestión de cambios	Sí	Conforme
	Plan de prevención de pérdida de la información	Sí	Conforme
	Gestión de la continuidad del negocio	No	No aplica
	Penetración y análisis de vulnerabilidades	Sí	Conforme
FUNCIONALIDAD	Juego responsable	No	No aplica
	Contrato, Aceptación, copia y modificación	No	No aplica
	Registro de usuario y comprobación de las prohibiciones	No	No aplica
	Cuenta de juegos, cobros y pagos	No	No aplica
	Límites de los depósitos	No	No aplica
	Registro y trazabilidad	No	No aplica
	Terminales y sesión de usuario	No	No aplica
	Canales de comunicación	No	No aplica
	Sistema de control interno	No	No aplica
FUNCIONALIDAD SINGULAR	Porcentaje de retorno y tablas de premios	Sí	Conforme
	Generador de números aleatorios	Sí	Conforme
	Lógica del juego	Sí	Conforme
	Registro y trazabilidad	Sí	Conforme
	Terminales y sesión de usuario	Sí	Conforme
	Canales de comunicación	No	No aplica
	Comportamiento ante errores técnicos	Sí	Conforme
	Juegos en <<vivo>>	No	No aplica
	Funcionalidades varias	Sí	Conforme
	Botes progresivos	Sí	Conforme
	Sistema de control interno	No	No aplica
	Registro de la configuración de la sesión destinada al juego de máquinas de azar	No	No aplica

6.2. DETALLE DEL CUMPLIMIENTO DE LOS REQUISITOS DE SEGURIDAD.

A continuación, se detallan los resultados obtenidos para cada área auditada:

Política de seguridad

Área y referencia del requisito	Referencia	Calificación	Observación
El operador dispone de procedimientos de seguridad		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
Los procedimientos de seguridad han sido comunicados a la totalidad de sus empleados y, en su caso, a las entidades colaboradoras.		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.

Análisis y Gestión de riesgos

Área y referencia del requisito	Referencia	Calificación	Observación
El operador dispone de un plan de análisis y gestión de riesgos.	Risk Management & Controls Policy.pdf (Evidencia Documental)	Conforme	
Se realiza una revisión periódica del análisis de riesgos.	Screenshot Risk Assessment 2022.pdf (Evidencia Documental)	Conforme	
La organización tiene identificados los componentes críticos del Sistema Técnico de Juego.	Managed Environment Software Change Procedure.pdf (Evidencia Documental)	Conforme	1.- Equipo de Juegos 1.1.- Componentes backend • Servidor de juegos • Servidor de billar (Jackpot Engine) • Motor de juego Carbine • Reglas del juego Superbus • Servidor Feed

Área y referencia del requisito	Referencia	Calificación	Observación
			• RNG 1.2.- Componentes frontales • Marco Orion • Juegos Orion • Juegos Tamborine • Juegos Lamington 2.- Equipo de distribución • Servidor de integración • Servidor de bonificación 3.- Equipo de Business Insights • Servidor de gestión • Servidor de configuración • Servidor de autenticación 4.- Equipo de calidad • Ninguno Todos los componentes críticos se definen en la página 4 del Procedimiento de cambio de software del entorno gestionado.
El operador tiene reforzada la seguridad de todos los componentes críticos.	Security issue static analysis.png (Evidencia Remota) Third party dependency check.png (Evidencia Remota) Peer Review.png (Evidencia Remota)	Conforme	

Organización de la Seguridad de la Información

Área y referencia del requisito	Referencia	Calificación	Observación
El operador dispone de un marco de gestión para la seguridad de la información que establece las funciones y responsabilidades de los trabajadores.	Access Control Policy.pdf (Evidencia Documental)	Conforme	En la política de control de acceso se recogen correctamente los diferentes roles y responsabilidades de los trabajadores de la compañía, diferenciándose entre los siguientes grupos: 1.- Artista 2.- Desarrollador 3.- Operaciones de IT 4.- Finanzas / Administración / Recursos Humanos 5.- Ejecutivo 6.- Asistencia a proveedores (terceros) 7.- Soporte interno 8.- Compliance 9.- Seguridad de la información

Seguridad en la comunicación con los participantes

Área y referencia del requisito	Referencia	Calificación	Observación
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		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
Las comunicaciones son cifradas en los casos de transmisión de datos personales		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.

Área y referencia del requisito	Referencia	Calificación	Observación
(registro de usuario) o económicos (cuenta de juego)			
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		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
Se establece, por defecto o por el participante, una contraseña inicial de usuario		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
Durante el proceso de definición de la contraseña de usuario, el participante es informado sobre buenas prácticas en la elección de contraseñas seguras		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
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		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
La contraseña no puede contener ninguno de los siguientes datos: el		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.

Área y referencia del requisito	Referencia	Calificación	Observación
nombre del usuario, el seudónimo, el nombre o apellidos o la fecha de nacimiento del participante			
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		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
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		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
El sistema del operador está diseñado para requerir la autenticación del participante ante cada inicio de sesión de usuario, y en 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		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.

Área y referencia del requisito	Referencia	Calificación	Observación
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		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
El operador dispone de un procedimiento para detectar dentro de lo razonable acceso no autorizados a la cuenta de los participantes, intentos de suplantación de identidad o acceso a sus datos personales		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
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		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.

Seguridad de recursos humanos y terceros

Área y referencia del requisito	Referencia	Calificación	Observación
El plan de seguridad incluye acciones de capacitación, gestión de contrataciones, modificaciones y rescisiones de contratos, teniendo especial atención a los permisos de acceso a la información y a los componentes críticos.	Information Security Policy.pdf (Evidencia Documental) Annual Information Security Awareness Training 2023 Certificate_Dominique Spanier.pdf (Evidencia Remota)	Conforme	El plan de seguridad recoge en su apartado "Training" que todos los empleados participan anualmente en una formación sobre seguridad de la información. La compañía adjunta además a modo de evidencia un diploma de dicha formación. También se recogen las acciones relativas al acceso de la información.
En caso de que empresas externas requieran acceso, involucrarse en procesos, tratar información o acceso a las instalaciones, productos o servicios relacionados con la actividad de juego, dichas empresas externas deberán cumplir todos los requisitos obligatorios del resto de trabajadores.	5042 - Viadex Playtech Reseller Agreement (DB) 12 September 2022 Executed Version-1.pdf (Evidencia Documental)	Conforme	Se cuenta con un correcto documento(acuerdo) que recoge todas las pretensiones/requisitos que cualquier empresa externa y sus trabajadores tendrán que cumplir a la hora de requerir acceso, involucrarse en procesos o tratar información relacionada con la compañía.

Seguridad física y medioambiental

Área y referencia del requisito	Referencia	Calificación	Observación
Los planes de seguridad incluyen la seguridad perimetral necesaria para aquellas áreas que disponen de componentes críticos o información	c8-dub.pdf (Evidencia Documental) c8-gib.pdf (Evidencia Documental)	Conforme	Requisito validado por el certificado ISO27001de cada uno de los Centros de Datos.

Área y referencia del requisito	Referencia	Calificación	Observación
sensible, como barreras físicas o acceso mediante tarjeta, etc.	c8-malta.pdf (Evidencia Documental) ISO 27001 Jersey and Guernsey.pdf (Evidencia Documental)		
El acceso al control físico a las instalaciones que contienen los equipos por parte de empleados y personal externo: elementos físicos, procedimientos de autorización, registros de acceso y servicios de grabación.	c8-dub.pdf (Evidencia Documental) c8-gib.pdf (Evidencia Documental) c8-malta.pdf (Evidencia Documental) ISO 27001 Jersey and Guernsey.pdf (Evidencia Documental)	Conforme	Requisito validado por el certificado ISO27001de cada uno de los Centros de Datos.
Control de acceso a las comunicaciones cableadas en caso de que las transmisiones no sean cifradas.	c8-dub.pdf (Evidencia Documental) c8-gib.pdf (Evidencia Documental) c8-malta.pdf (Evidencia Documental) ISO 27001 Jersey and Guernsey.pdf (Evidencia Documental)	Conforme	Requisito validado por el certificado ISO27001de cada uno de los Centros de Datos.

Área y referencia del requisito	Referencia	Calificación	Observación
Los componentes críticos están protegidos frente riesgos medioambientales como inundaciones, fuegos o riesgos causados por personas, etc.	c8-dub.pdf (Evidencia Documental) c8-gib.pdf (Evidencia Documental) c8-malta.pdf (Evidencia Documental) ISO 27001 Jersey and Guernsey.pdf (Evidencia Documental)	Conforme	Requisito validado por el certificado ISO27001de cada uno de los Centros de Datos.
Los equipos críticos están protegidos contra cortes de energía u otros tipos de interrupciones causadas por errores en las instalaciones.	c8-dub.pdf (Evidencia Documental) c8-gib.pdf (Evidencia Documental) c8-malta.pdf (Evidencia Documental) ISO 27001 Jersey and Guernsey.pdf (Evidencia Documental)	Conforme	Requisito validado por el certificado ISO27001de cada uno de los Centros de Datos.
Los equipamientos y las instalaciones disponen de un correcto mantenimiento.	c8-dub.pdf (Evidencia Documental) c8-gib.pdf (Evidencia Documental)	Conforme	Requisito validado por el certificado ISO27001de cada uno de los Centros de Datos.

Área y referencia del requisito	Referencia	Calificación	Observación
	c8-malta.pdf (Evidencia Documental) ISO 27001 Jersey and Guernsey.pdf (Evidencia Documental)		
La información contenida en los equipos debe ser correctamente eliminada o destruida en caso de reutilización o retiro de dicho equipo.	c8-dub.pdf (Evidencia Documental) c8-gib.pdf (Evidencia Documental) c8-malta.pdf (Evidencia Documental) ISO 27001 Jersey and Guernsey.pdf (Evidencia Documental)	Conforme	Requisito validado por el certificado ISO27001de cada uno de los Centros de Datos.
Aquellos equipos que contengan información no podrán ser trasladados fuera de las instalaciones sin autorización.	c8-dub.pdf (Evidencia Documental) c8-gib.pdf (Evidencia Documental) c8-malta.pdf (Evidencia Documental) ISO 27001 Jersey and Guernsey.pdf (Evidencia Documental)	Conforme	Requisito validado por el certificado ISO27001de cada uno de los Centros de Datos.

Gestión de comunicaciones y Operaciones

Área y referencia del requisito	Referencia	Calificación	Observación
Los componentes críticos deberán ser monitorizados para impedir el uso de otras versiones que no sean las homologadas.	systems monitoring_1.png (Evidencia Remota) systems monitoring_2.png (Evidencia Remota)	Conforme	
Se garantiza la integridad y confidencialidad en la comunicación entre componentes.	SSL Server Test.pdf (Evidencia Remota)	Conforme	Se garantiza la integridad y confidencialidad en las comunicaciones a través de SSL, un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web. El cliente adjunta evidencia remota.
Las responsabilidades se dividirán en áreas con el fin de minimizar la posibilidad de accesos no autorizados y daños potenciales. Las áreas serán desarrollo, test y producción.	IGS Network Diagram (Malta) Segregation - Eyecon Malta Instance - IGS Logical Layout StellaV.pdf (Evidencia Remota)	Conforme	
Los servicios de terceros incluirán métricas de seguridad y controles en los contratos y serán auditados y monitorizados.	C8 MSA v4 - Eyecon Alderney Limited – signed.pdf (Evidencia Documental)	Conforme	Cuando se establecen relaciones con terceros se firma correctamente un contrato marco de servicios en el que se establecen las bases sobre seguridad y controles que los terceros tendrán que cumplir. La compañía adjunta como evidencia remota un ejemplo de contrato.
Se dispone de medidas de seguridad para la protección frente a código malicioso.	ClamAV Client Scans.png (Evidencia Remota) ClamAV Definitions Mirror.png	Conforme	Dispone de antivirus para la protección frente a código malicioso. Se adjuntan capturas de los escaneos mediante antivirus.

Área y referencia del requisito	Referencia	Calificación	Observación
	(Evidencia Remota)		
Las copias de seguridad se realizan con una frecuencia apropiada y se gestionan tal y como está documentado en las políticas de copias de seguridad.	Disaster Recovery Plan (Internet Gaming Systems).pdf (Evidencia Documental) Backups stored.png (Evidencia Remota)	Conforme	Todos los domingos se realiza una copia de seguridad completa de la base de datos MySQL y copias incrementales el resto de los días. Además, los registros binarios de repetición se escriben y se copian junto con los archivos de datos. Cada día estas copias de seguridad se copian en una máquina virtual independiente para mayor protección. Además, la compañía adjunta capturas de las copias de seguridad almacenadas y de las copias de seguridad programadas.
Existen medidas de seguridad para la red de comunicación.	Access Control Policy.pdf (Evidencia Documental)	Conforme	Los tokens de autenticación difieren entre entornos para evitar que las transacciones destinadas a un entorno lleguen a otro (tenga en cuenta que también existen restricciones de seguridad lógicas y de red adicionales, como la segregación de redes y las listas blancas, para ayudar en este sentido). Todos los dispositivos controlados por la empresa en la red corporativa se autentican mediante 802.1X y/o MAC. Cualquier dispositivo que no aparezca en la lista blanca o no esté autorizado por 802.1X se colocará en una VLAN de invitados con acceso únicamente a Internet. Internet público solamente. Sólo los equipos de Operaciones de TI y Seguridad de la Información podrán acceder a las redes de juegos de producción. El acceso a estas redes por parte de otros miembros del personal o proveedores autorizados tiene que estar bajo la supervisión de un miembro del personal de Operaciones de TI.

Área y referencia del requisito	Referencia	Calificación	Observación
			Los dispositivos ubicados en un Centro de datos están exentos de los controles de autenticación de red, ya que su ubicación se considera segura. Se aplican controles de acceso físico y políticas compensatorias.
Las medidas de seguridad incluyen la manipulación de dispositivos portables como el eliminado seguro de información o la destrucción de estos. Dichas medidas deben estar procedimentadas en un documento.	Data Destruction Policy.pdf (Evidencia Documental) 1017 Data destruction certificate.pdf (Evidencia Remota)	Conforme	Se cuenta con una correcta política de destrucción de datos, que indica las premisas a seguir. Además, la compañía cuenta con ShredEasy que es capaz de reducir el riesgo para su negocio con maquinaria de destrucción de discos duros de última generación y la destrucción completa de su hardware. Se adjunta el certificado de destrucción de datos.
Los relojes en los componentes, especialmente aquellos críticos deben estar sincronizados con una fuente fiable de tiempo. Existirán medidas de control para prevenir la manipulación de las marcas de tiempo, especialmente para los registros de auditoría.	NTP Server.png (Evidencia Remota) NTP Client.png (Evidencia Remota)	Conforme	La compañía cuenta con un servidor NTP (Network Time Protocol) que sirve para configurar, sincronizar y mantener la hora actual en los dispositivos conectados a la red. Se adjuntan evidencias remotas de la configuración NTP de la empresa.
Los registros de auditoria son generados y almacenados para las actividades de todos los usuarios, incluyendo excepciones y eventos sobre la seguridad de la información por un periodo mínimo de 2 años.	SD-43645.pdf (Evidencia Remota)	Conforme	

Área y referencia del requisito	Referencia	Calificación	Observación
Los registros de auditoria estarán protegidos frente alteraciones y usos inadecuados.	SD-43645.pdf (Evidencia Remota) Access Control Policy.pdf (Evidencia Documental)las	Conforme	
Las actividades de administración del sistema y operación del sistema deben estar almacenadas.	Auditd.png (Evidencia Remota)	Conforme	
Los registros de auditoria deben ser analizados periódicamente. Se deberán tomar las acciones correspondientes dependiendo los incidentes detectados.	SD-43645.pdf (Evidencia Remota) Security Breach Procedure.pdf (Evidencia Documental)	Conforme	

Control de Acceso

Área y referencia del requisito	Referencia	Calificación	Observación
La política de acceso a información está documentada		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
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		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.

Área y referencia del requisito	Referencia	Calificación	Observación
Los usuarios siguen buenas prácticas en el uso de contraseñas y protegen adecuadamente la documentación y soportes en su puesto de trabajo		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
Los usuarios únicamente tienen acceso a los servicios que han sido autorizados a usar		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
No existen usuarios genéricos y todos los usuarios acceden con su usuario propio único		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
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 Dirección General de Ordenación del Juego u otro personal que actúe en su nombre		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
Las redes están segregadas en función del área y responsabilidad de la tarea o función		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
El acceso a los sistemas operativos requiere un mecanismo de autenticación seguro		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.

Área y referencia del requisito	Referencia	Calificación	Observación
Se restringe y se controla el uso de programas que permiten evitar los controles de acceso y de seguridad		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
Las sesiones tienen un tiempo máximo de duración de la conexión y un tiempo de desconexión por inactividad		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
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		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
Se gestionan los riesgos asociados a dispositivos móviles		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
Si existe teletrabajo, se comprueba que el riesgo asociado está gestionado en el marco del plan de seguridad		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.

Compra, desarrollo y mantenimiento de los sistemas

Área y referencia del requisito	Referencia	Calificación	Observación
Se considerará el impacto en la seguridad en caso de compra, desarrollo y mantenimiento de los sistemas de información.	Security issue static analysis.png (Evidencia Remota) Third party dependency check.png	Conforme	

Área y referencia del requisito	Referencia	Calificación	Observación
	(Evidencia Remota) Peer Review.png (Evidencia Remota)		

Gestión de incidentes de seguridad

Área y referencia del requisito	Referencia	Calificación	Observación
Existe un procedimiento documentado sobre la gestión de incidentes de seguridad.	Security Incident Management Policy.pdf (Evidencia Documental)	Conforme	
Todos los incidentes de seguridad son registrados y los hechos, impactos y medidas adoptadas documentadas de forma clara y concisa.	Security Incident Management Policy.pdf (Evidencia Documental) Security Breach Procedure.pdf (Evidencia Documental)	Conforme	Todos los empleados informan inmediatamente al equipo de Operaciones de TI de cualquier sospecha de incidente de seguridad y/o cualquierevento inusual, quedando este registrado. Al informar, adjuntan todas las pruebas (por ejemplo, registros, capturas de pantalla). Utilizandose uno de los siguientes canales de comunicación: - Crear un ticket de servicio en Jira (https://intranet.eyecon.com.au/jira/) - Enviar un correo electrónico a servicedesk@eyecon.com.au - Si se produce un incidente de seguridad en una jurisdicción en la que Eyecon informa de incidentes de seguridad a reguladores específicos, Eyecon se asegura de que esto se informa inmediatamente a los reguladores pertinentes o, si corresponde, a los operadores.

Área y referencia del requisito	Referencia	Calificación	Observación
			Todos los sucesos registrados son evaluados y el Equipo de Seguridad decide si tienen que clasificarse como incidente de seguridad de la información. El Jefe de TI (ESPL) es responsable de organizar la respuesta al ataque y de coordinar todas las actividades relacionadas.

Gestión de cambios

Área y referencia del requisito	Referencia	Calificación	Observación
Existe un procedimiento de gestión de cambios en equipos y componentes del sistema técnico de juego en el entorno de producción.	Change Management Policy.pdf (Evidencia Documental) Change Management Procedures Schedule.pdf (Evidencia Documental) Managed Environment Software Change Procedure.pdf (Evidencia Documental)	Conforme	
Existe un proceso de aprobación interna de cambios (petición de cambio, aprobación de los responsables).	Change Management Policy.pdf (Evidencia Documental) Change Management Procedures Schedule.pdf	Conforme	

Área y referencia del requisito	Referencia	Calificación	Observación
	(Evidencia Documental) Managed Environment Software Change Procedure.pdf (Evidencia Documental)		
Se conserva un registro de cambios (peticiones, decisiones adoptadas) y podrán ser objeto de posterior auditoría.	Change Log_Jira 2023-10-03T19_11_52+1000.xlsx (Evidencia Remota)	Conforme	
En el caso de cambios en componentes críticos, deberá evaluarse si se trata de un cambio sustancial.	RP-484.doc.pdf (Evidencia Remota)	Conforme	
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.	GS 3.12.1_2023.png (Evidencia Remota) GS 1.7.5_2019.png (Evidencia Remota)	Conforme	

Plan de prevención de pérdida de información

Área y referencia del requisito	Referencia	Calificación	Observación
El operador dispone de un plan que garantiza que no hay perdidas en la información y transacciones que puedan afectar al desarrollo de los juegos, los derechos de los participantes o interés	Business Continuity Plan Overview – IGS.pdf (Evidencia Documental)	Conforme	

Área y referencia del requisito	Referencia	Calificación	Observación
público. El plan incluye los riesgos que toma el operador.			
Las copias de la información están guardadas convenientemente en un lugar remoto de la información que debe ser guardada. Dichas copias están protegidas de accesos no autorizados.	Backup Schedule.png (Evidencia Remota) Backups stored.png (Evidencia Remota) Access Control Policy.pdf (Evidencia Documental)	Conforme	
El operador dispone de procedimientos documentados de acción en caso de pérdida de información que incluya mecanismos con las quejas de los usuarios, la continuación de los juegos o apuestas interrumpidas, y otro tipo de situaciones que requieran de actuación.	Business Continuity Plan Overview – IGS.pdf (Evidencia Documental)	Conforme	
En caso de pérdida de información, el operador informará a la DGOJ inmediatamente, indicando las acciones tomadas y una estimación del impacto de la pérdida.	Security Incident Management Policy.pdf (Evidencia Documental) Reporting Schedule – Eyecon Alderney Limited.pdf (Evidencia Documental)	Conforme	

Gestión de continuidad de negocio

Área y referencia del requisito	Referencia	Calificación	Observación
Existe una gestión de continuidad del negocio ante desastres que incluye medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio, así como una réplica de la Unidad Central de Juegos que permita el normal desarrollo de la actividad.		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.
El plan de continuidad considera: - 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. - La retirada de fondos. El tiempo máximo para prestar de nuevo estos servicios será de una semana. - La continuación de juegos incompletos o apuestas pendientes y pago de premios válidamente conseguidos. El tiempo máximo para prestar de nuevo estos servicios será de un mes.		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.

Área y referencia del requisito	Referencia	Calificación	Observación
- Restablecimiento completo de todos los servicios.			
En todos los escenarios se incluye la información de los servicios recuperados y el tiempo máximo de recuperación.		No aplica	No aplica ya que estamos en Auditoria 2. Este campo solo se requiere en las Auditorías 1 y 3.

Penetración y análisis de vulnerabilidades

Área y referencia del requisito	Referencia	Calificación	Observación
En el último año el sistema técnico de juego ha pasado un test de penetración y un análisis de vulnerabilidades.	Eyecon Web Application Security Assessment v0.3.pdf (Evidencia Documental)	Conforme	
Existe un plan de análisis, al menos anual, de vulnerabilidades.	Eyecon Web Application Security Assessment v0.3.pdf (Evidencia Documental)	Conforme	

6.3. DETALLE DEL CUMPLIMIENTO DE LOS REQUISITOS DE FUNCIONALIDAD GENERAL.

Juego Responsable

Descripción	Referencia	Calificación	Observaciones
Acciones preventivas contra el juego patológico y su operativa		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Contrato, Aceptación, copia y modificación

Descripción	Referencia	Calificación	Observaciones
Contrato de juego		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Obligaciones del operador en relación con los participantes		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Política de privacidad		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Registro de usuario y comprobación de las prohibiciones

Descripción	Referencia	Calificación	Observaciones
Conservación de copia de los documentos aportados		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Servicios de verificación ofrecidos por la Dirección General de Ordenación del Juego		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Descripción	Referencia	Calificación	Observaciones
Activación del registro de usuario y limitación en la participación.		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Revisión periódica de los registros de usuario		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Cancelación del registro de usuario		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Suspensión por inactividad		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Medidas de prevención del fraude		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Registro y comunicación en relación a la suspensión cautelar del registro de usuario		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Registro de usuario activo único		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Cuenta de juegos, cobros y pagos

Descripción	Referencia	Calificación	Observaciones
Obligaciones del operador en relación con los participantes		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Funcionalidad de la cuenta de juego		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Procedimiento de control de los depósitos de los participantes		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Historial		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Prohibición de transferencias entre participantes		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Cuentas asociadas a registros de usuario en estado diferente a activo		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Registro de las operaciones de pago y cobro		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Descripción	Referencia	Calificación	Observaciones
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Procedimiento de control de las operaciones de pago y cobro		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Límites de los depósitos

Descripción	Referencia	Calificación	Observaciones
Límites de los depósitos		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Registro y trazabilidad

Descripción	Referencia	Calificación	Observaciones
Registros y logs del sistema técnico de juego		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Descripción	Referencia	Calificación	Observaciones
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Requisitos de la Unidad Central de Juegos		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Terminales y sesión de usuario

Descripción	Referencia	Calificación	Observaciones
Identificación de terminales		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Funcionalidad del terminal		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Terminales físicos de carácter accesorio		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Sesión de usuario		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Canales de comunicación

Descripción	Referencia	Calificación	Observaciones
Actividades de juego realizadas a través de sitio web		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Actividades de juego realizadas a través de mensajería de texto de servicios telefónicos fijos o móviles.		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Redirección al dominio «.es»		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Sistema de control interno

Descripción	Referencia	Calificación	Observaciones
Indisponibilidad del SCI y suspensión de la oferta de juego		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Calidad de la información del SCI		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Conservación de la información del SCI		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Descripción	Referencia	Calificación	Observaciones
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

6.4. DETALLE DEL CUMPLIMIENTO DE REQUISITOS DE FUNCIONALIDAD SINGULAR.

Porcentaje de retorno y tablas de premios

Descripción	Referencia	Calificación	Observaciones
Reglamentación básica del juego		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Porcentaje de retorno al participante		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
	RTP-468.pdf (Evidencia Remota)	Conforme	

Descripción	Referencia	Calificación	Observaciones
	RTP-557.pdf (Evidencia Remota) RTP-626.pdf (Evidencia Remota)		
Tablas de premios	Game Config and Paytable File Versions (1).png (Evidencia Remota) Game Config and Paytable File Versions (2).png (Evidencia Remota) Game Config and Paytable File Versions.PNG (Evidencia Remota) Game Config File (2).png (Evidencia Remota) Game Config File (3).png (Evidencia Remota) Game Config File Changes (1).png (Evidencia Remota) Game Config File Changes (2).png (Evidencia Remota)	Conforme	

Descripción	Referencia	Calificación	Observaciones
	Game Config File Changes 2.PNG (Evidencia Remota) Game Config File Changes.PNG (Evidencia Remota) Game Config File.PNG (Evidencia Remota) Game Paytable Generated File.PNG (Evidencia Remota)		

Generador de números aleatorios

Descripción	Referencia	Calificación	Observaciones
Homologación del GNA	RNG.ESP.EYECON.1008.01_eSigned (Evidencia Documental) RNGSignature.png (Evidencia remota)	Conforme	
Fallos en el GNA	Daily RNG Report_19.07.2023.pdf (Evidencia Remota) Eyecon RNG Certification Overview.pdf (Evidencia Documental)	Conforme	

Descripción	Referencia	Calificación	Observaciones
	RNG Monitoring Procedure.pdf (Evidencia Documental) RNG Statistical Testing.pdf (Evidencia Remota)		
Resemillado del GNA		No aplica	El cliente implementa un GNA criptográficamente seguro. Un GNA de este tipo generalmente toma su semilla inicial en función de la entropía del sistema, nunca se resemilla explícitamente y no necesariamente será necesario semillar nuevamente.

Lógica del juego

Descripción	Referencia	Calificación	Observaciones
Controles de la lógica del juego	Software Development Policy.pdf (Evidencia Documental) IGS Firewall Standard.pdf (Evidencia Documental)	Conforme	
	Live RTP Monitoring Procedure.pdf (Evidencia Documental)	Conforme	

Descripción	Referencia	Calificación	Observaciones
	Daily Jackpot RTP Report email.pdf (Evidencia Remota) config audit report for SD-37552.png (Evidencia Remota) Game Session Report.png (Evidencia Remota) Game Session single ID report.png (Evidencia Remota) Jackpot Win report.png (Evidencia Remota) Jackpot Audit report.png (Evidencia Remota) Jackpot Ledger.png (Evidencia Remota) Game Session - Details.png (Evidencia Remota) Game Session - Device Details.png (Evidencia Remota)		

Descripción	Referencia	Calificación	Observaciones
	Jackpot Example Game Session.png (Evidencia Remota) FW_ Sky Bingo Daily Jackpot Reports for 2023-03-27 (Evidencia Remota) Information Retention Policy Schedule.pdf (Evidencia Documental) Information Retention Policy.pdf (Evidencia Documental) RNG Monitoring Procedure.pdf (Evidencia Documental) AML Investigation Procedure.pdf (Evidencia Documental)		
	SD-42035.pdf (Evidencia Remota)	Conforme	

Registro y trazabilidad

Descripción	Referencia	Calificación	Observaciones
Requisitos de la Unidad Central de Juegos	Game Session Report.png (Evidencia Remota)	Conforme	

Descripción	Referencia	Calificación	Observaciones
	Game Session single ID report.png (Evidencia Remota) Game Session - Details.png (Evidencia Remota) Game Session - Device Details.png (Evidencia Remota)		
Registros y logs del sistema técnico de juego		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Terminales y sesión de usuario

Descripción	Referencia	Calificación	Observaciones
Identificación de terminales		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Funcionalidad del terminal		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Integridad del terminal		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Registro de las sesiones de usuario		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
	Game Session Report.png (Evidencia Remota)	Conforme	

Descripción	Referencia	Calificación	Observaciones
	Game Session - Details.png (Evidencia Remota) Game Session - Device Details.png (Evidencia Remota) Game Session single ID report.png (Evidencia Remota)		
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Canales de comunicación

Descripción	Referencia	Calificación	Observaciones
Actividades de juego realizadas a través de mensajería de texto de servicios telefónicos fijos o móviles.		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Actividades de juego a través de servicios de comunicaciones por voz.		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Descripción	Referencia	Calificación	Observaciones
Actividades de juego a través de medios de comunicación audiovisual		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Comportamiento ante errores técnicos

Descripción	Referencia	Calificación	Observaciones
Deshabilitación de un juego o de una sesión de usuario	Disconnection Policy.pdf (Evidencia Documental) ReggaeRhythmDISABLED.png (Evidencia Remota) ReggaeRhythmENABLED.png (Evidencia Remota) STELLAV-RequestTypes-051021-1419-19.pdf (Evidencia Remota)	Conforme	
Juego incompleto	Reggae reconstructions 1.png (Evidencia Remota) Reggae reconstructions 2.png (Evidencia Remota)		Auditoría B2B, las políticas de desconexión relacionadas con la plataforma quedan fuera del alcance.

Descripción	Referencia	Calificación	Observaciones
	Disconnection Policy.pdf (Evidencia Documental) Disaster Recovery Plan (Internet Gaming Systems) (Evidencia Documental)		
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Juegos <<en vivo>>

Descripción	Referencia	Calificación	Observaciones
Juegos <<en vivo>>		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Funcionalidades varias

Descripción	Referencia	Calificación	Observaciones
Jugadores virtuales utilizados por participantes		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Juegos a través de canales de comunicación «en diferido»	AML Investigation Procedure.pdf (Evidencia Documental) Access Control Policy.pdf (Evidencia Documental) IGS Firewall Standard.pdf (Evidencia Documental) Jackpot Win report.png (Evidencia Remota) jackpot audit report.png (Evidencia Remota)	Conforme	

Botes progresivos

Descripción	Referencia	Calificación	Observaciones
Botes, botes progresivos, y premios adicionales	SD-37552.doc.pdf (Evidencia Documental)	Conforme	Las cuentas quedan fuera del alcance para esta auditoría B2B.

Descripción	Referencia	Calificación	Observaciones
	config audit report for SD-37552.png (Evidencia Remota) config audit report for SD-37552_addition.png (Evidencia Remota) Jackpot Win report.png (Evidencia Remota) Jackpot Audit report.png (Evidencia Remota)		
	SD-37552.doc.pdf (Evidencia Documental) config audit report for SD-37552.png (Evidencia Remota) config audit report for SD-37552_addition.png (Evidencia Remota) Jackpot Win report.png (Evidencia Remota) Jackpot Audit report.png (Evidencia Remota)	Conforme	
	monthly_jackpot_rtp_report_20211001.xls (Evidencia Remota)	Conforme	Una vez creado el sistema de gestión de botes no permite que se hagan modificaciones a los parámetros del bote

Descripción	Referencia	Calificación	Observaciones
	monthly_jackpot_rtp_report_20221001.xls (Evidencia Remota) Daily RNG Report_19.07.2023.pdf (Evidencia Remota) Daily Jackpot RTP Report email.pdf (Evidencia Remota) SkyBingoDailyJackpotGames_20230328.xls (Evidencia Remota) SkyBingoDailyJackpotGames_20230615.xls (Evidencia Remota) SkyBingoDailyJackpotGames_20230801.xls (Evidencia Remota) SkyBingoDailyJackpotPlayers_20230328.xls (Evidencia Remota) SkyBingoDailyJackpotPlayers_20230615.xls (Evidencia Remota)		una vez creado. Para poder realizar cambios se debe crear un nuevo bote actualizando las configuraciones deseadas. La lógica para determinar los ganadores de los botes y la redirección del bote en los que parte del bote acumulado es redirigido a otro fondo está contenida en el código fuente que se evalúa externamente por terceros. No se pueden realizar cambios a los botes en vivo. El proveedor tiene implementado un sistema de informes diarios de botes que se envían por correo electrónico a los operadores para su revisión, así como múltiples informes de monitorización interna. Las cuentas quedan fuera del alcance para esta auditoría B2B.

Descripción	Referencia	Calificación	Observaciones
	SkyBingoDailyJackpotPlayers_20230801.xls (Evidencia Remota) SkyBingoDailyJackpotWinners_20230328.xls (Evidencia Remota) SkyBingoDailyJackpotWinners_20230615.xls (Evidencia Remota) SkyBingoDailyJackpotWinners_20230801.xls (Evidencia Remota)		

Sistema de control interno

Descripción	Referencia	Calificación	Observaciones
Indisponibilidad del SCI y suspensión de la oferta de juego		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
Calidad de la información del SCI		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.
		No aplica	Fuera del alcance para la auditoría bienal de proveedor B2B.

Registro de la configuración de la sesión destinada al juego de máquinas de azar

Descripción	Referencia	Calificación	Observaciones
Registro de la configuración de la sesión destinada al juego de máquinas de azar		No aplica	El sistema de configuración del usuario corre a cargo del operador de plataforma.

7. DESCRIPCIÓN DEL SOPORTE DIGITAL QUE ACOMPAÑARÁ AL INFORME DE AUDITORÍA.

El informe de auditoría se acompaña de un anexo en soporte digital, y está estructurado de la siguiente manera:

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

8. INFORMACIÓN ADICIONAL/OBSERVACIONES.

Sin observaciones.

9. CONCLUSIÓN.

De acuerdo con las pruebas realizadas y los resultados obtenidos, BMM confirma que el elemento sometido a auditoria[1] para el operador Eyecon Alderney Limited descrito en la sección 2 del presente informe, ha sido auditado y los resultados están descritos en el presente informe.

Atentamente,

30378334A RUBÉN ALBERTO BAPTISTA (C:B64622251)
Firmado digitalmente por 30378334A RUBÉN ALBERTO BAPTISTA (C:B64622251)
Fecha: 2023.11.02 12:54:41 +01'00'

Rubén Baptista

SVP Operations EURSAM

Y0177716D JULIEN POTTIEZ (C:B64622251)
Firmado digitalmente por Y0177716D JULIEN POTTIEZ (C:B64622251)
Fecha: 2023.11.03 10:18:20 +01'00'

Julien Pottiez

VP of Security EURSAM

[1]Los resultados incluidos en este documento se refieren única y exclusivamente a la muestra ensayada, tal y como se describe en el apartado correspondiente.