

Informe Definitivo de Certificación de Seguridad Eyecon Alderney Limited

Diciembre 2019



CONTENIDOS

1. INTRODUCCIÓN	2
2. RESTRICCIONES DE USO DE ESTE INFORME	3
3. IDENTIFICACIÓN DE LA CERTIFICACIÓN.....	4
4. DESCRIPCIÓN DEL OBJETO DE LA CERTIFICACIÓN	5
5. RESUMEN EJECUTIVO DE LA CERTIFICACIÓN DE LA SEGURIDAD	7
5.1 CALIFICACIÓN GLOBAL	7
5.2 CUADRO RESUMEN DEL CUMPLIMIENTO DE LOS REQUISITOS DE SEGURIDAD.....	7
5.3 CUADRO RESUMEN DE LOS ANÁLISIS DE AUDITORÍA ESPECÍFICOS	8
6. DETALLE DEL CUMPLIMIENTO DE LOS REQUISITOS DE SEGURIDAD	9
6.1. POLÍTICA DE SEGURIDAD	9
6.2. ANÁLISIS Y GESTIÓN DE RIESGOS	10
6.3. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....	13
6.4. SEGURIDAD EN LA COMUNICACIÓN DE LOS PARTICIPANTES	13
6.5. SEGURIDAD DE RECURSOS HUMANOS Y TERCEROS	17
6.6. SEGURIDAD FÍSICA Y MEDIOAMBIENTAL	17
6.7. GESTIÓN DE COMUNICACIONES Y OPERACIONES.....	19
6.8. CONTROL DE ACCESO.....	22
6.9. COMPRA, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	25
6.10. GESTIÓN DE INCIDENTES DE SEGURIDAD	25
6.11. GESTIÓN DE CAMBIOS.....	26
6.12. PLAN DE PREVENCIÓN DE PÉRDIDA DE INFORMACIÓN	27
6.13. GESTIÓN DE CONTINUIDAD DE NEGOCIO.....	27
6.14. PENETRACIÓN Y ANÁLISIS DE VULNERABILIDADES.....	29
7. DETALLE DE LOS ANÁLISIS DE AUDITORÍA ESPECÍFICOS.....	30
7.1. ANÁLISIS DE AUDITORÍA DE LOS COMPONENTES CRÍTICOS	30
7.2. ANÁLISIS DE AUDITORÍA DE LA GESTIÓN DE CAMBIOS	31
7.3. ANÁLISIS DE AUDITORÍA DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO Y PREVENCIÓN DE LA PÉRDIDA DE INFORMACIÓN.....	32
8. DESCRIPCIÓN DEL LUGAR, EQUIPO Y FECHAS DE REALIZACIÓN DE LA CERTIFICACIÓN	34
9. DESCRIPCIÓN DEL SOPORTE DIGITAL QUE ACOMPAÑARÁ AL INFORME DE CERTIFICACIÓN	35

1. INTRODUCCIÓN

El 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 los requisitos técnicos de las actividades del juego establece en sus artículos 16 y 17, que los Operadores deberán presentar un Informe Definitivo de Certificación de su sistema técnico de juego.

La metodología de evaluación y modelo de informe sigue las indicaciones proporcionadas por la Dirección General de Ordenación del Juego en Resolución de 6 de octubre de 2014, 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.

2. RESTRICCIONES DE USO DE ESTE INFORME

Este informe definitivo de certificación de la seguridad ha sido preparado para su utilización por parte de Eyecon Alderney Limited, en adelante Eyecon o el proveedor, y no debe ser utilizado por ninguna otra sociedad ni con otra finalidad diferente a la indicada, sin nuestro consentimiento previo por escrito. Asimismo, cualquier referencia a este informe que se incluya en cualquier documento de un tercero, debe ser previamente acordada con Ernst & Young, S.L.

Ernst & Young, S.L. no acepta ninguna responsabilidad como resultado de la utilización de este informe en un sentido diferente al indicado con anterioridad.

3. IDENTIFICACIÓN DE LA CERTIFICACIÓN

A continuación, se incluye información identificativa de la certificación de seguridad realizada sobre el sistema técnico utilizado por Eyecon para el desarrollo de su actividad en el marco de la Ley 13/2011, de 27 de mayo, de regulación del juego.

Identificación de la Certificación	
Tipo de informe	Informe Definitivo de Certificación de Seguridad
Código de identificación	EYCDSEYE20191211
Destinatario del informe	Eyecon Alderney Limited
Entidad Certificadora	Ernst & Young, S.L.
Dirección	Calle de Raimundo Fernández Villaverde, 65 28003 Madrid, España
CIF	B78970506
Equipo de Trabajo	Pablo Sierra Carriba Alfredo Díaz Contreras Borja Martín Sanz
Firmante del Informe	Elena Maestre García  Socio Ernst & Young, S.L.
Fechas de realización de los trabajos de certificación	23/07/2019 - 10/12/2019
Fecha de emisión del informe de certificación	11/12/2019

4. DESCRIPCIÓN DEL OBJETO DE LA CERTIFICACIÓN

En el presente Informe Definitivo de Certificación de la Seguridad se han evaluado los requisitos de seguridad del sistema técnico de juego efectivamente empleado por Eyecon Alderney Limited, en relación con los procedimientos, procesos, planes y medidas de seguridad efectivamente implementados.

A continuación, se incluye el listado de Centros de Procesado de Datos donde se alberga el sistema técnico de juego objeto de certificación.

CPD	Calle, número	Ciudad	País	Tipo	Razón Social del proveedor de alojamiento
CPD1	Limited c/o Vodafone Malta Ltd MAR Building Cannon Road Qormi QRM 9039	Qormi	Malta	Hosting	Continent 8 Technologies
CPD2	Admiralty Tunnel 77 Queensway Rd Gibraltar GX11 1AA	Gibraltar	Gibraltar	Hosting	Continent 8 Technologies
CPD3	First Tower Lane Data Centre First Tower Lane St Peter Port Guernsey GY12RZ	St Peter Port	Guernsey	Hosting	JT Global
CPD4	Centenary House, La Vrangue, St Peter Port, Guernsey, GY1 2EY	St Peter Port	Guernsey	Hosting	Continent 8 Technologies
CPD5	Unit B10, Ballycoolin Business & Technology Park, Blanchardstown, Dublin 15	Dublin	Irlanda	Hosting	Continent 8 Technologies

Adicionalmente, se ha evidenciado que ambos Centros de Procesado de Datos cuentan con la certificación ISO27001:2013.

La relación de los componentes software objeto de certificación son:

Nombre del componente	Versión	Descripción	SHA-1	Crítico
Game Server	1.7.7	Contiene la lógica del juego del lado del servidor y de los componentes RNG. Facilita la comunicación con el navegador del jugador y los sistemas externos para las llamadas de apuestas.	f32877db2725016d7e8c191969cedf7af66a764f	Sí
Carbine	5.3.27	Componente del lado del servidor contenido en el servidor de juegos donde se ejecuta toda la lógica del juego.	9983390c4697be4317f8f8be1574c3e124aa0d4b9	Sí
RNG	1.0.1	Componente RNG	39c3c581d88f9674aa0765af51a56bd26955efd9	Sí

Feed Server	1.0.20	Proporciona fuentes de datos a los clientes del juego, incluidos los niveles de grupo de Jackpot.	bb4543587743a8a3594bc841fb57196d28cad599	Sí
Pool Server	1.0.33	Proporciona la gestión de los grupos de Jackpot.	d76aa2111918f2b76c2d6fc5c47dcf923b2958f1	Sí
Game Reporting Server	1.2.0	Proporciona informes visuales de los registros históricos del juego.	fe8f123af1f64189e05a63d0953582a63a24d134	No
Warehouse Reporting Server	1.0.14	Proporciona acceso a los registros de almacenamiento de datos subyacentes para fines de informes.	23ecce696123b5dcb25cd1ce3e06383f9be06552	No
Bonusing Server	1.8.0	Proporciona funcionalidad de bonificación de giro gratis, no es necesario para el juego regular.	484d2ece29d1775c3fccf16a8deae894093924c	No
Warehouse Replication Agent	1.0.18	Almacena una copia de seguridad local de todos los registros del juego, también proporciona un medio para que esos registros se copien en un almacén remoto con el fin de cumplir con los requisitos de informes de datos y retención.	71843d2184489a5aa7d5d504928f4051f5fd8b60	Sí
Warehouse Replication Server	1.0.16	Este componente utiliza el agente de replicación de almacén para copiar de forma remota los registros del juego en una instalación de almacenamiento de datos remoto.	9e9b17d0c1de9f369296a4bf476a3db0dc5cc181	Sí
Warehouse Server	1.0.31	Este componente almacena una copia de seguridad local de los registros de auditoría de juegos replicados de forma remota. También transforma esos registros en tablas de informes resumidas.	084bada75e4e245d33131f98f4034b2fe9df1740	Sí

5. RESUMEN EJECUTIVO DE LA CERTIFICACIÓN DE LA SEGURIDAD

5.1 Calificación global

La tabla de calificación global muestra el cumplimiento general de los requisitos técnicos del sistema de juego efectivamente utilizado por el Operador.

Calificación global	Resultado
Calificación global de la seguridad	Conforme
Convalidación ISO 27001	Sí

5.2 Cuadro resumen del cumplimiento de los requisitos de seguridad

Se presenta una tabla resumen con el número de requisitos evaluados, agrupados por áreas.

Área	Número de requisitos	Número de requisitos conformes	Número de requisitos convalidados (ISO27001)	Número de requisitos no conformes	Número de requisitos no aplica
Política de seguridad.	2	2	0	0	0
Análisis y gestión de riesgos.	14	7	0	0	7
Organización de la seguridad de la información.	1	1	0	0	0
Seguridad en la comunicación con los participantes.	13	0	0	0	13
Seguridad en los recursos humanos y terceros.	3	3	0	0	0
Seguridad física y medioambiental.	9	0	9	0	0
Gestión de comunicaciones y operaciones.	14	14	0	0	0
Control de acceso.	13	12	0	0	1
Compra, desarrollo y mantenimiento de los sistemas.	1	1	0	0	0
Gestión de incidentes de seguridad.	2	2	0	0	0
Gestión de cambios.	5	5	0	0	0
Plan de prevención de pérdida de información.	3	3	0	0	0
Gestión de continuidad de negocio.	6	4	0	0	2
Test de penetración y análisis de vulnerabilidades	2	2	0	0	0

5.3 Cuadro resumen de los análisis de auditoría específicos

A continuación, se describen los análisis de auditoría específicos realizados durante los trabajos de certificación.

5.3.1 Análisis de auditoría de los componentes críticos

El análisis correspondiente a la identificación de los componentes críticos ha sido evaluado como conforme.

5.3.2 Análisis de auditoría de la gestión de cambios

El análisis correspondiente a la auditoría de gestión de cambios ha sido evaluado como conforme.

5.3.3 Análisis de auditoría de la gestión de continuidad de negocio y prevención de la pérdida de información

En la tabla siguiente se indica la calificación global del análisis de auditoría correspondiente a la gestión de la continuidad de negocio:

Calificación	Conforme
--------------	----------

En la tabla que se presenta a continuación se indican los tiempos máximos de recuperación y de pérdida de información ante un desastre.

Tiempo máximo de recuperación ante un desastre:	4 horas
Tiempo máximo de pérdida de información ante un desastre:	5 minutos

6. DETALLE DEL CUMPLIMIENTO DE LOS REQUISITOS DE SEGURIDAD

6.1. Política de seguridad

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
El operador dispone de procedimientos de seguridad.	Conforme	<p>Se ha evidenciado que se ha desarrollado una política de seguridad que define las directrices en materia de seguridad.</p> <p>La política de seguridad aplica a todos los usuarios que acceden a información o redes de comunicaciones de Eyecon, ya sea trabajadores, colaboradores, o bien terceros externos a la misma.</p> <p>En el documento se definen los objetivos de seguridad y las medidas que se deben implementar para lograr la seguridad de la información, equipos y servicios IT.</p> <p>Las principales medidas adoptadas para cumplir con los objetivos de seguridad se centran en:</p> <ul style="list-style-type: none"> - Definición de responsabilidades - Clasificación de la información. - Seguridad del personal. - Seguridad física. - Seguridad lógica y del software. - Seguridad de los datos. - Continuidad de negocio. - Gestión de brechas e incidentes de seguridad. - Formación. 	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Los procedimientos de seguridad han sido comunicados a la totalidad de sus empleados y, en su	Conforme	La política de seguridad aplica a todos los usuarios que acceden a información o redes de comunicaciones de Eyecon, ya sea trabajadores,	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

caso, a las entidades colaboradoras.		colaboradores, o bien terceros. Todo el personal es informado de las políticas y procedimientos de seguridad, ya que esta se encuentra publicada en la intranet y se envía un email de notificación a todos los empleados.	
--------------------------------------	--	---	--

6.2. Análisis y gestión de riesgos

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
El operador dispone de un plan de análisis y gestión de riesgos.	Conforme	Se ha evidenciado que Eyecon dispone de un plan de análisis y gestión de los riesgos que afectan al sistema técnico de juego. El plan de análisis y gestión de riesgos está basado en la comparación de la práctica actual con la norma ISO:31000 que proporciona unos principios y directrices para la gestión del riesgo y el proceso implementado en el nivel estratégico y operativo. Esto permite a Eyecon identificar qué necesita cambiar y preparar, e implementar un plan para hacerlo, manteniendo un monitoreo y una revisión continuos para garantizar la vigencia y la mejora continua.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Se realiza una revisión periódica del análisis de riesgos.	Conforme	Se ha evidenciado que se realizan revisiones periódicas del análisis de riesgos. Se adjunta una revisión de abril de 2019.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
La organización tiene identificados los componentes críticos del Sistema Técnico de Juego.	Conforme	Se ha evidenciado que se han identificado los componentes críticos que implementan el sistema técnico de juego.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
La relación de componentes críticos incluye el registro de usuario.	No aplica	La gestión del registro de usuario es responsabilidad del Operador.	

La relación de componentes críticos incluye la cuenta de juego.	No aplica	La gestión de la cuenta de juego es responsabilidad del Operador.	
La relación de componentes críticos incluye el procesamiento de los medios de pago.	No aplica	La gestión del procesamiento de los medios de pago es responsabilidad del Operador.	
La relación de componentes críticos incluye para el generador de números aleatorios: los componentes del sistema técnico de juego que transmiten o procesan números aleatorios que serán objeto del resultado de los juegos y la integración de los resultados del generador de números aleatorios en la lógica del juego.	Conforme	Se ha evidenciado que se han identificado los componentes críticos que implementan Generador de Números Aleatorios.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
La relación de componentes críticos incluye aquellos componentes que almacenan, manipulan o transmiten información sensible de los clientes, como datos personales, de autenticación, etc.	No aplica	La gestión de los componentes que almacenan, manipulan o transmiten información sensible de los participantes es responsabilidad el Operador.	
La relación de componentes críticos incluye aquellos componentes que almacenan el estado puntual de los juegos.	Conforme	Se ha evidenciado que se han identificado los componentes críticos que almacenan el estado puntual de los juegos.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
La relación de componentes críticos incluye las conexiones con la Dirección General de	No aplica	La gestión de las conexiones con la Dirección General de Ordenación del Juego es responsabilidad el Operador.	

Ordenación del Juego.			
La relación de componentes críticos incluye el sistema de control interno: el capturador y el almacén.	No aplica	La gestión del Sistema de Control interno es responsabilidad del Operador.	
La relación de componentes críticos incluye los puntos de acceso y las comunicaciones de y hacia los componentes críticos anteriores.	Conforme	Se ha evidenciado que entre los componentes críticos se incluyen los puntos de acceso y las comunicaciones de y hacia los demás componentes críticos.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
La relación de componentes críticos incluye las redes de comunicación que transmiten información sensible de participantes.	No aplica	La gestión de los componentes que incluye la gestión de las redes que comunican o transmiten información sensible de los participantes es responsabilidad el Operador.	
El operador tiene reforzada la seguridad de todos los componentes críticos.	Conforme	<p>Se ha evidenciado que Eyecon tiene reforzada la seguridad de todos los componentes críticos citados anteriormente.</p> <p>Como se indica en la Política de desarrollo de software de Eyecon, todos los cambios de software deben ser revisados con especial atención. Todos los componentes críticos del backend están sujetos a análisis estático automatizado, incluso frente a vulnerabilidades comunes como OWASP Top 10. Se adjuntan evidencias de los controles técnicos sobre los riesgos de seguridad durante el desarrollo.</p> <p>Adicionalmente, los componentes críticos se encuentran bajo la protección de antivirus y firewall de Palo Alto.</p> <p>Los componentes críticos pasan un test de penetración y análisis de</p>	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

		<p>vulnerabilidades de forma al menos anual.</p> <p>Asimismo, se ha verificado que los Centros de Procesado de Datos donde se encuentra el software de juego, cuentan con el certificado ISO27001.</p>	
--	--	--	--

6.3. Organización de la Seguridad de la Información

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
La organización ha definido un marco de gestión para la seguridad de la información, indicando las funciones y responsabilidad de su personal.	Conforme	<p>La política de seguridad de la información establece todas las responsabilidades de Seguridad de la Información. Esto se apoya en la directiva de control de acceso que describe los roles y cada nivel de acceso que se concede dentro del sistema.</p> <p>Los permisos de Eyecon se rigen por el principio de mínimos privilegios. Cada cual tiene acceso a los sistemas que necesita para realizar su trabajo.</p> <p>Asimismo, el acceso a todos los sistemas o dispositivos gestionados o propiedad de Eyecon debe ser autorizado por el propietario del sistema y/o el jefe de infraestructura de IT, operaciones y seguridad de Eyecon y/o el director del equipo de sistemas.</p> <p>Adicionalmente se estipularon unas normas para todos los trabajadores donde se estipula la necesidad de segregación de tareas para evitar conflictos de interés.</p>	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

6.4. Seguridad en la comunicación de los participantes

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
El operador ha adoptado mecanismos de	No aplica	Eyecon no se comunica de forma directa con los usuarios finales del sistema	

autenticación que permiten al sistema de juego identificar al participante, y que, a su vez, permiten al participante identificar al sistema de juego.		de juego. La evaluación de este requisito es responsabilidad del Operador.	
Las comunicaciones son cifradas en los casos de transmisión de datos personales (registro de usuario) o económicos (cuenta de juego).	No aplica	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	
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	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	
Se establece, por defecto o por el participante, una contraseña inicial de usuario.	No aplica	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	
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	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	
La longitud mínima de la contraseña es de 8 caracteres o dígitos, e incluye al menos elementos de tres de los	No aplica	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es	

siguientes grupos: números, letras minúsculas, letras mayúsculas y otros símbolos.		responsabilidad del Operador.	
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	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	
La contraseña no puede contener ninguno de los siguientes datos: el nombre del usuario, el seudónimo, el nombre o apellidos o la fecha de nacimiento del participante.	No aplica	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	
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	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	
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	No aplica	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	

introducción de la contraseña.			
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	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	
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	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	
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	Eyecon no se comunica de forma directa con los usuarios finales del sistema de juego. La evaluación de este requisito es responsabilidad del Operador.	

6.5. Seguridad de recursos humanos y terceros

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
El operador dispone de un plan de Seguridad del Personal.	Conforme	Se ha evidenciado que Eyecon dispone de una política de formación y desarrollo de sus empleados.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
El plan incluye acciones formativas para todos los empleados de la organización, prestando especial atención a los permisos de acceso a información y componentes críticos.	Conforme	El plan de formación contempla acciones formativas para todos los empleados en materia de seguridad. Se adjuntan como evidencia los certificados obtenidos por los empleados de Eyecon en materia de seguridad.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
En los casos en los que el operador necesite servicios de terceros que impliquen acceso, procesamiento, comunicación o tratamiento de la información, o bien el acceso a instalaciones, productos o servicios relacionados con el juego, éstos terceros deben cumplir la totalidad de los requisitos de seguridad exigibles al resto del personal.	Conforme	Se ha comprobado que en los casos en los que el operador utiliza servicios de terceros, se recogen en el SLA las medidas de seguridad oportunas.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

6.6. Seguridad física y medioambiental

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
Existe un plan de seguridad física de los componentes del sistema técnico de juego.	Convalidado	ISO 27001	Ver ISO 27001
La seguridad perimetral para las	Convalidado	ISO 27001	Ver ISO 27001

áreas que contienen componentes críticos e información sensible está definida.			
Existe un Control de acceso físico a las instalaciones en las cuales se encuentren los equipos, tanto para empleados como para personal externo, y que este control incluye elementos físicos, procedimientos de autorización, registros de acceso y servicios de vigilancia.	Convalidado	ISO 27001	Ver ISO 27001
Está contemplada la protección frente a riesgos ambientales: agua, fuego, provocados por personas, etc.	Convalidado	ISO 27001	Ver ISO 27001
Los equipos críticos están protegidos frente a cortes del suministro eléctrico y otras interrupciones causadas por fallos en instalaciones de soporte y que el cableado de suministro eléctrico está protegido de daños.	Convalidado	ISO 27001	Ver ISO 27001
Están definidos los mecanismos de control de acceso al cableado de comunicaciones si transporta información crítica sin cifrar.	Convalidado	ISO 27001	Ver ISO 27001
Se proporciona y está previsto el adecuado mantenimiento de las instalaciones y equipos.	Convalidado	ISO 27001	Ver ISO 27001

Los dispositivos que contienen información son borrados de manera segura o destruidos antes de ser reutilizados o retirados.	Convalidado	ISO 27001	Ver ISO 27001
Los equipos que contienen información no pueden ser trasladados fuera de las instalaciones seguras sin la correspondiente autorización.	Convalidado	ISO 27001	Ver ISO 27001

6.7. Gestión de comunicaciones y operaciones

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
Los componentes críticos son monitorizados para evitar que puedan utilizarse versiones diferentes de la homologada.	Conforme	Se ha comprobado que Eyecon dispone de un procedimiento para desplegar componentes software. Cualquier despliegue requiere de una solicitud, tras la cual se estudia y valora esta, comprobando si afecta a componentes críticos y si está homologada.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
La comunicación entre los componentes de los sistemas técnicos de juego garantiza la integridad y la confidencialidad.	Conforme	Las transacciones que se realizan están todas protegidas mediante los protocolos SSL y TLS.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Las tareas se segregan entre las diferentes áreas de responsabilidad, para minimizar la posibilidad de acceso no autorizado y potenciales daños.	Conforme	Se ha evidenciado que las tareas se encuentran segregadas entre los diferentes grupos de usuarios definidos en la política de control de acceso. Se adjunta captura de pantalla donde se observan los diferentes grupos de usuarios.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

Se han separado las tareas de desarrollo, pruebas y producción.	Conforme	Se ha evidenciado que se han separado las tareas de desarrollo, pruebas y producción. Se adjunta captura de pantalla donde se muestran las diferentes redes y las reglas para estas.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Los servicios proporcionados por terceras partes incluyen controles y métricas de seguridad en los contratos y son periódicamente auditados y monitorizados.	Conforme	Se ha evidenciado que los contratos con terceras partes incluyen controles y métricas de seguridad. Adicionalmente, se ha verificado que se realizan revisiones trimestrales.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Se han adoptado medidas de protección contra código malicioso.	Conforme	Eyecon únicamente permite instalar software a sus usuarios desde el centro de software aprobado. Adicionalmente, cuenta con antivirus instalado en los servidores y firewall de Palo Alto.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Se hacen regularmente copias de seguridad con la frecuencia adecuada y se conservan custodiadas según quede recogido en el plan de copias de seguridad.	Conforme	Se ha evidenciado que se cuenta con un procedimiento de realización de copias de seguridad en el que se detallan los diferentes tipos de copias y periodicidades con las que se realizan. Se realizan copias de seguridad que permitan recuperar todos los datos y software de Eyecon, de tal forma que los sistemas operativos y aplicaciones sean totalmente recuperables.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Se han adoptado medidas de seguridad en la red de comunicaciones.	Conforme	Las transacciones que se realizan están todas protegidas mediante los protocolos SSL y TLS. Adicionalmente, cuenta con antivirus instalado en los servidores y firewall de Palo Alto.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Se han adoptado medidas de seguridad en la	Conforme	Eyecon ha desarrollado una política de destrucción de datos, que aplica a todo el	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

manipulación de soportes portátiles, así como de borrado seguro o de destrucción de los mismos y que se ha plasmado en un procedimiento documentado.		personal de este y de terceros. En él se define qué hacer con cada activo de información. Se adjunta certificado de destrucción segura y confidencial.	
Los relojes de todos los componentes, especialmente de los críticos, están sincronizados con una fuente de tiempo fiable y el operador ha establecido medidas y controles para evitar la manipulación de las marcas de tiempo o su alteración posterior, especialmente en los registros de auditoría.	Conforme	Se ha evidenciado que todos los componentes están sincronizados con una fuente de tiempo fiable mediante el protocolo NTP.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Se genera y guarda registro de auditoría de actividad de todos los usuarios, excepciones y eventos de seguridad de la información durante un periodo mínimo de 2 años.	Conforme	Se ha evidenciado que Eyecon utiliza la herramienta Graylog, para la administración y análisis de registros. Desde la herramienta se conservan los registros de auditoría, excepciones y eventos de seguridad de todos los usuarios con acceso a los sistemas.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Los registros de auditoría están protegidos frente a la alteración y el acceso indebido.	Conforme	Todos los logs registrados se centralizan en la herramienta Graylog, de modo que estos siempre se encuentran duplicados (máquina de origen y graylog). Los permisos sobre los registros se manejan desde Graylog, se basan en roles y previenen los cambios o borrados.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Las actividades del Administrador del Sistema y del operador del	Conforme	Se ha evidenciado que Eyecon utiliza la herramienta "auditd" para registrar todos los	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

Sistema están siendo registradas.		comandos ejecutados por los administradores. Adicionalmente también se registra esta información a través de la aplicación Graylog.	
Se realiza un análisis periódico de los registros de auditoría y se toman acciones en función de las incidencias detectadas.	Conforme	Se ha comprobado que los registros de auditoría se revisan periódicamente por el equipo de seguridad. Se adjunta un ejemplo de revisión de los registros de auditoría de conexiones a través de VPN.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

6.8. Control de acceso

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
La política de acceso a información está documentada.	Conforme	Se ha evidenciado que, en la política de control de acceso, destinada a los usuarios de los sistemas de información, de modo que cada usuario pueda acceder únicamente a los recursos que precise para el desarrollo de sus funciones.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
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.	Conforme	Se ha evidenciado que los usuarios son identificados de forma inequívoca en los diferentes sistemas a los que acceden mediante usuario y contraseña. Adicionalmente se ha evidenciado la revisión periódica de los privilegios de los usuarios.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Los usuarios siguen buenas prácticas en el uso de contraseñas y protegen adecuadamente la documentación y soportes en su puesto de trabajo.	Conforme	Se ha comprobado que se ha definido una política de contraseñas y que esta es efectiva. Se ha evidenciado que se fuerza a los usuarios a elegir una contraseña con un nivel de seguridad adecuado.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

Los usuarios únicamente tienen acceso a los servicios que han sido autorizados a usar.	Conforme	Se ha comprobado que Eyecon ha establecido una serie grupos con diferentes roles, dependiendo del tipo de usuario. De este modo, los usuarios de cada grupo únicamente tendrán acceso a los servicios a los que han sido autorizados a utilizar. Se adjuntan evidencias de las diferentes opciones que da el sistema dependiendo del rol del usuario.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
No existen usuarios genéricos y todos los usuarios acceden con su usuario propio único.	Conforme	Se ha verificado que no existen usuarios genéricos y que los usuarios acceden con su propio usuario único. Adicionalmente, se realizan revisiones periódicas de los usuarios.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
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.	Conforme	Se ha verificado que todos los accesos al sistema quedan registrados. Todos los accesos se realizan a través de usuario y contraseña.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Las redes están segregadas en función del área y responsabilidad de la tarea o función.	Conforme	Se ha comprobado que las redes están segregadas en función del área y responsabilidad de la función que desempeñan. Se adjunta una evidencia de la configuración del firewall que impide el acceso a producción a los desarrolladores.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
El acceso a los sistemas operativos requiere un mecanismo de	Conforme	El acceso a los sistemas operativos se realiza a través de un usuario y contraseña. La contraseña	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

autenticación seguro.		debe cumplir con la política de contraseñas definida. Se ha comprobado que todos los accesos al sistema quedan registrados.	
Se restringe y se controla el uso de programas que permiten evitar los controles de acceso y de seguridad.	Conforme	Todo el software se despliega de manera centralizada mediante scripts controlados mediante Ansible. Los usuarios sin derechos administrativos únicamente pueden instalar software previamente aprobado desde el centro de software. Cualquier otro despliegue o instalación requiere hacer una solicitud.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Las sesiones tienen un tiempo máximo de duración de la conexión y un tiempo de desconexión por inactividad.	Conforme	Se ha evidenciado que las sesiones tienen un máximo de duración y que tras 5 minutos de inactividad se cierra la sesión automáticamente.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
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.	Conforme	Únicamente el personal autorizado tiene acceso a los datos reales. Los permisos de cada usuario dependen del grupo al que pertenecen. Se adjuntan capturas donde se aprecia que no todos los usuarios tienen acceso a la misma información.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Se gestionan los riesgos asociados a dispositivos móviles.	No aplica	Eyecon no permite conectarse a la red corporativa o de producción desde dispositivos móviles.	
Si existe teletrabajo, se comprueba que el riesgo asociado está gestionado en el marco del plan de seguridad.	Conforme	Se ha evidenciado que se ha desarrollado una política que afecta al teletrabajo.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

6.9. Compra, desarrollo y mantenimiento de los sistemas

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
Existe un plan de seguridad en la toma de decisiones de compra, desarrollo y mantenimiento de los sistemas de información.	Conforme	<p>Se ha evidenciado la existencia de un procedimiento para la gestión de compras y mantenimiento de los sistemas.</p> <p>Para las nuevas adquisiciones es necesario crear una petición, en la que se valorará la solicitud, así como los posibles proveedores.</p> <p>Se adjuntan evidencias de las evaluaciones y formularios de compra.</p>	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

6.10. Gestión de incidentes de seguridad

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
Existe un procedimiento documentado de gestión de incidentes de seguridad.	Conforme	<p>Se ha comprobado que se dispone de una política de gestión de incidentes de seguridad. La política incluye los siguientes puntos:</p> <ul style="list-style-type: none"> - Detección de incidentes de seguridad - Reporte de incidentes de seguridad - Tratamiento de incidentes de seguridad - Equipos de respuesta ante incidentes 	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Existe un registro de incidentes de seguridad (con hechos, impactos y medidas adoptadas).	Conforme	Los procedimientos de gestión de incidentes incluyen el registro y seguimiento de todos los incidentes mediante la herramienta de ticketing, Jira.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

6.11. Gestión de cambios

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
Existe un procedimiento de gestión de cambios en equipos y componentes del sistema técnico de juego en el entorno de producción.	Conforme	Para poder realizar un cambio es necesario crear una solicitud, que quede registrada en un ticket JIRA. Una vez que el ticket ha sido creado es evaluado para decidir si el cambio se aprueba o no.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Existe un proceso de aprobación interna de cambios (petición de cambio, aprobación de los responsables).	Conforme	Se ha evidenciado que existe un proceso de aprobación interna por el que pasan los cambios una vez son solicitados.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Se conserva un registro de cambios (peticiones, decisiones adoptadas) y podrán ser objeto de posterior auditoría.	Conforme	Se ha evidenciado que se mantiene un registro de cambios realizados y su detalle. Todos los cambios solicitados y realizados quedan registrados en JIRA. De cada cambio se conservar al menos, la fecha de solicitud del cambio, título, descripción, estado y personal que ha notificado el cambio.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
En el caso de cambios en componentes críticos, deberá evaluarse si se trata de un cambio sustancial.	Conforme	Se ha evidenciado que ante una solicitud de cambios en los componentes críticos se incluye una evaluación para determinar si se trata de un cambio sustancial o no.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
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.	Conforme	Se ha comprobado que se conservan las copias de los binarios de los elementos software de todas las versiones anteriores a la actual.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

6.12. Plan de prevención de pérdida de información

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
Existe un plan de prevención de pérdida de datos o transacciones que afecten al desarrollo de los juegos, a los derechos de los participantes o al interés público.	Conforme	Se ha evidenciado que se cuenta con un procedimiento de realización de copias de seguridad en el que se detallan los diferentes tipos de copias de seguridad, la periodicidad con la que se realizan y el tiempo que se conservan.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Existe un plan de medidas para cumplir con el plan de prevención de pérdida de información y que incluye la ubicación donde se conservan las copias de la información y las medidas de seguridad de protección de la copia frente a accesos no autorizados.	Conforme	Se ha evidenciado que se cuenta con un procedimiento de realización de copias de seguridad en el que se detallan los diferentes tipos de copias de seguridad y la periodicidad con la que se realizan. También se indica que tiempo que se conserva cada tipo de copia de seguridad. La ubicación donde se almacenan las copias de seguridad debe cumplir con la política de seguridad física.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Existe un procedimiento de actuación en caso de pérdida de información que incluye los mecanismos de atención de reclamaciones y mecanismos de continuación de juegos interrumpidos.	Conforme	Se ha evidenciado que Eyecon en su Plan de Continuidad de Negocio ha definido procedimientos de actuación en caso de pérdida de información, que incluye los mecanismos de atención de reclamaciones y continuación de juegos interrumpidos.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

6.13. Gestión de continuidad de negocio

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
Existe una gestión de continuidad del negocio ante	Conforme	Se ha evidenciado que Eyecon cuenta con un plan de continuidad de negocio	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

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.		<p>para casos en los que se dé un desastre físico, lógico o hardware que afecte a la infraestructura.</p> <p>En el plan de continuidad de negocio desarrollado se describe el protocolo a seguir ante la ocurrencia de un desastre o incidente y el impacto que pueden provocar estos.</p> <p>El plan de contingencia consistirá en resolver el incidente mediante un Backup o reestableciendo el servicio en el centro de procesamiento de datos secundario, dependiendo del alcance del incidente.</p>	
El plan de continuidad considera el 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.	No aplica	La implementación de las medidas necesarias para dar cumplimiento a este control es responsabilidad de la plataforma de juego.	
El plan de continuidad considera la retirada de fondos. El tiempo máximo para prestar de nuevo estos servicios será de una semana.	No aplica	La implementación de las medidas necesarias para dar cumplimiento a este control es responsabilidad de la plataforma de juego.	
El plan de continuidad considera 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.	Conforme	Se ha verificado que el plan de continuidad considera la continuación de juegos incompletos y el pago de premios. La continuación de los servicios sería instantánea, ya que la configuración del sistema está diseñada para no tener interrupción en las operaciones.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
El plan de continuidad considera el restablecimiento	Conforme	Se ha verificado que el plan de continuidad considera la restauración	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

completo de todos los servicios.		del sistema de juego completo.	
En todos los escenarios se incluye la información de los servicios recuperados y el tiempo máximo de recuperación.	Conforme	Se ha verificado que para los escenarios anteriores se incluyen los servicios recuperados y el tiempo máximo de recuperación para cada uno de ellos.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

6.14. Penetración y análisis de vulnerabilidades

Área y referencia del requisito	Calificación	Observaciones	Referencia documental
En el último año el sistema técnico de juego ha pasado un test de penetración y un análisis de vulnerabilidades.	Conforme	Se ha evidenciado que durante el último año se ha realizado un análisis de vulnerabilidades y test de penetración. Se ha comprobado que no existen vulnerabilidades críticas en el sistema evaluado y que se han realizado recomendaciones para las vulnerabilidades encontradas. Se adjunta el test de penetración y análisis de vulnerabilidades realizado sobre la aplicación de los juegos.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad
Existe un plan de análisis, al menos anual, de vulnerabilidades.	Conforme	Se ha evidenciado que durante el último año se ha realizado un análisis de vulnerabilidades y test de penetración. Se ha comprobado que no existen vulnerabilidades críticas en el sistema evaluado y que se han realizado recomendaciones para las vulnerabilidades encontradas. Se adjunta el test de penetración y análisis de vulnerabilidades realizado sobre la aplicación de los juegos. Adicionalmente, Eyecon realiza análisis continuos de vulnerabilidades contra todos los hosts del entorno de producción.	Ver Requisitos técnicos / Eyecon - Plan de trabajo Certificación de Seguridad

7. DETALLE DE LOS ANÁLISIS DE AUDITORÍA ESPECÍFICOS

7.1. Análisis de auditoría de los componentes críticos

La relación de los componentes software evaluados es la siguiente:

Nombre del componente	Versión	Descripción	SHA-1	Crítico
Game Server	1.7.7	Contiene la lógica del juego del lado del servidor y los componentes RNG. Facilita la comunicación con el navegador del jugador y los sistemas externos para las llamadas de apuestas.	f32877db2725016d7e8c191969cedf7af66a764f	Sí
Carbine	5.3.27	Componente del lado del servidor contenido en el servidor de juegos donde se ejecuta toda la lógica del juego.	9983390c4697be4317f8f8be1574c3e124aa0d4b9	Sí
RNG	1.0.1	Componente RNG	39c3c581d88f9674aa0765af51a56bd26955efd9	Sí
Feed Server	1.0.20	Proporciona fuentes de datos a los clientes del juego, incluidos los niveles de grupo de Jackpot.	bb4543587743a8a3594bc841fb57196d28cad599	Sí
Pool Server	1.0.33	Proporciona la gestión de los grupos de Jackpot.	d76aa2111918f2b76c2d6fc5c47dcf923b2958f1	Sí
Game Reporting Server	1.2.0	Proporciona informes visuales de los registros históricos del juego.	fe8f123af1f64189e05a63d0953582a63a24d134	No
Warehouse Reporting Server	1.0.14	Proporciona acceso a los registros de almacenamiento de datos subyacentes para fines de informes.	23ecce696123b5dcb25cd1ce3e06383f9be06552	No
Bonusing Server	1.8.0	Proporciona funcionalidad de bonificación de giro gratis, no es necesario para el juego regular.	484d2ece29d1775c3fccf16a8deae894093924c	No
Warehouse Replication Agent	1.0.18	Almacena una copia de seguridad local de todos los registros del juego, también proporciona un medio para que esos registros se copien en un almacén remoto con el fin de cumplir con los requisitos de informes de datos y retención.	71843d2184489a5aa7d5d504928f4051f5fd8b60	Sí
Warehouse Replication Server	1.0.16	Este componente utiliza el agente de replicación de almacén para copiar de forma	9e9b17d0c1de9f369296a4bf476a3db0dc5cc181	Sí

		remota los registros del juego en una instalación de almacenamiento de datos remoto.		
Warehouse Server	1.0.31	Este componente almacena una copia de seguridad local de los registros de auditoría de juegos replicados de forma remota. También transforma esos registros en tablas de informes resumidas.	084bada75e4e245d33131f98f4034b2fe9df1740	Sí

Se ha evidenciado que todos los componentes críticos citados anteriormente tienen reforzada la seguridad.

Se ha proporcionado la política de seguridad en la que se describen las principales medidas de seguridad implementadas para proteger el sistema técnico de juego. Se ha verificado que Eyecon cuenta con un análisis de riesgos que es revisado periódicamente.

Como se indica en la Política de desarrollo de software de Eyecon, todos los cambios de software deben ser revisados con especial atención. Todos los componentes críticos del backend están sujetos a análisis estático automatizado, incluso frente a vulnerabilidades comunes como OWASP Top 10. Se adjuntan evidencias de los controles técnicos sobre los riesgos de seguridad durante el desarrollo.

Adicionalmente, los componentes críticos se encuentran bajo la protección de antivirus y firewall de Palo Alto.

Además, se ha verificado que al menos con una periodicidad anual se realiza un análisis de vulnerabilidad y test de penetración el sistema técnico de juego.

Asimismo, se ha verificado que los Centros de Procesado de Datos dónde se encuentra el software de juego, cuentan con el certificado ISO27001.

Ver Documentación / Information Security Policy

Ver Requisitos técnicos / Análisis de riesgos / Review Risk Analysis

Ver Requisitos técnicos / Análisis de riesgos / Análisis automatizados

Ver Documentación / Managed Environment Software Change Procedure

Ver Requisitos técnicos / Gestión de comunicaciones y operaciones / Malware Protection

Ver Requisitos técnicos / Penetración y análisis de vulnerabilidades

Ver ISO 27001

7.2. Análisis de auditoría de la gestión de cambios

Eyecon ha desarrollado una política de gestión de cambios. Para poder realizar un cambio es necesario crear un ticket con la necesidad de realizar un cambio a través de la herramienta de ticketing JIRA. Una vez creado el ticket, este queda a la espera de ser evaluado por los responsables del área al que afecte el cambio. Tanto si el cambio es aprobado o no, quedará registrado mediante el ticket.

Si el cambio es aprobado este debe de seguir un flujo de trabajo que conlleva una serie de evaluaciones y pruebas antes de ser implantado en el entorno de producción.

Los pasos por los que pasa un cambio son:

- Creación de ticket (solicitud del cambio)
- Evaluación de solicitud
- Desarrollo
- Pruebas
- Implementación del cambio

Se ha comprobado que se guarda un registro de los cambios y el detalle de estos.

Ver Documentación / Change Management Policy

Ver Documentación / Managed Environment Software Change Procedure

Ver Requisitos técnicos / Gestión de cambios / 2019-06 Change Management Records

Ver Requisitos técnicos / Gestión de cambios / [#RP-104] 2019-03 #5 SGH Localised GS_IS_BPS_WGRS_CV Release

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

A continuación, se analiza el tiempo máximo de recuperación ante un desastre, así como el tiempo máximo de pérdida de información ante un desastre.

Análisis del tiempo máximo de recuperación ante un desastre	
RTO (Recovery Time Objective):	4 horas
Medidas suficientes:	Sí
Descripción de las medidas técnicas:	<p>La prioridad cuando surge una contingencia es estabilizar y dar continuidad a las actividades y dependencias del sistema. Para ello Eyecon ha desarrollado un Plan de Continuidad de Negocio donde el tiempo máximo definido para la continuación de los servicios es de 4 horas.</p> <p>En el plan de continuidad de negocio desarrollado se contemplan diferentes escenarios y como actuar si se da alguno de estos. Los registros de juego se replican en tiempo real al sistema de almacenamiento de datos global, alojado en un centro diferente al de procedencia de los datos. Adicionalmente, los registros también se almacenan y se copian localmente dentro del centro de origen de los datos.</p> <p>Para conseguir este tiempo, el equipo de Eyecon puede realizar dos acciones dependiendo de la causa y magnitud de la incidencia:</p> <ul style="list-style-type: none"> • Restaurar el sistema a través de una copia de seguridad. • Restaurar el sistema en una réplica.

Análisis del tiempo máximo de pérdida de información ante un desastre	
RPO (Recovery Point Objective):	5 minutos
Medidas suficientes:	Sí
Descripción de las medidas técnicas:	<p>Se ha definido un plan de procedimientos de copias de seguridad y recuperación de componentes con el objetivo de evitar la pérdida de información y minimizar los riesgos asociados. Adicionalmente, los servidores de bases de datos están diseñados con un clúster activo-pasivo y un servidor de replicación independiente, con todos los almacenes de datos replicados en dos SAN independientes y las transacciones son replicadas en tiempo real.</p> <p>Se tienen configurados varios tipos de copias de seguridad, dependiendo de los datos que almacene cada una. Los tipos de copias de seguridad, periodicidad y tiempo de retención se pueden consultar en la política que contiene el programa de retención de información. Ver Documentación / Information Retention Policy Schedule.</p> <p>Las copias pueden ser:</p> <ul style="list-style-type: none"> • Diarias <ul style="list-style-type: none"> ○ Completa ○ Diferencial • Semanal <ul style="list-style-type: none"> ○ Completa <p>Se realiza una copia de seguridad de las bases de datos al menos diariamente, con registros de transacciones cada 5 minutos, para permitir un punto de recuperación.</p>

8. DESCRIPCIÓN DEL LUGAR, EQUIPO Y FECHAS DE REALIZACIÓN DE LA CERTIFICACIÓN

Los trabajos de certificación han sido realizados por el equipo que se detalla a continuación:

- Pablo Sierra Carriba (Manager)
- Alfredo Díaz Contreras (Jefe de proyecto)
- Borja Martín Sanz (Consultor)

Los trabajos se han realizado desde la sede de EY en Madrid, situada en Calle de Raimundo Fernández Villaverde, 65 - 28003 Madrid.

Los trabajos se han realizado entre el 23 de julio de 2019 y el 10 de diciembre de 2019, ambos inclusive.

9. DESCRIPCIÓN DEL SOPORTE DIGITAL QUE ACOMPAÑARÁ AL INFORME DE CERTIFICACIÓN

El presente informe de certificación se encuentra estructurado de la siguiente manera:

- Informe de certificación completo en formato digital.
- Documentación: Directorio que contiene la documentación proporcionada para evidenciar el cumplimiento de los requisitos evaluados.
- Requisitos técnicos: Directorio que contiene todas las evidencias técnicas proporcionadas para evidenciar el cumplimiento de los requisitos evaluados.
- ISO 27001: Directorio que contiene los documentos proporcionados para la convalidación de ciertos requisitos con la ISO 27001.