GLI®

MARCO DE SEGURIDAD DEL JUEGO

GLI-GSF-1

AUDITORÍA DE CONTROLES COMUNES DE SEGURIDAD DE LA INFORMACIÓN DEL JUEGO (GIS)

Versión 1.0 BORRADOR – Publicado el 30 de julio de 2024

Contenido

1. INTRODUCCIÓN

1.1. Declaración General

La integridad y precisión del funcionamiento de un entorno de producción del juego (GPE por sus siglas en inglés) depende en gran medida de los procedimientos operativos, configuraciones e infraestructura de la red. Con las amenazas cada vez más emergentes para las operaciones de juego, los organismos reguladores dependen en gran medida de la experiencia de una empresa de seguridad independiente (ISF) calificada para realizar evaluaciones de seguridad de juego como una adición esencial a las pruebas y certificación de los Componentes Críticos del Sistema de un GPE por parte de un laboratorio de pruebas independiente (ITL). Este módulo del Marco de Seguridad del Juego de GLI (GLI-GSF-1) establece los controles comunes de seguridad de la información del juego (GIS por sus siglas en inglés) necesarios para auditar el Sistema de Gestión de Seguridad de la Información del Juego (GISMS) de una Empresa de Juego para garantizar una gestión eficaz de la seguridad en el GPE de una Empresa de Juego. Estos controles comunes de GIS se aplican a las GPE utilizadas para todas las formas de juego, como los juegos de casino, lotería, apuestas de eventos y juegos interactivos. Dependiendo del tipo de Empresa de Juego, también se pueden aplicar módulos adicionales del GLI-GSF.

NOTA: El marco de seguridad de juegos de GLI (GLI-GSF) completo está disponible de forma gratuita en www.gaminglabs.com.

1.2. Entorno de Producción del Juego (GPE)

Un GPE se refiere al entorno operativo donde se realizan, administran y entregan las actividades de juego y los servicios relacionados a los clientes en vivo o en tiempo real. Abarca la infraestructura física y virtual, los sistemas, el software y los procesos necesarios para facilitar diversas formas de juego, así como juegos de casino, lotería, apuestas de eventos y juegos interactivos. El GPE también abarca los sistemas de la oficina auxiliar (backend), aplicaciones de la empresa, y la infraestructura que interactúan y/o respaldan las actividades de juego. Las características clave de un GPE incluyen:

a. Componentes críticos del sistema: Esto incluye las plataformas de hardware y software que respaldan la ejecución de actividades de juego, como dispositivos de juego, mesas de juego, sistemas de juego, sistemas de lotería, sistemas de apuestas de eventos, y sistemas o aplicaciones de juego interactivos.
b. Módulos criptográficos: Los módulos criptográficos utilizados en el GPE son responsables de las funciones criptográficas, incluido el cifrado y descifrado de datos sensibles, utilizando algoritmos que cumplen las normas vigentes aceptadas por la industria, como ISO/IEC 19790, FIPS 140-2, o equivalentes.
c. Procesamiento de transacciones: El GPE procesa las transacciones monetarias relacionadas con las actividades de juego, incluidas las apuestas, pagos, depósitos, retiros y transacciones financieras con los clientes.
d. Medidas de seguridad: Se implementan medidas de seguridad sólidas para salvaguardar la seguridad, integridad, confidencialidad y disponibilidad de los componentes críticos del sistema, datos confidenciales, transacciones financieras e información de los usuarios contra el acceso no autorizado, fraude, manipulación y amenazas cibernéticas.
e. Gestión de riesgos: El GPE emplea prácticas de gestión de riesgos para identificar, evaluar, mitigar y monitorear los riesgos asociados con las operaciones de juego, incluidos los riesgos operativos, riesgos financieros, riesgos regulatorios y riesgos tecnológicos.
f. Operación continua: Un GPE generalmente opera las 24 horas del día, los 7 días de la semana para satisfacer la demanda de los clientes y maximizar la generación de ingresos. Esto requiere una alta disponibilidad, confiabilidad y resiliencia de la infraestructura y los sistemas para minimizar el tiempo de inactividad y las interrupciones.
g. Monitoreo y control: Existen mecanismos de monitoreo, vigilancia y control en tiempo real para supervisar las actividades de juego, detectar anomalías, garantizar el cumplimiento de las reglas y regulaciones y responder rápidamente a incidentes GIS, fraude u otros problemas.
h. Cumplimiento normativo: El cumplimiento de las regulaciones de juego, los requisitos de licencia y los estándares de la industria es esencial en un GPE para garantizar el juego limpio, la protección de los

clientes, las prácticas de juego responsable y el cumplimiento de las obligaciones legales y reglamentarias.

1.3. Sistema de Gestión de Seguridad de la Información del Juego (GISMS)

Un GISMS es un marco estructurado y un conjunto de procesos diseñados para salvaguardar los datos confidenciales, activos y componentes críticos del sistema de una Empresa de Juego dentro de su GPE contra el acceso, divulgación, alteración o destrucción no autorizados. Abarca políticas, procedimientos, controles y prácticas de gestión de riesgos específicamente adaptadas a los desafíos únicos y requisitos regulatorios de la industria del juego, lo que implica la identificación de riesgos de GIS, la implementación de controles y salvaguardas adecuados, el monitoreo y la evaluación continuos de las medidas de seguridad y la mejora continua para adaptarse a las amenazas cambiantes y los requisitos de cumplimiento.

1.4. Propósito del Marco

Garantizar la seguridad e integridad de las actividades de juego es primordial para mantener la confianza del público en el sector. Por lo tanto, los casinos, loterías, operaciones de apuestas de eventos, operaciones de juegos interactivos y otras empresas de juego deben establecer y mantener un marco claramente definido y documentado para lograr y preservar la confianza pública en sus operaciones. El objetivo es alinear los GIS de tal manera que las operaciones de juego puedan funcionar como otras operaciones de comercio electrónico para garantizar un entorno seguro y estable con las características seguras de las operaciones en industrias paralelas.

2. AUDITORÍAS DE GIS

2.1. Visión General de la Auditoría

La auditoría de GIS se realiza con la intención de identificar cualquier caso real o potencial de incumplimiento, vulnerabilidad o debilidad, y garantizar que se preserve la integridad, confidencialidad, y disponibilidad de la información bajo el control de la Empresa de Juego. Este enfoque se basa en gran medida en la seguridad por capas para reducir el riesgo para los sistemas informáticos y de red. El enfoque por capas proporciona redundancia y refuerza el modelo de seguridad general, ya que se deben vulnerar varias capas de seguridad antes de acceder a un almacén de datos crítico.

NOTA: El enfoque de la guía de GIS detallada en el GLI-GSF-1 se centra en los controles comunes de seguridad de la información del juego, otros métodos de evaluación se discuten en los módulos de soporte del GLI-GSF.

2.2. Métodos de Auditoría

Una auditoría de GIS utiliza una serie de métodos de evaluación, incluidos los siguientes métodos, cuyos resultados se utilizan para respaldar la determinación de la eficacia del control de GIS a lo largo del tiempo:

a. Entrevista: Un tipo de método de evaluación que se caracteriza por el proceso de llevar a cabo discusiones con individuos o grupos dentro de una Empresa de Juego para facilitar la comprensión, lograr aclaraciones o conducir a la localización de pruebas.
b. Examinar: Tipo de método de evaluación que se caracteriza por el proceso de verificar, inspeccionar, revisar, observar, estudiar o analizar uno o más objetos de evaluación para facilitar la comprensión, lograr aclaraciones u obtener evidencia.
c. Prueba: Tipo de método de evaluación que se caracteriza por el proceso de ejercitar uno o más objetos de auditoría en condiciones especificadas para comparar el comportamiento real con el esperado.

2.3. Tareas de Auditoría

A continuación se presentan las actividades de auditoría de alto nivel sugeridas. En el Apéndice se detallan los requisitos mínimos de control común de GIS con más detalle. Se dirige a los usuarios de este documento al Apéndice para asegurarse de que no se pase por alto ningún control GIS necesario. Los controles GIS

enumerados en el Apéndice no son exhaustivos y pueden incluirse controles GIS adicionales en función de los requisitos reglamentarios y el alcance de la evaluación.

2.3.1. Revisión de la Documentación Presentada

En primer lugar, la ISF evalúa los controles de GIS existentes de la Empresa de Juego mediante la recopilación y revisión de la documentación pertinente para comprender y evaluar mejor los aspectos pertinentes del GPE en relación con el GIS general, y para determinar si la documentación complementa adecuadamente los controles técnicos. Un ejemplo de parte de la documentación que se espera que se revise incluye, pero no se limita a:

a. Política de GIS
b. Acceso de usuarios
c. Procedimientos de desarrollo y pruebas
d. Acuerdo de Nivel de Servicio
e. Política de uso de los servicios de red
f. Controles de detección, prevención y recuperación para protegerse contra código malintencionado
g. Política de copia de seguridad de datos
h. Procedimientos establecidos para que los medios se eliminen de forma segura
i. Procedimientos para el manejo y almacenamiento de información (para proteger la información de la divulgación no autorizada o el uso indebido)
j. Programa de Gestión del Cambio
k. Procedimientos para monitorear el uso de los medios de procesamiento de información
l. Políticas, planes operativos y procedimientos para las actividades de teletrabajo
m. Política sobre el uso de controles criptográficos
n. Diagrama de red

2.3.2. Entrevistas con Personal Clave

Después de recopilar y revisar la documentación relevante, la ISF entrevista al personal clave (usuarios, administradores y gerencia) para identificar prácticas no documentadas y obtener retroalimentación. Como parte del proceso de entrevistas, la ISF discute las prácticas reales en uso y a lo largo de las otras fases de la evaluación, la ISF identifica los procedimientos en uso basados en los resultados técnicos de la evaluación. Esta información permite a la ISF identificar brechas de procedimiento y buenas prácticas que no están completamente documentadas en las políticas y procedimientos formales. Además, el ISF midel nivel de conocimiento de los usuarios durante las entrevistas para determinar si los usuarios ajenos a la función de TI tienen un nivel adecuado de comprensión de GIS y su papel en la protección de la información y otros activos críticos. Se entrevistará como mínimo a las siguientes personas clave responsables de establecer la política de GIS y de aplicarla.

a. Persona con la responsabilidad general de la operación de juego
b. Oficial de cumplimiento
c. Responsable de seguridad de la información
d. Personal operativo
e. Desarrolladores de software

2.3.3. Evaluación de Controles Administrativos

La ISF realiza pruebas y evaluaciones para evaluar la eficacia y la idoneidad de estas medidas administrativas para mitigar los riesgos y garantizar el cumplimiento de los requisitos de seguridad. Por lo general, esta evaluación aborda los siguientes temas:

a. Políticas, normas y directrices
b. Seguridad Organizacional
c. Gestión de Operaciones
d. Actualización de parches y administración
e. Monitoreo del acceso y uso del sistema
f. Procedimientos de gestión de cambios

g. Clasificación y Control de Activos
h. Planes de contingencia
i. Respuesta a incidentes de GIS

2.3.4. Evaluación de Controles Técnicos

La ISF realiza pruebas y evaluaciones para evaluar la eficacia y la idoneidad de estas salvaguardas técnicas para mitigar los riesgos y proteger los datos confidenciales. Por lo general, esta evaluación aborda los siguientes temas:

a. Diseño de Infraestructura
b. Topografía de Redes / Pruebas de Penetración
c. Seguridad de redes y comunicaciones
d. Controles de acceso lógico
e. Seguridad de los sistemas operativos (SO)
f. Controles de software malintencionado
g. Diseño y configuración de bases de datos
h. Controles criptográficos
i. Monitoreo del sistema
j. Informes y registro
k. Controles de desarrollo del sistema

2.3.5. Evaluación de Controles Físicos y Ambientales

La ISF realiza pruebas y evaluaciones para evaluar la eficacia y la idoneidad de estos controles en la protección contra amenazas físicas, peligros ambientales y acceso no autorizado a áreas sensibles. Por lo general, esta evaluación aborda los siguientes temas:

a. Ubicación y seguridad de las instalaciones
b. Seguridad perimetral
c. Controles de acceso
d. Seguridad de los equipos
e. Detección de intrusos
f. Sistemas de alarma
g. Sistemas de vigilancia
h. Calefacción, ventilación y aire acondicionado
i. Sistemas de energía
j. Cableado de alimentación y comunicaciones
k. Detección y extinción de incendios
l. Respuesta a emergencias

2.3.6. Evaluación de Riesgos

La ISF realiza una evaluación de riesgos para identificar problemas de no conformidad con cualquier control aplicable, y cualquier amenaza y vulnerabilidad potencial que no se enumere explícitamente en el GLI-GSF, pero que se observó durante la auditoría y puede constituir un riesgo.

2.4. Frecuencia de Auditoría

2.4.1. Auditoría Inicial

La Empresa de Juego debe tener una auditoría de GIS realizada por una ISF dentro de los noventa días posteriores al inicio de las operaciones de juego de la Empresa de Juego dentro de esa jurisdicción, a menos que el organismo regulador haya aconsejado lo contrario. Cualquier aplazamiento de esta auditoría según lo solicitado por la Empresa de Juego, junto con un cronograma de auditoría actualizado, será autorizado por el organismo regulador.

NOTA: Se recomienda que los organismos reguladores permitan flexibilidad para los cronogramas de auditoría de las empresas de juego multijurisdiccionales para permitir la consolidación de las auditorías de múltiples jurisdicciones en un cronograma común.

2.4.2. Auditoría Anual

La Empresa de Juego debe, por regla general, tener otra auditoría de GIS realizada por una ISF dentro de los doce meses posteriores a la auditoría de GIS anterior, a menos que el organismo regulador haya aconsejado lo contrario. Cualquier aplazamiento de esta auditoría según lo solicitado por la Empresa de Juego, junto con un cronograma de auditoría actualizado, será autorizado por el organismo regulador.

NOTA: Se recomienda que los organismos reguladores permitan flexibilidad para los cronogramas de auditoría de las empresas de juego multijurisdiccionales para permitir la consolidación de las auditorías de múltiples jurisdicciones en un cronograma común.

2.4.3. Auditorías Adicionales

Es posible que se necesiten auditorías de GIS adicionales con mayor frecuencia en función de la crtiticidad de los cambios dentro del GPE, como las adiciones y/o cambios que pueden afectar o proporcionar acceso a datos confidenciales y/o componentes críticos del sistema. Dichas auditorías de SIG, según lo requiera el organismo regulador y/o la Empresa de Juego, pueden centrarse en funciones específicas de, adiciones a, y/o cambios en el GPE.

2.5. Informes de Auditoría de GIS

Los resultados de una auditoría de GIS determinarán para la administración las areas de las operaciones en las que se debe considerar la posibilidad de mejorar y recomendarán estrategias para mejorar esas areas. El informe de auditoría de GIS debe presentarse al organismo regulador a más tardar sesenta días después de que se haya completado la auditoría de GIS. El informe de auditoría de GIS debe incluir todo lo siguiente:

a. El nombre y una breve historia de la Empresa de Juego, mencionando su modelo de negocio y las actividades de juego ofrecidas o Proveedores de Servicios utilizados, así como la ubicación, número de empleados, sitio web, certificaciones reales, descripción de alto nivel de la infraestructura, incluido el centro de datos, etc.
b. El nombre de la ISF, afiliación de la empresa, información de contacto y calificaciones y experiencia de las personas que llevaron a cabo la auditoría;
c. La(s) fecha(s) de la auditoría, incluida la fecha de solicitud, fecha de inicio, fecha de finalización, fecha del informe y fecha de vencimiento;
d. El alcance de la auditoría, que incluye:
    i. Una visión general de alto nivel del trabajo realizado y del entorno de control en funcionamiento;
    ii. Los controles con los que se llevó a cabo la auditoría;
    iii. Los componentes críticos del sistema que se revisaron
    iv. Cómo se identificaron los componentes críticos del sistema y si la auditoría incluyó aplicaciones, redes, bases de datos y/o sistemas operativos;
    v. Una indicación de las condiciones de la auditoría, incluidos los controles excluidos de la auditoría y las razones de su exclusión;
e. El enfoque de auditoría, que incluye preguntas basadas en la indagación, observación, pruebas, personas clave entrevistadas;
f. Evidencia obtenida durante la auditoría para corroborar los resultados de la auditoría, incluyendo:
    i. Los documentos que fueron revisados, incluyendo versión y fechas, personal entrevistado;
    ii. Los nombres, fechas y versiones de la documentación revisada;
    iii. Los nombres, funciones y ubicaciones del personal entrevistado;
    iv. Los lugares visitados;
    v. Los detalles de los recorridos realizados;
    vi. Las muestras revisadas para verificar el cumplimiento;
g. Los resultados de la auditoría, indicando para cada control su estado como conforme, observación, no conformidad menor o no conformidad mayor;

h. Hallazgos, que incluyen:
   i. Una explicación de las no conformidades identificadas;
   ii. Evidencia que respalde y describa las no conformidades;
   iii. Impacto o impacto potencial de las no conformidades;
   iv. Medidas correctivas recomendadas para abordar las no conformidades existentes y realizar mejoras;
i. La respuesta de la Empresa de Juego a los hallazgos y las medidas correctivas recomendadas, incluidas las fechas de resolución y las personas responsables; y
j. Otros factores relevantes, como si los GISMS cumplen o han sido auditados con otros requisitos (p. ej. ISO/IEC 27001, WLA-SCS, NIST-CSF, etc.)

2.6. Acciones Correctivas

Si el informe de auditoría de GIS de la ISF recomienda una acción correctiva, la Empresa de Juego debe proporcionar a la ISF y al organismo regulador un plan de remediación y cualquier plan de mitigación de riesgos que detalle las acciones y el cronograma de la Empresa de Juego para implementar la acción correctiva.

a. Las no conformidades se abordarán a través del proceso de acción correctiva de la Empresa de juego, que incluye:
   i. Medidas adoptadas para determinar el alcance de la no conformidad específica y contenerla.
   ii. Investigación de la causa raíz para determinar las causas más básicas de la no conformidad.
   iii. Acciones tomadas para corregir la no conformidad y, en respuesta a la causa raíz, eliminar la recurrencia de la no conformidad.
b. Las acciones correctivas para abordar las no conformidades importantes identificadas se llevarán a cabo de inmediato y se notificará a la ISF y al organismo regulador de las acciones tomadas dentro de los treinta días, a menos que el organismo regulador especifique lo contrario. La ISF realizará una auditoría de seguimiento en un plazo de noventa días para confirmar las acciones tomadas, evaluar su eficacia y determinar si las no conformidades han sido resueltas.
c. Las acciones correctivas para abordar las no conformidades menores identificadas deberán ser documentadas y enviadas por la Empresa de Juego a la ISF y al organismo regulador para su revisión en un plazo de treinta días, a menos que el organismo regulador especifique lo contrario. Si las acciones se consideran satisfactorias, se les dará seguimiento en la próxima auditoría programada.
d. Una vez que se hayan tomado las medidas correctivas, la Empresa de Juego proporcionará a la ISF y al organismo regulador la documentación que evidencie la finalización.
e. La Empresa de Juego debe mantener registros de acciones correctivas, incluyendo evidencia objetiva, durante al menos cinco años, a menos que el organismo regulador especifique lo contrario.

2.7. Empresa de Seguridad Independiente (ISF)

La auditoría de GIS será realizada por personas con calificaciones suficientes, lo que significa que la ISF contratará a personas suficientemente calificadas, competentes y experimentadas. Estas personas deberán:

a. Tener una formación académica pertinente o proporcionar de otra manera las cualificaciones pertinentes para evaluar a las GPE;
b. Obtener y mantener certificaciones suficientes para demostrar competencia y experiencia como profesional de seguridad calificado por juntas de certificación reconocidas, ya sea a nivel nacional o internacional. Las siguientes certificaciones pueden demostrar la idoneidad para completar la auditoría de GIS:
   i. Auditor Líder ISO/IEC 27001;
   ii. Auditor Certificado de Sistemas de Información (CISA);
   iii. Gerente Certificado de Seguridad de la Información (CISM);
   iv. Profesional Certificado en Seguridad de Sistemas de Información (CISSP);
c. Tener al menos cinco años de experiencia en la realización de auditorías de GIS en la industria del juego; y
d. Cumplir con cualquier otro requisito prescrito por el organismo regulador.

NOTA: Nada de lo aquí expuesto pretende prohibir que el personal del organismo regulador actúe como ISF, siempre que cumpla los requisitos de esta sección y sea independiente de la Empresa de Juego auditada.

APÉNDICE: CONTROLES DE SEGURIDAD DE LA INFORMACIÓN DE JUEGO (GIS)

Los Controles de Seguridad de la Información de Juego (GIS por sus siglas en inglés), como se especifica en este Apéndice, indicarán a qué Grupo de Implementación de Juego (GIG) se aplica el control. Para ayudar a las Empresas de Juego de cualquier tamaño, los GIGs están divididos en tres grupos, basados en el perfil de riesgo y los recursos que una Empresa de Juego tiene a su disposición para implementar el GLI-GSF. Cada GIG identifica un conjunto de los Controles SIG que necesita implantar. El GIG2 se basa en el GIG1, y el GIG3 comprende todos los Controles de GIS.

GIG	Descripción del Grupo de Implementación del Juego (GIG)
GIG1	La GLI-GSF define el Grupo de Implementación 1 (GIG1) como higiene esencial de seguridad en el juego y representa un estándar mínimo emergente de GIS para todas las Empresas de Juego. Los controles SIG incluidos en GIG1 son los que toda empresa de juego debe aplicar para defenderse de los ataques más comunes. Una empresa de juego GIG1 tiene normalmente una experiencia en seguridad limitada para dedicarla a la protección de los activos críticos y del personal. Una preocupación común de las empresas de juego es mantener sus operaciones de juego en funcionamiento, ya que tienen una tolerancia limitada al tiempo de inactividad. La criticidad de los datos sensibles que intentan proteger es baja y se refiere principalmente a la información financiera y de los empleados. Los controles de GIS seleccionados para GIG1 deben poder implementarse con una experiencia limitada en seguridad del juegos y estar destinados a frustrar ataques generales, no dirigidos. Estos controles de GIS también se diseñarán normalmente para trabajar en conjunción con hardware y software comerciales listos para usar (COTS) para oficinas pequeñas o domésticas.
GIG2	Los controles de GIS seleccionados para GIG2 pueden ayudar a los equipos de seguridad a hacer frente a una mayor complejidad operativa. Algunos controles de GIS dependerán de la tecnología de nivel empresarial de juego y de conocimientos especializados para su correcta instalación y configuración. Una empresa de juego de GIG2 emplea a personas responsables de gestionar y proteger la infraestructura de GPE. Estas Empresas de Juego típicamente apoyan a múltiples departamentos con diferentes perfiles de riesgo basados en la función del trabajo y la misión. Las pequeñas unidades de Empresas de Juego pueden tener cargas de cumplimiento normativo. Las empresas de juego GIG2 a menudo almacenan y procesan datos sensibles y pueden soportar breves interrupciones del servicio. Una de las principales preocupaciones es la pérdida de confianza del público si se produce una brecha. Todas las empresas de juego que lleven a cabo operaciones de juego presenciales en las que el GPE se comunique continuamente a través de Internet/redes públicas (por ejemplo, loterías, casinos con sistemas externos, apuestas deportivas minoristas, etc.) deben tratarse como empresas de juego GIG2, a menos que el organismo regulador especifique lo contrario.
GIG3	Una empresa de juego GIG3 suele emplear a expertos en seguridad del juego especializados en las distintas facetas de la seguridad del juego (por ejemplo, gestión de riesgos, pruebas de penetración, seguridad de las aplicaciones). Los activos críticos de una Empresa de Juego GIG3 contienen datos sensibles o funciones que están sujetas a la supervisión reglamentaria y de cumplimiento. Una empresa de juego GIG3 deberá abordar la disponibilidad de los servicios y la integridad y confidencialidad de los datos sensibles.. Los ataques exitosos pueden causar daños significativos al bienestar público. Los controles de GIS seleccionados para GIG3 deberán reducir los ataques selectivos de un adversario sofisticado y reducir el impacto de los ataques de día cero. Todas las empresas de juego que lleven a cabo operaciones de juego en línea (por ejemplo, juegos interactivos, apuestas en eventos en línea, etc.) deben tratarse como empresas de juego GIG3, a menos que el organismo regulador especifique lo contrario.

A. Adopción de Controles de Seguridad Críticos de CIS

Para establecer una línea de base clara y razonable para los controles de GIS, el GLI-GSF incorpora por referencia los siguientes controles de los Controles de Seguridad Críticos del Centro para la Seguridad de Internet (CIS), Versión 8, que deben ser cumplidos por cada Organización de Juego (Empresa). La columna de la derecha indica el Grupo de Implementación del Juego (GIG) al que se aplica el Control de GIS.

NOTA: El documento completo de controles críticos de seguridad del CIS está disponible de forma gratuita en www.cisecurity.org.

CIS-1	Inventario y Control de Activos Empresariales	GIG
CIS-1.1	Establecer y Mantener un Inventario Detallado de Activos Empresariales	GIG1
CIS-1.2	Abordar los Activos no Autorizados	GIG1
CIS-2	Inventario y Control de Activos de Software	GIG
CIS-2.1	Establecer y Mantener un Inventario de Software	GIG1
CIS-2.2	Asegúrese de que el Software Autorizado sea Compatible Actualmente	GIG1
CIS-2.3	Abordar el Software no Autorizado	GIG1
CIS-3	Protección de Datos	GIG
CIS-3.1	Establecer y Mantener un Proceso de Gestión de Datos	GIG1
CIS-3.2	Establecer y Mantener un Inventario de Datos	GIG1
CIS-3.4	Aplicar la Retención de Datos	GIG1
CIS-3.5	Eliminar los Datos de Forma Segura	GIG1
CIS-3.6	Cifrar los Datos en los Terminales de los Usuarios	GIG1
CIS-3.7	Establecer y Mantener un Esquema de Clasificación de Datos	GIG2
CIS-3.9	Cifrar Datos en Medios Extraíbles	GIG2
CIS-3.10	Cifrar Datos Confidenciales en Tránsito	GIG2
CIS-3.11	Cifrar Datos Confidenciales en Reposo	GIG2
CIS-3.14	Registrar el Acceso a Datos Confidenciales	GIG3
CIS-4	Configuración Segura de Activos y Software de la Empresa	GIG
CIS-4.1	Establecer y Mantener un Proceso de Configuración Seguro	GIG1
CIS-4.2	Establecer y Mantener un Proceso de Configuración Seguro para la Infraestructura de Red	GIG1
CIS-4.3	Configurar el Bloqueo Automático de Sesiones en Activos Empresariales	GIG1
CIS-4.4	Implementar y Administrar un Firewall en los Servidores	GIG1
CIS-4.6	Gestionar de Forma Segura los Activos y el Software de la Empresa	GIG1
CIS-4.7	Administrar Cuentas Predeterminadas en Activos y Software de la Empresa	GIG1
CIS-4.8	Desinstalar o Deshabilitar Servicios Innecesarios en los Activos y el Software de la Empresa	GIG2
CIS-4.9	Configuración de Servidores DNS de Confianza en Activos Empresariales	GIG2
CIS-4.10	Aplicar el Bloqueo Automático de Dispositivos en Dispositivos Portátiles de Terminal de Usuario	GIG2
CIS-5	Gestión de Cuentas	GIG
CIS-5.1	Establecer y Mantener un Inventario de Cuentas	GIG1
CIS-5.2	Usar Contraseñas Únicas	GIG1
CIS-5.3	Desactivar Cuentas Inactivas	GIG1

CIS-5.4	Restringir los Privilegios de Administrador a Cuentas de Administrador Dedicadas	GIG1
CIS-5.5	Establecer y Mantener un Inventario de Cuentas de Servicio	GIG2
CIS-5.6	Centralizar la Gestión de Cuentas	GIG2
CIS-6	Gestión del Control de Acceso	GIG
CIS-6.1	Establecer un Proceso de Concesión de Acceso	GIG1
CIS-6.2	Establecer un Proceso de Revocación de Acceso	GIG1
CIS-6.3	Requerir MFA para Aplicaciones Expuestas Externamente	GIG1
CIS-6.4	Requerir MFA para el Acceso Remoto a la Red	GIG1
CIS-6.5	Requerir MFA para el Acceso Administrativo	GIG1
CIS-6.7	Centralizar el Control de Acceso	GIG2
CIS-6.8	Definir y Mantener el Control de Acceso Basado en Roles	GIG3
CIS-7	Gestión Continua de Vulnerabilidades	GIG
CIS-7.1	Establecer y Mantener un Proceso de Gestión de Vulnerabilidades	GIG1
CIS-7.2	Establecer y Mantener un Proceso de Corrección	GIG1
CIS-7.3	Realizar una Gestión Automatizada de Parches del Sistema Operativo	GIG1
CIS-7.4	Realizar una Gestión Automatizada de Parches de Aplicaciones	GIG1
CIS-7.5	Realizar Análisis Automatizados de Vulnerabilidades de los Activos Internos de la Empresa	GIG2
CIS-7.6	Realizar Análisis Automatizados de Vulnerabilidades de Activos Empresariales Expuestos Externamente	GIG2
CIS-7.7	Corrección de Vulnerabilidades Detectadas	GIG2
CIS-8	Gestión de Registros de Auditoría	GIG
CIS-8.1	Establecer y Mantener un Proceso de Gestión de Registros de Auditoría	GIG1
CIS-8.2	Recopilación de Registros de Auditoría	GIG1
CIS-8.3	Garantizar un Almacenamiento Adecuado de los Registros de Auditoría	GIG1
CIS-8.4	Estandarizar la Sincronización Horaria	GIG2
CIS-8.5	Recopilar Registros de Auditoría Detallados	GIG2
CIS-8.9	Centralizar los Registros de Auditoría	GIG2
CIS-8.10	Conservar Registros de Auditoría	GIG2
CIS-8.11	Realizar Revisiones de Registros de Auditoría	GIG2
CIS-8.12	Recopilación de Registros de Proveedores de Servicios	GIG3
CIS-9	Protecciones de Correo Electrónico y Navegador Web	GIG
CIS-9.1	Asegúrese de Usar Solo Navegadores y Clientes de Correo Electrónico Totalmente Compatibles	GIG1
CIS-9.2	Usar Servicios de Filtrado de DNS	GIG1
CIS-9.7	Implementar y Mantener Protecciones Antimalware para Servidores de Correo Electrónico	GIG3
CIS-10	Defensas Contra Malware	GIG
CIS-10.1	Implementación y Mantenimiento de Software Antimalware	GIG1
CIS-10.2	Configurar Actualizaciones Automáticas de Firmas Antimalware	GIG1
CIS-10.6	Administrar de Forma Centralizada el Software Antimalware	GIG2
CIS-10.7	Usar Software Antimalware Basado en el Comportamiento	GIG2
CIS-11	Recuperación de Datos	GIG
CIS-11.1	Establecer y Mantener un Proceso de Recuperación de Datos	GIG1
CIS-11.2	Realizar Copias de Seguridad Automatizadas	GIG1

CIS-11.3	Proteger los Datos de Recuperación	GIG1
CIS-11.4	Establecer y Mantener una Instancia Aislada de Datos de Recuperación	GIG1
CIS-11.5	Recuperación de Datos de Prueba	GIG2
CIS-12	**Gestión de la Infraestructura de Red**	**GIG**
CIS-12.1	Asegúrese de que la Infraestructura de Red esté Actualizada	GIG1
CIS-12.2	Establecer y Mantener una Arquitectura de Red Segura	GIG2
CIS-12.3	Gestionar de Forma Segura la Infraestructura de Red	GIG2
CIS-12.4	Establecer y Mantener Diagrama(s) de Arquitectura	GIG2
CIS-12.6	Uso de Protocolos Seguros de Gestión de Red y Comunicación	GIG2
CIS-13	**Monitoreo y Defensa de Redes**	**GIG**
CIS-13.1	Centralizar las Alertas de Eventos de Seguridad	GIG2
CIS-13.2	Implementar una Solución de Detección de Intrusiones Basada en Host	GIG2
CIS-13.3	Implementar una Solución de Detección de Intrusiones en la Red	GIG2
CIS-13.4	Realizar Filtrado de Tráfico Entre Segmentos de Red	GIG2
CIS-13.7	Implementar una Solución de Prevención de Intrusiones Basada en Host	GIG3
CIS-13.8	Implementar una Solución de Prevención de Intrusiones en la Red	GIG3
CIS-13.9	Implementar el Control de Acceso a Nivel de Puerto	GIG3
CIS-13.10	Realizar Filtrado de la Capa de Aplicación	GIG3
CIS-14	**Capacitación en Habilidades y Concienciación en Seguridad**	**GIG**
CIS-14.1	Establecer y Mantener un Programa de Concienciación Sobre Seguridad	GIG1
CIS-14.2	Capacitar a los Miembros de la Fuerza Laboral para que Reconozcan los Ataques de Ingeniería Social	GIG1
CIS-14.3	Capacitar a los Miembros de la Fuerza Laboral Sobre las Mejores Prácticas de Autenticación	GIG1
CIS-14.4	Capacitar a la Fuerza Laboral Sobre las Mejores Prácticas de Manejo de Datos	GIG1
CIS-14.6	Capacitar a los Miembros de la Fuerza Laboral Sobre el Reconocimiento y la Notificación de Incidentes de Seguridad	GIG1
CIS-14.9	Llevar a Cabo una Formación en Materia de Seguridad y Formación en Habilidades Específicas para Cada Función	GIG2
CIS-15	**Gestión de Proveedores de Servicios**	**GIG**
CIS-15.1	Establecer y Mantener un Inventario de Proveedores de Servicios	GIG1
CIS-15.2	Establecer y Mantener una Política de Gestión de Proveedores de Servicios	GIG2
CIS-15.3	Clasificar Proveedores de Servicios	GIG2
CIS-15.4	Asegúrese de que los Contratos de los Proveedores de Servicios Incluyan Requisitos de Seguridad	GIG2
CIS-15.5	Evaluar a los Proveedores de Servicios	GIG3
CIS-15.6	Supervisar a los Proveedores de Servicios	GIG3
CIS-15.7	Retirar de Forma Segura a los Proveedores de Servicios	GIG3
CIS-16	**Seguridad del Software de la Aplicación**	**GIG**
CIS-16.1	Establecer y Mantener un Proceso Seguro de Desarrollo de Aplicaciones	GIG2
CIS-16.2	Establecer y Mantener un Proceso para Aceptar y Abordar las Vulnerabilidades del Software	GIG2
CIS-16.3	Realizar un Análisis de la Causa Raíz de las Vulnerabilidades de Seguridad	GIG2
CIS-16.4	Establecer y Administrar un Inventario de Componentes de Software de Terceros	GIG2
CIS-16.5	Utilizar Componentes de Software de Terceros Actualizados y de Confianza	GIG2

CIS-16.6	Establecer y Mantener un Sistema y un Proceso de Clasificación de Severidad para las Vulnerabilidades de las Aplicaciones	GIG2
CIS-16.8	Sistemas de Producción y no Producción Separados	GIG2
CIS-16.9	Capacitar a los Desarrolladores en Conceptos de Seguridad de Aplicaciones y Codificación Segura	GIG2
CIS-16.12	Implementación de Comprobaciones de Seguridad a Nivel de Código	GIG2
CIS-16.13	Realizar Pruebas de Penetración de Aplicaciones	GIG3
CIS-17	Gestión de la Respuesta a Incidentes	GIG
CIS-17.1	Designar Personal para Gestionar los Incidentes	GIG1
CIS-17.2	Establecer y Mantener Información de Contacto para Informar Incidentes de Seguridad	GIG1
CIS-17.3	Establecer y Mantener un Proceso Empresarial para Informar de Incidentes	GIG1
CIS-17.4	Establecer y Mantener un Proceso de Respuesta a Incidentes	GIG2
CIS-17.5	Asignar Roles y Responsabilidades Clave	GIG2
CIS-17.6	Definir Mecanismos de Comunicación Durante la Respuesta a Incidentes	GIG2
CIS-17.7	Realizar Ejercicios Rutinarios de Respuesta a Incidentes	GIG2
CIS-17.8	Realizar Revisiones Posteriores al Incidente	GIG2
CIS-17.9	Establecer y Mantener Límites de Incidentes de Seguridad	GIG3
CIS-18	Pruebas de Penetración	GIG
CIS-18.1	Establecer y Mantener un Programa de Pruebas de Penetración	GIG2
CIS-18.2	Realizar Pruebas Periódicas de Penetración Externa	GIG2
CIS-18.3	Corregir los Resultados de las Pruebas de Penetración	GIG2
CIS-18.4	Validar las Medidas de Seguridad	GIG3
CIS-18.5	Realizar Pruebas Periódicas de Penetración Interna	GIG3

B. Controles Comunes Adicionales de GIS

Además de los controles de seguridad críticos de CIS adoptados anteriormente, los siguientes controles comunes GIS adicionales se aplican a los GPE utilizados para todas las formas de juego. La columna de la derecha indica el Grupo de Implementación del Juego (GIG) al que se aplica el Control de GIS.

GIS-1	Funciones críticas de los componentes del sistema del GPE	GIG
GIS-1.1	**Reloj interno del GPE**	
GIS-1.1.1	El GPE mantendrá un reloj interno que refleje la fecha y hora actuales, que se utilizará para proporcionar el sellado de tiempo de todas las transacciones, cambios de configuración y eventos significativos, y como reloj de referencia para la presentación de informes.	**GIG1**
GIS-1.1.2	Los cambios en la fecha y hora del reloj interno, o en las fuentes de tiempo aprobadas, se registrarán en un registro que indique: a. La fecha y hora de los cambios; b. Motivo y descripción de los cambios, incluidos los valores inicial y final; y c. ID de cuenta de usuario que realizó y/o autorizó los cambios.	**GIG1**
GIS-1.2	**Verificación de componentes críticos del sistema**	
GIS-1.2.1	Se verificará que los componentes críticos del sistema del GPE son idénticos a los aprobados por el organismo regulador mediante un procedimiento de verificación de firmas, que se realizará: a. Tras la instalación/actualización de los componentes; b. Al encenderse o recuperarse de un estado de apagado; c. Al menos una vez cada 24 horas; y d. A petición.	**GIG1**
GIS-1.2.2	El procedimiento de verificación de la firma deberá: a. Opere independientemente de cualquier proceso o software de seguridad dentro del sistema. b. Emplee un algoritmo hash criptográfico que produzca un resumen de mensajes de al menos 128 bits. Otras metodologías de ensayo se revisarán caso por caso. c. Incluya uno o más pasos analíticos para comparar las firmas actuales de los componentes críticos del sistema en el GPE con las firmas de las versiones aprobadas actuales de los componentes críticos del sistema.	**GIG1**
GIS-1.2.3	El resultado del procedimiento de verificación de la firma se registrará en un registro del sistema, que debe a. Detallar lo siguiente para cada verificación: i. La fecha y hora de la verificación; ii. Identificación de cada Componente Crítico del Sistema verificado; iii. Los resultados de firma esperados y generados, incluida la indicación de cualquier error de programa o discrepancia de firma; iv. Cuando se realiza bajo demanda, ID de cuenta de usuario que inició el procedimiento de verificación; b. Ser accesible para el organismo regulador en un formato que permita el análisis de cada verificación por parte del organismo regulador; y c. Constituyen parte de los datos sensibles que se recuperarán en caso de desastre o fallo de equipos o software.	**GIG1**
GIS-1.2.4	Cualquier fallo en la verificación de la firma de cualquier Componente Crítico del Sistema requerirá una notificación del fallo de verificación que se comunicará a la Empresa del Juego y al organismo regulador según sea necesario.	**GIG1**

GIS-1.2.5	Deberá existir un proceso para responder a las fallas de verificación de firmas, incluida la determinación de la causa de la falla y la realización de las correcciones o reinstalaciones asociadas del componente crítico del sistema necesarias de manera oportuna.	**GIG1**
GIS-2	**Seguridad de la información de los juegos (GIS)**	**GIG**
GIS-2.1	**Política de GIS**	
GIS-2.1.1	Se definirá e implementará una política de GIS para describir el enfoque de la empresa de juegos de azar para la gestión de GIS y su implementación, y para garantizar que los riesgos se identifiquen, mitiguen y suscriban mediante planes de contingencia.	**GIG1**
GIS-2.1.2	La política de GIS tendrá una disposición que exija la revisión a intervalos planificados y cuando se produzcan cambios GISnificativos en los procesos del GPE o de la Empresa de Juegos que alteren el perfil de riesgo del sistema.	**GIG1**
GIS-2.1.3	La política de GIS deberá ser aprobada por la gerencia y comunicada y reconocida por el personal relevante de la Empresa de Juego y el personal relevante del Proveedor de Servicios.	**GIG1**
GIS-2.1.4	La política de GIS delineará las funciones y responsabilidades de seguridad del personal de Gaming Enterprise y del personal relevante del Proveedor de Servicios para la operación, el servicio y el mantenimiento del GPE.	**GIG1**
GIS-2.2	**Política de control de acceso**	
GIS-2.2.1	Se establecerá y documentará una política de control de acceso, que se revisará periódicamente en función de los requisitos empresariales y de seguridad para el acceso físico y lógico a el GPE, incluido el acceso remoto permitido por el organismo regulador.	**GIG1**
GIS-2.2.2	Existirá un procedimiento formal de registro y cancelación de registro de usuarios para conceder y revocar el acceso a el GPE.	**GIG1**
GIS-2.2.3	La asignación y el uso de los derechos y privilegios de acceso de los usuarios se restringirán y controlarán en función de los requisitos empresariales y del principio de privilegios mínimos.	**GIG2**
GIS-2.2.4	Al personal solo se le proporcionará acceso a los servicios o instalaciones para los que haya sido específicamente autorizado a utilizar.	**GIG1**
GIS-2.2.5	La gerencia revisará y confirmará los derechos y privilegios de acceso de los usuarios a intervalos regulares utilizando un proceso formal.	**GIG2**
GIS-2.3	**Asignación de responsabilidades de seguridad**	
GIS-2.3.1	Las responsabilidades en materia de seguridad se documentarán y aplicarán de manera efectiva.	**GIG2**
GIS-2.3.2	Se establecerá formalmente un foro de seguridad compuesto por la gerencia para monitorear y revisar la política de GIS para garantizar su idoneidad, adecuación y efectividad continuas, mantener actas formales de las reuniones y reunirse periódicamente según lo requiera el organismo regulador.	**GIG2**
GIS-2.3.3	Existirá una función de seguridad que se encargará delaborar y aplicar estrategias y planes de acción en materia de seguridad.	**GIG2**
GIS-2.3.4	La función de seguridad participará y revisará todos los procesos relacionados con los aspectos de seguridad de la Empresa de juego, incluidos, entre otros, la protección de la información, las comunicaciones, la infraestructura física y los procesos de juego.	**GIG2**
GIS-2.3.5	La función de seguridad no reportará a la alta dirección y no residirá en la función de TI ni reportará a ella.	**GIG2**
GIS-2.3.6	La función de seguridad tendrá las competencias y estará suficientemente facultada y tendrá acceso a todos los recursos necesarios para permitir una evaluación, gestión y reducción del riesgo adecuadas.	**GIG2**
GIS-2.3.7	El jefe de la función de seguridad será miembro del foro de seguridad y será responsable de recomendar políticas y cambios en materia de seguridad.	**GIG2**
GIS-2.4	**Privacidad de la información de identificación personal (PII)**	
GIS-2.4.1	Cualquier PII obtenida con respecto al usuario se protegerá de conformidad con la política de privacidad y las regulaciones y estándares de privacidad locales observados por el organismo regulador, así como con los requisitos contractuales.	**GIG1**
GIS-2.4.2	Cualquier PII que no esté sujeta a divulgación de conformidad con la política de privacidad se mantendrá confidencial, excepto cuando la divulgación de esa información sea requerida por ley.	**GIG1**
GIS-2.4.3	Deberán existir procedimientos para la seguridad, el intercambio y el uso controlado de la información de identificación personal según lo requiera el organismo regulador.	**GIG1**

GIS-2.4.4	La Empresa de Juegos designará a una o más personas con la responsabilidad principal del diseño, la implementación y la evaluación continua de los procedimientos y prácticas relacionados con la seguridad y el intercambio de información personal.	**GIG1**
GIS-2.4.5	Se establecerán procedimientos para determinar la naturaleza y el alcance de toda la información personal recopilada por la Empresa del juego, incluidos los tipos de información recopilada, las fuentes de recopilación y los fines de uso.	**GIG1**
GIS-2.4.6	Cuando el organismo regulador lo requiera, se proporcionará a los usuarios un método para solicitar la confirmación del procesamiento de PII, acceso a una copia de su PII e información de procesamiento relacionada, actualizaciones de su PII y restricciones de borrado o procesamiento de su PII. a. Se establecerán procedimientos para registrar y procesar estas solicitudes, mantener registros de las mismas y proporcionar las razones de cualquier denegación o rechazo. b. Se informará a los usuarios cuando la empresa de juegos no tenga la intención de cumplir con su solicitud y se les proporcionará información sobre cómo presentar una queja ante el organismo regulador.	**GIG1**
GIS-2.4.7	Cuando así lo requiera el organismo regulador y a petición del usuario, la Empresa de Juegos enviará a los usuarios la PII que hayan recibido del mismo cliente, en un formato estructurado, de uso común y legible por máquina, y transmitirá la PII a otra Empresa de Juego, cuando sea técnicamente factible hacerlo. Esto solo se aplica a: a. PII que el usuario ha proporcionado a la Empresa de Juegos de Azar o PII que se procesa por medios automatizados (es decir, esto excluiría cualquier registro en papel); y b. Casos en los que la base para el procesamiento es el consentimiento de PII, o que los datos se están procesando para cumplir un contrato o pasos preparatorios de un contrato.	**GIG1**
GIS-2.4.8	Cuando así lo exija el organismo regulador, el usuario tiene derecho a oponerse al tratamiento de la PII: a. Sobre la base de intereses legítimos o la realización de una tarea de interés público o en el ejercicio de la autoridad pública; b. Se utiliza en marketing directo, incluida la elaboración de perfiles en la medida en que esté relacionada con dichas actividades de marketing; y c. Con fines de investigación científica o histórica o con fines estadísticos.	**GIG1**
GIS-2.4.9	Existirán procedimientos para que la Empresa de Juego cumpla con las solicitudes de los usuarios para que se borre la información personal y/o para evitar o restringir el procesamiento de la información personal, incluidas, las siguientes circunstancias: a. Cuando la PII ya no sea necesaria en relación con el propósito para el que se recopiló/procesó originalmente; b. Cuando el usuario retira su consentimiento; c. Cuando el usuario se opone al procesamiento de PII y no existe un interés legítimo primordial para continuar con el procesamiento; d. La información personal fue procesada ilegalmente; o e. La PII se borrará para cumplir con una obligación legal.	**GIG1**
GIS-2.4.10	Cuando lo prohíba el organismo regulador, la Empresa de Juego no podrá utilizar únicamente la toma de decisiones automatizada que: a. Produce efectos jurídicos al mecenas como los que dan lugar a que el mecenas sea sometido a la vigilancia de una autoridad competente; o b. Afecta significativamente al usuario de manera similar (por ejemplo, tiene el potencial de influir en las circunstancias, el comportamiento o las elecciones del usuario).	**GIG1**
GIS-2.5	**Aseguramiento de las transacciones financieras dentro del GPE**	
GIS-2.5.1	Los métodos de pago utilizados para las transacciones financieras en el GPE estarán protegidos contra el uso fraudulento.	**GIG1**
GIS-2.5.2	La recopilación de datos sensibles directamente relacionados con cada transacción financiera dentro del GPE se limitará únicamente a los datos sensibles estrictamente necesarios para la transacción.	**GIG1**

GIS-2.5.3	Deberán existir procesos para verificar la protección de los datos sensibles directamente relacionados con cada transacción financiera dentro del GPE, incluida cualquier IIP proporcionada por el usuario o datos relacionados con el pago.	**GIG1**
GIS-2.5.4	Todos los canales de comunicación dentro del GPE que transmitan detalles de transacciones financieras emplearán cifrado para proteger contra la interceptación.	**GIG1**
GIS-3	**Operación y seguridad del GPE**	**GIG**
GIS-3.1	**Procedimientos de seguridad**	
GIS-3.1.1	La Empresa de Juego supervisará los Componentes Críticos del Sistema y la transmisión de datos de todo el GPE, incluidas las comunicaciones, los paquetes de datos, las redes, las aplicaciones, así como los componentes y las transmisiones de datos de cualquier servicio del Proveedor de Servicios involucrado, con el objetivo de garantizar la integridad, la fiabilidad y la accesibilidad, así como para identificar comportamientos anómalos.	**GIG2**
GIS-3.1.2	La Empresa de Juego supervisará y ajustará la capacidad y el consumo de recursos para garantizar que se mantenga la disponibilidad.	**GIG1**
GIS-3.1.3	La Empresa de Juego mantendrá un registro del rendimiento del sistema, incluida una función para compilar informes de rendimiento.	**GIG2**
GIS-3.1.4	La Empresa de Juego supervisará su GPE con el fin de detectar, prevenir, mitigar y responder a los ataques y compromisos técnicos activos y pasivos comunes.	**GIG1**
GIS-3.1.5	La Empresa de Juegos establecerá procedimientos para recopilar y analizar inteligencia de amenazas, y para actuar en consecuencia de manera adecuada.	**GIG2**
GIS-3.2	**Mal funcionamiento del GPE**	
GIS-3.2.1	Tras la detección de un mal funcionamiento, la Empresa de Juego iniciará una investigación para determinar la causa raíz del mal funcionamiento.	**GIG1**
GIS-3.2.2	La investigación implicará una revisión exhaustiva de los registros, informes, registros y registros de vigilancia relevantes asociados con el Componente Crítico del Sistema afectado.	**GIG1**
GIS-3.2.3	Sobre la base de los hallazgos documentados de la investigación, se tomarán las medidas adecuadas para reparar o reemplazar los componentes críticos del sistema responsables del mal funcionamiento.	**GIG1**
GIS-3.2.4	Antes de restablecer el funcionamiento de los componentes críticos del sistema, se llevarán a cabo actividades de verificación para garantizar su integridad y funcionalidad.	**GIG1**
GIS-3.2.5	La Empresa de Juego deberá presentar un informe de mal funcionamiento ante el organismo regulador apropiado que documente los detalles del mal funcionamiento.	**GIG1**
GIS-3.3	**Gestión de incidentes GIS**	
GIS-3.3.1	La Empresa de Juego definirá, supervisará y documentará, así como informará, investigará, responderá y resolverá los incidentes GIS, incluidas las infracciones detectadas y la piratería o manipulación sospechada o real del GPE.	**GIG1**
GIS-3.3.2	Todos los incidentes GIS deberán ser respondidos dentro de un período de tiempo establecido aprobado por el organismo regulador y documentado formalmente.	**GIG1**
GIS-3.3.3	En caso de que se produzca un incidente GIS que comprometa la seguridad o integridad de los datos sensibles, se notificará al organismo regulador, a los usuarios afectados y a otras autoridades pertinentes. La notificación deberá incluir detalles sobre la naturaleza del incidente GIS, los riesgos potenciales y las medidas adoptadas para mitigar el impacto.	**GIG1**
GIS-3.3.4	El plan de respuesta a incidentes GIS debe incluir procedimientos documentados para manejar varios tipos de incidentes GIS.	**GIG1**
GIS-3.3.5	Se establecerán procedimientos para la recuperación controlada de incidentes GIS, incluida la restauración de los sistemas afectados y los datos sensibles a un buen estado conocido.	**GIG1**
GIS-3.4	**Ubicación física de los servidores**	
GIS-3.4.1	Los servidores de GPE, los datos confidenciales, la información y otros activos asociados se alojarán en una o más ubicaciones seguras que pueden estar ubicadas localmente, dentro de un solo sitio o lugar, o pueden estar ubicadas de forma remota fuera del sitio o lugar según lo permita el organismo regulador.	**GIG1**
GIS-3.4.2	Cada ubicación segura deberá tener suficiente protección contra la alteración, la manipulación o el acceso no autorizado.	**GIG1**

GIS-3.4.3	Cada emplazamiento seguro estará equipado con un sistema de vigilancia que se ajustará a los procedimientos establecidos por el organismo regulador.	**GIG1**
GIS-3.4.4	Se diseñarán e implementarán medidas de seguridad para trabajar en lugares seguros.	**GIG1**
GIS-3.4.5	Los perímetros de seguridad se definirán y utilizarán para proteger cada ubicación segura.	**GIG1**
GIS-3.4.6	Cada lugar seguro deberá estar protegido por controles de entrada apropiados para garantizar que el acceso esté restringido únicamente al personal autorizado. La MFA se utilizará para el acceso físico, a menos que la ubicación segura cuente con personal en todo momento.	**GIG1**
GIS-3.4.7	Los dispositivos de acceso a la ubicación segura, como el deslizamiento magnético, las tarjetas de proximidad, las tarjetas con chip integrado, los llaveros, deben ser controlados por personal autorizado.	**GIG1**
GIS-3.4.8	Todos los intentos de acceso físico a cada ubicación segura se registrarán en un registro en el que se indique: a. La fecha y hora del intento de acceso; b. Identificación de la persona que intenta acceder; c. Identificación del sitio o lugar seguro al que se accede; d. Indicación de si el intento de acceso ha tenido éxito o no; y e. Si el intento de acceso se ha realizado correctamente, la duración del acceso.	**GIG1**
GIS-3.4.9	Cada lugar seguro debe estar equipado con controles para proporcionar protección física contra daños causados por incendios, inundaciones y otras amenazas ambientales y formas de desastres naturales o provocados por el hombre (por ejemplo, huracán, terremoto, etcétera).	**GIG1**
GIS-3.4.10	El GPE debe estar protegida contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.	**GIG1**
GIS-3.4.11	Los cables que transportan energía, datos o componentes críticos del sistema de soporte deben estar protegidos contra interceptaciones, interferencias o daños.	**GIG1**
GIS-3.4.12	Todos los componentes críticos del sistema deben estar provistos de energía primaria adecuada.	**GIG1**
GIS-3.4.13	Cuando el servidor sea una aplicación independiente, deberá tener un sistema de alimentación ininterrumpida (SAI) conectado y tener capacidad suficiente para permitir un apagado correcto y que conserve todos los datos confidenciales durante un corte de energía. Es aceptable que el sistema pueda ser un componente de una red que sea compatible con un SAI de toda la red, siempre que el servidor esté incluido como un dispositivo protegido por el SAI. Se debe utilizar un sistema de protección contra sobretensiones si no está incorporado en el SAI mismo.	**GIG1**
GIS-3.5	**Control de acceso lógico**	
GIS-3.5.1	El GPE deberá estar protegida lógicamente contra el acceso no autorizado mediante credenciales de autenticación permitidas por el organismo regulador, como contraseñas, MFA, certificados digitales, PIN, datos biométricos y otros métodos de acceso.	**GIG1**
GIS-3.5.2	Cada cuenta de usuario tendrá su propia credencial de autenticación individual, cuya provisión se controlará a través de un proceso formal.	**GIG1**
GIS-3.5.3	Los usuarios solo tendrán acceso a la funcionalidad y características apropiadas para su función y responsabilidades dentro del sistema.	**GIG1**
GIS-3.5.4	No será posible modificar los parámetros críticos del sistema del GPE, incluidas las políticas y parámetros de los sistemas operativos, las bases de datos, las redes y las aplicaciones (por ejemplo, la configuración de auditoría, la configuración de la complejidad de las contraseñas, los niveles de seguridad del sistema, las actualizaciones manuales de las bases de datos, etcétera), sin un proceso seguro autorizado. Los cambios en los parámetros críticos del sistema se registrarán en un registro que indique: a. La fecha y hora de los cambios; b. Se han cambiado los parámetros críticos del sistema; c. Motivo y descripción de los cambios, incluidos los valores inicial y final; y d. ID de cuenta de usuario que realizó y/o autorizó los cambios.	**GIG1**
GIS-3.5.5	El uso de las cuentas genéricas será limitado y, cuando se utilicen, se documentarán formalmente las razones de su uso.	**GIG1**
GIS-3.5.6	Los registros de credenciales de autenticación para la información secreta se mantendrán manualmente o mediante sistemas que registren automáticamente los cambios de autenticación y obliguen a cambiar las credenciales de autenticación.	**GIG1**

GIS-3.5.7	Todas las credenciales de autenticación almacenadas en el sistema se cifrarán o se cifrarán con hash en otros algoritmos criptográficos autorizados.	**GIG1**
GIS-3.5.8	Un método alternativo para restablecer las credenciales de autenticación (por ejemplo, contraseñas olvidadas) debe ser al menos tan seguro como el método principal. A estos efectos, se empleará un proceso de AMF.	**GIG2**
GIS-3.5.9	Las credenciales de autenticación perdidas o comprometidas y las credenciales de autenticación de los usuarios terminados se desactivarán, protegerán o destruirán tan pronto como sea razonablemente posible.	**GIG1**
GIS-3.5.10	El sistema debe tener múltiples niveles de acceso de seguridad para controlar y restringir diferentes clases de acceso al servidor, incluida la visualización, el cambio o la eliminación de archivos y directorios críticos. Se establecerán procedimientos para asignar, revisar, modificar y eliminar los derechos y privilegios de acceso a cada usuario, incluidos: a. Permitiendo la administración de las cuentas de usuario para proporcionar una adecuada separación de funciones. b. Limitar los usuarios que tienen los permisos necesarios para ajustar los parámetros críticos del sistema. c. La aplicación de parámetros de credencial de autenticación adecuados, como la longitud mínima y los intervalos de caducidad.	**GIG1**
GIS-3.5.11	Un proveedor de servicios puede, según sea necesario, acceder al sistema y a sus componentes asociados utilizando una cuenta de usuario invitado para el soporte del producto y del usuario o para actualizaciones/mejoras, según lo permitan el organismo regulador y la empresa de juego. Las cuentas de usuario invitado serán: a. Restringidas a través de controles de seguridad lógicos para acceder solo a la(s) aplicación(es) y/o base de datos necesaria(s) para el producto y el soporte al usuario o para proporcionar actualizaciones/mejoras; b. Monitoreadas continuamente por la empresa de juegos; y c. Deshabilitadas cuando no está en uso e inmediatamente después del propósito para el que se estableció la cuenta ya no es necesario.	**GIG1**
GIS-3.5.12	Se establecerán procedimientos para identificar y marcar las cuentas de usuario sospechosas para evitar su uso no autorizado, lo que incluye: a. Tener una notificación al administrador del sistema y el bloqueo del usuario, después de un número máximo de tres intentos incorrectos de autenticación; b. Marcación de cuentas sospechosas en las que se pueden haber robado credenciales de autenticación; y c. Invalidar cuentas y transferir información crítica almacenada de la cuenta a una nueva cuenta.	**GIG1**
GIS-3.5.13	Los intentos de acceso lógico a las aplicaciones del sistema o a los sistemas operativos se registrarán en un registro en el que se indique: a. La fecha y hora del intento de acceso; b. ID de cuenta de usuario; c. Dirección IP de la persona que intenta acceder; d. Indicación de si el intento de acceso ha tenido éxito o no; y e. Si el intento de acceso se ha realizado correctamente, la duración del acceso.	**GIG1**
GIS-3.5.14	El uso de programas de utilidad que puedan anular los controles de la aplicación o del sistema operativo debe estar restringido y estrictamente controlado.	**GIG1**
GIS-3.5.15	Las anulaciones, anulaciones, correcciones o cualquier otra actividad que requiera la intervención del usuario y que ocurran fuera del alcance normal de la operación del sistema se registrarán en un registro, indicando: a. La fecha y hora de las actividades; b. Componentes afectados por las actividades; c. Motivo y descripción de las actividades, incluidos los valores inicial y final; y d. ID de cuenta de usuario que realizó y/o autorizó las actividades.	**GIG1**
GIS-3.5.16	Para cada cuenta de usuario, la información que debe mantener y respaldar el GPE incluirá: a. ID de cuenta de usuario; b. Nombre individual y título o cargo;	**GIG1**

	c. Lista completa y descripción de las funciones que cada grupo o cuenta de usuario puede ejecutar; d. La fecha y hora en que se creó la cuenta; e. La fecha y hora del último acceso, incluida la dirección IP; f. La fecha y hora del último cambio de contraseña; g. La fecha y hora en que se desactivó/desactivó la cuenta; h. Descripción de los derechos de acceso o pertenencia a grupos de la cuenta, si corresponde; y i. Los estados actuales y anteriores de la cuenta de usuario (por ejemplo, activa, inactiva, cerrada, suspendida, etcétera).	
GIS-3.5.17	Solo el personal autorizado puede tener acceso a las cuentas de usuario inactivas o cerradas	**GIG1**
GIS-3.6	**Autenticación y autorización de usuarios**	
GIS-3.6.1	Se empleará un mecanismo seguro y controlado que pueda verificar que el personal autorizado está accediendo al componente crítico del sistema a pedido y de forma regular, según lo requiera el organismo regulador.	**GIG1**
GIS-3.6.2	Las sesiones activas se finalizarán si la autorización del usuario ha superado un número configurable de intentos fallidos.	**GIG1**
GIS-3.6.3	Cuando se utilicen, los métodos automatizados de identificación de equipos para autenticar las conexiones desde ubicaciones y equipos específicos deberán documentarse y se incluirán en la revisión de los derechos y privilegios de acceso.	**GIG2**
GIS-3.6.4	Cualquier información de autorización comunicada por el sistema con fines de identificación se obtendrá en el momento de la solicitud del sistema y no se almacenará en el componente del sistema.	**GIG2**
GIS-3.6.5	Cuando se realiza un seguimiento de las sesiones de usuario para la autorización, la información de autorización de la sesión de usuario siempre se creará de forma aleatoria, en la memoria, y se eliminará una vez finalizada la sesión del usuario.	**GIG2**
GIS-3.6.6	Las restricciones en los tiempos de conexión, tales como, entre otros, los tiempos de espera de sesión, se utilizarán para proporcionar seguridad adicional para aplicaciones de alto riesgo, como el acceso remoto.	**GIG1**
GIS-3.6.7	Si el sistema no recibe información de la persona dentro de los cinco minutos, o un período especificado por el organismo regulador, la sesión del usuario se agotará o se bloqueará, lo que requerirá que el personal restablezca su autorización para continuar.	**GIG1**
GIS-3.7	**Programación de servidores**	
GIS-3.7.1	El GPE deberá ser lo suficientemente seguro como para impedir cualquier capacidad de programación iniciada por el usuario en el servidor que pueda dar lugar a modificaciones en la base de datos. Sin embargo, es aceptable que los administradores de red o de sistemas realicen el mantenimiento autorizado de la infraestructura de red o la resolución de problemas de aplicaciones con suficientes derechos de acceso.	**GIG1**
GIS-3.7.2	El servidor también debe estar protegido contra la ejecución no autorizada de código móvil. Esto incluye evitar la ejecución de código potencialmente dañino que pueda introducirse a través de dispositivos móviles u otras fuentes externas.	**GIG2**
GIS-3.8	**Entornos virtualizados y en la nube**	
GIS-3.8.1	Las instancias de servidor redundantes no se ejecutarán en el mismo hipervisor.	**GIG2**
GIS-3.8.2	Cada instancia de servidor puede realizar solo una función.	**GIG2**
GIS-3.9	**Sistema de Retención de Documentos Electrónicos (ERDS)**	
GIS-3.9.1	El ERDS se configurará correctamente para mantener la versión original junto con todas las versiones posteriores que reflejen todos los cambios en los informes o registros que se almacenen en un formato modificable.	**GIG1**
GIS-3.9.2	El ERDS mantendrá una firma única para cada versión del registro, incluido el original.	**GIG1**
GIS-3.9.3	El ERDS conservará un registro de los cambios en todos los informes, incluido el ID de cuenta de usuario realizado los cambios, la fecha y la hora en que se produjeron los cambios y lo que se cambió.	**GIG1**

GIS-3.9.4	El ERDS proporcionará un método de indexación completa para localizar e identificar fácilmente el registro, que incluya al menos lo GISuiente (que puede ser introducido por el usuario): a. Fecha y hora en que se generó el registro; b. Componente crítico del sistema que genera el registro; c. Título y descripción del registro; d. ID de cuenta de usuario de quién genera el registro; y e. Cualquier otra información que pueda ser útil para identificar el registro y su propósito.	**GIG1**
GIS-3.9.5	El ERDS se configurará de manera que a. Limite el acceso para modificar o agregar informes o registros al sistema a través de la seguridad lógica de cuentas de usuario específicas; y b. Proporcione un registro de toda la actividad de la cuenta de usuario administrativo.	**GIG1**
GIS-3.9.6	El ERDS deberá estar debidamente protegido mediante medidas de seguridad físicas y lógicas (cuentas de usuario con acceso adecuado, niveles adecuados de registro de eventos, y documentar el control de versiones, etcétera).	**GIG1**
GIS-3.9.7	El ERDS deberá estar equipado para evitar la interrupción de la disponibilidad de los registros y la pérdida de datos a través de las mejores prácticas de redundancia de hardware y software, y los procesos de copia de seguridad.	**GIG1**
GIS-4	**Integridad de los datos**	**GIG**
GIS-4.1	**Gestión de datos confidenciales**	
GIS-4.1.1	La Empresa de Juego proporcionará un enfoque por capas para la seguridad de GPE para garantizar el almacenamiento y el procesamiento seguros de datos confidenciales utilizando métodos de protección razonables.	**GIG1**
GIS-4.1.2	Se implementarán métodos apropiados de manejo de datos, incluida la validación de la entrada y el rechazo de datos confidenciales corruptos.	**GIG2**
GIS-4.1.3	Se limitará el número de estaciones de trabajo en las que se pueda acceder a las aplicaciones críticas o a las bases de datos asociadas.	**GIG1**
GIS-4.1.4	Se utilizará cifrado o seguridad equivalente para los archivos y directorios que contengan datos sensibles. Si no se utiliza el cifrado, la Empresa de Juego restringirá a los usuarios la visualización del contenido de dichos archivos y directorios, lo que, como mínimo, proporcionará la segregación de las funciones y responsabilidades del sistema, así como la supervisión y el registro del acceso de cualquier persona a dichos archivos y directorios.	**GIG2**
GIS-4.1.5	Las alteraciones de los archivos de datos en tiempo real y de las tablas de la base de datos del GPE que se produzcan fuera de la ejecución normal del programa y del sistema operativo se registrarán en un registro en el que se indique: a. La fecha y hora de las alteraciones; b. Los archivos de datos en vivo y las tablas de bases de datos afectadas por las alteraciones; c. Motivo y descripción de las alteraciones, incluidos los archivos de datos en tiempo real y las tablas de bases de datos antes y después de las alteraciones; y d. ID de cuenta de usuario que realizó y/o autorizó la modificación.	**GIG1**
GIS-4.1.6	El GPE proporcionará un medio lógico para asegurar y proteger los datos sensibles contra la alteración, la manipulación o el acceso no autorizado, tanto externo como interno.	**GIG1**
GIS-4.1.7	El funcionamiento normal de cualquier componente crítico del sistema que contenga datos confidenciales no deberá tener ninguna opción o mecanismo que pueda comprometer los datos confidenciales.	**GIG1**
GIS-4.1.8	Ningún componente crítico del sistema puede tener un mecanismo por el cual un error haga que los datos confidenciales se borren automáticamente.	**GIG1**
GIS-4.1.9	Cualquier componente crítico del sistema que mantenga datos confidenciales en su memoria no permitirá la eliminación de la información a menos que primero haya transferido esa información a la base de datos asociada u otro componente seguro del sistema.	**GIG1**
GIS-4.1.10	La Empresa de Juego protegerá la confidencialidad, integridad, responsabilidad y disponibilidad de los datos confidenciales, cuando se mantengan en reposo en servidores, aplicaciones críticas y bases de datos asociadas que contengan datos confidenciales.	**GIG2**
GIS-4.1.11	El cifrado se aplicará para proteger la confidencialidad, integridad, responsabilidad y disponibilidad de los datos confidenciales cuando estén en uso, cuando se almacenen en sistemas informáticos	**GIG2**

	portátiles (por ejemplo, computadoras portátiles, dispositivos USB, etcétera) y cuando se mantengan en reposo en estaciones de trabajo.	
GIS-4.1.12	Los datos sensibles que no deban ocultarse, pero que deban autenticarse, utilizarán algún tipo de técnica de autenticación de mensajes.	**GIG2**
GIS-4.1.13	La autenticación utilizará un certificado de seguridad de una empresa de juego aprobada, que contenga información sobre a quién pertenece, quién lo emitió, fechas de validez, un número de serie único u otra identificación única que pueda usarse para verificar el contenido del certificado.	**GIG1**
GIS-4.1.14	Las bases de datos de producción que contengan datos sensibles residirán en redes separadas de los servidores que alojan las interfaces de los usuarios.	**GIG1**
GIS-4.1.15	Los datos sensibles se mantendrán en todo momento, independientemente de si el servidor está recibiendo energía.	**GIG1**
GIS-4.1.16	Se aplicarán medidas de prevención de fuga de datos sensibles a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita datos sensibles.	**GIG2**
GIS-4.1.17	Los datos sensibles se almacenarán de forma que se evite la pérdida de datos al sustituir piezas o módulos durante el mantenimiento normal.	**GIG1**
GIS-4.1.18	No se permitirá la alteración de datos sensibles sin controles de acceso supervisados. En caso de que se modifique algún dato sensible, se documentará o registrará la siguiente información: a. La fecha y hora de la alteración; b. Identificación de los datos sensibles alterados; c. Motivo y descripción de la alteración de los datos sensibles, incluyendo valores iniciales y finales; y d. ID de cuenta de usuario que realizó y/o autorizó la modificación.	**GIG1**
GIS-4.1.19	Toda pérdida irrecuperable de datos sensibles se registrará en un registro, indicando: a. La fecha y hora de la pérdida; b. Identificación de los datos sensibles perdidos; y c. Motivo y descripción de los datos sensibles perdidos.	**GIG1**
GIS-4.2	**Implementación del proceso de respaldo**	
GIS-4.2.1	La implementación del proceso de copia de seguridad se realizará al menos una vez al día o según lo especificado por el organismo regulador, aunque todos los métodos se revisarán caso por caso.	**GIG1**
GIS-4.2.2	Los datos confidenciales, las aplicaciones críticas y las bases de datos asociadas deben estar respaldados con salvaguardas de inmutabilidad para evitar alteraciones o eliminaciones, garantizando la integridad del GPE.	**GIG1**
GIS-4.2.3	Las copias duplicadas o redundantes de datos sensibles se conservarán en el GPE con soporte abierto para copias de seguridad y restauración.	**GIG1**
GIS-4.2.4	La copia de seguridad deberá estar contenida en un soporte físico no volátil o en una implementación arquitectónica equivalente.	**GIG1**
GIS-4.2.5	Si se utilizan HHD como almacenamiento de copia de seguridad, se garantizará la integridad de los datos en caso de fallo del disco.	**GIG1**
GIS-4.2.6	Una vez finalizado el proceso de respaldo, el almacenamiento de copia de seguridad se transfiere inmediatamente a una ubicación de almacenamiento físicamente separada de la ubicación que alberga los servidores y los datos confidenciales de los que se realiza la copia de seguridad (para almacenamiento temporal y permanente).	**GIG1**
GIS-4.2.7	La ubicación de almacenamiento de copia de seguridad debe estar protegida para evitar el acceso no autorizado y proporcionar una protección adecuada para evitar la pérdida permanente de datos confidenciales.	**GIG1**
GIS-4.2.8	Si la copia de seguridad se almacena en una plataforma en la nube, es posible que se almacene otra copia en una plataforma o región en la nube diferente.	**GIG2**
GIS-4.2.9	Los archivos de datos de respaldo y los componentes de recuperación de datos se gestionarán con al menos el mismo nivel de seguridad y controles de acceso que el GPE.	**GIG1**
GIS-4.2.10	Los archivos de datos de respaldo y los componentes de recuperación de datos se mantendrán, protegerán y probarán periódicamente de acuerdo con el proceso de respaldo acordado.	**GIG2**
GIS-4.3	**Falla y recuperación del sistema**	
GIS-4.3.1	La falla o los períodos significativos de indisponibilidad de un componente crítico del sistema (cualquier período de tiempo en que las operaciones se detengan para todos los usuarios y/o las	**GIG1**

	transacciones no puedan completarse con éxito para ningún usuario) se registrarán en un registro, indicando; a. Identificación del componente no disponible; b. La fecha y hora en que el componente dejó de estar disponible; y c. Motivo y descripción de la indisponibilidad del componente; d. La fecha y la hora en que el componente volvió a estar disponible.	
GIS-4.3.2	El GPE deberá tener suficiente redundancia y modularidad para que, en caso de fallo de un solo componente crítico del sistema o parte de un componente, las funciones del GPE y el proceso de auditoría de dichas funciones puedan continuar sin pérdida ni corrupción de datos sensibles.	**GIG1**
GIS-4.3.3	Cuando dos o más componentes críticos del sistema estén vinculados, se establecerá un procedimiento para que los componentes se prueben después de la instalación, pero antes de su uso en un GPE.	**GIG1**
GIS-4.3.4	El proceso de todas las operaciones de juego entre los componentes críticos del sistema no se verá afectado negativamente por el reinicio o la recuperación de cualquiera de los componentes (por ejemplo, las transacciones no deben perderse o duplicarse debido a la recuperación de un componente u otro).	**GIG1**
GIS-4.3.5	Tras el reinicio o la recuperación, los componentes críticos del sistema sincronizarán inmediatamente el estado de todas las transacciones, los datos confidenciales y las configuraciones entre sí.	**GIG1**
GIS-4.3.6	La Empresa de Juego deberá ser capaz de identificar y manejar adecuadamente la situación en la que se ha producido un reinicio maestro en cualquier Componente Crítico del Sistema.	**GIG1**
GIS-4.4	**Plan de Continuidad del Negocio y Recuperación ante Desastres**	
GIS-4.4.1	Se implementará un plan de continuidad del negocio y recuperación ante desastres para recuperar las operaciones de juego si el GPE se vuelve inoperable, incluidos, entre otros: a. Restauración de copias de seguridad de datos; b. Restablecimiento del programa; y c. Restauración de hardware redundante o de respaldo.	**GIG1**
GIS-4.4.2	El plan de continuidad de negocio y recuperación ante desastres tendrá en cuenta los desastres, incluidos, entre otros, los causados por el clima, el agua, las inundaciones, los incendios, los derrames y accidentes ambientales, la destrucción maliciosa, los actos de terrorismo o guerra, y las contingencias como huelgas, epidemias, pandemias, etcétera.	**GIG1**
GIS-4.4.3	El plan de continuidad de negocio y recuperación en caso de desastre abordará el método de almacenamiento de datos sensibles para minimizar las pérdidas. Si se utiliza la replicación asincrónica, se describirá el método para recuperar la información o se documentará la posible pérdida de información.	**GIG2**
GIS-4.4.4	El plan de continuidad de las actividades y recuperación en caso de desastre determinará las circunstancias en las que se invocará.	**GIG1**
GIS-4.4.5	El plan de continuidad de negocio y recuperación en caso de desastre abordará el establecimiento de un centro de recuperación físicamente separado del centro de producción. La distancia entre las dos ubicaciones debe determinarse en función de las posibles amenazas y peligros ambientales, cortes de energía y otras interrupciones, pero también debe tener en cuenta la dificultad potencial de la replicación de datos, así como la posibilidad de acceder al sitio de recuperación dentro de un tiempo razonable (objetivo de tiempo de recuperación). La utilización de plataformas en la nube para este fin se evaluará caso por caso.	**GIG2**
GIS-4.4.6	El plan de continuidad de negocio y recuperación en caso de desastre contendrá guías de recuperación que detallen los pasos técnicos necesarios para restablecer la funcionalidad del juego en el sitio de recuperación.	**GIG1**
GIS-4.4.7	El plan de continuidad de negocio y recuperación en caso de desastre abordará los procesos necesarios para reanudar las operaciones administrativas de las actividades de juego tras la activación del sistema recuperado para una serie de escenarios adecuados para el contexto operativo del sistema.	**GIG1**
GIS-4.4.8	El plan de continuidad del negocio y recuperación en caso de desastre se probará al menos una vez al año o según lo especificado por el organismo regulador. Se documentarán los resultados de los ensayos.	**GIG1**
GIS-5	**Comunicaciones**	**GIG**

GIS-5.1	**Conectividad**	
GIS-5.1.1	Solo los dispositivos autorizados podrán establecer comunicaciones entre cualquier componente crítico del sistema.	**GIG1**
GIS-5.1.2	El GPE proporcionará un método para a. Realizar la autenticación mutua para garantizar que los dispositivos autorizados solo se comuniquen con redes válidas; b. Inscribir y anular la inscripción de componentes críticos del sistema; y c. Habilite y deshabilite componentes críticos específicos del sistema.	**GIG1**
GIS-5.1.3	Solo los componentes críticos del sistema inscritos y habilitados pueden participar en las operaciones de juego.	**GIG1**
GIS-5.1.4	La condición predeterminada para los componentes críticos del sistema será anular la inscripción y deshabilitarla.	**GIG1**
GIS-5.1.5	El GPE registrará el establecimiento, la pérdida y el restablecimiento de las comunicaciones entre los componentes críticos del sistema.	**GIG1**
GIS-5.2	**Protocolo de comunicación**	
GIS-5.2.1	Cada componente crítico del sistema del GPE funcionará según lo indicado por un protocolo de comunicación seguro documentado.	**GIG1**
GIS-5.2.2	Todos los protocolos deben utilizar técnicas de comunicación que tengan mecanismos adecuados de detección y recuperación de errores, que estén diseñados para evitar intrusiones, interferencias, escuchas, alteraciones no autorizadas y manipulaciones. Cualquier implementación alternativa se revisará caso por caso y será aprobada por el organismo regulador.	**GIG1**
GIS-5.2.3	Todas las comunicaciones críticas de datos sensibles emplearán cifrado y autenticación para su integridad.	**GIG1**
GIS-5.2.4	Las comunicaciones en la red segura solo serán posibles entre componentes críticos del sistema autorizados que hayan sido inscritos y autenticados como válidos en la red. No se permitirán comunicaciones no autorizadas a componentes y/o puntos de acceso.	**GIG1**
GIS-5.2.5	Las comunicaciones se endurecerán para que sean inmunes a todos los posibles ataques de mensajes con formato incorrecto.	**GIG1**
GIS-5.2.6	La falta de comunicaciones no afectará a la integridad de los datos sensibles.	**GIG1**
GIS-5.2.7	Después de una interrupción o apagado del sistema, la comunicación con todos los componentes críticos del sistema necesarios para el funcionamiento de GPE no se establecerá ni autenticará hasta que la rutina de reanudación del programa, incluidas las autopruebas, se complete con éxito.	**GIG1**
GIS-5.3	**Protocolos de tunelización cifrados**	
GIS-5.3.1	Se utilizará uno de los siguientes protocolos de tunelización cifrados o equivalentes para proteger la comunicación de todos los datos confidenciales a través de la WLAN: a. Protocolo de autenticación extensible protegido (EAP protegido o PEAP); b. Protocolo de autenticación extensible - Seguridad de la capa de transporte (EAP-TLS); c. Protocolo de autenticación extensible - Seguridad de la capa de transporte en túnel (EAP-TTLS); d. Red privada virtual (VPN) con L2TP/IPsec; e. Protocolo de túnel punto a punto (PPTP); o f. Capa de sockets seguros (SSL).	**GIG1**
GIS-5.3.2	Los protocolos de tunelización cifrados se autenticarán con el protocolo ligero de acceso a directorios (LDAP), el servicio de usuario de acceso telefónico de autenticación remota (RADIUS), los servidores Kerberos o Microsoft Active Directory o equivalentes, así como con las bases de datos locales almacenadas en el controlador del portal seguro.	**GIG1**
GIS-5.4	**Comunicaciones a través de Internet/Redes públicas**	
GIS-5.4.1	Las comunicaciones entre cualquier componente crítico del sistema que tenga lugar a través de Internet/redes públicas se protegerán contra actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas mediante el cifrado de los paquetes de datos o la utilización de un protocolo de comunicaciones seguro para garantizar la confidencialidad e integridad de la transmisión.	**GIG1**

GIS-5.4.2	Los datos confidenciales siempre se cifrarán a través de Internet/red pública y se protegerán contra transmisiones incompletas, desvíos, modificación no autorizada de mensajes, divulgación, duplicación o reproducción.	**GIG1**
GIS-5.5	**Comunicaciones inalámbricas de red de área local (WLAN)**	
GIS-5.5.1	El uso de las comunicaciones WLAN debe ser seguro y solo se utilizará cuando proceda y no en zonas donde pueda ser potencialmente perjudicial.	**GIG1**
GIS-5.5.2	Las comunicaciones entre dispositivos inalámbricos en la WLAN utilizarán protocolos diseñados para asegurar, autenticar y cifrar redes inalámbricas.	**GIG1**
GIS-5.5.3	Se requerirá la autenticación multifactor (MFA) a nivel de red inalámbrica y dispositivo.	**GIG1**
GIS-5.5.4	Los esquemas de autenticación que utilicen una infraestructura de clave pública (PKI) requerirán la validación de certificados, idealmente en ambas direcciones (por ejemplo, certificados de cliente).	**GIG1**
GIS-5.5.5	Se utilizarán estándares de cifrado avanzado (AES) o equivalentes con un cifrado mínimo de 256 bits para respaldar los servicios de integridad y confidencialidad.	**GIG1**
GIS-5.5.6	La llave maestra por pares (PMK) utilizada tendrá una vida útil de veinticuatro horas o menos. Alternativamente, es aceptable que el PMK se cambie durante el tiempo de inactividad por mantenimiento preprogramado de acuerdo con los controles adoptados por la empresa de juego.	**GIG1**
GIS-5.5.7	La clave maestra de grupo (GMK) utilizada tendrá una vida útil de ocho horas o menos.	**GIG1**
GIS-5.5.8	No se utilizará la privacidad equivalente por cable (WEP). Si no es posible que el GPE utilice el protocolo WPA2, la implementación de WEP como método seguro de cifrado y autenticación se considerará caso por caso.	**GIG1**
GIS-5.6	**Puntos de acceso inalámbricos (WAP)**	
GIS-5.6.1	Un WAP permite que los dispositivos inalámbricos se conecten a una red cableada mediante transporte inalámbrico (por ejemplo, Wi-Fi) y transmitan datos entre los dispositivos inalámbricos y el resto de la red.	**GIG1**
GIS-5.6.2	El nombre de usuario y la contraseña de administración predeterminados se cambiarán de los valores predeterminados de fábrica a un valor seguro controlado de acuerdo con la Empresa de Juego.	**GIG1**
GIS-5.6.3	La contraseña de red predeterminada se cambiará de la predeterminada de fábrica a un valor seguro controlado de acuerdo con la Empresa de Juego.	**GIG1**
GIS-5.6.4	El SSID se cambiará del valor predeterminado de fábrica a un valor seguro que no contenga ninguna referencia al nombre del sitio, al fabricante o a cualquier otra referencia que se pueda discernir fácilmente.	**GIG1**
GIS-5.6.5	El acceso a las funciones administrativas del WAP se restringirá a las conexiones desdel lado cableado de la red que utilice un protocolo seguro con una cuenta de usuario privilegiada definida por la Empresa de Juego.	**GIG1**
GIS-5.6.6	Si el enrutador admite la autenticación WPA2, todos los WAP deben ser compatibles con IEEE 802.11 y estar configurados con el modo empresarial habilitado o con una clave precompartida segura.	**GIG1**
GIS-5.7	**Equipo de comunicación de red (NCE)**	
GIS-5.7.1	La Empresa de Juegos proporcionará una ubicación segura para la colocación, operación y uso de NCE.	**GIG1**
GIS-5.7.2	El NCE se instalará de acuerdo con un plan definido y se mantendrán registros de todos los NCE instalados.	**GIG1**
GIS-5.7.3	Las NCE se construirán de tal manera que sean resistentes a los daños físicos del hardware o a la corrupción del software contenido por el uso normal.	**GIG1**
GIS-5.7.4	NCE deberá estar físicamente protegido contra el acceso no autorizado.	**GIG1**
GIS-5.7.5	Las comunicaciones del GPE a través de NCE deben estar lógicamente protegidas contra el acceso no autorizado.	**GIG1**
GIS-5.7.6	Las NCE con almacenamiento integrado limitado deberán, si el registro de auditoría se llena, deshabilitar todas las comunicaciones o descargar los registros a un servidor de registro dedicado.	**GIG1**
GIS-5.8	**Sistema de Detección de Intrusos/Sistema de Prevención de Intrusiones (IDS/IPS)**	

GIS-5.8.1	Se instalará un IDS/IPS que incluya uno o más componentes que puedan escuchar las comunicaciones internas y externas, así como detectar o prevenir: a. Ataques de denegación de servicio distribuido (DDOS); b. Shellcode de atravesar la red; c. suplantación de identidad (spoofing) del protocolo de resolución de direcciones (ARP); y d. Otros indicadores de ataque "Man-In-The-Middle" (Intermediario) y cortan las comunicaciones inmediatamente si se detectan.	**GIG1**
GIS-5.8.2	El IDS/IPS escaneará la red en busca de puntos de acceso no autorizados o sospechosos o dispositivos conectados a cualquier punto de acceso en la red al menos trimestralmente o según lo especificado por el organismo regulador.	**GIG2**
GIS-5.8.3	El IDS/IPS desactivará automáticamente cualquier dispositivo no autorizado o sospechoso conectado al GPE.	**GIG2**
GIS-5.8.4	El IDS/IPS mantendrá un registro de acceso para: a. Contener información completa y exhaustiva sobre todos los dispositivos involucrados, incluida la hora y la fecha, el nombre y el identificador de hardware de todos los dispositivos que solicitan acceso a la red; y b. Ser capaz de ser conciliado con todos los demás dispositivos de red dentro del GPE.	**GIG1**
GIS-5.9	**Gestión de la seguridad de la red**	
GIS-5.9.1	La Empresa de Juego revisará y actualizará las políticas y procedimientos para garantizar que la red sea segura y que las amenazas y vulnerabilidades se aborden en consecuencia.	**GIG1**
GIS-5.9.2	Las redes estarán separadas lógicamente de manera que no haya tráfico de red en un enlace de red que no pueda ser atendido por los hosts de ese enlace.	**GIG1**
GIS-5.9.3	Todas las funciones de gestión de la red autenticarán a todos los usuarios de la red y cifrarán todas las comunicaciones de gestión de la red.	**GIG1**
GIS-5.9.4	La falla de un solo artículo no resultará en una denegación de servicio.	**GIG1**
GIS-5.9.5	Todos los puntos de entrada y salida de la red deben estar identificados, gestionados, controlados y monitoreados las 24 horas del día, los 7 días de la semana.	**GIG2**
GIS-5.9.6	Todos los concentradores de red, servicios y puertos de conexión deben estar protegidos para evitar el acceso no autorizado a la red.	**GIG1**
GIS-5.9.7	Los servicios no utilizados y los puertos no esenciales se bloquearán físicamente o se desactivará el software siempre que sea posible.	**GIG1**
GIS-5.9.8	Los protocolos sin estado, como UDP (User Datagram Protocol), no se utilizarán para datos confidenciales sin transporte con estado. Tenga en cuenta que aunque HTTP (Protocolo de transporte de hipertexto) técnicamente no tiene estado, si se ejecuta en TCP (Protocolo de control de transmisión) que tiene estado, esto está permitido.	**GIG1**
GIS-5.9.9	Todos los cambios en la infraestructura de red se registrarán en un registro en el que se indique: a. La fecha y hora de los cambios; b. Motivo y descripción de los cambios, incluidos los valores inicial y final; y c. ID de cuenta de usuario que realizó y/o autorizó los cambios.	**GIG1**
GIS-5.10	**Teletrabajo e informática móvil**	
GIS-5.10.1	No se permitirá el teletrabajo, excepto en circunstancias en las que pueda garantizarse la seguridad del punto final.	**GIG1**
GIS-5.10.2	Se establecerá una política formal y se adoptarán medidas de seguridad de apoyo para proteger contra los riesgos del uso de instalaciones informáticas y de comunicación móviles.	**GIG1**
GIS-6	**Proveedores de servicios**	**GIG**
GIS-6.1	**Relaciones con los proveedores de servicios**	
GIS-6.1.1	La asignación de responsabilidad entre un Proveedor de Servicios y la Empresa de Juego para gestionar los controles de seguridad no exime a una Empresa de Juego de la responsabilidad de garantizar que los datos confidenciales estén debidamente protegidos de acuerdo con los requisitos aplicables.	**GIG1**
GIS-6.1.2	Se acordarán políticas y procedimientos claros entre el Proveedor de servicios y la Empresa de juego para todos los requisitos de seguridad, y las responsabilidades de operación, gestión e informes se definirán y comprenderán claramente para cada requisito aplicable.	**GIG2**

GIS-6.1.3	Cuando se compartan datos sensibles con proveedores de servicios, se establecerán acuerdos formales de tratamiento de datos que establezcan los derechos y obligaciones de cada parte en relación con la protección de los datos sensibles, entre ellos: a. El objeto y la duración del tratamiento; b. La naturaleza y finalidad del tratamiento; c. El tipo de datos que se van a tratar; d. Cómo se almacenan los datos; e. El detalle de la seguridad que comprende los datos; f. Los medios utilizados para transferir los datos de una empresa de juegos a otra; g. Los medios utilizados para recuperar datos sobre ciertas personas; h. El método para garantizar que se cumpla un programa de retención; i. Los medios utilizados para eliminar o eliminar los datos; y j. Las categorías de datos.	**GIG2**
GIS-6.2	**Comunicaciones con proveedores de servicios**	
GIS-6.2.1	El GPE deberá ser capaz de comunicarse de forma segura con los proveedores de servicios mediante cifrado y autenticación sólida.	**GIG1**
GIS-6.2.2	Todos los eventos de inicio de sesión que involucren a los proveedores de servicios se registrarán en un archivo de auditoría.	**GIG1**
GIS-6.2.3	La comunicación con los proveedores de servicios no interferirá ni degradará las funciones normales del GPE.	**GIG1**
GIS-6.2.4	Los datos del Proveedor de Servicios no afectarán a las comunicaciones de los usuarios.	**GIG1**
GIS-6.2.5	Los proveedores de servicios estarán en una red segmentada separada de los segmentos de red que alojan las conexiones de los usuarios.	**GIG1**
GIS-6.2.6	Los juegos se desactivarán en todas las conexiones de red, excepto en las del GPE.	**GIG1**
GIS-6.2.7	El GPE no encaminará los paquetes de datos de los proveedores de servicios directamente a el GPE y viceversa.	**GIG1**
GIS-6.2.8	El GPE no actuará como enrutador IP entre el GPE y los proveedores de servicios.	**GIG1**
GIS-6.2.9	Se impedirá que los proveedores de servicios no autorizados vean o alteren los datos confidenciales.	**GIG1**
GIS-7	**Controles técnicos**	**GIG**
GIS-7.1	**Requisitos del Servicio de Nombres de Dominio (DNS)**	
GIS-7.1.1	La Empresa de Juego utilizará un servidor DNS primario seguro y un servidor DNS secundario seguro que estén lógica y físicamente separados entre sí, mejorando la resistencia contra puntos únicos de fallo y posibles ataques.	**GIG2**
GIS-7.1.2	El servidor DNS primario deberá estar ubicado físicamente en un centro de datos seguro o en un host virtualizado en un hipervisor debidamente protegido o equivalente para evitar el acceso no autorizado.	**GIG2**
GIS-7.1.3	El acceso lógico y físico a los servidores DNS se restringirá al personal autorizado a través de la autenticación multifactor (MFA), lo que garantiza que solo los usuarios autenticados puedan acceder a los servidores DNS y que los registros DNS se mantengan seguros contra cambios maliciosos y no autorizados.	**GIG2**
GIS-7.1.4	No se permitirán las transferencias de zona a hosts arbitrarios. Esta restricción evita que partes no autorizadas accedan o repliquen los datos de la zona DNS, lo que reduce el riesgo de exposición o manipulación de datos.	**GIG2**
GIS-7.1.5	Se requiere un método para evitar la corrupción de caché, como las extensiones de seguridad de DNS (DNSSEC).	**GIG2**
GIS-7.1.6	El bloqueo del registro debe estar en su lugar, por lo que cualquier solicitud para cambiar los servidores DNS deberá verificarse manualmente.	**GIG2**
GIS-7.2	**Controles criptográficos**	
GIS-7.2.1	Se desarrollará e implementará una política sobre el uso de controles criptográficos para la protección de datos confidenciales, asegurando que todos los controles criptográficos utilicen módulos criptográficos para una ejecución y protección seguras.	**GIG1**
GIS-7.2.2	El grado de cifrado utilizado deberá ser adecuado a la sensibilidad de los datos.	**GIG1**

GIS-7.2.3	El uso de métodos de cifrado se revisará periódicamente para verificar que los algoritmos de cifrado y las longitudes de clave actuales son seguros.	**GIG1**
GIS-7.2.4	El método de cifrado incluirá el uso de diferentes claves de cifrado, de modo que los algoritmos de cifrado puedan modificarse o sustituirse para corregir las deficiencias lo antes posible. Las demás metodologías se examinarán caso por caso.	**GIG1**
GIS-7.2.5	La gestión de las claves de cifrado a lo largo de todo su ciclo de vida seguirá procesos definidos establecidos por la Empresa de Juego.	**GIG1**
GIS-7.2.6	La Empresa de Juego establecerá procedimientos para obtener o generar claves de cifrado, asegurándose de que solo el personal autorizado participe en el proceso.	**GIG1**
GIS-7.2.7	Las claves de cifrado se almacenarán en un medio de almacenamiento seguro y redundante después de haber sido cifradas a través de un método de cifrado diferente y/o utilizando una clave de cifrado diferente.	**GIG1**
GIS-7.2.8	Se establecerán procedimientos para controlar las fechas de caducidad de las claves de cifrado, cuando proceda.	**GIG1**
GIS-7.2.9	Se definirán procedimientos para revocar rápidamente las claves de cifrado en caso de compromiso, pérdida o acceso no autorizado.	**GIG1**
GIS-7.2.10	Se establecerán procedimientos para cambiar de forma segura el conjunto de claves de cifrado actual, incluida la generación de nuevas claves y la retirada de las antiguas.	**GIG1**
GIS-7.2.11	La Empresa de Juego implementará procedimientos para recuperar los datos protegidos con claves de cifrado revocadas o caducadas durante un período definido después de que las claves dejen de ser válidas.	**GIG1**
GIS-7.3	**Endurecimiento de componentes críticos del sistema**	
GIS-7.3.1	Las configuraciones de los componentes críticos del sistema deben establecerse, documentarse, implementarse, supervisarse y revisarse.	**GIG1**
GIS-7.3.2	Los procedimientos de configuración para los componentes críticos del sistema abordarán todas las vulnerabilidades de seguridad conocidas y serán coherentes con las mejores prácticas aceptadas por la industria para el endurecimiento del sistema.	**GIG1**
GIS-7.3.3	La idoneidad y eficacia de las medidas adoptadas para endurecer los componentes críticos del sistema se evaluarán periódicamente y, si procede, se introducirán cambios para mejorar el endurecimiento.	**GIG2**
GIS-7.3.4	Todos los parámetros de configuración predeterminados o estándar se eliminarán de todos los componentes críticos del sistema en los que se presente un riesgo para la seguridad.	**GIG1**
GIS-7.3.5	Solo se implementará una función principal por servidor para evitar que coexistan en el mismo servidor funciones que requieran diferentes niveles de seguridad.	**GIG1**
GIS-7.3.6	Se implementarán características de seguridad adicionales para cualquier servicio, protocolo o demonio requerido que se considere inseguro.	**GIG1**
GIS-7.3.7	Los parámetros de seguridad del sistema se configurarán para evitar el uso indebido.	**GIG1**
GIS-7.3.8	Se eliminarán todas las funcionalidades innecesarias, como scripts, controladores, características, subsistemas, sistemas de archivos y servidores web innecesarios.	**GIG1**
GIS-7.4	**Generación y almacenamiento de registros**	
GIS-7.4.1	Deben establecerse y documentarse procedimientos para monitorear, administrar y responder de manera centralizada a las actividades, excepciones, fallas y eventos adversos de los usuarios.	**GIG2**
GIS-7.4.2	Los informes o registros de seguridad deben estar predefinidos y generados en cada componente crítico del sistema para monitorear y rectificar anomalías, fallas y alertas.	**GIG1**
GIS-7.4.3	Los informes o registros de seguridad deben estar protegidos contra la manipulación y el acceso no autorizado.	**GIG2**
GIS-7.4.4	Los informes o registros de seguridad se revisarán periódicamente según lo requiera la Empresa de Juego y/o el organismo regulador.	**GIG1**
GIS-8	**Acceso remoto y cortafuegos**	**GIG**
GIS-8.1	**Seguridad de acceso remoto**	
GIS-8.1.1	La seguridad del acceso remoto se revisará caso por caso, junto con la implementación de la tecnología actual y la aprobación del organismo regulador.	**GIG1**
GIS-8.1.2	Los métodos de acceso a distancia deberán estar debidamente protegidos y gestionados.	**GIG1**

GIS-8.1.3	El GPE tendrá la capacidad de habilitar o deshabilitar el acceso remoto, y el estado predeterminado se establecerá en deshabilitado	**GIG1**
GIS-8.1.4	El acceso remoto solo aceptará las conexiones remotas permitidas por la aplicación de firewall y la configuración del sistema.	**GIG1**
GIS-8.1.5	El acceso remoto se limitará únicamente a las funciones de la aplicación necesarias para que los usuarios realicen sus tareas laborales.	**GIG1**
GIS-8.1.6	No se permite ninguna funcionalidad de administración de usuarios remotos no autorizada (agregar usuarios, cambiar permisos, etcétera).	**GIG1**
GIS-8.1.7	Está prohibido el acceso remoto no autorizado al sistema operativo o a cualquier base de datos que no sea la recuperación de información utilizando las funciones existentes.	**GIG1**
GIS-8.1.8	El GPE mantendrá un registro de actividad en el que se represente toda la información de acceso a distancia. Los registros de acceso remoto incluirán, como mínimo, lo siguiente: a. ID de cuenta de usuario que realizó y/o autorizó el acceso remoto, incluida la verificación de la autorización; b. Direcciones IP remotas, números de puerto, protocolos y, cuando sea posible, direcciones MAC; c. Hora y fecha en que se realizó la conexión y duración de la conexión; d. Motivo del acceso remoto y descripción del trabajo a realizar; e. Actividad mientras se está conectado, incluidas las áreas específicas a las que se accede y los cambios realizados.	**GIG1**
GIS-8.2	**Seguridad del cortafuegos**	
GIS-8.2.1	Todas las comunicaciones, incluido el acceso remoto, deberán pasar a través de al menos un cortafuegos (firewall) aprobado a nivel de aplicación. Esto incluye las conexiones hacia y desde cualquier host que no sea del sistema utilizado por la Empresa de Juego.	**GIG1**
GIS-8.2.2	El cortafuegos se situará en el límite de dos dominios de seguridad cualesquiera.	**GIG1**
GIS-8.2.3	Un dispositivo en el mismo dominio de difusión que el host del sistema no debe tener una instalación que permita establecer una ruta de red alternativa que omita el firewall.	**GIG2**
GIS-8.2.4	Cualquier ruta de red alternativa que exista con fines de redundancia también deberá pasar a través de al menos un firewall a nivel de aplicación.	**GIG1**
GIS-8.2.5	Solo las aplicaciones relacionadas con el firewall pueden residir en el firewall.	**GIG1**
GIS-8.2.6	Las cuentas de usuario en el firewall deben estar limitadas (por ejemplo, solo administradores de red o sistema).	**GIG1**
GIS-8.2.7	El cortafuegos rechazará todas las conexiones, excepto las que hayan sido específicamente aprobadas.	**GIG1**
GIS-8.2.8	El cortafuegos rechazará todas las conexiones de destinos que no puedan residir en la red desde la que se originó el mensaje (por ejemplo, direcciones RFC1918 en el lado público de un cortafuegos de Internet).	**GIG1**
GIS-8.2.9	El cortafuegos solo permitirá el acceso remoto mediante cifrado.	**GIG1**
GIS-8.2.10	El cortafuegos deberá ser capaz de registrar la información de auditoría de forma que se preserve y proteja la información contra pérdidas o alteraciones. Esta información incluye lo siguiente: a. Todos los cambios en la configuración del cortafuegos; b. Todos los intentos de conexión exitosos y fallidos a través del firewall; y c. Las direcciones IP de origen y destino, los números de puerto, los protocolos y las direcciones MAC.	**GIG1**
GIS-8.2.11	Para intentos de conexión fallidos a través del firewall, se puede utilizar un parámetro configurable para denegar más solicitudes de conexión y notificar al administrador del sistema, en caso de que se exceda el umbral predefinido.	**GIG1**
GIS-9	**Revisión de la gestión de activos críticos y cambios**	**GIG**
GIS-9.1	**Gestión de activos**	
GIS-9.1.1	Se contabilizarán todos los activos físicos o lógicos que contengan, procesen o comuniquen datos sensibles, incluidos los que componen el GPE.	**GIG1**
GIS-9.1.2	Existirán procedimientos para agregar nuevos activos y retirar activos del servicio.	**GIG1**
GIS-9.1.3	Se incluirá una política sobre el uso aceptable de los activos asociados con el GPE.	**GIG1**

GIS-9.1.4	El propietario designado de cada activo deberá: a. Garantizar que la información y los activos se clasifiquen adecuadamente en función de sus requisitos de confidencialidad, integridad, responsabilidad y disponibilidad; y b. Definir las restricciones de acceso y las clasificaciones en función de los criterios de clasificación establecidos y el principio de mínimo privilegio.	**GIG1**
GIS-9.1.5	Deberá existir un procedimiento para garantizar que la contabilidad registrada de los activos se compare con los activos reales al menos una vez al año o a intervalos requeridos por el organismo regulador y se tomen las medidas apropiadas con respecto a las discrepancias.	**GIG1**
GIS-9.1.6	La protección contra copia para evitar la duplicación o modificación no autorizada del software con licencia puede implementarse siempre que: a. El método de protección contra copias está completamente documentado y verificado que la protección funciona como se describe; o b. El programa o componente implicado en la aplicación de la protección contra copias puede verificarse individualmente mediante la metodología aprobada por el organismo regulador.	**GIG1**
GIS-9.1.7	Para garantizar su disponibilidad continua, integridad y confidencialidad de la información, los activos deben ser correctamente mantenidos, inspeccionados y revisados a intervalos regulares para garantizar que estén libres de defectos o mecanismos que puedan interferir con su funcionamiento.	**GIG1**
GIS-9.1.8	Los medios de almacenamiento se gestionarán a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la Empresa del juego.	**GIG1**
GIS-9.1.9	Los activos se dispondrán de forma segura y protegida utilizando procedimientos documentados.	**GIG1**
GIS-9.1.10	Los datos sensibles almacenados en componentes críticos del sistema, dispositivos o en cualquier otro medio de almacenamiento se eliminarán cuando ya no sean necesarios.	**GIG1**
GIS-9.1.11	Antes de su eliminación o reutilización, se comprobará que los activos que contengan medios de almacenamiento para asegurarse de que cualquier software con licencia, así como los datos sensibles, se han eliminado o sobrescrito de forma segura.	**GIG1**
GIS-9.2	**Registro de Activos Críticos (CAR)**	
GIS-9.2.1	Se desarrollará y mantendrá un CAR para cualquier activo que afecte a la funcionalidad del GPE o que influya en la forma en que el entorno almacena o gestiona los datos sensibles.	**GIG1**
GIS-9.2.2	La estructura del CAR incluirá los componentes de hardware y software, así como las interrelaciones y dependencias de los componentes.	**GIG1**
GIS-9.2.3	Se documentarán en el CAR los siguientes elementos mínimos para cada activo: a. Un ID único que se asigna a cada activo individual; b. El nombre/definición de cada activo; c. Un número de versión del activo enumerado; d. Identificación de las características de los activos (por ejemplo, componente del sistema, base de datos, máquina virtual, hardware); e. El "propietario" responsable del activo; f. La ubicación geográfica de los activos de hardware; g. Códigos de relevancia sobre el papel del activo en el logro o aseguramiento de los criterios de clasificación.	**GIG1**
GIS-9.2.4	Los criterios de clasificación son los siguientes: a. Confidencialidad de datos sensibles (por ejemplo, información de identificación y transacciones); b. Integridad del sistema, específicamente cualquier activo que afecte la funcionalidad del sistema y/o tenga una influencia en la forma en que se almacenan y/o manejan los datos confidenciales; c. Disponibilidad de datos sensibles; y d. Responsabilidad de la actividad del usuario y cuánta influencia tiene el activo en la actividad del usuario.	**GIG1**
GIS-9.2.5	A cada uno de los criterios de clasificación se le asignará un código de relevancia de: a. 1 - Sin relevancia: El activo no puede tener un impacto negativo en los criterios; b. 2 - Cierta relevancia: El activo puede tener un impacto en los criterios; o	**GIG1**

	c. 3 - Relevancia sustancial: Los criterios están relacionados o dependen del activo.	
GIS-9.3	**Gestión del cambio**	
GIS-9.3.1	Se implementará un CMP para gestionar las actualizaciones del GPE y sus componentes críticos del sistema en función de la propensión a las actualizaciones frecuentes del sistema y la tolerancia al riesgo elegida. En el caso de un GPE que requiere actualizaciones frecuentes, se puede utilizar un CMP basado en el riesgo para permitir una mayor eficiencia en la implementación de actualizaciones. Los CMP basados en el riesgo suelen incluir una categorización de los cambios propuestos en función del impacto normativo y definen los procedimientos de certificación asociados para cada categoría.	**GIG1**
GIS-9.3.2	Los procedimientos de cambio de programa deberán ser adecuados para garantizar que solo se implementen en el GPE las versiones autorizadas de los programas y sus modificaciones.	**GIG1**
GIS-9.3.3	Se debe establecer un mecanismo de control de versiones de software adecuado para todos los componentes de software, el código fuente y los controles binarios.	**GIG1**
GIS-9.3.4	Se conservará un registro CML de todas las nuevas instalaciones y/o modificaciones del sistema, incluidas: a. La fecha de la instalación o modificación; b. Detalles del motivo o la naturaleza de la instalación o el cambio, como nuevo software, reparación del servidor, modificaciones significativas de la configuración; c. Los componentes que se van a cambiar, incluido el número de identificación único del CAR, la información de la versión y, si el componente que se cambia es de hardware, la ubicación física de este componente; d. La identidad del usuario o usuarios que realizan la instalación o modificación; y e. La identidad del/de los usuario/s responsable de autorizar la instalación o modificación.	**GIG1**
GIS-9.3.5	Se debe implementar una estrategia para cubrir la posibilidad de una instalación incorrecta o un problema de campo con uno o más cambios implementados: a. Cuando una parte externa, como una tienda de aplicaciones, sea una parte interesada en el proceso de lanzamiento, esta estrategia cubrirá la gestión de lanzamientos a través de la parte externa. Esta estrategia puede tener en cuenta la gravedad del problema. b. De lo contrario, esta estrategia abarcará la vuelta a la última implementación (plan de reversión), incluidas copias de seguridad completas de versiones anteriores de software y una prueba del plan de reversión antes de la implementación en el GPE.	**GIG1**
GIS-9.3.6	Se establecerá una política que aborde los procedimientos de cambio de emergencia. Los cambios de emergencia deben ser aprobados, ensayados, documentados y monitoreados.	**GIG1**
GIS-9.3.7	Se establecerán procedimientos para probar y migrar los cambios, incluida la identificación del personal autorizado para la aprobación antes de la publicación.	**GIG1**
GIS-9.3.8	Habrá segregación de funciones dentro del proceso de lanzamiento.	**GIG1**
GIS-9.3.9	Se conservará documentación técnica y de usuario, como manuales y guías de usuario, en la que se describan los sistemas en uso y el funcionamiento, incluido el hardware.	
GIS-9.3.10	Deberán establecerse procedimientos que garanticen que la documentación técnica y de usuario se actualice como resultado de un cambio.	**GIG1**
GIS-9.4	**Ciclo de vida de desarrollo del sistema**	
GIS-9.4.1	La adquisición y el desarrollo de nuevo software seguirán los procesos definidos establecidos por la Empresa de Juego y/o el organismo regulador.	**GIG1**
GIS-9.4.2	El GPE estará separada lógica y físicamente de los entornos de desarrollo y prueba, de modo que no pueda existir una conexión directa entre el GPE y cualquier otro entorno.	**GIG1**
GIS-9.4.3	En su caso, se establecerá la delegación de responsabilidades.	**GIG1**
GIS-9.4.4	La Empresa de Juego establecerá y documentará un método para desarrollar software de forma segura, lo que incluye seguir los estándares de la industria y las mejores prácticas para la codificación.	**GIG1**
GIS-9.4.5	Las consideraciones sobre los GIS se integrarán a lo largo de todo el ciclo de vida del desarrollo de software, desde la recopilación inicial de requisitos hasta la implementación y el mantenimiento.	**GIG1**
GIS-9.4.6	La metodología de ensayo documentada incluirá disposiciones para: a. Verifique que el software de prueba no esté implementado en el GPE;	**GIG1**

	b. Seleccione, proteja y administre adecuadamente los datos de prueba; y c. Evite el uso de datos confidenciales reales u otros datos de producción sin procesar en las pruebas.	
GIS-9.4.9	Toda la documentación relacionada con el desarrollo de software y aplicaciones estará disponible y conservada durante todo su ciclo de vida.	**GIG1**
GIS-9.5	**Gestión de parches**	
GIS-9.5.1	La Empresa de Juego tendrá políticas de gestión de parches acordadas con el organismo regulador, ya sea desarrolladas y respaldadas por la Empresa de Juego o por un Proveedor de Servicios.	**GIG1**
GIS-9.5.2	La Empresa de Juego supervisará y aplicará parches a todos los Componentes Críticos del Sistema involucrados en la recopilación, el procesamiento, el almacenamiento y la transmisión de datos confidenciales.	**GIG1**
GIS-9.5.3	Siempre que sea posible, todos los parches se probarán en un entorno de desarrollo y pruebas configurado de forma idéntica al GPE de destino.	**GIG1**
GIS-9.5.4	En circunstancias en las que las pruebas de parche no puedan realizarse a fondo a tiempo para cumplir con los plazos del nivel de gravedad de la alerta y si lo autoriza el organismo regulador, las pruebas de parche se gestionarán mediante el riesgo, ya sea aislando o eliminando el componente no probado de la red o aplicando el parche y las pruebas a posteriori.	**GIG1**

ANEXO I: CALIFICACIÓN DE LOS RIESGOS

El siguiente sistema de calificación, basado en el *Sistema Común de Calificación de Vulnerabilidades (CVSS)* y la *ISO/IEC 31010 Gestión de Riesgos – Técnicas de Evaluación de Riesgos*, se utilizará para evaluar la gravedad de las amenazas y vulnerabilidades de seguridad. Intenta asignar calificaciones de gravedad a las amenazas y vulnerabilidades, lo que permite priorizar las respuestas y los recursos según el nivel de gravedad. Las calificaciones se calculan en función de una fórmula que depende de varias métricas que se aproximan a la facilidad de explotación y al impacto de la explotación.

Métricas base: Estas métricas representan las cualidades más fundamentales e inmutables intrínsecas a la vulnerabilidad.

a. Vector de acceso: Mide la distancia a la que puede estar un atacante para atacar un objetivo.

b. Complejidad de acceso: mide la complejidad del ataque necesario para explotar la vulnerabilidad una vez que un atacante ha obtenido acceso al sistema objetivo.

c. Autenticación: Midel número de veces que un atacante se autenticará en el sistema objetivo para explotar la vulnerabilidad.

d. Impacto en la integridad: midel impacto en la integridad de una explotación exitosa de la vulnerabilidad en el sistema objetivo.

e. Impacto en la confidencialidad: midel impacto en la confidencialidad de una explotación exitosa de la vulnerabilidad en el sistema objetivo.

f. Impacto en la disponibilidad: midel impacto en la disponibilidad de una explotación exitosa de la vulnerabilidad en el sistema objetivo.

Métricas temporales: Estas métricas representan las características dependientes del tiempo que evolucionan a lo largo de la vida útil de la vulnerabilidad.

a. Explotabilidad: Mide la complejidad del proceso para explotar la vulnerabilidad en el sistema objetivo.

b. Nivel de corrección: midel nivel de una solución disponible.

c. Confianza del informe: Midel grado de confianza en la existencia de las amenazas y la credibilidad de su informe.

Clasificaciones de gravedad:

Severidad	Puntuación	Acción requerida
Crítico	**9.0 – 10.0**	Una vulnerabilidad crítica que debe abordarse de inmediato.
Alto	**7.0 – 8.9**	Una vulnerabilidad que presenta un alto riesgo y que requiere atención inmediata y planificación para remediarla en un futuro próximo.
Medio	**4.0 – 6.9**	Una vulnerabilidad que presenta un riesgo medio y requiere investigación y planificación para abordarla durante futuras mejoras de seguridad del sistema.
Bajo	**0.1 – 3.9**	Una vulnerabilidad que presenta un riesgo bajo y que debe abordarse durante el mantenimiento rutinario del sistema.
Información	**0.0**	Una observación o hallazgo digno de mención para una posible mejora para cumplir con las mejores prácticas de la industria.

DEFINICIONES DE TÉRMINOS

Término	Descripciones
Acceso	Posibilidad de hacer uso de cualquier recurso del GPE.
Control de acceso	El proceso de otorgar o denegar solicitudes específicas para obtener y usar datos confidenciales y servicios relacionados específicos de un sistema; y para entrar en instalaciones físicas específicas que albergan infraestructuras críticas de redes o sistemas.
Protocolo de resolución de direcciones (ARP)	Protocolo utilizado para traducir direcciones IP en direcciones MAC para admitir la comunicación en una red de área local inalámbrica o cableada.
Controles administrativos	Políticas, procedimientos y directrices implementados por una Empresa de Juego para gestionar sus GISMS.
Estándares de cifrado avanzados (AES)	Cifrado de bloques simétricos que puede cifrar (cifrar) y descifrar (descifrar) información.
Algoritmo	Un conjunto finito de instrucciones inequívocas realizadas en una secuencia prescrita para lograr un objetivo, especialmente una regla o procedimiento matemático utilizado para calcular un resultado deseado. Los algoritmos son la base de la mayoría de la programación informática.
Aplicación	Software informático diseñado para ayudar a un usuario a realizar una tarea específica.
Auditoría	Un registro que muestra quién ha accedido a un sistema y qué operaciones ha realizado el usuario durante un período determinado.
Autenticación	Verificar la identidad de un usuario, proceso, paquete de software o dispositivo, a menudo como requisito previo para permitir el acceso a los recursos del GPE
Disponibilidad	Garantizar el acceso oportuno y fiable a la información y su utilización.
Copia de seguridad	Una copia de los archivos y programas realizados para facilitar la recuperación si es necesario.
Biometría	Un dato de identificación biológica, como huellas dactilares o patrones de retina.
Puente	Divide las redes para reducir el tráfico general de la red. Un puente permite o impide que los datos pasen a través de él mediante la lectura de la dirección MAC.
Aplicaciones de la Empresa	Aplicaciones que funcionan como un servicio compartido para que los usuarios recopilen, procesen, mantengan, utilicen, compartan, difundan o eliminen datos sensibles dentro del GPE con fines de auditoría de cumplimiento y respuesta a incidentes de seguridad.
Plan de Continuidad del Negocio y Recuperación ante Desastres	Un plan para procesar aplicaciones críticas y prevenir la pérdida de datos en caso de una falla importante de hardware o software o la destrucción de las instalaciones.
Corrupción de caché	Un ataque en el que el atacante inserta datos corruptos en la base de datos de caché del Servicio de nombres de dominio (DNS).
Tecnología de las Comunicaciones	Cualquier método utilizado, y los componentes empleados, para facilitar la transmisión y recepción de información, incluida la transmisión y recepción por sistemas que utilizan redes alámbricas, inalámbricas, por cable, de radio, de microondas, de luz, de fibra óptica, de satélite o de datos informáticos, incluidas Internet e intranets.
Cumple	Se consideró que la política y las pruebas examinadas cumplían plenamente con el GLI-GSF.
Confidencialidad	Preservar las restricciones autorizadas de acceso y divulgación de la información, incluidos los medios para proteger la privacidad personal y la información sujeta a derechos de propiedad.
Plan de contingencia	Política y procedimientos de administración diseñados para mantener o restaurar las operaciones de juego, posiblemente en una ubicación alternativa, en caso de emergencias, fallas del sistema o desastres.

Término	Descripciones
Componente crítico del sistema	Cualquier hardware, software, tecnología de comunicaciones, otros equipos o componentes implementados en un GPE para permitir la participación de los usuarios en los juegos, y cuya falla o compromiso pueda conducir a la pérdida de los derechos de los usuarios, ingresos gubernamentales o acceso no autorizado a los datos utilizados para generar informes para el organismo regulador. Ejemplos de componentes críticos del sistema incluyen, pero no se limitan a: • Componentes que registran, almacenan, procesan, comparten, transmiten o recuperan datos sensibles. • Componentes que generan, transmiten o procesan números aleatorios utilizados para determinar el resultado de juegos y eventos. • Componentes que almacenan los resultados o el estado actual del juego, la apuesta o los fondos disponibles de un usuario. • Programas de software que controlan comportamientos relacionados con cualquier norma técnica y/o requisito reglamentario aplicable, como ejecutables, librerías, configuraciones de juegos o sistemas, archivos del sistema operativo, componentes que controlan los informes requeridos del sistema y elementos de bases de datos que afectan a los juegos o a las operaciones del sistema. • Puntos de entrada y salida de los componentes anteriores, incluidos otros sistemas que se comunican directamente con los componentes críticos del sistema. • Tecnología de las comunicaciones y redes que transmiten datos sensibles. • Redes y sistemas corporativos que interactúan con el GPE y desde los cuales los atacantes podrían usar para moverse lateralmente hacia el GPE, incluidas las redes de los casinos corporativos y las redes corporativas de los operadores en línea.
Módulo criptográfico	Hardware, software, firmware o una combinación de los mismos que implementan funciones criptográficas como cifrado, descifrado, firmas, hashing y gestión de claves. El objetivo principal de un módulo criptográfico es proporcionar un procesamiento y almacenamiento seguros de claves y operaciones.
Integridad de los datos	La propiedad de que los datos son precisos y coherentes y no han sido alterados de manera no autorizada durante el almacenamiento, durante el procesamiento y mientras están en tránsito.
Denegación de servicio distribuido (DDoS)	Un tipo de ataque en el que se utilizan varios sistemas comprometidos, generalmente infectados con un programa de software destructivo, para atacar un solo sistema. Las víctimas de un ataque DDoS consisten tanto en el sistema objetivo final como en todos los sistemas utilizados y controlados maliciosamente por el hacker en el ataque distribuido.
Servicio de nombres de dominio (DNS)	La base de datos de Internet distribuida globalmente que (entre otras cosas) asigna nombres de máquinas a números IP y viceversa.
Dominio	Un grupo de equipos y dispositivos en una red que se administran como una unidad con reglas y procedimientos comunes.
Protocolo de configuración dinámica de host (DHCP)	Un servicio de red que permite a los dispositivos solicitar una configuración desde un punto central. Primero, una solicitud se transmite a través del segmento de red, luego los servidores responden a esa máquina específica con una dirección, por cuánto tiempo es válida esa dirección y otros detalles pertinentes.
Ancho de banda efectivo	La cantidad de datos que realmente se pueden transferir a través de una red por unidad de tiempo. El ancho de banda efectivo a través de Internet suele ser considerablemente menor que el ancho de banda de cualquiera de los enlaces constituyentes.

Término	Descripciones
Encriptación	La conversión de datos en un formulario, llamado texto cifrado, que no puede ser fácilmente entendido por personas no autorizadas. Cuando el cifrado no sea posible debido a una limitación tecnológica o de rendimiento, se aplicarán en su lugar otras medidas de protección razonables, que se revisarán caso por caso.
Clave de cifrado	Una clave que se ha cifrado para ocultar el valor del texto sin formato subyacente.
Aplicaciones expuestas externamente	Aplicaciones orientadas al público y detectables mediante reconocimiento y exploración de la red desde la Internet pública fuera de la red de la empresa. Esto no se aplica a las aplicaciones destinadas al uso de los usuarios.
Activos de la empresa expuestos al exterior	Activos orientados al público y detectables mediante el reconocimiento del Sistema de Nombres de Dominio y el escaneado de la red desde la Internet pública fuera de la red de la empresa. Esto no se aplica a los activos destinados al uso de los usuarios.
Cortafuegos	Un componente de un sistema informático o red que está diseñado para bloquear el acceso o el tráfico no autorizados y, al mismo tiempo, permitir la comunicación externa.
Empresas de Juego	Entidades que supervisan o están integradas en la funcionalidad de un GPE, incluida la gestión de datos sensibles.
Seguridad de la información de juego (GIS)	Proteger los datos confidenciales y los componentes críticos del sistema contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados con el fin de proporcionar integridad, confidencialidad y disponibilidad.
Sistema de gestión de seguridad de la información del juego (GISMS)	Un sistema de gestión definido y documentado que consiste en un conjunto de políticas, procesos y sistemas para gestionar los riesgos de los datos sensibles de una Empresa de Juego, activos, y componentes críticos del sistema dentro de un GPE, con el objetivo de garantizar niveles aceptables de riesgo de GIS.
Entorno de Producción del Juego (GPE)	El entorno operativo en el que las actividades de juego y los servicios relacionados se llevan a cabo, se gestionan y se ofrecen a los clientes en directo o en tiempo real. Abarca la infraestructura física y virtual, los sistemas, el software y los procesos necesarios para facilitar diversas formas de juego y/o gestionar datos confidenciales, así como los sistemas y la infraestructura de la oficina auxiliar (backend) que sirven de interfaz y/o apoyo a las actividades de juego.
Portal	Cualquier dispositivo, sistema o aplicación de software que pueda realizar la función de traducir datos de un formato a otro. La característica clave de un portal de enlace es que convierte el formato de los datos, no los datos en sí.
Política de GIS	Un documento que delinea la estructura de gestión de la seguridad y asigna claramente las responsabilidades de seguridad y sienta las bases necesarias para medir de forma fiable el progreso y el cumplimiento.
Incidente de GIS	Un suceso que real o potencialmente pone en peligro la integridad, confidencialidad, o disponibilidad de un GPE o de los datos confidenciales que el GPE procesa, almacena o transmite, o que constituye una violación o amenaza inminente de violación de las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable.
Plan de respuesta a incidentes de GIS	La documentación de un conjunto predeterminado de instrucciones o procedimientos cuando se encuentra un ciberataque malicioso contra el GPE de una empresa de juego.
Pertenencia a grupos	Un método de organización de cuentas de usuario en una sola unidad (por puesto de trabajo) mediante el cual el acceso a las funciones del sistema puede modificarse a nivel de unidad y los cambios surten efecto para todas las cuentas de usuario asignadas a la unidad.
Algoritmo hash	Función que convierte una cadena de datos en una salida de cadena alfanumérica de longitud fija.

Término	Descripciones
Protocolo de transporte de hipertexto (HTTP)	El protocolo subyacente utilizado para definir cómo se formatean y transmiten los mensajes, y qué acciones deben realizar los servidores y navegadores en respuesta a varios comandos.
Concentrador (hub)	Conecta dispositivos en una red de par trenzado. Una hub no realiza ninguna tarea además de la regeneración de señales.
Integridad	Protección contra la modificación o destrucción indebidas de la información, e incluye garantizar el no repudio y la autenticidad de la información.
Sistema de detección de intrusos/Sistema de prevención de intrusiones (IDS/IPS)	Un sistema que inspecciona toda la actividad de la red entrante y saliente e identifica patrones sospechosos que pueden indicar un ataque a la red o al sistema por parte de alguien que intenta entrar en un sistema o ponerlo en peligro. Utilizada en seguridad informática, la detección de intrusiones se refiere al proceso de monitorear las actividades de la computadora y la red y analizar esos eventos para buscar signos de intrusión en el GPE.
Internet	Un sistema interconectado de redes que conecta computadoras de todo el mundo a través de TCP/IP.
Dirección de protocolo de Internet (dirección IP)	Número único de un equipo que se utiliza para determinar dónde se deben entregar los mensajes transmitidos por Internet. La dirección IP es análoga a un número de casa para el correo postal ordinario.
Seguridad de IP (IPSec)	Un conjunto de protocolos para proteger las comunicaciones de Protocolo de Internet (IP) mediante la autenticación y el cifrado de cada paquete IP de un flujo de datos. IPsec también incluye protocolos para establecer la autenticación mutua entre los agentes al inicio de la sesión y la negociación de las claves cifradas que se utilizarán durante la sesión.
Kerberos	Protocolo de autenticación de red diseñado para proporcionar una autenticación sólida para aplicaciones cliente/servidor mediante criptografía de clave secreta.
Clave	Valor utilizado para controlar las funciones criptográficas, como el descifrado, cifrado, firmas, hashing, etc.
Gestión de claves	Actividades que impliquen el manejo de claves cifradas y otros parámetros de seguridad relacionados (por ejemplo, contraseñas) durante todo el ciclo de vida de las claves, incluida su generación, almacenamiento, establecimiento, entrada y salida, y puesta a cero.
Utilización de enlaces	El porcentaje de tiempo que un enlace de comunicaciones está involucrado en la transmisión de datos.
Código de autenticación de mensajes (MAC)	Suma de comprobación criptográfica de los datos que utiliza una clave simétrica para detectar modificaciones accidentales e intencionadas de los datos.
Malware	Un programa que se inserta en un sistema, generalmente de forma encubierta, con la intención de comprometer la integridad, confidencialidad, o disponibilidad de los datos, las aplicaciones o el sistema operativo de la víctima, o de molestar o interrumpir a la víctima.
Ataque "Man-in-The-Middle" (Intermediario)	Un ataque en el que el atacante transmite en secreto y posiblemente altera la comunicación entre dos partes que creen que se están comunicando directamente entre sí.
No conformidad mayor (MaNC)	Se ha identificado una falla fundamental (sistemática) que afecta a varios controles y significa que no se pueden cumplir las políticas generales de seguridad. Puede ser: • Una serie de no conformidades menores contra un control pueden representar una falla total del sistema y, por lo tanto, considerarse una no conformidad mayor; o • Cualquier no conformidad que resulte en el probable envío de un producto no conforme. Una condición que puede resultar en la falla o reducir materialmente la usabilidad de los productos o servicios para su propósito previsto; o

Término	Descripciones
	• Es probable que una no conformidad que el juicio y la experiencia indiquen resulte en la falla del sistema o reduzca materialmente su capacidad para asegurar procesos y productos controlados. Hasta que se resuelva, un problema de este tipo normalmente significará que la Empresa de Juego no cumple con el GLI-GSF.
Autenticación de mensajes	Medida de seguridad destinada a establecer la autenticidad de un mensaje por medio de un autenticador dentro de la transmisión derivada de ciertos elementos predeterminados del propio mensaje.
No conformidad menor (MiNC)	Un control no se ha abordado o no cumple con el GLI-GSF (no sistemático) y que el juicio y la experiencia indican que no es probable que resulte en la falla del sistema o reduzca su capacidad para asegurar procesos o productos controlados. Puede ser: • Una falla en alguna parte del sistema en relación con un control; o • Un solo lapso observado en el seguimiento de un elemento del sistema. Un curso de acción para remediar esto debe proporcionarse con un cronograma apropiado.
Código móvil	Código ejecutable que se mueve de un equipo a otro, incluyendo tanto código legítimo como código malicioso como virus informáticos.
Autenticación multifactor (MFA)	Un tipo de autenticación que utiliza dos o más de los siguientes elementos para verificar la identidad de un usuario: • Información conocida solo por el usuario (por ejemplo, una contraseña, un patrón o respuestas a preguntas de seguridad); • Un artículo poseído por un usuario (por ejemplo, un token electrónico, un token físico o una tarjeta de identificación); y • Los datos biométricos de un usuario (por ejemplo, huellas dactilares, reconocimiento facial o de voz).
Equipos de comunicación de red (NCE)	Uno o más dispositivos que controlan la comunicación de datos en un sistema, incluidos, entre otros, cables, conmutadores, puentes, concentradores, enrutadores, puntos de acceso inalámbricos y teléfonos.
Tarjeta de interfaz de red (NIC)	Mecanismo por el cual los terminales y sistemas se conectan a la red. Las NIC pueden ser tarjetas de expansión complementarias, tarjetas PCMCIA o interfaces integradas.
Observación (OBS)	Existe una política, pero no cumple plenamente con el GLI-GSF o la evidencia de respaldo (o la falta della) planteó posibles preocupaciones. Cualquier problema que pueda convertirse en una no conformidad si no se trata hasta la próxima auditoría se marca con este estado.
Contraseña	Cadena de caracteres (letras, números y otros símbolos) que se utiliza para autenticar una identidad o para verificar la autorización de acceso.
Información de identificación personal (PII)	Datos confidenciales que podrían usarse para identificar a un usuario en particular. Los ejemplos incluyen un nombre legal, fecha de nacimiento, lugar de nacimiento, número de seguro social (o número de identificación gubernamental equivalente), número de licencia de conducir, número de pasaporte, dirección residencial, número de teléfono, dirección de correo electrónico, número de instrumento de débito, número de tarjeta de crédito, número de cuenta bancaria u otra información personal si lo define el organismo regulador.
Número de identificación personal (PIN)	Un código numérico asociado a un individuo y que permite el acceso seguro a un dominio, cuenta, red, sistema, etc.
Controles Físicos y Ambientales	Las medidas implementadas para proteger los activos físicos, las instalaciones y las condiciones ambientales que albergan los sistemas e infraestructura del Entorno de Producción del Juego.
Puerto	Un punto físico de entrada o salida de un módulo que proporciona acceso al módulo para señales físicas, representadas por flujos de información lógica (los puertos separados físicamente no comparten el mismo pin o cable físico).

Término	Descripciones
Proxy	Una aplicación que "rompe" la conexión entre el cliente y el servidor. El proxy acepta ciertos tipos de tráfico que entran o salen de una red, lo procesa y lo reenvía. Esto cierra efectivamente el camino recto entre las redes internas y externas, lo que dificulta que un atacante obtenga direcciones internas y otros detalles de la red interna.
Protocolo	Conjunto de reglas y convenciones que especifican el intercambio de información entre dispositivos, a través de una red u otro medio.
Acceso remoto	Cualquier acceso desde fuera del sistema o de la red del sistema, incluido cualquier acceso desde otras redes dentro del mismo sitio o lugar.
Riesgo	La probabilidad de que una amenaza tenga éxito en su ataque contra una red o sistema.
Enrutador	Conecta redes entre sí. Un enrutador utiliza la dirección de red configurada por software para tomar decisiones de reenvío.
Protocolo de comunicación segura	Un protocolo de comunicación que proporciona la confidencialidad, autenticación y protección de la integridad del contenido adecuadas.
Secure Shell (SSH)	Permite tunelizar cualquier otro protocolo de forma segura.
Certificado de seguridad	Información, a menudo almacenada como un archivo de texto que utiliza el protocolo Transport Socket Layer (TSL) para establecer una conexión segura. Para que se cree una conexión TSL, ambas partes deben tener un certificado de seguridad válido.
Datos confidenciales	Información que debe tratarse de forma segura, como PII, datos de juego, números de validación, datos de localización, credenciales de autenticación, PIN, contraseñas, transacciones financieras, transferencias de fondos, información de seguimiento de clientes, paquetes de software, semillas y claves seguras, semillas de GNA y cualquier información que afecte a los resultados.
Servidor	Una instancia en ejecución de software que es capaz de aceptar solicitudes de clientes y el equipo que ejecuta dicho software. Los servidores operan dentro de una arquitectura cliente-servidor, en la que los "servidores" son programas informáticos que se ejecutan para atender las solicitudes de otros programas ("clientes").
Proveedores de Servicio	Entidades que ofrecen plataformas, software y servicios a las empresas de juego. Algunos ejemplos son los consultores informáticos, los proveedores de servicios gestionados, las plataformas de software como servicio (SaaS) y los proveedores de servicios en la nube. Los proveedores y vendedores de terceros también se consideran proveedores de servicios.
Identificador de conjunto de servicios (SSID)	Nombre que identifica una LAN inalámbrica 802.11 determinada.
Código de shell	Un pequeño fragmento de código utilizado como carga útil en la explotación de la seguridad. Shellcode explota la vulnerabilidad y permite a un atacante la capacidad de reducir la seguridad de la información de un sistema.
Protocolo simple de administración de red (SNMP)	Protocolo utilizado para configurar, ver y, en general, administrar dispositivos en red. Las impresoras en red, conmutadores, etc. a menudo implementan este protocolo de forma predeterminada.
Ingeniería Social	Un intento de engañar a alguien para que revele información (por ejemplo, una contraseña) que puede usarse para atacar sistemas o redes. Los ataques de ingeniería social incluyen intrusiones no técnicas en un GPE utilizando información adquirida a través de la interacción humana y se basan en trucos que se aprovechan de que un individuo no esté familiarizado con la tecnología y los protocolos emergentes.
Código fuente	Texto de la lista de comandos que se compilarán o ensamblarán en un programa informático ejecutable.
Protocolo sin estado	Un esquema de comunicaciones que trata cada solicitud como una transacción independiente que no está relacionada con ninguna solicitud

Término	Descripciones
	anterior, de modo que la comunicación consta de pares independientes de solicitudes y respuestas.
Interruptor	Conecta dispositivos en una red 802.3. Un interruptor reenvía los datos a su destino mediante la dirección MAC integrada en cada paquete.
Administrador de Sistemas	La(s) persona(s) responsable(s) de mantener el funcionamiento estable del GPE (incluida la infraestructura de software y hardware y el software de aplicación).
Controles técnicos	Los mecanismos de seguridad implementados dentro de los sistemas y la infraestructura del entorno de producción del juego para proteger contra el acceso no autorizado, violaciones de datos y otras amenazas de seguridad.
Amenaza	Cualquier circunstancia o evento con el potencial de afectar negativamente las operaciones de la red (incluida la misión, funciones, imagen o reputación), activos o personas a través de un sistema mediante el acceso no autorizado, la destrucción, divulgación, modificación de la información y/o denegación de servicio; la posibilidad de que una fuente de amenaza explote con éxito una vulnerabilidad en particular; cualquier peligro potencial para una red que alguien o algo pueda identificar como vulnerable y, por lo tanto, tratar de explotar.
Sello de tiempo	Un registro del valor actual de la fecha y la hora que se agrega a un mensaje en el momento en que se crea el mensaje.
Protocolo de control de transmisión/Protocolo de Internet (TCP/IP)	Conjunto de protocolos de comunicaciones utilizados para conectar hosts en Internet.
Acceso no autorizado	Una persona obtiene acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso.
Protocolo de datagramas de usuario (UDP)	Un protocolo de transporte que no garantiza la entrega. Por lo tanto, es más rápido, pero menos confiable.
Verificación	Garantizar, mediante la comprobación de la firma electrónica, que cualquier paquete de software es una copia auténtica del software creado por su fabricante y, en su caso, una copia exacta del software certificada por el Laboratorio de Pruebas Independiente (ITL por sus siglas en inglés).
Control de versiones	El método por el cual se verifica que los componentes críticos del sistema aprobados en evolución funcionan en un estado aprobado.
Red privada virtual (VPN)	Una red lógica que se establece sobre una red física existente y que normalmente no incluye todos los nodos presentes en la red física.
Virus	Un programa autorreplicante, normalmente con intenciones maliciosas, que se ejecuta y se propaga modificando otros programas o archivos.
Escáner de virus	Software utilizado para prevenir, detectar y eliminar virus informáticos, incluidos malware, gusanos y troyanos.
Vulnerabilidad	Software, hardware u otras debilidades en una red o sistema que pueden proporcionar una "puerta" a la introducción de una amenaza.
Apuesta	Cualquier compromiso de créditos o dinero por parte del cliente que tenga un impacto en el resultado del juego.
Protocolo equivalente por cable (WEP)	Un algoritmo que se rompe fácilmente y, por lo tanto, está en desuso para proteger las redes inalámbricas IEEE 802.11. Originalmente estaba destinado a permitir el mismo nivel de protección que una conexión por cable, pero pronto se descubrieron fallas después de su adopción que lo hicieron apenas mejor que ninguna protección.
Punto de acceso inalámbrico (WAP)	Proporciona capacidades de red a los dispositivos de red inalámbrica. Un WAP se utiliza a menudo para conectarse a una red cableada, actuando así como enlace entre las partes cableadas e inalámbricas de la red.
Wi-Fi	La tecnología estándar de red de área local inalámbrica (WLAN) para conectar computadoras y dispositivos electrónicos entre sí y/o a Internet.

Término	Descripciones
Acceso protegido Wi-Fi (WPA)	El sucesor de WEP. Su autenticación se puede romper en determinadas circunstancias, pero las frases de contraseña suficientemente complejas son lo suficientemente seguras para la mayoría de los usos.
Estación de Trabajo	Una interfaz para que el personal autorizado acceda a las funciones reguladas del GPE.