GLI®

MARCO DE SEGURIDAD DEL JUEGO

GLI-GSF-1

SEGURIDAD DE LA INFORMACIÓN DEL JUEGO (GIS)

AUDITORÍA DE CONTROLES

Versión 1.0 – Publicado el 7 de febrero de 2025

Contenido

1. INTRODUCCIÓN

1.1. Declaración General

La integridad y la precisión del funcionamiento de un entorno de producción de juegos (GPE por sus siglas en inglés) dependen en gran medida de los procedimientos operativos, las configuraciones y la infraestructura de 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 Firma 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).

a. 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) necesarios para auditar el Sistema de Gestión de Seguridad de la Información del Juego (GISMS) de una Empresa de Juego.
b. Estos controles GIS comunes se aplican a las GPE utilizadas para todas las formas de juego, como los juegos de casino, la lotería, las apuestas de eventos y los juegos interactivos.
c. Este módulo se puede utilizar junto con el GLI-GSF-2, que proporciona un punto de referencia para realizar evaluaciones de seguridad técnica de juegos (GTS) del GPE de una empresa de juegos.
d. Dependiendo del tipo de empresa de juegos, también se pueden aplicar módulos adicionales de GLI-GSF.

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

1.2. Rol de gestión de datos confidenciales y empresariales de juegos

Garantizar la seguridad de un GPE es una responsabilidad colectiva que abarca las múltiples entidades que componen la Empresa de Juegos, como el operador, y sus proveedores, fabricantes, vendedores, prestadores de servicios y otras entidades que tienen un papel en la supervisión o el funcionamiento de un GPE o en la prestación de servicios integrales para su función. Cada entidad desempeña un papel crucial en el mantenimiento de la integridad, disponibilidad y confidencialidad del entorno, especialmente cuando se trata de datos sensibles, que como mínimo consisten en lo siguiente, según corresponda:

a. Registros de auditoría y bases de datos del sistema que registran la información utilizada para determinar el resultado, el pago, el canje y el seguimiento de la información del usuario;
b. Información contable y de eventos significativos relacionados con los componentes críticos del sistema del GPE;
c. Semillas RNG y cualquier otra información que afecte los resultados de los juegos y las apuestas;
d. Claves de cifrado, donde la implementación elegida requiere la transmisión de claves;
e. Números de validación asociados con cuentas de usuarios, instrumentos de apuestas y cualquier otra transacción de juego;
f. Transferencias de fondos hacia y desde cuentas de usuarios, cuentas de pago electrónico y con fines de juego;
g. Paquetes de software dentro del GPE;
h. Cualquier dato de ubicación relacionado con la actividad del empleado o cliente (por ejemplo, administración de cuentas, juegos en línea, etc.);
i. Cualquiera de la siguiente información registrada para cualquier empleado o cliente:
    i. Número de identificación gubernamental (número de seguro social, número de identificación del contribuyente, número de pasaporte o equivalente);
    ii. Información financiera personal (números de instrumentos de crédito o débito, números de cuentas bancarias, etc.);
    iii. Credenciales de autenticación en relación con cualquier cuenta de usuario o cuenta de usuario;
    iv. Cualquier otra información de identificación personal (PII, por sus siglas en inglés) que deba mantenerse confidencial; y
j. Cualquier otro dato considerado sensible por el Organismo Regulador o la Empresa de Juego.

NOTA: Este documento no pretende definir qué entidades son responsables de garantizar el GIS. Es responsabilidad de las múltiples entidades que componen la Empresa de Juegos de Azar ponerse de acuerdo sobre la responsabilidad.

1.3. Entorno de producción de juegos (GPE)

Un GPE se refiere al entorno operativo donde se realizan, administran y entregan a los usuarios las actividades de juego y los servicios relacionados 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, como los juegos de casino, la lotería, las apuestas de eventos y los juegos interactivos. El GPE también abarca los sistemas de backend, las aplicaciones empresariales 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 los dispositivos de red, servidores, dispositivos informáticos, componentes virtuales, hardware y plataformas de 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 juegos interactivos.
b. Módulos criptográficos: Los módulos criptográficos utilizados dentro del GPE son responsables de las funciones criptográficas, incluido el cifrado y descifrado de datos confidenciales, utilizando algoritmos que cumplen con los estándares actuales aceptados 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, los pagos, los depósitos, los retiros y las transacciones financieras con los clientes.
d. Medidas de seguridad: Se implementan sólidas medidas de seguridad para salvaguardar la integridad, confidencialidad y disponibilidad de los componentes críticos del sistema, los datos confidenciales, las transacciones financieras y la información de los usuarios contra el acceso no autorizado, el fraude, la manipulación y las 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, los riesgos financieros, los riesgos regulatorios y los 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 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 con prontitud a incidentes de GIS, fraude u otros problemas.
h. Cumplimiento regulatorio: 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 responsables y el cumplimiento de las obligaciones legales y reglamentarias.

1.4. 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, los activos y los componentes críticos del sistema de una empresa de juegos dentro de su GPE contra el acceso, la divulgación, la alteración o la destrucción no autorizados. Abarca políticas, procedimientos, controles y prácticas de gestión de riesgos específicamente adaptadas a los desafíos únicos y los 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.

1.5. 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 juegos deben establecer y mantener un marco claramente definido y documentado para lograr y preservar la confianza del público en sus operaciones. El objetivo es alinear la 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.

1.6. Normas y directrices de seguridad consultadas

Cada módulo del GLI-GSF se basó en estándares y directrices de seguridad de uso común que proporcionan una base aceptada por la industria para desarrollar prácticas efectivas de gestión de GIS. GLI reconoce y agradece a los Organismos Reguladores y otros participantes de la industria que han reunido reglas, regulaciones, normas técnicas y otros documentos que han sido influyentes en el desarrollo de este documento.

1.7. Adopción y observancia

Este módulo del GLI-GSF puede ser adoptado en su totalidad o en parte por cualquier Organismo Regulador que desee implementar un conjunto completo de Controles de GIS Comunes.

2. AUDITORÍAS DE CONTROLES DE GIS

2.1. Resumen de la auditoría

La Auditoría de Controles de GIS se realiza con la intención de identificar cualquier caso real o potencial de incumplimiento, vulnerabilidades o debilidades, y garantizar que se preserve la integridad, confidencialidad y disponibilidad de la información bajo el control de la Empresa de Juego. Esta metodología se basa en gran medida en la seguridad por capas para reducir el riesgo para los sistemas informáticos y de red al proporcionar redundancia y reforzar el modelo de seguridad general, ya que se deben violar varias capas de seguridad antes de acceder a un almacén de datos confidenciales.

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

2.2. Métodos de auditoría

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

a. Entrevista: Un tipo de método de evaluación caracterizado por el proceso de llevar a cabo discusiones con individuos o grupos dentro de una empresa de juegos para facilitar la comprensión, lograr aclaraciones o conducir a la localización de pruebas.
b. Examinar: Tipo de método de evaluación caracterizado 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 caracterizado por el proceso de ejercitar uno o más objetos de auditoría bajo condiciones específicas para comparar el comportamiento real con el esperado.

2.3. Tareas de auditoría

A continuación se presentan las actividades de auditoría de controles de GIS de alto nivel sugeridas. En el Apéndice se detallan los controles de GIS comunes mínimos con más detalle. Los usuarios de este documento deben consultar el Apéndice para asegurarse de que no se pasa por alto ningún control de GIS necesario. Los Controles de GIS enumerados en el Apéndice no son exhaustivos y se pueden incluir Controles de GIS adicionales en función de los requisitos reglamentarios y el alcance de la evaluación.

2.3.1. Revisión de la documentación presentada

La ISF primero evalúa los Controles de GIS existentes de la Empresa de Juegos de Azar mediante la recopilación y revisión de la documentación relevante para comprender y evaluar mejor los aspectos pertinentes de el GPE en relación con la SIG en general, y para determinar si la documentación complementa adecuadamente los controles técnicos. Un ejemplo de parte de la documentación que se espera revisar incluye, pero no se limita a:

a. Política de la GIS
b. Acceso de los 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 y protegida
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 supervisar el uso de los servicios 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 el 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, la ISF mide el nivel de concienciación de los usuarios durante las entrevistas para determinar si los usuarios ajenos a la función de TI tienen un nivel adecuado de comprensión de la GIS y su papel en la protección de los datos confidenciales y otros activos críticos. Se debe entrevistar como mínimo al siguiente personal clave responsable de establecer y aplicar la política de la GIS.

a. Persona con la responsabilidad general de la operación de juego
b. Oficial de cumplimiento
c. Oficial de la GIS o jefe de la función de la GIS
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. Parches y actualización de administración
e. Monitoreo del acceso y uso del sistema
f. Procedimientos de gestión del cambio
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
c. Seguridad Técnica de Juegos (GTS)
d. Seguridad de redes y comunicaciones
e. Controles de acceso lógico
f. Seguridad de los sistemas operativos (SO)
g. Controles de software malintencionado
h. Diseño y configuración de bases de datos
i. Controles criptográficos
j. Monitoreo del sistema
k. Informes y registro
l. Controles de desarrollo del sistema

2.3.5. Evaluación de Controles Físicos y Ambientales

La ISF realiza pruebas y evaluaciones para evaluar la efectividad y la idoneidad de estos controles para protegerse 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 las no conformidades con cualquier Control de GIS aplicable, y cualquier amenaza y vulnerabilidad potencial que puede no estar explícitamente enumerada en el GLI-GSF, pero que se observó durante la auditoría y puede constituir un riesgo. La ISF debe utilizar un sistema de puntuación apropiado para la seguridad del juego (por ejemplo, CVSS, ISO/IEC 31010, etc.) para asignar niveles de gravedad (menores o mayores) a no conformidades, vulnerabilidades y amenazas, permitiendo la priorización de respuestas y recursos. El sistema de puntuación utilizado por la ISF debe identificarse en el informe de auditoría de los controles de GIS.

2.4. Frecuencia de auditoría

2.4.1. Auditoría inicial

La Empresa de Juegos de Azar debe tener una Auditoría de Controles de GIS realizada por una ISF dentro de los noventa días posteriores a que la Empresa de Juegos de Azar comience las operaciones de juego dentro de esa jurisdicción, a menos que el Organismo Regulador haya aconsejado lo contrario. Cualquier aplazamiento de la Auditoría de Controles de GIS solicitado por la Empresa de Juego, junto con un cronograma actualizado, debe ser autorizado por el Organismo Regulador.

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

2.4.2. Auditoría Anual

La Empresa de Juegos de Azar debe, por regla general, realizar otra Auditoría de Controles de GIS por parte de una ISF dentro de los doce meses posteriores a la Auditoría de Controles de GIS anterior, a menos que el Organismo Regulador haya aconsejado lo contrario. Cualquier aplazamiento de la Auditoría de Controles de GIS solicitado por la Empresa de Juego, junto con un cronograma actualizado, debe ser autorizado por el Organismo Regulador.

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

2.4.3. Auditorías adicionales

La Empresa de Juegos debe, como regla general, tener Auditorías de Controles de GIS adicionales realizadas por una ISF después de cualquier cambio crítico dentro del GPE, como actualizaciones y modificaciones de infraestructura o aplicaciones, o la instalación de nuevos Componentes Críticos del Sistema. La determinación de lo que constituye un "cambio crítico" se basa en el proceso de evaluación de riesgos de la empresa de juegos, la configuración específica del GPE y los requisitos del organismo regulador. Sin embargo, cualquier cambio que pueda afectar a la seguridad del GPE o permitir el acceso a datos confidenciales y/o componentes críticos del sistema puede ser considerado un "cambio crítico" por la Empresa de juego.

2.5. Informes de auditoría

Los resultados de una auditoría de controles de GIS identifican para las empresas de juegos de azar las áreas de las operaciones en las que se debe considerar la mejora y recomiendan estrategias para mejorar esas áreas. El informe de Auditoría de Controles de GIS debe presentarse al Organismo Regulador a más tardar noventa días después de que se haya completado la Auditoría de Controles de GIS, a menos que el Organismo Regulador haya aconsejado lo contrario. El informe de auditoría de controles de GIS debe incluir todo lo siguiente:

a. Resumen ejecutivo:
   i. El nombre y la información de contacto de la Empresa de Juegos;
   ii. Una breve descripción del modelo de negocio de la empresa de juegos, las actividades de juego ofrecidas, los proveedores de servicios utilizados, la ubicación, el número de empleados, el sitio web, las certificaciones y una descripción de alto nivel de la infraestructura de TI (incluidos los centros de datos, los servicios en la nube, etc.)
b. Detalles de la auditoría de controles de GIS:
   i. El nombre de la ISF, la afiliación de la empresa, la información de contacto y las calificaciones y experiencia de las personas que llevaron a cabo la Auditoría de Controles de GIS;
   ii. La(s) fecha(s) de la Auditoría de Controles de GIS, incluida la fecha de solicitud, la fecha de inicio, la fecha de finalización y la fecha del informe;
c. Alcance de la Auditoría de Controles de GIS:
   i. Una visión general de alto nivel del trabajo realizado, especificando los entornos (por ejemplo, desarrollo, producción) que operan y los controles de GIS con los que se llevó a cabo la auditoría de controles de GIS.
   ii. Identificación de los componentes críticos del sistema y los activos revisados, detallando cómo se seleccionaron estos componentes y activos como parte de la auditoría de controles de GIS.
   iii. Herramientas y técnicas específicas utilizadas durante la Auditoría de Controles de GIS, incluidos los nombres de software, las versiones y los sitios web oficiales de las herramientas empleadas.
d. Metodología:
   i. Una descripción detallada del enfoque de auditoría, incluidas las preguntas basadas en la investigación, la observación, las pruebas y las personas clave entrevistadas.
   ii. Cualquier limitación o exclusión en la auditoría de controles de GIS, con justificaciones (por ejemplo, ciertos sistemas estaban fuera del alcance debido a requisitos comerciales).
e. Pruebas recopiladas:
   i. Documentación revisada, incluidos los nombres, las fechas y las versiones.
   ii. Personal entrevistado, con roles, ubicaciones, nombres, fechas y versiones de las entrevistas.
   iii. Evidencia (por ejemplo, capturas de pantalla, registros) que ilustre claramente las no conformidades identificadas, incluidos los comandos y las herramientas utilizadas para detectar estos problemas.
   iv. Técnicas de muestreo utilizadas para verificar la posición de seguridad, incluido el tamaño y la naturaleza de la muestra.
f. Hallazgos y resultados:
   i. Un resumen de las no conformidades detectadas, clasificadas por gravedad (p. ej., menor, mayor).
   ii. Una explicación detallada de cada no conformidad, respaldada por pruebas (por ejemplo, capturas de pantalla, registros).
   iii. Una auditoría del impacto o riesgo potencial asociado con cada no conformidad identificada, teniendo en cuenta el entorno específico de la Empresa de Juego.
   iv. Pasos de corrección recomendados para cada no conformidad identificada, con niveles de prioridad y plazos sugeridos para la mitigación.

v. La respuesta de la empresa de juegos a los hallazgos y resultados, incluidos los pasos de corrección recomendados.

2.6. Remediación

Si el informe de Auditoría de Controles de GIS de la ISF recomienda la remediación, la Empresa de Juegos de Azar debe proporcionar al Organismo Regulador y a la ISF, si así lo requiere el Organismo Regulador, un plan de remediación y cualquier plan de mitigación de riesgos que detalle las acciones y el cronograma de la Empresa de Juegos para implementar los pasos de corrección.

a. Cada no conformidad debe abordarse a través del proceso de corrección de la Empresa de juegos, lo que incluye:
   i. Acciones tomadas para determinar el alcance y contener la no conformidad específica.
   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, para eliminar la recurrencia de la no conformidad.
b. Las medidas correctivas para abordar cada no conformidad importante identificada deben llevarse a cabo de inmediato y el Organismo Regulador y la ISF, si así lo requiere el Organismo Regulador, deben ser notificados de las acciones tomadas dentro de los treinta días, a menos que el Organismo Regulador especifique lo contrario. Si así lo requiere el Organismo Regulador, la ISF debe realizar una auditoría de seguimiento dentro de un plazo razonable especificado en el plan de remediación para confirmar las acciones tomadas, evaluar su eficacia y determinar si las no conformidades se han resuelto.
c. Los pasos de remediación para abordar cada no conformidad menor identificada deben ser documentados y enviados por la Empresa de Juegos al Organismo Regulador y a la ISF, si así lo requiere el 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 debe dar seguimiento en la próxima auditoría programada.
d. Una vez que se hayan tomado las medidas correctivas, la Empresa de Juegos de Azar debe proporcionar al Organismo Regulador y a la ISF, si así lo requiere el Organismo Regulador, la documentación que evidencie su finalización.
e. La Empresa de Juegos de Azar debe mantener registros de corrección, incluidas pruebas objetivas, durante al menos cinco años, a menos que el Organismo Regulador especifique lo contrario.

2.7. Empresa de seguridad independiente (ISF)

La Auditoría de Controles de GIS debe ser llevada a cabo por personas con suficientes calificaciones, lo que significa que la ISF debe emplear a personas suficientemente calificadas, competentes y experimentadas. A menos que el Organismo Regulador especifique lo contrario, estas personas deben:

a. Tener una formación académica pertinente o, de otro modo, proporcionar las cualificaciones pertinentes para evaluar el 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 Controles 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 seguridad de la información dentro de la industria del juego o, cuando sea aceptable para el Organismo Regulador, otra experiencia relevante en la auditoría de los controles de seguridad de una industria similar; y
d. Cumplir con cualquier otro requisito prescrito por el organismo regulador.

NOTA: Nada de lo aquí contenido tiene la intención de prohibir que el personal calificado del Organismo Regulador actúe como ISF, siempre que sean independientes de la Empresa de Juegos de Azar que se está auditando.

3. CONTROLES Y EXCEPCIONES DE GIS ALTERNATIVOS

3.1. Controles de GIS alternativos

Se reconoce que los Controles de GIS aplicables a una Empresa de Juegos de Azar pueden variar en función de su tamaño, estructura de propiedad, alcance y complejidad de las operaciones, estrategia corporativa y perfil de riesgo. El Organismo Regulador puede, a su discreción, aprobar la implementación de Controles de GIS alternativos en lugar de los enumerados en el Apéndice a petición de la Empresa de Juego.

a. Para cada control de GIS enumerado para el que la empresa de juegos de azar desee utilizar un control de GIS alternativo, la empresa de juegos debe demostrar cómo el control de GIS alternativo:
   i. Protege la integridad de los juegos ofrecidos por la Empresa de Juegos;
   ii. Salvaguarda los activos críticos utilizados en relación con el GPE; y
   iii. Logra un nivel de seguridad e integridad suficiente para cumplir el propósito del control de GIS que pretende reemplazar.
b. Una empresa de juegos solo puede implementar un control de GIS alternativo con la aprobación del organismo regulador.
c. La prueba de la aprobación del Organismo Regulador del Control de GIS alternativo debe proporcionarse al ISF y ser evaluada como parte de la Auditoría anual de Controles de GIS.

NOTA: Es responsabilidad del Organismo Regulador determinar cuándo es aceptable o permitido que una Empresa de Juegos utilice Controles de GIS alternativos.

3.2. Pequeñas empresas de juegos

El Organismo Regulador puede, a su discreción, permitir que una pequeña Empresa de Juegos de Azar quede exenta del cumplimiento de los Controles de GIS enumerados en el Apéndice siempre que:

a. Los ingresos brutos anuales del juego de la pequeña empresa de juegos de azar no superan un umbral establecido por el organismo regulador; y
b. La pequeña empresa de juegos implementa controles de GIS alternativos que cumplen con los requisitos de la sección anterior.

NOTA: Nada de lo contenido en este documento tiene la intención de prohibir que el Organismo Regulador utilice criterios alternativos o adicionales para definir una pequeña Empresa de Juego.

3.3. Empresas benéficas de juegos

El Organismo Regulador podrá, a su discreción, permitir que una Empresa de Juego benéfica quede exenta del cumplimiento de los Controles de GIS enumerados en el Apéndice siempre que:

a. Todas las ganancias son en beneficio de una organización benéfica;
b. La Empresa de Juegos de Azar benéfica es operada en su totalidad por los empleados o voluntarios de la organización benéfica, y no por operadores independientes en beneficio de una organización benéfica;
c. Los ingresos brutos anuales del juego de la empresa benéfica del juego no superan un umbral establecido por el organismo regulador; y
d. La empresa benéfica de juegos implementa controles de GIS alternativos que cumplen con los requisitos de la sección anterior.

NOTA: Nada de lo contenido en este documento tiene la intención de prohibir que el Organismo Regulador utilice criterios alternativos o adicionales para definir una Empresa de Juego benéfica.

3.4. Excepciones de ISF

El Organismo Regulador puede, a su discreción, permitir que una pequeña Empresa de Juegos de Azar o una Empresa de Juego de Beneficencia utilice una función de auditoría interna o un empleado calificado dentro de la Empresa de Juego o empresa matriz de la Empresa de Juego, que sea independiente de la Empresa de Juego como ISF, para sus Auditorías de Controles de GIS.

NOTA: Es responsabilidad del Organismo Regulador determinar cuándo es aceptable o permitido que una pequeña Empresa de Juego o una Empresa de Juego benéfica realice la Auditoría de Controles de GIS en estas circunstancias.

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

Los controles de seguridad de la información de juego (GIS), tal como se especifica en este apéndice, indican a qué grupo de implementación de juegos (GIG) se aplica el control de GIS. Para ayudar a las empresas de juegos de todos los tamaños, los GIG se dividen en tres grupos, según el perfil de riesgo y los recursos que una empresa de juegos tiene disponibles para implementar el GLI-GSF. Cada GIG identifica un conjunto de controles de GIS que deben implementar. GIG2 se basa en GIG1, y GIG3 se compone de todos los controles de GIS.

GIG	Descripción del Grupo de Implementación de Juegos (GIG)
GIG1	El GLI-GSF define el Grupo de Implementación 1 (GIG1) como la higiene esencial de la seguridad del juego y representa un estándar mínimo emergente de GIS para todas las empresas de juego. Los controles de GIS incluidos en GIG1 son los que toda empresa de juegos debe aplicar para defenderse de los ataques más comunes. Una empresa de juegos GIG1 suele tener una experiencia limitada en seguridad para dedicarse a proteger los activos y el personal críticos. Una preocupación común de las empresas de juegos es mantener operativas sus operaciones de juego, ya que tienen una tolerancia limitada al tiempo de inactividad. La criticidad de los datos sensibles que intentan proteger es baja y rodea 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 de juegos y estar destinados a frustrar ataques generales no dirigidos. Estos controles de GIS también se diseñarán normalmente para funcionar junto con hardware y software comercial listo para usar (COTS) de oficinas pequeñas o en casa.
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 Gaming y de la experiencia especializada para instalarlos y configurarlos correctamente. Una empresa de juegos GIG2 emplea a personas que son responsables de administrar y proteger la infraestructura del GPE. Estas empresas de juegos suelen apoyar a varios departamentos con diferentes perfiles de riesgo en función de la función y la misión del trabajo. Las unidades de Pequeña Empresa de Juego pueden tener cargas de cumplimiento regulatorio. Las empresas de juegos GIG2 a menudo almacenan y procesan datos confidenciales y pueden soportar breves interrupciones del servicio. Una de las principales preocupaciones es la pérdida de confianza del público si se produce una infracción. Todas las empresas de juegos de azar que ejecutan operaciones de juego terrestres en las que el GPE se comunica 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 juegos GIG3 suele emplear a expertos en seguridad de juegos que se especializan en las diferentes facetas de la seguridad de los juegos (por ejemplo, gestión de riesgos, pruebas de penetración, seguridad de aplicaciones). Los activos críticos de GIG3 Gaming Enterprise contienen datos o funciones confidenciales que están sujetos a supervisión regulatoria y de cumplimiento. Una empresa de juegos GIG3 debe abordar la disponibilidad de los servicios y la integridad y confidencialidad de los datos confidenciales. Los ataques exitosos pueden causar un daño significativo a la información de identificación personal (PII). Los controles de GIS seleccionados para GIG3 deben reducir los ataques dirigidos de un adversario sofisticado y reducir el impacto de los ataques de día cero. Todas las empresas de juegos que ejecutan operaciones de juegos en línea (por ejemplo, juegos interactivos, apuestas de eventos en línea, etc.) deben tratarse como empresas de juegos 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 8.1, que deben ser cumplidos por cada Empresa de Juego (Empresa). La columna del lado derecho indica el Grupo de implementación de juegos (GIG) aplicable al que se aplica el control CIS.

NOTA: El Documento completo de Controles de Seguridad Críticos 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	Dirección: 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	Elimine los datos de forma segura	GIG1
CIS-3.6	Cifre los datos en los dispositivos de los usuarios finales	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	Cifre datos confidenciales en reposo	GIG2
CIS-3.14	Registre 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 sesión en activos empresariales	GIG1
CIS-4.4	Implementar y administrar un firewall en servidores	GIG1
CIS-4.6	Gestione de forma segura los activos y el software de la empresa	GIG1
CIS-4.7	Administre las cuentas predeterminadas en los activos y el 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	Configurar servidores DNS de confianza en activos empresariales	GIG2
CIS-4.10	Aplicar el bloqueo automático de dispositivos en dispositivos portátiles de usuario final	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	Centralice 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	Centralice 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	Realice análisis automatizados de vulnerabilidades de los activos internos de la empresa	GIG2
CIS-7.6	Realice análisis automatizados de vulnerabilidades de los 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	Garantice un almacenamiento adecuado de registros de auditoría	GIG1
CIS-8.4	Estandarizar la sincronización de tiempo	GIG2
CIS-8.5	Recopile registros de auditoría detallados	GIG2
CIS-8.9	Centralice los 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	Garantizar el uso de solo navegadores y clientes de correo electrónico totalmente compatibles	GIG1
CIS-9.2	Usar servicios de filtrado de DNS	GIG1
CIS-9.7	Implemente y mantenga 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	Administre 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	Administre 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 redes y comunicaciones	GIG2
CIS-13	Monitoreo y defensa de redes	GIG
CIS-13.1	Centralice las alertas de eventos de seguridad	GIG2
CIS-13.2	Implemente una solución de detección de intrusiones basada en host	GIG2
CIS-13.3	Implementación de una solución de detección de intrusiones en la red	GIG2
CIS-13.4	Realizar el filtrado de tráfico entre segmentos de red	GIG2
CIS-13.7	Implemente una solución de prevención de intrusiones basada en host	GIG3
CIS-13.8	Implemente una solución de prevención de intrusiones en la red	GIG3
CIS-13.9	Implemente el control de acceso a nivel de puerto	GIG3
CIS-13.10	Realizar el filtrado de la capa de aplicación	GIG3
CIS-14	Capacitación en habilidades y concientización en seguridad	GIG
CIS-14.1	Establecer y mantener un programa de concienciación sobre seguridad	GIG1
CIS-14.2	Capacite a los miembros de la fuerza laboral para que reconozcan los ataques de ingeniería social	GIG1
CIS-14.3	Capacite 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 cómo reconocer y reportar incidentes de seguridad	GIG1
CIS-14.9	Llevar a cabo capacitación en habilidades y concienciación sobre seguridad específica de 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	Desmantelar de forma segura a los proveedores de servicios	GIG3
CIS-16	Seguridad del software de aplicaciones	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 análisis de causa raíz en vulnerabilidades de seguridad	GIG2
CIS-16.4	Establecer y administrar un inventario de componentes de software de terceros	GIG2
CIS-16.5	Utilice componentes de software de terceros actualizados y de confianza	GIG2
CIS-16.6	Establecer y mantener un sistema y un proceso de clasificación de gravedad 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 Respuesta a Incidentes	GIG
CIS-17.1	Designar personal para gestionar la gestión de incidentes	GIG1
CIS-17.2	Establecer y mantener información de contacto para informar de 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 umbrales 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	Remediar los hallazgos 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 de GIS comunes adicionales

Además de los controles de seguridad críticos de CIS adoptados anteriormente, los siguientes controles de GIS adicionales se aplican a los GPE utilizados para todas las formas de juego. La columna del lado derecho indica el Grupo de implementación de juegos (GIG) aplicable al que se aplica el control de GIS.

GIS-1	Funciones del programa de control crítico del GPE	GIG
GIS-1.1	**Reloj interno del GPE**	
GIS-1.1.1	El GPE debe mantener un reloj interno que refleje la fecha y la hora actuales que se debe utilizar para proporcionar la marca de tiempo de todas las transacciones, cambios de configuración y eventos significativos, y como reloj de referencia para la generación de informes mediante el Protocolo de tiempo de red (NTP) o equivalente.	**GIG1**
GIS-1.1.2	Los cambios en la fecha y hora del reloj interno, o en las fuentes de tiempo aprobadas, deben registrarse en un registro de auditoría, indicando: 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 firmas del Programa de Control Crítico**	
GIS-1.2.1	Los Programas de Control Críticos deben ser identificados y documentados para que la Empresa de Juegos de Azar verifique la integridad del GPE.	**GIG1**
GIS-1.2.2	Cada Programa de Control Crítico debe ser verificado como idéntico a los aprobados por el Organismo Regulador a través de un procedimiento de verificación de firma, que debe realizarse: a. Tras la instalación/actualización de componentes; b. Al encenderse o recuperarse de un estado de apagado; c. Al menos una vez cada 24 horas; y d. Por solicitud.	**GIG1**
GIS-1.2.3	El procedimiento de verificación de firma debe: a. Operar independientemente de cualquier proceso o software de seguridad dentro del sistema. b. Emplear un algoritmo hash criptográfico que produzca un resumen de mensajes de al menos 128 bits. Otras metodologías de prueba deben revisarse caso por caso. c. Incluir uno o más pasos analíticos para comparar las firmas actuales de los Programas de Control Crítico en el GPE con las firmas de las versiones actuales aprobadas de los Programas de Control Crítico.	**GIG1**
GIS-1.2.4	El resultado del procedimiento de verificación de firmas debe registrarse en un registro de auditoría, detallando para cada verificación: a. La fecha y hora de la verificación; b. Identificación de cada Programa de Control Crítico verificado; c. Los resultados de firma esperados y generados, incluida la indicación de cualquier error de programa o discrepancia de firma; y d. Cuando se realiza bajo demanda, ID de cuenta de usuario que inició el procedimiento de verificación.	**GIG1**
GIS-1.2.5	Cualquier fallo en la verificación de la firma de cualquier Programa de Control Crítico debe requerir una notificación del fallo de verificación que se comunique a la Empresa de Juego y al Organismo Regulador según sea necesario.	**GIG1**
GIS-1.2.6	Debe 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 Programa de Control Crítico necesarias de manera oportuna.	**GIG1**
GIS-2	**Seguridad de la información del juego (GIS)**	**GIG**
GIS-2.1	**Política de GIS**	
GIS-2.1.1	Se debe definir e implementar 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 debe tener una disposición que requiera revisión al menos una vez al año o a intervalos planificados requeridos por el Organismo Regulador y cuando ocurran cambios	**GIG1**

	significativos en los procesos del GPE o de la Empresa de Juegos que alteren el perfil de riesgo del sistema.	
GIS-2.1.3	La política de GIS debe ser aprobada por la gerencia y comunicada y reconocida por el personal pertinente dentro de la Empresa de Juego.	**GIG1**
GIS-2.1.4	La política de GIS debe delinear las funciones y responsabilidades de seguridad del personal relevante dentro de la Empresa de Juegos para la operación, el servicio y el mantenimiento del GPE. Algunas de estas funciones y responsabilidades de seguridad pueden asignarse en función de las evaluaciones de riesgos realizadas por la Empresa de juegos.	**GIG1**
GIS-2.2	**Política de control de acceso**	
GIS-2.2.1	Se debe establecer y documentar una política de control de acceso en función de los requisitos empresariales y de seguridad para el acceso físico y lógico al GPE, incluido el acceso remoto.	**GIG1**
GIS-2.2.2	La política de control de acceso debe revisarse al menos una vez al año o según lo requiera la Empresa de Juego y/o el Organismo Regulador.	**GIG1**
GIS-2.2.3	Debe existir un procedimiento formal de registro y cancelación de registro de usuarios para conceder y revocar el acceso al GPE.	**GIG1**
GIS-2.2.4	La asignación y el uso de los derechos y privilegios de acceso de los usuarios deben restringirse y controlarse en función de los requisitos empresariales y del principio de privilegios mínimos.	**GIG2**
GIS-2.2.5	El personal solo debe tener acceso a los servicios o instalaciones para los que ha sido específicamente autorizado a utilizar.	**GIG1**
GIS-2.2.6	La gerencia debe utilizar un proceso formal para revisar y confirmar los derechos y privilegios de acceso de los usuarios al menos una vez al año o según lo requiera la Empresa de Juego y/o el Organismo Regulador.	**GIG2**
GIS-2.3	**Asignación de responsabilidades en materia de GIS**	
GIS-2.3.1	Las responsabilidades de la GIS deben documentarse e implementarse de manera efectiva.	**GIG2**
GIS-2.3.2	Se debe establecer formalmente un foro de GIS 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 al menos cada seis meses o a intervalos regulares requeridos por el Organismo Regulador.	**GIG2**
GIS-2.3.3	Debe existir una función de GIS que sea responsable de desarrollar e implementar estrategias de seguridad y planes de acción de acuerdo con la empresa de juegos en general.	**GIG2**
GIS-2.3.4	La función de GIS debe estar involucrada en la revisión de todas las tareas y procesos necesarios con respecto a los aspectos de SIG de la Empresa de Juego, incluidos, entre otros, la protección de la información y los datos confidenciales, las comunicaciones, la infraestructura virtual y física, el personal y la seguridad operativa general.	**GIG2**
GIS-2.3.5	La función de GIS debe informar a la dirección ejecutiva con respecto a la gestión de los riesgos de seguridad.	**GIG2**
GIS-2.3.6	Para evitar un conflicto de intereses entre las operaciones y la gestión de riesgos de seguridad, la función de GIS debe ser independiente de la función de TI, a menos que el Organismo Regulador autorice lo contrario.	**GIG2**
GIS-2.3.7	La función de GIS debe tener las competencias y estar suficientemente capacitada, así como tener acceso a todos los recursos necesarios para permitir una evaluación, gestión y reducción de riesgos adecuadas.	**GIG2**
GIS-2.3.8	El jefe de la función de GIS debe ser miembro del foro de la GIS y ser responsable de recomendar políticas y cambios en la GIS.	**GIG2**
GIS-2.4	**Programa de Privacidad de Información de Identificación Personal (PII)**	
GIS-2.4.1	La Empresa del Juego debe establecer y mantener un programa de privacidad para proporcionar protecciones técnicas y organizativas adecuadas para la PII recopilada o procesada por la Empresa del Juego.	**GIG1**
GIS-2.4.2	El programa de privacidad debe tener en cuenta la equidad y transparencia generales de la forma en que la Empresa de Juego procesa la información personal de las personas y protege dicha información de conformidad con las regulaciones y estándares de privacidad locales observados por el Organismo Regulador.	**GIG1**
GIS-2.4.3	La Empresa de Juegos de Azar debe designar 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 procesamiento de la información personal.	**GIG1**

GIS-2.4.4	La Empresa del Juego debe establecer procedimientos para determinar la naturaleza y el alcance de toda la PII recopilada y procesada por la Empresa del Juego, incluidos los tipos de información recopilada y procesada, las fuentes de recopilación y los fines de uso.	**GIG1**
GIS-2.4.5	La Empresa del Juego debe adherirse y poner a disposición del público un aviso de privacidad para informar a las personas de las actividades de procesamiento de PII de la Empresa del Juego, incluyendo, sin limitación, a. Información relacionada con el propósito de la recopilación de PII; b. Si la PII se compartirá o venderá a otras entidades; y c. La forma de ejercer los derechos individuales, en su caso.	**GIG1**
GIS-2.4.6	Si una empresa de juegos de azar utiliza la toma de decisiones automatizada, la empresa de juegos debe establecer procedimientos para la gobernanza de dicho proceso para garantizar que no se infrinjan los derechos legales del individuo.	**GIG1**
GIS-2.5	**Aseguramiento de las transacciones financieras dentro de la AME**	
GIS-2.5.1	Los métodos de pago utilizados para las transacciones financieras en el GPE deben estar protegidos contra el uso fraudulento.	**GIG1**
GIS-2.5.2	La Empresa de Juegos solo debe recopilar los datos confidenciales estrictamente necesarios para la transacción financiera.	**GIG1**
GIS-2.5.3	Deben existir procesos para verificar la protección de los datos confidenciales directamente relacionados con cada transacción financiera dentro del GPE, incluida cualquier información de identificación personal proporcionada por el usuario o datos relacionados con el pago.	**GIG1**
GIS-2.5.4	Cualquier canal de comunicación dentro del GPE que transmita detalles de transacciones financieras debe emplear cifrado para proteger contra la interceptación.	**GIG1**
GIS-3	**Operación y seguridad de el GPE**	**GIG**
GIS-3.1	**Procedimientos de seguridad**	
GIS-3.1.1	La Empresa de Juegos debe supervisar 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 juegos debe supervisar y ajustar la capacidad y el consumo de recursos de GPE para garantizar que se mantenga la disponibilidad.	**GIG1**
GIS-3.1.3	La empresa de juegos debe mantener un registro de auditoría del rendimiento del GPE, incluida una función para compilar informes de rendimiento.	**GIG2**
GIS-3.1.4	La empresa de juegos debe supervisar su GPE para detectar, prevenir, mitigar y responder a los ataques y compromisos técnicos activos y pasivos comunes.	**GIG1**
GIS-3.1.5	La empresa de juegos debe establecer procedimientos para recopilar y analizar inteligencia de amenazas, y actuar en consecuencia de manera adecuada.	**GIG2**
GIS-3.1.6	La Empresa de Juego debe establecer procedimientos para supervisar, gestionar y responder de forma centralizada a las actividades de los usuarios, las excepciones, el mal funcionamiento y los eventos adversos.	**GIG2**
GIS-3.2	**Mal funcionamiento del GPE**	
GIS-3.2.1	Tras la detección de un mal funcionamiento, la Empresa de Juegos debe iniciar una investigación para determinar la causa raíz del mal funcionamiento.	**GIG1**
GIS-3.2.2	La investigación debe implicar una revisión exhaustiva de los registros, informes, registros de auditoría 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 deben tomar las medidas adecuadas para reparar o reemplazar los componentes críticos del sistema responsables del mal funcionamiento.	**GIG1**
GIS-3.2.4	Antes de restaurar los componentes críticos del sistema a la operación, se deben realizar actividades de verificación para garantizar su integridad y funcionalidad.	**GIG1**
GIS-3.2.5	De acuerdo con los requisitos reglamentarios, la Empresa de Juego debe presentar un informe de mal funcionamiento ante el Organismo Regulador correspondiente que documente los detalles del mal funcionamiento.	**GIG1**
GIS-3.3	**Gestión de incidentes de GIS**	

GIS-3.3.1	La Empresa de Juego debe definir, supervisar y documentar, así como informar, investigar, responder y resolver incidentes de GIS, incluidas las infracciones detectadas y la piratería o manipulación sospechada o real del GPE.	**GIG1**
GIS-3.3.2	Todos los incidentes de GIS deben ser respondidos dentro de un período de tiempo establecido aprobado por el Organismo Regulador y documentado formalmente.	**GIG1**
GIS-3.3.3	En el caso de un incidente de GIS que comprometa la seguridad o integridad de los datos confidenciales: a. Las personas afectadas, el Organismo Regulador y otras autoridades pertinentes deben ser notificadas de inmediato de la infracción. b. La violación debe informarse de inmediato al organismo regulador y otras autoridades relevantes, incluidos los detalles sobre la naturaleza del incidente de GIS, los riesgos potenciales y las medidas adoptadas para mitigar el impacto.	**GIG1**
GIS-3.3.4	El plan de respuesta a incidentes de GIS debe incluir procedimientos documentados para manejar varios tipos de incidentes de GIS.	**GIG1**
GIS-3.3.5	Se deben establecer procedimientos para la recuperación controlada de incidentes de GIS, incluida la restauración de los sistemas afectados y los datos confidenciales 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 deben estar alojados 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 debe tener suficiente protección contra la alteración, la manipulación o el acceso no autorizado.	**GIG1**
GIS-3.4.3	Cada ubicación segura debe estar equipada con un sistema de vigilancia que debe cumplir con los procedimientos establecidos por el Organismo Regulador.	**GIG1**
GIS-3.4.4	Se deben diseñar e implementar medidas de seguridad para trabajar en lugares seguros.	**GIG1**
GIS-3.4.5	Los perímetros de seguridad deben definirse y usarse para proteger cada ubicación segura.	**GIG1**
GIS-3.4.6	Cada ubicación segura debe estar protegida por controles de entrada apropiados para garantizar que el acceso esté restringido solo al personal autorizado.	**GIG1**
GIS-3.4.7	Para el acceso físico a cada ubicación segura, se debe utilizar un proceso de MFA auditable, a menos que la ubicación segura tenga personal en todo momento.	**GIG1**
GIS-3.4.8	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-3.4.9	Todos los intentos de acceso físico a cada ubicación segura deben registrarse en un registro de auditoría, indicando: 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 sido exitoso o no; y e. Si el intento de acceso se ha realizado correctamente, la duración del acceso.	**GIG1**
GIS-3.4.10	Cada ubicación segura debe estar equipada 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, huracanes, terremotos, etc.).	**GIG1**
GIS-3.4.11	El GPE debe protegerse de sobretensiones, fallos y otras interrupciones causadas por fallos en el soporte de los servicios públicos.	**GIG1**
GIS-3.4.12	Los cables que transportan energía, datos o componentes críticos del sistema de soporte deben protegerse contra intercepciones, interferencias o daños.	**GIG1**
GIS-3.4.13	Todos los componentes críticos del sistema deben estar provistos de energía primaria adecuada.	**GIG1**
GIS-3.4.14	Cuando el servidor es una aplicación independiente, debe tener un sistema de alimentación ininterrumpida (SAI) conectado y debe tener capacidad suficiente para permitir un apagado correcto y que conserve todos los datos confidenciales durante una pérdida de energía. Es aceptable que el sistema pueda ser un componente de una red que esté soportada por un SAI de toda la red, siempre que el servidor esté incluido como un dispositivo protegido por el SAI. Un	**GIG1**

	sistema de protección contra sobretensiones debe estar en uso si no está incorporado en el propio SAI.	
GIS-3.5	**Control de acceso lógico**	
GIS-3.5.1	El GPE debe estar lógicamente protegido contra el acceso no autorizado mediante credenciales de autenticación permitidas por el organismo regulador, como contraseñas, MFA, certificados digitales, PIN, biometría y otros métodos de acceso.	**GIG1**
GIS-3.5.2	Cada cuenta de usuario debe tener su propia credencial de autenticación individual, cuya provisión debe controlarse a través de un proceso formal.	**GIG1**
GIS-3.5.3	Los usuarios solo deben tener acceso a la funcionalidad y características apropiadas para su rol y responsabilidades dentro del sistema.	**GIG1**
GIS-3.5.4	No debe ser posible modificar los parámetros críticos del sistema del GPE, incluidas las políticas y los 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, etc.), sin un proceso seguro autorizado. Los cambios en los parámetros críticos del sistema deben registrarse en un registro de auditoría, indicando: 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 cuentas genéricas debe ser limitado y, cuando se utilicen, las razones para su uso deben documentarse formalmente.	**GIG1**
GIS-3.5.6	Los registros de las credenciales de autenticación deben mantenerse manualmente o mediante sistemas que registren automáticamente los cambios de autenticación y fuercen los cambios de credenciales de autenticación.	**GIG1**
GIS-3.5.7	Todas las credenciales de autenticación almacenadas en el sistema deben estar cifradas o cifradas 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. Para estos fines se debe emplear un proceso de MFA.	**GIG2**
GIS-3.5.9	Las credenciales de autenticación perdidas o comprometidas y las credenciales de autenticación de los usuarios finalizados deben desactivarse, protegerse o destruirse tan pronto como sea razonablemente posible.	**GIG1**
GIS-3.5.10	El sistema debe tener varios 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. Deben existir procedimientos para asignar, revisar, modificar y eliminar derechos y privilegios de acceso a cada usuario, incluidos: a. Permitir que la administración de las cuentas de usuario proporcione 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 expiración.	**GIG1**
GIS-3.5.11	Un Proveedor de Servicios dentro de la Empresa de Juego puede, según sea necesario, acceder al sistema y a sus componentes asociados utilizando una cuenta de usuario invitado para el soporte de productos y usuarios o actualizaciones/mejoras, según lo permitan el Organismo Regulador y la Empresa de Juego. Las cuentas de usuario invitado deben ser: a. Restringidas a través de controles 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. Ya no es necesario desactivarlas cuando no están en uso e inmediatamente después del propósito para el que se estableció la cuenta.	**GIG1**
GIS-3.5.12	Deben existir 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;	**GIG1**

	b. Marcado 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.	
GIS-3.5.13	Cualquier intento de acceso lógico a las aplicaciones del sistema o sistemas operativos debe registrarse en un registro de auditoría, indicando: 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 sido exitoso 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 restringirse y controlarse estrictamente.	**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 deben registrarse en un registro de auditoría, indicando: a. La fecha y hora de las actividades; b. Componentes afectados por las actividades; c. Motivo y descripción de las actividades, incluyendo valores iniciales y finales; 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 debe incluir: a. ID de cuenta de usuario; b. Nombre individual y título o cargo; 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 al grupo de la cuenta, si procede; y i. Los estados actuales y anteriores de la cuenta de usuario (por ejemplo, activo, inactivo, cerrado, suspendido, etc.).	**GIG1**
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 debe emplear 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 deben finalizarse si la autorización del usuario ha superado un número configurable de intentos fallidos.	**GIG1**
GIS-3.6.3	Cuando se utilizan, los métodos automatizados de identificación de equipos para autenticar conexiones desde ubicaciones y equipos específicos deben estar documentados y deben incluirse 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 debe obtenerse en el momento de la solicitud del sistema y no almacenarse 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 sesión de usuario siempre se debe crear de forma aleatoria, en la memoria, y debe eliminarse una vez finalizada la sesión del usuario.	**GIG2**
GIS-3.6.6	Las restricciones en los tiempos de conexión, como, entre otros, los tiempos de espera de sesión, deben usarse para proporcionar seguridad adicional para aplicaciones de alto riesgo, como el acceso remoto.	**GIG1**
GIS-3.7	**Programación de servidores**	
GIS-3.7.1	El GPE debe ser lo suficientemente seguro como para evitar cualquier capacidad de programación iniciada por el usuario no autorizada 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 de 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	**Nube y entornos virtualizados**	
GIS-3.8.1	Si los datos confidenciales se almacenan, procesan o transmiten en un entorno virtualizado o en la nube, se deben aplicar los controles de GIS adecuados a ese entorno. Por lo general, esto implica validar tanto la infraestructura como el uso de instancias de servidor dentro de la nube o el entorno de virtualización.	**GIG2**
GIS-3.8.2	Las instancias de servidor redundantes en un entorno virtualizado o en la nube no deben ejecutarse en el mismo hipervisor.	**GIG2**
GIS-3.8.3	Cada instancia de servidor en un entorno virtualizado o en la nube puede realizar solo una función crítica.	**GIG3**
GIS-3.9	**Uso opcional de un sistema electrónico de retención de documentos (ERDS)**	
GIS-3.9.1	El ERDS debe configurarse correctamente para mantener la versión original junto con todas las versiones posteriores que reflejen todos los cambios en los informes o registros de auditoría que se almacenan en un formato modificable.	**GIG1**
GIS-3.9.2	El ERDS debe mantener una firma única para cada versión del registro de auditoría, incluido el original.	**GIG1**
GIS-3.9.3	El ERDS debe conservar un registro de auditoría 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 debe proporcionar un método de indexación completa para localizar e identificar fácilmente el registro de auditoría que incluya al menos lo siguiente (que puede ser introducido por el usuario): a. Fecha y hora en que se generó el registro de auditoría; b. Componente crítico del sistema que genera el registro de auditoría; c. Título y descripción del registro de auditoría; d. ID de cuenta de usuario de quién está generando el registro de auditoría; y e. Cualquier otra información que pueda ser útil para identificar el registro de auditoría y su propósito.	**GIG1**
GIS-3.9.5	El ERDS debe configurarse para a. Limitar el acceso para modificar o agregar informes o registros de auditoría al sistema a través de la seguridad lógica de cuentas de usuario específicas; y b. Proporcionar un registro de auditoría de toda la actividad de la cuenta de usuario administrativo.	**GIG1**
GIS-3.9.6	El ERDS debe 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, etc.).	**GIG1**
GIS-3.9.7	El ERDS debe 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 juegos debe proporcionar un enfoque por capas para la seguridad del GPE para garantizar el almacenamiento y el procesamiento seguros de datos confidenciales utilizando métodos de protección razonables.	**GIG1**
GIS-4.1.2	La Empresa de Juego debe implementar una política para mantener los datos confidenciales durante al menos cinco años, a menos que el Organismo Regulador especifique lo contrario, y de acuerdo con las regulaciones y estándares locales de retención de datos observados por el Organismo Regulador.	**GIG1**
GIS-4.1.3	Se deben implementar métodos adecuados para el manejo de datos confidenciales, incluida la validación de la entrada y el rechazo de datos confidenciales dañados.	**GIG2**
GIS-4.1.4	Se debe utilizar cifrado o seguridad equivalente para los archivos y directorios que contengan datos confidenciales. Si no se utiliza el cifrado, la Empresa de Juego debe restringir a los usuarios la visualización del contenido de dichos archivos y directorios, lo que, como mínimo, debe proporcionar 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 autorizadas de los archivos de datos en tiempo real y de las tablas de bases de datos del GPE que se produzcan fuera de la ejecución normal del programa y del sistema operativo deben registrarse en un registro de auditoría, indicando: 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 debe proporcionar un medio lógico para asegurar y proteger los datos confidenciales 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 debe 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 debe permitir la eliminación de la información a menos que primero haya transferido esa información a la base de datos asociada u otros componentes seguros del sistema.	**GIG1**
GIS-4.1.10	La Empresa de Juegos debe proteger la confidencialidad, integridad, responsabilidad y disponibilidad de los datos confidenciales cuando se mantienen en reposo en servidores, aplicaciones críticas y bases de datos asociadas que contienen datos confidenciales, incluida la limitación del número de estaciones de trabajo a las que se puede acceder.	**GIG2**
GIS-4.1.11	El cifrado debe aplicarse para proteger la confidencialidad, la integridad, la responsabilidad y la disponibilidad de los datos confidenciales cuando están en uso, cuando se almacenan en sistemas informáticos portátiles (por ejemplo, computadoras portátiles, dispositivos USB, etc.) y cuando se mantienen en reposo en estaciones de trabajo.	**GIG2**
GIS-4.1.12	Los datos confidenciales que no es necesario ocultar, pero que deben autenticarse, deben usar algún tipo de técnica de autenticación de mensajes.	**GIG2**
GIS-4.1.13	La autenticación debe utilizar un certificado de seguridad de una Empresa de juegos aprobada, que contenga información sobre a quién pertenece, quién lo emitió, fechas de validez, un número de serie único u otra identificación única que se pueda utilizar para verificar el contenido del certificado.	**GIG1**
GIS-4.1.14	Las bases de datos de producción que contienen datos confidenciales deben residir en redes separadas de los servidores que alojan las interfaces de usuario.	**GIG1**
GIS-4.1.15	Los datos confidenciales deben mantenerse en todo momento, independientemente de si el servidor está recibiendo energía.	**GIG1**
GIS-4.1.16	Las medidas de prevención de fuga de datos confidenciales deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita datos confidenciales.	**GIG2**
GIS-4.1.17	Los datos sensibles deben almacenarse de tal manera que se evite la pérdida de los datos al reemplazar piezas o módulos durante el mantenimiento normal.	**GIG1**

GIS-4.1.18	No se debe permitir la alteración de datos confidenciales sin controles de acceso supervisados. En caso de que se modifique algún dato confidencial, se debe documentar o registrar 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, incluidos los valores inicial y final; y d. ID de cuenta de usuario que realizó y/o autorizó la modificación.	**GIG1**
GIS-4.1.19	Cualquier pérdida irrecuperable de datos sensibles debe registrarse en un registro de auditoría, 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-4.1.20	Los datos confidenciales deben ser accesibles para el Organismo Regulador en un formato que permita el análisis por parte del Organismo Regulador.	**GIG1**
GIS-4.2	**Implementación del proceso de copia de seguridad**	
GIS-4.2.1	La implementación del proceso de copia de seguridad debe ocurrir al menos una vez al día o según lo especificado por el organismo regulador, aunque todos los métodos deben revisarse caso por caso.	**GIG1**
GIS-4.2.2	Se debe realizar una copia de seguridad de los datos confidenciales, las aplicaciones críticas y las bases de datos asociadas con medidas de seguridad de inmutabilidad para evitar alteraciones o eliminaciones, lo que garantiza la integridad del GPE.	**GIG1**
GIS-4.2.3	Las copias duplicadas o redundantes de datos confidenciales deben mantenerse en el GPE con soporte abierto para copias de seguridad y restauración.	**GIG1**
GIS-4.2.4	La copia de seguridad debe estar contenida en un medio 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 debe garantizar la integridad de los datos en caso de que se produzca un fallo en el disco.	**GIG1**
GIS-4.2.6	Una vez finalizado el proceso de copia de seguridad, 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 está haciendo una copia de seguridad (para almacenamiento temporal y permanente).	**GIG1**
GIS-4.2.7	La ubicación de almacenamiento de la copia de seguridad debe estar protegida para evitar el acceso no autorizado y proporcionar la protección adecuada para evitar la pérdida permanente de cualquier dato confidencial.	**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 en la nube o región diferente.	**GIG2**
GIS-4.2.9	Los archivos de datos de copia de seguridad y los componentes de recuperación de datos deben administrarse con al menos el mismo nivel de seguridad y controles de acceso que el GPE.	**GIG1**
GIS-4.2.10	De acuerdo con el proceso de copia de seguridad acordado, los archivos de datos de copia de seguridad y los componentes de recuperación de datos deben mantenerse, protegerse y probarse al menos una vez al año o según lo especificado por el organismo regulador.	**GIG2**
GIS-4.3	**Fallo del sistema y recuperación**	
GIS-4.3.1	El GPE debe tener suficiente redundancia y modularidad para que, si falla algún componente crítico del sistema o parte de un componente, las funciones del GPE y el proceso de auditoría de esas funciones puedan continuar sin pérdida o corrupción de datos confidenciales.	**GIG1**
GIS-4.3.2	Los períodos significativos de indisponibilidad de cualquier componente crítico del sistema (cualquier período de tiempo en que las operaciones se detengan para todos los usuarios y/o las transacciones no se puedan completar con éxito para ningún usuario) deben registrarse en un registro de auditoría, 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 hora en que el componente volvió a estar disponible.	**GIG1**
GIS-4.3.3	Cuando se vinculan dos o más componentes críticos del sistema, debe existir 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 debe verse 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 deben sincronizar inmediatamente el estado de todas las transacciones, los datos confidenciales y las configuraciones entre sí.	**GIG1**
GIS-4.3.6	La empresa de juegos debe 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 debe contar con 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, los siguientes: a. Restauración de copias de seguridad de datos; b. Restauración del programa; y c. Restauración de hardware redundante o de respaldo.	**GIG1**
GIS-4.4.2	El plan de continuidad del negocio y recuperación ante desastres debe considerar 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, etc.	**GIG1**
GIS-4.4.3	El plan de continuidad del negocio y recuperación ante desastres debe abordar el método de almacenamiento de datos confidenciales para minimizar la pérdida. Si se utiliza la replicación asincrónica, se debe describir el método para recuperar información o se debe documentar la posible pérdida de información.	**GIG2**
GIS-4.4.4	El plan de continuidad de las actividades y recuperación en caso de desastre debe delinear las circunstancias en las que se invocará.	**GIG1**
GIS-4.4.5	El plan de continuidad del negocio y recuperación ante desastres debe abordar el establecimiento de un sitio de recuperación físicamente separado del sitio 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).	**GIG3**
GIS-4.4.6	El plan de continuidad del negocio y recuperación ante desastres debe contener guías de recuperación que detallen los pasos técnicos necesarios para restablecer la funcionalidad de juego en el sitio de recuperación.	**GIG1**
GIS-4.4.7	El plan de continuidad del negocio y recuperación ante desastres debe abordar los procesos necesarios para reanudar las operaciones administrativas de las actividades de juego después de la activación del sistema recuperado para una variedad de escenarios apropiados para el contexto operativo del sistema.	**GIG1**
GIS-4.4.8	El plan de continuidad del negocio y recuperación ante desastres debe probarse al menos una vez al año o según lo especifique el organismo regulador. Los resultados de las pruebas deben estar documentados.	**GIG1**
GIS-5	**Comunicaciones**	**GIG**
GIS-5.1	**Conectividad**	
GIS-5.1.1	Solo se debe permitir que los dispositivos autorizados establezcan comunicaciones entre cualquier componente crítico del sistema.	**GIG1**
GIS-5.1.2	El GPE debe proporcionar 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 debe ser anular la inscripción y deshabilitarla.	**GIG1**

GIS-5.1.5	El GPE debe registrar el establecimiento, la pérdida y el restablecimiento de las comunicaciones entre los componentes críticos del sistema en un registro de auditoría.	**GIG1**
GIS-5.2	**Protocolo de comunicación**	
GIS-5.2.1	Cada componente crítico del sistema del GPE debe funcionar 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 debe ser revisada caso por caso y aprobada por el Organismo Regulador.	**GIG1**
GIS-5.2.3	Todas las comunicaciones críticas de datos confidenciales deben emplear cifrado y autenticación para la integridad.	**GIG1**
GIS-5.2.4	Las comunicaciones en la red segura solo deben ser posibles entre componentes críticos del sistema autorizados que se hayan inscrito y autenticado como válidos en la red. No se deben permitir comunicaciones no autorizadas a componentes y/o puntos de acceso.	**GIG1**
GIS-5.2.5	Las comunicaciones deben endurecerse para que sean inmunes a todos los posibles ataques de mensajes con formato incorrecto.	**GIG1**
GIS-5.2.6	La falla de las comunicaciones no debe afectar la integridad de los datos confidenciales.	**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 del GPE no debe establecerse y autenticarse hasta que la rutina de reanudación del programa, incluidas las autopruebas, se complete con éxito.	**GIG1**
GIS-5.3	**Comunicaciones a través de Internet/Redes públicas**	
GIS-5.3.1	Las comunicaciones entre cualquier componente crítico del sistema que tenga lugar a través de Internet/redes públicas, deben protegerse contra actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas mediante el cifrado de los paquetes de datos o mediante la utilización de un protocolo de comunicaciones seguro para garantizar la confidencialidad e integridad de la transmisión.	**GIG1**
GIS-5.3.2	Los datos confidenciales siempre deben cifrarse a través de Internet/red pública y protegerse contra transmisiones incompletas, desvíos, modificación no autorizada de mensajes, divulgación, duplicación o reproducción.	**GIG1**
GIS-5.4	**Comunicaciones inalámbricas de red de área local (WLAN)**	
GIS-5.4.1	El uso de las comunicaciones WLAN debe ser seguro y solo debe usarse cuando sea apropiado y no en áreas donde pueda ser potencialmente dañino.	**GIG1**
GIS-5.4.2	Las comunicaciones entre dispositivos inalámbricos en la WLAN deben utilizar protocolos diseñados para proteger, autenticar y cifrar redes inalámbricas.	**GIG1**
GIS-5.4.3	La autenticación multifactor (MFA) debe ser necesaria en el nivel de red inalámbrica y dispositivo.	**GIG1**
GIS-5.4.4	Los esquemas de autenticación que utilizan la infraestructura de clave pública (PKI) deben requerir la validación de certificados, idealmente en ambas direcciones (por ejemplo, certificados de cliente).	**GIG1**
GIS-5.4.5	Se deben utilizar estándares de cifrado avanzados (AES) o equivalentes con un cifrado mínimo de 256 bits para respaldar los servicios de integridad y confidencialidad.	**GIG1**
GIS-5.4.6	La clave maestra por pares (PMK) utilizada debe tener una vida útil de veinticuatro horas o menos. Alternativamente, es aceptable que el PMK se cambie durante el tiempo de inactividad de mantenimiento preprogramado de acuerdo con los controles de GIS adoptados por la empresa de juegos.	**GIG1**
GIS-5.4.7	La clave maestra de grupo (GMK) utilizada debe tener una vida útil de ocho horas o menos.	**GIG1**
GIS-5.4.8	No se debe utilizar 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 debe revisarse caso por caso.	**GIG1**
GIS-5.4.9	Se debe utilizar 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);	**GIG1**

	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 tunelización punto a punto (PPTP); o f. Capa de sockets seguros (SSL).	
GIS-5.4.10	Los protocolos de tunelización cifrados deben autenticarse en el protocolo ligero de acceso a directorios (LDAP), el servicio de usuario de marcado de autenticación remota (RADIUS), los servidores Kerberos o Microsoft Active Directory o equivalentes, así como en las bases de datos locales almacenadas en el controlador de puerta de enlace segura.	**GIG1**
GIS-5.5	**Puntos de acceso inalámbricos (WAP)**	
GIS-5.5.1	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-5.5.2	El nombre de usuario y la contraseña de administración predeterminados deben cambiarse de los valores predeterminados de fábrica a un valor seguro controlado de acuerdo con la empresa de juegos.	**GIG1**
GIS-5.5.3	La contraseña de red predeterminada debe cambiarse de la predeterminada de fábrica a un valor seguro controlado de acuerdo con la empresa de juegos.	**GIG1**
GIS-5.5.4	El SSID debe cambiarse 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-5.5.5	El acceso a las funciones administrativas del WAP debe restringirse a las conexiones desde el lado cableado de la red que utilice un protocolo seguro con una cuenta de usuario privilegiada definida por la empresa de juegos.	**GIG1**
GIS-5.5.6	Si el router 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-5.6	**Equipo de comunicación de red (NCE)**	
GIS-5.6.1	La Empresa de Juegos debe proporcionar una ubicación segura para la colocación, el funcionamiento y el uso de NCE.	**GIG1**
GIS-5.6.2	El NCE debe instalarse de acuerdo con un plan definido y se deben mantener registros de todos los NCE instalados.	**GIG1**
GIS-5.6.3	Los NCE deben construirse 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-5.6.4	NCE debe estar físicamente protegido contra el acceso no autorizado.	**GIG1**
GIS-5.6.5	Las comunicaciones del GPE a través del NCE deben estar lógicamente protegidas contra el acceso no autorizado.	**GIG1**
GIS-5.6.6	NCE con almacenamiento integrado limitado debe, si el registro de auditoría se llena, deshabilitar toda la comunicación o descargar los registros de auditoría a un servidor de registro de auditoría dedicado.	**GIG1**
GIS-5.7	**Sistema de Detección de Intrusiones/Sistema de Prevención de Intrusiones (IDS/IPS)**	
GIS-5.7.1	Se debe instalar un IDS/IPS que incluya uno o más componentes que puedan escuchar tanto las comunicaciones internas como las externas, así como detectar o prevenir: a. Ataques de denegación de servicio distribuido (DDoS); b. Shellcode de atravesar la red; c. suplantación de identidad del Protocolo de resolución de direcciones (ARP); y d. Otros indicadores de ataque Man-In-The-Middle (MITM) y cortan las comunicaciones inmediatamente si se detectan.	**GIG1**
GIS-5.7.2	El IDS/IPS debe escanear la red en busca de puntos de acceso o dispositivos no autorizados o no autorizados conectados a cualquier punto de acceso en la red al menos trimestralmente o según lo especificado por el organismo regulador.	**GIG2**
GIS-5.7.3	El IDS/IPS debe desactivar automáticamente cualquier dispositivo no autorizado o no autorizado conectado al GPE.	**GIG2**
GIS-5.7.4	El IDS/IPS debe mantener un registro de auditoría para el acceso que debe: 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	**GIG1**

	b. Ser capaz de conciliar con todos los demás dispositivos de red dentro del GPE.	
GIS-5.8	**Gestión de la seguridad de la red**	
GIS-5.8.1	La empresa de juegos debe revisar y actualizar las políticas y procedimientos para garantizar que la red sea segura y que las amenazas y vulnerabilidades se aborden en consecuencia.	**GIG1**
GIS-5.8.2	Las redes deben estar separadas lógicamente de modo que no haya tráfico de red en un enlace de red que no pueda ser atendido por los hosts de ese enlace.	**GIG1**
GIS-5.8.3	Todas las funciones de administración de red deben autenticar a todos los usuarios de la red y cifrar todas las comunicaciones de administración de red.	**GIG1**
GIS-5.8.4	La falla de un solo artículo no debe resultar en una denegación de servicio (DOS).	**GIG1**
GIS-5.8.5	Todos los puntos de entrada y salida de la red deben ser identificados, gestionados, controlados y monitorizados las 24 horas del día, los 7 días de la semana.	**GIG2**
GIS-5.8.6	Todos los concentradores de red, servicios y puertos de conexión deben estar protegidos para evitar el acceso no autorizado a la red.	**GIG1**
GIS-5.8.7	Los servicios no utilizados y los puertos no esenciales deben bloquearse físicamente o deshabilitarse el software siempre que sea posible.	**GIG1**
GIS-5.8.8	Los protocolos sin estado, como el Protocolo de datagramas de usuario (UDP), no se deben usar para datos confidenciales sin transporte con estado. Tenga en cuenta que, aunque el Protocolo de transporte de hipertexto (HTTP) técnicamente no tiene estado, si se ejecuta en el Protocolo de control de transmisión (TCP), que tiene estado, esto está permitido.	**GIG1**
GIS-5.8.9	Todos los cambios en la infraestructura de red deben registrarse en un registro de auditoría, indicando: 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-5.9	**Teletrabajo e informática móvil**	
GIS-5.9.1	El teletrabajo solo debe permitirse en circunstancias en las que se pueda garantizar la seguridad del terminal.	**GIG1**
GIS-5.9.2	Se debe establecer una política formal y se deben adoptar medidas de seguridad de apoyo para proteger contra los riesgos del uso de las instalaciones móviles de computación y comunicación.	**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 las demás entidades dentro de la Empresa de Juego para la gestión de los Controles de GIS 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	Cuando se compartan datos sensibles con proveedores de servicios, deben existir acuerdos formales de procesamiento 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 rodea a 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.	**GIG1**
GIS-6.2	**Comunicaciones con proveedores de servicios**	
GIS-6.2.1	El GPE debe 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 deben registrarse en un registro de auditoría.	**GIG1**
GIS-6.2.3	La comunicación con los proveedores de servicios no debe interferir ni degradar las funciones normales del GPE.	**GIG1**

GIS-6.2.4	Los datos del Proveedor de Servicios no deben afectar las comunicaciones de los usuarios.	**GIG1**
GIS-6.2.5	Los proveedores de servicios deben estar en una red segmentada separada de los segmentos de red que alojan conexiones de usuarios.	**GIG1**
GIS-6.2.6	Los juegos deben estar deshabilitados en todas las conexiones de red, excepto en las del GPE.	**GIG1**
GIS-6.2.7	El GPE no debe enrutar paquetes de datos de los proveedores de servicios directamente al GPE y viceversa.	**GIG1**
GIS-6.2.8	Los GPE no deben actuar como enrutadores IP entre el GPE y los proveedores de servicios.	**GIG1**
GIS-6.2.9	Se debe evitar que los proveedores de servicios no autorizados vean o alteren 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 juegos debe utilizar un servidor DNS primario seguro y un servidor DNS secundario seguro que estén lógica y físicamente separados entre sí, lo que mejora la resistencia contra puntos únicos de falla y posibles ataques.	**GIG2**
GIS-7.1.2	El servidor DNS principal debe 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 debe restringirse 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 deben permitir las transferencias de zona a hosts arbitrarios. Esta restricción evita que partes no autorizadas accedan a los datos de la zona DNS o los repliquen, lo que reduce el riesgo de exposición o manipulación de datos.	**GIG2**
GIS-7.1.5	Se requiere un método para evitar el envenenamiento 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 debe desarrollar e implementar 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 debe ser adecuado a la sensibilidad de los datos.	**GIG1**
GIS-7.2.3	El uso de métodos de cifrado debe revisarse al menos una vez al año o según lo especificado por el organismo regulador para verificar que los algoritmos de cifrado actuales y las longitudes de las claves sean seguros.	**GIG1**
GIS-7.2.4	El método de cifrado debe incluir el uso de diferentes claves de cifrado para que los algoritmos de cifrado puedan cambiarse o reemplazarse para corregir las debilidades tan pronto como sea posible. Otras metodologías deben examinarse caso por caso.	**GIG1**
GIS-7.2.5	La gestión de las claves de cifrado a lo largo de todo su ciclo de vida debe seguir los procesos definidos establecidos por la Empresa de Juego.	**GIG1**
GIS-7.2.6	La Empresa de Juegos de Azar debe establecer 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 deben almacenarse en un medio de almacenamiento seguro y redundante después de haber sido cifradas a través de un método de cifrado diferente y/o mediante el uso de una clave de cifrado diferente.	**GIG1**
GIS-7.2.8	Deben establecerse procedimientos para controlar las fechas de vencimiento de las claves de cifrado, cuando corresponda.	**GIG1**
GIS-7.2.9	Se deben definir procedimientos para revocar rápidamente las claves de cifrado en caso de compromiso, pérdida o acceso no autorizado.	**GIG1**
GIS-7.2.10	Se deben establecer 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 juegos debe implementar 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 deben abordar todas las vulnerabilidades de seguridad conocidas y ser 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 deben evaluarse al menos una vez al año o según lo especificado por el organismo regulador y, si procede, se deben realizar cambios para mejorar el endurecimiento.	**GIG2**
GIS-7.3.4	Todos los parámetros de configuración predeterminados o estándar deben eliminarse de todos los componentes críticos del sistema en los que se presente un riesgo de seguridad.	**GIG1**
GIS-7.3.5	Solo se debe implementar una función principal por servidor para evitar que las funciones que requieren diferentes niveles de seguridad coexistan en el mismo servidor.	**GIG1**
GIS-7.3.6	Se deben implementar características de seguridad adicionales para los servicios, protocolos o demonios necesarios que se consideren inseguros.	**GIG1**
GIS-7.3.7	Los parámetros de seguridad del sistema deben configurarse para evitar el uso indebido.	**GIG1**
GIS-7.3.8	Se deben eliminar todas las funcionalidades innecesarias, como scripts, controladores, características, subsistemas, sistemas de archivos y servidores web innecesarios.	**GIG1**
GIS-7.4	**Generación y almacenamiento de informes o registros de seguridad**	
GIS-7.4.1	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-7.4.2	Los informes o registros de seguridad deben estar protegidos contra la manipulación y el acceso no autorizado.	**GIG2**
GIS-7.4.3	Los informes o registros de seguridad deben revisarse al menos cada noventa días o según lo especifique 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 debe revisarse 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 remoto deben estar debidamente protegidos y gestionados.	**GIG1**
GIS-8.1.3	El GPE debe tener la capacidad de habilitar o deshabilitar el acceso remoto, y el estado predeterminado debe establecerse en deshabilitado	**GIG1**
GIS-8.1.4	El acceso remoto solo debe aceptar las conexiones remotas permitidas por la aplicación de firewall y la configuración del sistema.	**GIG1**
GIS-8.1.5	El acceso remoto debe limitarse solo 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, etc.).	**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 debe mantener un registro de auditoría que represente toda la información y la actividad de acceso remoto. Los registros de acceso remoto deben incluir 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, deben pasar por al menos un firewall de nivel de aplicación aprobado. 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 firewall debe estar ubicado en el límite de dos dominios de seguridad diferentes.	**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 debe pasar a través de al menos un firewall de 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 firewall debe rechazar todas las conexiones, excepto aquellas que han sido específicamente aprobadas.	**GIG1**
GIS-8.2.8	El cortafuegos debe rechazar todas las conexiones de destinos que no puedan residir en la red desde la que se originó el mensaje (por ejemplo, direcciones de RFC1918 en el lado público de un cortafuegos de Internet).	**GIG1**
GIS-8.2.9	El cortafuegos solo debe permitir el acceso remoto mediante cifrado.	**GIG1**
GIS-8.2.10	El firewall debe ser capaz de registrar la siguiente información en un registro de auditoría de una manera que preserve y asegure la información contra pérdidas o alteraciones: 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, cuando sea posible, 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 deben contabilizar todos los activos físicos o lógicos que albergan, procesan o comunican datos confidenciales, incluidos los que componen el GPE.	**GIG1**
GIS-9.1.2	Deben existir procedimientos para agregar nuevos activos y eliminar activos del servicio.	**GIG1**
GIS-9.1.3	Se debe incluir una política sobre el uso aceptable de los activos asociados con el GPE.	**GIG1**
GIS-9.1.4	El propietario designado de cada activo debe: 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	Debe 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 adecuadas 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 se verifica 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 al menos una vez al año o a intervalos regulares requeridos por el Organismo Regulador para garantizar que estén libres de defectos o mecanismos que puedan interferir con su operación.	**GIG1**
GIS-9.1.8	Los medios de almacenamiento deben gestionarse 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 de juego.	**GIG1**
GIS-9.1.9	Los activos deben eliminarse de forma segura y protegida utilizando procedimientos documentados.	**GIG1**
GIS-9.1.10	Los datos confidenciales almacenados en componentes críticos del sistema, dispositivos o en cualquier otro medio de almacenamiento deben eliminarse cuando ya no sean necesarios.	**GIG1**

GIS-9.1.11	Antes de su eliminación o reutilización, los activos que contienen medios de almacenamiento deben comprobarse para asegurarse de que cualquier software con licencia, así como los datos confidenciales, se hayan eliminado o sobrescrito de forma segura (es decir, no solo se hayan eliminado).	**GIG1**
GIS-9.2	**Registro de Activos Críticos (CAR)**	
GIS-9.2.1	Se debe desarrollar y mantener un CAR para cualquier activo que afecte a la funcionalidad del GPE o que influya en la forma en que el entorno almacena/maneja los datos confidenciales.	**GIG1**
GIS-9.2.2	La estructura del CAR debe incluir los componentes de hardware y software y las interrelaciones y dependencias de los componentes.	**GIG1**
GIS-9.2.3	Los siguientes elementos mínimos deben documentarse en el CAR 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 recurso 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; y 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 influencia en cómo 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 c. 3 - Relevancia sustancial: Los criterios están relacionados o dependen del activo.	**GIG1**
GIS-9.3	**Gestión del cambio (CMP)**	
GIS-9.3.1	Se debe implementar un CMP para manejar 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 deben 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	Debe existir 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 debe conservar una CML de todas las nuevas instalaciones y/o modificaciones al sistema, incluyendo: 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:	**GIG1**

	a. Cuando una parte externa, como una tienda de aplicaciones, es una parte interesada en el proceso de lanzamiento, esta estrategia debe cubrir 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 debe abarcar 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.	
GIS-9.3.6	Se debe contar con una política que aborde los procedimientos de cambio de emergencia. Los cambios de emergencia deben ser aprobados, probados, documentados y monitoreados.	**GIG1**
GIS-9.3.7	Deben existir procedimientos para las pruebas y la migración de los cambios, incluida la identificación del personal autorizado para la aprobación antes del lanzamiento.	**GIG1**
GIS-9.3.8	Debe haber segregación de funciones dentro del proceso de lanzamiento.	**GIG1**
GIS-9.3.9	Se debe mantener documentación técnica y de usuario, como manuales y guías de usuario, que describan los sistemas en uso y el funcionamiento, incluido el hardware.	
GIS-9.3.10	Deben existir procedimientos para garantizar 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 deben seguir los procesos definidos por la Empresa de Juego y/o el Organismo Regulador.	**GIG1**
GIS-9.4.2	El GPE debe estar lógica y físicamente separada 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 juegos debe establecer y documentar 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 de GIS deben integrarse a lo largo del 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 prueba documentada debe incluir disposiciones para a. Verifique que el software de prueba no esté implementado en el GPE; 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.	**GIG1**
GIS-9.4.9	Toda la documentación relacionada con el desarrollo de software y aplicaciones debe estar disponible y conservarse durante todo su ciclo de vida.	**GIG1**
GIS-9.5	**Gestión de parches**	
GIS-9.5.1	La Empresa de Juegos debe contar con políticas de gestión de parches aprobadas por el Organismo Regulador, ya sean desarrolladas y respaldadas por la Empresa de Juegos.	**GIG1**
GIS-9.5.2	La empresa de juegos debe supervisar y aplicar parches a todos los componentes críticos del sistema implicados 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 deben probarse 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 se pueden realizar a fondo a tiempo para cumplir con los plazos del nivel de gravedad de la alerta, las pruebas de parche deben gestionarse 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**

DEFINICIONES DE TÉRMINOS

Término	Descripciones
Acceso	Posibilidad de hacer uso de cualquier recurso del GPE.
Control de acceso	El proceso de conceder o denegar solicitudes específicas para obtener y utilizar 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 implementadas por una empresa de juegos para gestionar sus GISMS.
Estándares de cifrado avanzados (AES)	Cifrado de bloque simétrico 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.
Registro de auditoría	Un registro auditable de acciones, eventos o cambios dentro de un GPE, que captura detalles como las actividades de los usuarios, los intentos de acceso, las alteraciones y las operaciones del sistema para garantizar la seguridad, el cumplimiento y la responsabilidad 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
Credenciales de autenticación	Cualquier contraseña, autenticación multifactor, certificados digitales, PIN, datos biométricos, preguntas y respuestas de seguridad y cualquier otro método de acceso a la cuenta (por ejemplo, deslizamiento magnético, tarjetas de proximidad, tarjetas con chip integrado).
Disponibilidad	Garantizar el acceso y uso oportuno y confiable de la información.
Copia de seguridad	Una copia de los archivos y programas realizados para facilitar la recuperación si es necesario.
Biometría	Una entrada de identificación biológica, como huellas dactilares, patrones de retina, datos de reconocimiento facial o huellas de voz
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 Negocio	Aplicaciones que funcionan como un servicio compartido para que los usuarios recopilen, procesen, mantengan, utilicen, compartan, difundan o eliminen datos confidenciales 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.
Envenenamiento 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 de datos alámbricas, inalámbricas, de cable, de radio, de microondas, de luz, de fibra óptica, de satélite o informáticas, incluidas Internet y las intranets.
Cumple	Se consideró que la política y las pruebas examinadas cumplían plenamente con el GLI-GSF.

Término	Descripciones
Confidencialidad	Preservar las restricciones autorizadas sobre el acceso y la divulgación de la información, incluidos los medios para proteger la privacidad personal y la información 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.
Programa de Control Crítico	Programas de software que controlan comportamientos relacionados con cualquier norma técnica y/o requisito reglamentario aplicable, como ejecutables, bibliotecas, 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 las operaciones de juegos o del sistema.
Componente crítico del sistema	Cualquier hardware, software, programas de control críticos, tecnología de comunicaciones, otros equipos o componentes implementados en un GPE para permitir la participación de los usuarios en los juegos, y cuyo fallo o compromiso pueda provocar 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 confidenciales. • Componentes que podrían afectar a la seguridad de los datos confidenciales o al GPE. • 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. • Puntos de entrada y salida de los componentes anteriores, incluidos otros sistemas que se comunican directamente con los componentes críticos del sistema. • Tecnología de comunicaciones y redes que transmiten datos confidenciales, incluidos los equipos de comunicación de red (NCE) y los controles de seguridad de red. • Componentes que proporcionan servicios de seguridad, incluidos servidores de autenticación, servidores de control de acceso, sistemas de gestión de eventos e información de seguridad (SIEM), sistemas de seguridad física, sistemas de vigilancia, sistemas de autenticación multifactor (MFA), sistemas antimalware/antivirus. • Componentes que facilitan la segmentación, incluidos los controles de seguridad internos de la red. • Componentes de virtualización, como máquinas virtuales, conmutadores/enrutadores virtuales, dispositivos virtuales, aplicaciones/escritorios virtuales e hipervisores. • Infraestructura y componentes en la nube, tanto externos como locales, e incluyendo instancias de contenedores o imágenes, nubes privadas virtuales, administración de identidades y accesos basada en la nube, componentes que residen en las instalaciones o en la nube, mallas de servicios con aplicaciones en contenedores y herramientas de orquestación de contenedores. • Tipos de servidores, incluidos web, aplicaciones, bases de datos, autenticación, correo, proxy, protocolo de tiempo de red (NTP) y sistema de nombres de dominio (DNS). • Dispositivos de usuario final, como computadoras, computadoras portátiles, estaciones de trabajo, estaciones de trabajo administrativas, tabletas y dispositivos móviles.

Término	Descripciones
	• Aplicaciones, software y componentes de software, aplicaciones sin servidor, incluidas todas las aplicaciones compradas, suscritas (por ejemplo, software como servicio), personalizadas y creadas internamente, incluidas las aplicaciones internas y externas (por ejemplo, Internet). • Herramientas, repositorios de código y sistemas que implementan la administración de la configuración de software o para la implementación de objetos en el GPE o en componentes que pueden afectar al GPE. • Redes y sistemas corporativos que interactúan con el GPE y desde los cuales los atacantes podrían usar para moverse lateralmente hacia el GPE (por ejemplo, las redes de los casinos corporativos y las redes corporativas de los operadores en línea). • Cualquier otro componente que el Organismo Regulador o la Empresa de Juegos de Azar consideren crítico para el GPE
Módulo criptográfico	Hardware, software, firmware o combinación de los mismos que implementan funciones criptográficas como cifrado, descifrado, firmas, hash y administración de claves. El objetivo principal de un módulo criptográfico es proporcionar procesamiento y almacenamiento seguros de claves y operaciones.
Integridad de los datos	La propiedad de que los datos son precisos y coherentes y no se han alterado de forma no autorizada en el almacenamiento, durante el procesamiento y mientras están en tránsito.
Denegación de servicio distribuido (DDoS)	Un tipo de ataque en el que se utilizan múltiples 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.
Dominio	Un grupo de equipos y dispositivos en una red que se administran como una unidad con reglas y procedimientos comunes.
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.
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, 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.
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 deben implementar otras medidas de protección razonables en su lugar y revisarse caso por caso.
Clave de cifrado	Una clave que se ha cifrado para disfrazar el valor del texto sin formato subyacente.
Aplicaciones expuestas externamente	Aplicaciones que están orientadas al público y que se pueden detectar a través del reconocimiento y el análisis de red desde la Internet pública fuera de la red de la empresa. Esto no se aplica a las aplicaciones destinadas al uso del usuario.
Activos empresariales expuestos externamente	Activos que están orientados al público y que se pueden detectar a través del reconocimiento del Sistema de nombres de dominio y el escaneo de red desde la Internet pública fuera de la red de la empresa. Esto no se aplica a los activos destinados al uso del usuario.

Término	Descripciones
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.
Empresa de juegos	Un operador y cualquier proveedor, fabricante, vendedor, prestador de servicios y/u otras entidades que tengan un papel en la supervisión del funcionamiento de un GPE, o que presten servicios integrales para su función, incluida la gestión de datos confidenciales.
Seguridad de la información del juego (GIS)	Proteger los datos confidenciales y los componentes críticos del sistema contra el acceso, el uso, la divulgación, la interrupción, la modificación o la destrucción no autorizados para proporcionar integridad, confidencialidad y disponibilidad.
Sistema de gestión de seguridad de la información del juego (GISMS)	Un sistema de gestión definido y documentado que consta de un conjunto de políticas, procesos y sistemas para gestionar los riesgos de los datos confidenciales, los activos y los componentes críticos del sistema de una empresa de juegos dentro de un GPE, con el objetivo de garantizar niveles aceptables de riesgo de la GIS.
Entorno de producción de juegos (GPE)	El entorno operativo donde se realizan, administran y entregan a los usuarios las actividades de juego y los servicios relacionados 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 y/o gestionar datos confidenciales, así como los sistemas y la infraestructura de backend que interactúan y/o respaldan las actividades de juego.
Puerta de Enlace	Cualquier dispositivo, sistema o aplicación de software que pueda realizar la función de traducir datos de un formato a otro. La característica clave de una puerta 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 pone en peligro real o potencialmente 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 o procedimientos de GIS, 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 juegos.
Membresía de grupo	Un método de organización de las 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.
Protocolo de transporte de hipertexto (HTTP)	El protocolo subyacente que se usa para definir cómo se formatean y transmiten los mensajes, y qué acciones deben realizar los servidores y exploradores en respuesta a varios comandos.
Concentrador	Conecta dispositivos en una red de par trenzado. Un hub no realiza ninguna tarea además de la regeneración de señales.
Integridad	Proteger contra la modificación o destrucción indebida de la información e incluye garantizar el no repudio y la autenticidad de la información.
Internet	Un sistema interconectado de redes que conecta ordenadores 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.
Sistema de Detección de Intrusiones/Sistema de	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

Término	Descripciones
Prevención de Intrusiones (IDS/IPS)	sistema de alguien que intenta entrar o comprometer un sistema. 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.
Seguridad 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 agentes al comienzo de la sesión y la negociación de las claves de cifrado que se utilizarán durante la sesión.
Kerberos	Un protocolo de autenticación de red diseñado para proporcionar una autenticación segura para aplicaciones cliente/servidor mediante el cifrado de clave secreta.
Clave	Un valor utilizado para controlar funciones criptográficas, como descifrado, cifrado, descifrado, firmas, hash, etc.
Gestión de claves	Actividades que implican el manejo de claves de cifrado 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 se dedica a transmitir datos.
No conformidad grave	Se ha identificado un fallo fundamental (sistemático) que afecta a varios controles de GIS y significa que no se pueden cumplir las políticas de GIS generales. 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 importante; • Cualquier falta de conformidad que resulte en el probable envío de un producto no conforme. Una condición que puede resultar en el fracaso o reducir materialmente la usabilidad de los productos o servicios para su propósito previsto; o • Una no conformidad que el juicio y la experiencia indican es probable que resulte en la falla del sistema o que reduzca materialmente su capacidad para asegurar procesos y productos controlados.
Malfuncionamiento	Cuando un componente crítico del sistema no funciona según lo previsto.
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, aplicaciones o sistema operativo de la víctima, o de molestar o interrumpir a la víctima.
Ataque "Hombre en el medio"	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.
Autenticación de mensajes	Medida de seguridad diseñada para establecer la autenticidad de un mensaje por medio de un autenticador dentro de la transmisión derivada de ciertos elementos predeterminados del propio mensaje.
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.
No conformidad leve	Un control de GIS no se ha abordado o no cumple con el GLI-GSF (no sistemático) y ese juicio y experiencia indican que no es probable que resulte en la falla del sistema o reduzca su capacidad para garantizar procesos o productos controlados. Puede ser: • Un error en alguna parte del sistema en relación con un control; o • Un solo lapso observado en el seguimiento de un elemento del sistema.
Código móvil	Código ejecutable que se mueve de un equipo a otro, incluyendo tanto código legítimo como código malicioso como virus informáticos.

Término	Descripciones
Autenticación multifactor (MFA)	Un tipo de autenticación que usa dos o más de los siguientes para verificar la identidad de un usuario: • Información que solo conoce el usuario (por ejemplo, una contraseña, PIN 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, patrones de retina, datos de reconocimiento facial o huellas de voz).
Equipo de comunicación de red (NCE)	Tecnología de comunicaciones que controla la comunicación de datos en un sistema, incluidos, entre otros, NIC, cables, conmutadores, puentes, concentradores, enrutadores, puntos de acceso inalámbricos y teléfonos, dispositivos de red VoIP, puntos de acceso inalámbricos, dispositivos de red y otros dispositivos de seguridad.
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	Un hallazgo que vale la pena destacar para una posible mejora para cumplir con las mejores prácticas de la industria.
Contraseña	Cadena de caracteres (letras, números y otros símbolos) que se usa para autenticar una identidad o para verificar la autorización de acceso.
Información de identificación personal (PII)	Datos confidenciales que podrían usarse para identificar a una persona en particular. Los ejemplos incluyen un nombre legal, fecha de nacimiento, lugar de nacimiento, número de identificación gubernamental (número de seguro social, número de identificación del contribuyente, número de pasaporte o equivalente), información financiera personal (números de instrumentos de crédito o débito, números de cuentas bancarias, etc.) u otra información personal si así 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 y la infraestructura del Entorno de Producción de Juegos.
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).
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.
Protocolo	Conjunto de reglas y convenciones que especifica el intercambio de información entre dispositivos, a través de una red u otros medios.
Organismo regulador	El organismo gubernamental o equivalente que regula o controla las operaciones de los juegos de azar.
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 (router) 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, la autenticación y la protección de la integridad del contenido adecuadas.
Shell seguro (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, ambos lados deben tener un certificado de seguridad válido.

Término	Descripciones

Datos confidenciales	Información que debe manejarse de manera segura, incluidas, entre otras, según corresponda:
	• Registros de auditoría y bases de datos del sistema que registran la información utilizada para determinar el resultado, el pago, el canje y el seguimiento de la información del usuario;
	• Información contable y de eventos significativos relacionados con los componentes críticos del sistema del GPE;
	• semillas RNG y cualquier otra información que afecte los resultados de los juegos y las apuestas;
	• Claves de cifrado, donde la implementación elegida requiere la transmisión de claves;
	• Números de validación asociados con cuentas de usuarios, instrumentos de apuestas y cualquier otra transacción de juego;
	• Transferencias de fondos hacia y desde cuentas de usuarios, cuentas de pago electrónico y con fines de juego;
	• Paquetes de software dentro del GPE;
	• Cualquier dato de ubicación relacionado con la actividad del empleado o cliente (por ejemplo, administración de cuentas, juegos en línea, etc.);
	• Cualquiera de la siguiente información registrada para cualquier empleado o cliente:
	  • Número de identificación gubernamental (número de seguro social, número de identificación del contribuyente, número de pasaporte o equivalente);
	  • Información financiera personal (números de instrumentos de crédito o débito, números de cuentas bancarias, etc.);
	  • Credenciales de autenticación en relación con cualquier cuenta de usuario o cuenta de usuario;
	  • Cualquier otra información de identificación personal (PII, por sus siglas en inglés) que deba mantenerse confidencial; y
	• Cualquier otro dato considerado sensible por el Organismo Regulador o la Empresa de Juego.

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 servicios	Entidades que ofrecen plataformas, software y servicios a empresas de juegos. Algunos ejemplos son los consultores de TI, los proveedores de servicios gestionados, las plataformas de software como servicio (SaaS) y los proveedores de servicios en la nube. Los proveedores y vendedores externos también se consideran proveedores de servicios.
Identificador de conjunto de servicios (SSID)	Un nombre que identifica una LAN inalámbrica 802.11 en particular.
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.
Verificación de firma	Garantizar mediante la verificación de 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).
Ingeniería Social	Un intento de engañar a alguien para que revele información (por ejemplo, una contraseña) que se puede usar 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 una persona no esté familiarizada con la tecnología y los protocolos emergentes.

Término	Descripciones
Código fuente	Una lista de texto de comandos que se compilarán o ensamblarán en un programa informático ejecutable.
Protocolo sin estado	Esquema de comunicaciones que trata cada solicitud como una transacción independiente que no está relacionada con ninguna solicitud anterior, de modo que la comunicación consta de pares independientes de solicitudes y respuestas.
Interruptor	Conecta dispositivos en una red 802.3. Un switch reenvía los datos a su destino mediante la dirección MAC incrustada 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 e infraestructura del entorno de producción de juegos para proteger contra el acceso no autorizado, las 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, las funciones, la imagen o la reputación), los activos o las personas a través de un sistema a través del acceso no autorizado, la destrucción, la divulgación, la modificación de la información y / o DoS; 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.
Marca 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 comunicación 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.
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.
Vulnerabilidad	Software, hardware u otras debilidades en una red o sistema que pueden proporcionar una "puerta" para la introducción de una amenaza.
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 un 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.
Acceso protegido Wi-Fi (WPA)	El sucesor de WEP. Su autenticación se puede romper en ciertas 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.