GLI®

MARCO DE SEGURIDAD DEL JUEGO

GLI-GSF-4

AUDITORÍA DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN DEL JUEGO (GIS) – JUEGO PRESENCIAL

Versión 1.0 BORRADOR – Publicado el 25 de julio de 2025

Contenido

1. INTRODUCCIÓN

1.1. Declaración general

La integridad y precisión de la operación de un entorno de producción de juegos (GPE) depende 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 empresa de seguridad independiente (ISF) calificada para realizar evaluaciones de seguridad de juego como una adición esencial a las pruebas y certificación de los componentes críticos del sistema de un GPE por parte de un laboratorio de pruebas independiente (ITL).

a. Este módulo del Marco de Seguridad del Juego GLI, GLI-GSF-4, establece los Controles de Seguridad de la Información del Juego (GIS) adicionales al GLI-GSF-1, que son necesarios para auditar el Sistema de Gestión de Seguridad de la Información del Juego (GISMS) de una Empresa de Juego para garantizar una gestión eficaz de la seguridad en el GPE de una Empresa de Juego utilizado en operaciones de juego presenciales, como un casino, sala de juego, hipódromo u otro lugar o ubicación física de juego, que ofrezca dispositivos de juego, juegos de mesa, bingo, lotería, apuestas de eventos o cualquier otra forma de juego presencial.
b. Este módulo está destinado a ser evaluado como un complemento del GLI-GSF-1, que proporciona los controles de GIS comunes necesarios para auditar el GISMS de una empresa de juegos.
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 pueden aplicarse módulos adicionales de GLI-GSF.

NOTA: Todo el Marco de Seguridad para Juegos de GLI (GLI-GSF) está disponible de forma gratuita a www.gaminglabs.com.

1.2. Rol de gestión de datos confidenciales y empresas 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, proveedores 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 a 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 confidenciales. Para obtener información adicional, consulte la sección "Rol de gestión de datos confidenciales y empresas de juegos" del GLI-GSF-1.

NOTA: Este documento no pretende definir qué entidades son responsables de cumplir con cada control de GIS. Es responsabilidad de las múltiples entidades que componen la Empresa de Juegos acordar la responsabilidad.

1.3. Entorno de producción del juego (GPE)

Un GPE se refiere al entorno operativo en el que las actividades de juego presenciales y los servicios relacionados se llevan a cabo, gestionan y presentan a los clientes en vivo o en tiempo real. Abarca la infraestructura física y virtual, los sistemas, el software y los procesos necesarios para facilitar diversas formas de juegos presenciales, como los juegos en vivo y electrónicos, la lotería minorista y las apuestas de eventos minoristas. El GPE también abarca los sistemas de backend, las aplicaciones comerciales y la infraestructura que interactúan y / o respaldan las actividades de juego presenciales. Las características clave de un GPE se describen en la sección "Entorno de producción de juegos (GPE)" del GLI-GSF-1.

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 al involucrar la identificación de riesgos de GIS, la implementación de controles y salvaguardas apropiados, 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 presenciales es primordial para mantener la confianza pública en el sector. Por lo tanto, las empresas de juegos que ofrecen juegos presenciales deben establecer y mantener un marco claramente definido y documentado para lograr y preservar la confianza pública en sus operaciones. El objetivo es alinear 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 pautas 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, estándares técnicos 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 que se aplicarán a los juegos presenciales junto con los controles de GIS comunes del GLI-GSF-1.

2. AUDITORÍAS DE CONTROLES PRESENCIALES DE GIS (LGIS)

2.1. Descripción general de la auditoría

La Auditoría de Controles de LGIS 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 Juegos. 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-4 está en los controles específicos de seguridad de la información para los juegos terrestres que se aplicarán, además de los controles comunes de seguridad de la información para los juegos en GLI-GSF-1, otros métodos de evaluación se discuten en los módulos de soporte del GLI-GSF.

2.2. Métodos de auditoría

Una auditoría de controles de LGIS utiliza una variedad de métodos de evaluación que incluyen los siguientes métodos, cuyos resultados se utilizan para respaldar la determinación de la efectividad del control de LGIS a lo largo del tiempo. Se puede encontrar información adicional sobre los "Métodos de auditoría" en el GLI-GSF-1.

2.3. Tareas de auditoría

El Apéndice detalla los controles de LGIS mínimos con más detalle. Los usuarios de este documento son dirigidos al Apéndice, así como al Apéndice del GLI-GSF-1 para asegurarse de que no se pasen por alto los controles de GIS necesarios. Los controles de LGIS enumerados en el Apéndice no son exhaustivos y, además de los controles de GIS comunes del GLI-GSF-1, se pueden incluir controles de GIS adicionales en función de los requisitos reglamentarios y el alcance de la evaluación. La información sobre las actividades de auditoría de controles de alto nivel de LGIS se puede encontrar en la sección "Tareas de auditoría" en el GLI-GSF-1.

2.4. Frecuencia de auditoría

Además, según el calendario de las Auditorías de Controles de LGIS expresado en la sección "Frecuencia de Auditoría" del GLI-GSF-1, la Empresa de Juegos debe, como regla, tener Auditorías de Controles de LGIS adicionales realizadas por un ISF después de cualquier cambio crítico que pueda afectar la seguridad del GPE o permitir el acceso a datos confidenciales y/o Componentes Críticos del Sistema. Estas auditorías pueden centrarse específicamente en los cambios críticos y los componentes críticos del sistema afectados por los cambios. Estos cambios críticos pueden incluir, entre otros

a. Despliegue de nuevos sistemas
    i. Integración de sistemas de monitoreo y control, sistemas de validación, controladores de jackpot, sistemas sin efectivo, motores de apuestas de eventos y otros sistemas de juego en línea nuevos o muy modificados
    ii. Lanzamiento de nuevas verticales de juego (por ejemplo, apuestas de eventos, juegos de mesa electrónicos)
    iii. Expansión de la huella de juego que resulta en la adición de equipos de juego electrónicos, lugares de juego y nuevas áreas de juego
b. Cambios en la infraestructura y la arquitectura del backend
    i. Migración a un nuevo proveedor de nube o alojamiento
    ii. Adopción de modelos de contenedorización, microservicios o sin servidor
    iii. Despliegue de nuevos centros de datos (especialmente interjurisdiccionales)
c. Modificaciones al almacenamiento y manejo de datos confidenciales
    i. Cambios en el almacenamiento, el registro, el cifrado o la retención de datos confidenciales
    ii. Cambios en la residencia de datos confidenciales (por ejemplo, mover el almacenamiento primario de datos confidenciales de una ubicación a otra)
d. Principales actualizaciones de la base de código o de la plataforma
    i. Actualizaciones significativas de los componentes críticos del sistema
    ii. Uso de nuevos frameworks de desarrollo o lenguajes de programación

iii. Integración de funciones basadas en IA (por ejemplo, análisis de comportamiento, detección de fraudes)

e. Cambios en los sistemas de pago o transacciones financieras
   i. Integración de nuevos procesadores de pagos, billeteras o API bancarias
   ii. Introducción de métodos de pago alternativos
   iii. Cambios en los mecanismos de retiro, depósito o pago
   iv. Ajuste a la lógica de las transacciones financieras en todo el sistema
f. Cambios en los incentivos para los clientes y las soluciones sin efectivo
   i. Introducción de nuevas ofertas de incentivos y métodos de juego sin efectivo
   ii. Cambios en las funciones de bonificación externas, promociones y métodos de acceso a la cuenta
   iii. Integración con proveedores de incentivos de terceros y proveedores externos sin efectivo
g. Activadores de respuesta a incidentes
   i. Cualquier violación de datos, compromiso de servicio o evento de fraude
   ii. Detección de malware, dispositivos tramposos o actividad de colusión
h. Cualquier otro cambio que el Organismo Regulador considere crítico

NOTA: Ciertos cambios críticos también pueden requerir que se realice un análisis de vulnerabilidades o pruebas de seguridad técnica de juegos (GTS) específicamente en los cambios críticos y los componentes críticos del sistema afectados por los cambios. Consulte GLI-GSF-2 para obtener información adicional.

2.5. Informes de auditoría

Los resultados de una auditoría de controles de LGIS identifican para las empresas de juegos aquellas áreas en las operaciones donde se debe considerar la mejora y recomiendan estrategias para mejorar esas áreas. El informe de auditoría de controles de LGIS debe cumplir con los requisitos de "Informes de auditoría" que se especifican en el GLI-GSF-1.

2.6. Remediación

Si el informe de auditoría de controles de LGIS de la ISF recomienda la corrección, la empresa de juegos 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 de la empresa de juegos y el cronograma para implementar los pasos de remediación. Para obtener información adicional, consulte la sección "Remediación" del GLI-GSF-1.

2.7. Empresa de seguridad independiente (ISF)

La Auditoría de Controles de LGIS debe ser realizada por personas con calificaciones suficientes, lo que significa que el ISF debe emplear personas suficientemente calificadas, competentes y experimentadas. A menos que el Organismo Regulador especifique lo contrario, estas personas deben cumplir con los requisitos especificados para una "Empresa de Seguridad Independiente (ISF)" en el GLI-GSF-1.

APÉNDICE: CONTROLES DE SEGURIDAD DE LA INFORMACIÓN (GIS) DE JUEGOS PRESENCIALES

Además de los controles de GIS comunes especificados en el GLI-GSF-1 para las empresas de juego GIG1, GIG2 o GIG3 (según corresponda), los siguientes controles de GIS adicionales se aplican a los GPE de las empresas de juego que ofrecen juegos presenciales.

LGIS-1	**Verificación de integridad de componentes críticos del sistema**
LGIS-1.1	**Verificación de integridad de software, hardware y configuración**
LGIS-1.1.1	Se deben establecer e implementar procedimientos documentados para verificar periódicamente y bajo demanda que los programas de control críticos, los componentes de hardware y las configuraciones significativas sean auténticos, inalterados e idénticos a las versiones certificadas por un laboratorio de pruebas independiente aprobado y autorizado por el organismo regulador.
LGIS-1.1.2	Las verificaciones deben realizarse a intervalos definidos, como en la instalación inicial, después de cualquier programa de control crítico u otro reemplazo de componentes críticos del sistema, después de un mantenimiento significativo, periódicamente según lo definido por la evaluación de riesgos (por ejemplo, diaria o semanalmente para parámetros críticos) y a pedido del personal designado.
LGIS-1.2	**Registro de auditoría de verificación**
LGIS-1.2.1	Todas las actividades de verificación de integridad deben registrarse en un registro de auditoría de verificación al que el organismo regulador debe acceder a pedido.
LGIS-1.2.2	El registro de auditoría de verificación debe detallar lo siguiente para cada verificación de firma: a. La fecha y hora de la verificación; b. Descripción de los componentes o configuraciones verificadas; c. Detalles de cualquier discrepancia o falla detectada; d. Acciones correctivas tomadas y estado de resolución e. Cuando se realiza a pedido, la persona que inició el procedimiento de verificación;
LGIS-1.3	**Error de verificación**
LGIS-1.3.1	Cualquier falla en la verificación de integridad de cualquier Programa de Control Crítico debe requerir una notificación de la falla de verificación que se comunicará a la Empresa de Juegos.
LGIS-1.3.2	Cuando lo requiera el Organismo Regulador, la Empresa de Juegos debe informar al Organismo Regulador de cualquier falla en las actividades de verificación de integridad y las acciones correctivas tomadas sin demora indebida.
LGIS-2	**Procedimientos del sistema**
LGIS-2.1	**Detección y respuesta a eventos de reinicio maestro**
LGIS-2.1.1	La empresa de juegos debe establecer controles para detectar, identificar y responder adecuadamente a cualquier ocurrencia de un reinicio maestro en un componente crítico del sistema.
LGIS-2.1.2	El evento de restablecimiento maestro debe registrarse con una marca de tiempo, incluida la identificación del componente crítico del sistema relevante y el contexto del usuario.
LGIS-2.2	**Protección contra copia**
LGIS-2.2.1	Se puede implementar protección contra copia para evitar la duplicación o modificación no autorizada del software con licencia, incluidos los Programas de Control Críticos, siempre que: a. El método de protección contra copia está plenamente documentado y se verifica que la protección funciona como se describe; o b. El programa o componente involucrado en la aplicación de la protección contra copia puede verificarse individualmente mediante la metodología aprobada por el Organismo Regulador.
LGIS-3	**Personal de tecnología de la información (TI)**
LGIS-3.1	**Segregación de funciones**
LGIS-3.1.1	El personal de TI debe ser operativamente independiente de las funciones relacionadas con el juego dentro del lugar de juego.
LGIS-3.1.2	Se deben implementar políticas de GIS y procedimientos documentados para garantizar una separación funcional adecuada entre el personal de TI y los responsables de las operaciones financieras o de juego.

LGIS-3.1.3	Las políticas de GIS y los procedimientos documentados deben incluir, entre otros: a. Restricciones de acceso lógicas y físicas; b. Controles de acceso basados en roles (RBAC); y c. Monitoreo, registros de auditoría y revisiones de acceso.
LGIS-3.2	**Responsabilidades y restricciones del personal de TI**
LGIS-3.2.1	Todas las responsabilidades y restricciones de TI deben documentarse formalmente en procedimientos escritos, con roles y deberes comunicados al personal relevante y revisados periódicamente.
LGIS-3.2.2	El personal de TI debe estar restringido de: a. Acceder o manejar instrumentos financieros (por ejemplo, efectivo, instrumentos de apuestas o equivalentes) o activos financieros líquidos en cualquier forma; b. Acceso y revisión de registros contables y documentación de auditoría; y c. Iniciar, autorizar o aprobar entradas en libros mayores generales o subsidiarios. d. Acceder a formularios de pago u otros instrumentos que representen valor al cliente.
LGIS-3.2.3	El personal de TI no puede tener autoridad de signatario sobre: a. Instrumentos financieros (por ejemplo, efectivo, instrumentos de apuestas o equivalentes); y b. Formularios de pago u otros instrumentos que representen valor al jugador.
LGIS-3.2.4	Se debe impedir que el personal de TI tenga acceso no autorizado a lo siguiente: a. Consolas de servidor y terminales de usuario ubicadas dentro de las áreas de juego; b. Documentos fuente (por ejemplo, registros contables originales); y c. Archivos de datos de producción en vivo, excepto cuando estén específicamente autorizados para pruebas o resolución de problemas.
LGIS-3.2.5	El acceso del personal de TI a los datos de prueba en entornos que no son de producción está permitido bajo condiciones controladas establecidas por la empresa de juego.
LGIS-4	**Áreas de servidor seguras y armarios de datos**
LGIS-4.1	**Seguridad física de componentes e infraestructura**
LGIS-4.1.1	Todos los componentes de control críticos instalados localmente y la infraestructura de TI que no sea de juego se alojarán dentro de un área de servidor segura y armarios de datos dentro del lugar de juego.
LGIS-4.1.2	El área segura del servidor y los armarios de datos deben estar físicamente protegidos para evitar el acceso no autorizado, el daño ambiental y la interrupción del servicio.
LGIS-4.1.3	El área segura del servidor y los armarios de datos deben ubicarse lejos de áreas con alto riesgo de daño físico u observación no autorizada.
LGIS-4.2	**Vigilancia de áreas de servidores seguras y armarios de datos**
LGIS-4.2.1	Los sistemas de vigilancia deben proporcionar cobertura no solo para el área de juego, sino también para el área segura del servidor y los armarios de datos y todos los métodos para acceder al área segura del servidor y los armarios de datos.
LGIS-5	**Controles de acceso físico**
LGIS-5.1	**Restricciones de acceso y autorización**
LGIS-5.1.1	El acceso al área segura del servidor y a los armarios de datos estará estrictamente restringido al personal autorizado, tal y como se define en las políticas y procedimientos formales de control de acceso de la Empresa de Juego.
LGIS-5.1.2	La autorización debe basarse en roles y limitarse a la necesidad operativa.
LGIS-5.1.3	La Empresa de Juegos mantendrá un registro de acceso actualizado o un registro de todo el personal al que se le otorguen privilegios de acceso seguro al área del servidor.
LGIS-5.2	**Control de dispositivos de acceso**
LGIS-5.2.1	Los dispositivos de acceso (por ejemplo, llaves, tarjetas de acceso, llaveros) utilizados para ingresar al área segura del servidor o armarios de datos deben ser: a. Numerado y asignado de forma única; y b. Controlado y administrado por personal independiente de las operaciones de TI y las funciones de juego.
LGIS-5.2.2	La empresa de juegos debe mantener la documentación de cada tipo de dispositivo de acceso, sus funciones y los puestos de trabajo autorizados para ser asignados y usar ese dispositivo de acceso.
LGIS-5.2.3	La responsabilidad de la emisión, revocación y auditoría de los dispositivos de acceso debe asignarse claramente en la Política de GIS.

LGIS-5.2.4	Cada dispositivo de acceso solo debe ser: a. Asignado al personal que necesita el dispositivo de acceso para realizar sus tareas laborales; y b. Utilizado por el personal al que se asigna el dispositivo de acceso.
LGIS-5.2.5	La empresa de juegos debe mantener una lista de todos los números de dispositivos de acceso y el personal asignado a cada dispositivo de acceso.
LGIS-5.2.6	Cualquier dispositivo de acceso que pueda usarse en varios lugares de juego debe tratarse como una clave confidencial.
LGIS-6	**Controles de acceso lógico**
LGIS-6.1	**Integración de controles de acceso lógico**
LGIS-6.1.1	Se deben implementar controles de acceso lógico para complementar y reforzar las medidas de seguridad física. Los controles de acceso lógico incluyen, entre otros: a. Autenticación de usuario (por ejemplo, ID de cuenta de usuario únicos, contraseñas seguras, biometría, autenticación multifactor, etc.); b. Control de acceso basado en roles (RBAC) alineado con los principios de privilegios mínimos; c. Segmentación del sistema y la red para restringir las vías no autorizadas; d. Registro de auditoría y monitoreo de intentos y actividades de acceso; y e. Alertas automatizadas para accesos no autorizados o comportamientos anómalos.
LGIS-6.1.2	Los controles de acceso lógico garantizarán que solo el personal autorizado pueda acceder a los componentes de control críticos instalados localmente y a la infraestructura de TI no relacionada con el juego.
LGIS-6.2	**Identificación automatizada de equipos**
LGIS-6.2.1	Cuando se emplean, se deben usar métodos automatizados de identificación de equipos, como el filtrado de direcciones MAC, certificados de dispositivos, tokens de seguridad de hardware u otras técnicas criptográficas, para autenticar conexiones desde equipos y ubicaciones específicos.
LGIS-6.2.2	Los mecanismos automatizados de identificación de equipos deben: a. Estar completamente documentado, incluido el método de identificación, el equipo autorizado y los derechos de acceso asociados; b. Integrarse en los procedimientos lógicos de control de acceso de la organización; c. Ser incluido en las revisiones periódicas de los derechos de acceso de los usuarios y los privilegios del sistema para garantizar que el acceso siga siendo apropiado y autorizado; y d. Apoyar el no repudio asociando el acceso al sistema tanto con el usuario autenticado como con el equipo verificado.
LGIS-6.3	**Bloqueo automático de sesiones y seguridad**
LGIS-6.3.1	Las consolas de servidor, las estaciones de trabajo, los terminales de usuario, los dispositivos electrónicos portátiles (por ejemplo, tabletas electrónicas u otros terminales portátiles) o los quioscos dentro de un Lugar de juego deben protegerse automáticamente después de un período definido de inactividad para evitar el acceso no autorizado.
LGIS-6.3.2	Los métodos y procedimientos para el bloqueo automático de sesiones, para cada tipo de dispositivo, deben delinearse dentro de la Política de GIS e incluir como mínimo: a. El período definido de inactividad según lo determinado por la gerencia: i. Para dispositivos electrónicos portátiles, el período no debe exceder los 2 minutos. ii. Para todos los demás dispositivos, el período no debe exceder los 15 minutos. b. Para dispositivos electrónicos portátiles y quioscos: i. Las funciones y/o aplicaciones del sistema que están disponibles o a las que se puede acceder en o a través de cada dispositivo o quiosco; ii. Los controles sobre el acceso de los usuarios a las funciones y aplicaciones del sistema; y iii. Los procedimientos utilizados para proteger la red cuando dichos dispositivos/quioscos están en uso. c. En el caso de los dispositivos electrónicos portátiles, los controles sobre la protección física y la distribución de dichos dispositivos.

LGIS-7	**Acceso remoto a equipos, sistemas y otros componentes instalados**
LGIS-7.1	**Acceso remoto del proveedor**
LGIS-7.1.1	Se debe restringir el acceso remoto del proveedor a los equipos de juego electrónicos, los sistemas de juego y otros componentes críticos del sistema instalados en el lugar de juego.
LGIS-7.1.2	Se debe utilizar la autenticación multifactor si se requiere acceso remoto del proveedor para fines de mantenimiento o administración.
LGIS-7.1.3	Los métodos de acceso remoto deben ser mantenidos, controlados y supervisados por la empresa de juego, no por el Proveedor.
LGIS-7.2	**Acceso telefónico remoto**
LGIS-7.2.1	Si se permite la conexión telefónica remota al equipo de juego electrónico, los sistemas de juego y otros componentes críticos del sistema para el soporte de software, la operación de juego debe mantener un registro de acceso que incluya: a. Nombre del empleado que autoriza el acceso al módem; b. Nombre del programador autorizado o representante del proveedor de servicios; c. Motivo del acceso al módem; d. Descripción del trabajo realizado; y **e.** Fecha, hora y duración del acceso.
LGIS-8	**Seguridad de la red del lugar de juego**
LGIS-8.1	**Conectividad**
LGIS-8.1.1	Solo se debe permitir que los equipos autorizados establezcan comunicaciones entre los componentes críticos del sistema.
LGIS-8.1.2	La empresa de juegos debe proporcionar un método para a. Realizar autenticación mutua para garantizar que los equipos autorizados solo se comuniquen con redes válidas; b. Inscribir y anular la inscripción de componentes críticos del sistema; y c. Habilitar y deshabilitar componentes críticos específicos del sistema.
LGIS-8.1.3	Solo los componentes críticos del sistema inscritos y habilitados pueden participar en operaciones de juego.
LGIS-8.1.4	La condición predeterminada para los componentes críticos del sistema debe ser no inscrito y deshabilitado.
LGIS-8.1.5	El establecimiento, la pérdida y el restablecimiento de las comunicaciones entre los componentes críticos del sistema deben registrarse en un registro de auditoría.
LGIS-8.2	**Seguridad de conexión de equipos de juego electrónicos**
LGIS-8.2.1	Los equipos de juego electrónicos no deben conectarse a sus respectivos sistemas de juego a través de conexiones de red inseguras o no autorizadas.
LGIS-8.2.2	Se deben realizar auditorías periódicas de las conexiones y configuraciones de red de los equipos electrónicos de juego.
LGIS-8.2.3	Cualquier desviación de los métodos de conexión aprobados debe documentarse y justificarse.
LGIS-8.3	**Segmentación de red**
LGIS-8.3.1	La red de juego, que abarca todos los equipos de juego electrónicos, sistemas de juego y otros componentes críticos del sistema, debe estar lógica y/o físicamente separada (segmentada) de las redes corporativas/comerciales, las redes de invitados y cualquier otra red que no sea de juego dentro del lugar de juego.
LGIS-8.3.2	La empresa de juegos debe implementar redes de área local virtuales (VLAN) para la segmentación lógica y considerar conmutadores físicos separados para segmentos altamente críticos.
LGIS-8.3.3	Todas las rutas de comunicación entre la red de juegos y cualquier red que no sea de juegos deben documentarse explícitamente (detallando el origen, el destino, los puertos, los protocolos y la justificación comercial), ser aprobadas por la administración de TI y controladas estrictamente a través de firewalls configurados adecuadamente u otros dispositivos de protección de límites adecuados que se adhieran a una postura de seguridad de denegación predeterminada.
LGIS-8.4	**Puertos de acceso y protección de puertos de datos**
LGIS-8.4.1	Todos los puntos de acceso inalámbricos (WAP), puertos de datos por cable (WDP) y otras ubicaciones de acceso público en el Lugar de juego que brindan conectividad de red deben estar protegidos física/lógicamente o deshabilitados si no están en uso.

LGIS-8.4.2	Los WAP y WDP activos deben estar controlados por la seguridad del puerto de control de admisión de red (NAC) o un mecanismo equivalente para evitar conexiones de dispositivos no autorizadas.
LGIS-8.4.3	Los WAP y WDP deben ubicarse para minimizar las oportunidades de acceso físico directo no autorizado por parte del público en general
LGIS-8.4.4	Se deben usar cerraduras físicas, sellos a prueba de manipulaciones o bloqueadores de puertos en WDP no utilizados.
LGIS-8.4.5	El sistema de vigilancia debe proporcionar cobertura para WAP, WDP y otras ubicaciones de acceso público en el lugar de juego que brinden conectividad de red

DEFINICIONES DE TÉRMINOS

Término	Descripciones
Acceso	Capacidad para hacer uso de cualquier recurso del GPE.
Control de acceso	El proceso de otorgar o denegar solicitudes específicas para obtener y utilizar datos confidenciales y servicios relacionados específicos de un sistema; y para ingresar a instalaciones físicas específicas que albergan infraestructura crítica de red o sistema.
Protocolo de resolución de direcciones (ARP)	El 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 pautas implementadas por una empresa de juegos para administrar su GISMS.
Estándares de cifrado avanzados (AES)	Un cifrado de bloques simétrico que puede cifrar (encriptar) y descifrar (desencriptar) 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 auditoria	Un registro auditable de acciones, eventos o cambios dentro de un GPE, capturando detalles como actividades de usuario, intentos de acceso, alteraciones y operaciones del sistema para garantizar la seguridad, el cumplimiento y la contabilidad 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 en el GPE
Credenciales de autenticación	Cualquier contraseña, autenticación multifactor, certificados digitales, PIN, biometría, preguntas y respuestas de seguridad y cualquier otro método de acceso a la cuenta (por ejemplo, deslizamiento magnético, tarjetas de proximidad, tarjetas con chip integradas).
Disponibilidad	Garantizar el acceso y el uso oportunos y confiables de la información.
Copia de seguridad	Una copia de archivos y programas hechos 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 empresariales	Aplicaciones que funcionan como un servicio compartido para que los usuarios recopilen, procesen, mantengan, usen, 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 evitar la pérdida de datos en caso de una falla importante de hardware o software o destrucción de 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 por cable, inalámbricas, por cable, de radio, microondas, luz, fibra óptica, satélite o informática, incluidas Internet e intranets.
Cumple	Se consideró que la política y la evidencia observadas 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 gestión 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 los comportamientos en relación con cualquier estándar técnico y/o requisito reglamentario aplicable, como ejecutables, librerías, configuraciones de juegos o sistemas, archivos del sistema operativo, componentes que controlan los informes requeridos del sistema y elementos de bases de datos que afectan los juegos o las operaciones 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 cuya falla o compromiso pueda conducir a la pérdida de los derechos de los usuarios, ingresos gubernamentales o acceso no autorizado a los datos utilizados para generar informes para el Organismo Regulador. Los ejemplos de componentes críticos del sistema incluyen, entre otros: • Componentes que registran, almacenan, procesan, comparten, transmiten o recuperan datos confidenciales. • Componentes que podrían afectar la seguridad de los datos confidenciales o el 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 cliente. • Puntos de entrada y salida de los componentes anteriores, incluidos otros sistemas que se comunican directamente con los componentes críticos del sistema. • Tecnología y redes de comunicaciones que transmiten datos confidenciales, incluidos los equipos de comunicación de red (NCE) y los controles de seguridad de la 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 de red internos. • 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 que incluyen web, aplicación, base de datos, autenticación, correo, proxy, protocolo de tiempo de red (NTP) y sistema de nombres de dominio (DNS). • Dispositivos de terminales de usuario, 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 gestión 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, redes de casinos corporativos y redes corporativas de operadores en línea). • Cualquier otro componente considerado crítico para el GPE por el Organismo Regulador o la Empresa de Juegos
Módulo criptográfico	Hardware, software, firmware o combinación de los mismos que implementan funciones criptográficas como cifrado, descifrado, firmas, hash y administración de claves. El propósito principal de un módulo criptográfico es proporcionar un procesamiento y almacenamiento seguros de claves y operaciones.
Integridad de datos	La propiedad de que los datos son precisos y consistentes y no se han alterado de manera no autorizada en el almacenamiento, durante el procesamiento y mientras están en tránsito.
Denegación de servicio distribuida (DDOS)	Un tipo de ataque en el que se utilizan múltiples sistemas comprometidos, generalmente infectados con un programa de software destructivo, para apuntar a 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 pirata informático en el ataque distribuido.
Dominio	Un grupo de computadoras 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 los nombres de las máquinas a los 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 se transmite una solicitud a través del segmento de red, luego cualquier servidor responde a esa máquina específica con una dirección, cuánto tiempo es válida esa dirección y otros detalles pertinentes.
Equipos electrónicos de juego	Un dispositivo de juego, un juego de mesa electrónico, una estación de apuestas electrónicas, un componente de gestión de juegos en vivo, un terminal de lotería, un dispositivo de apuestas, un quiosco o cualquier otro componente crítico de juegos electrónicos y su Elemento de interfaz destinado a ser utilizado con un Sistema de juego.
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 una forma, llamada texto cifrado, que no puede ser fácilmente entendida 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 revisarlas caso por caso.
Clave de cifrado	Una clave que se ha cifrado para ocultar el valor del texto sin formato subyacente.
Aplicaciones expuestas externamente	Aplicaciones que son públicas y detectables a través del reconocimiento y el escaneo de red desde la Internet pública fuera de la red de la empresa. Esto no se aplica a las aplicaciones destinadas al uso de los usuarios.

Término	Descripciones
Activos empresariales expuestos externamente	Activos que son públicos y detectables 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.
Cortafuegos	Un componente de un sistema informático o red que está diseñado para bloquear el acceso o el tráfico no autorizados al mismo tiempo que permite la comunicación externa.
Empresa de juegos	Un operador y cualquier proveedor, fabricante, vendedor, proveedor de servicios y/u otras entidades que tengan un papel en la supervisión del funcionamiento de un GPE o en la prestación de servicios integrales a su función, incluida la gestión de datos confidenciales.
Seguridad de la información de juego (GIS)	Proteger los datos confidenciales y los componentes críticos del sistema contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar integridad, confidencialidad y disponibilidad.
Sistema de gestión de seguridad de la información de juegs (GISMS)	Un sistema de gestión definido y documentado que consiste en un conjunto de políticas, procesos y sistemas para gestionar los riesgos de los datos, activos y componentes críticos del sistema confidenciales de una empresa de juegos dentro de un GPE, con el objetivo de garantizar niveles aceptables de riesgo de GIS.
Entorno de producción del juego (GPE)	El entorno operativo donde las actividades de juego y los servicios relacionados se llevan a cabo, administran y entregan a los clientes en vivo o en tiempo real. Abarca la infraestructura física y virtual, los sistemas, el software y los procesos necesarios para facilitar diversas formas de juego y/o administrar datos confidenciales, así como los sistemas de backend y la infraestructura que interactúan y/o respaldan las actividades de juego.
Entrada	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 establece las bases necesarias para medir de manera confiable el progreso y el cumplimiento.
Incidente de GIS	Un suceso que ponga 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 de seguridad, los procedimientos de seguridad o las políticas de uso aceptable.
Plan de respuesta a incidentes de GIS	La documentación de un conjunto predeterminado de instrucciones o procedimientos cuando se encuentra un ciberataque malicioso contra el GPE de una empresa de juegos
Membresía de grupo	Un método para organizar 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 utilizado para definir cómo se formatean y transmiten los mensajes, y qué acciones deben realizar los servidores y navegadores en respuesta a varios comandos.
Concentrador	Conecta dispositivos en una red de par trenzado. Un concentrador no realiza ninguna tarea además de la regeneración de señales.
Personal de Tecnología de la Información (Personal de TI)	Personal que tiene acceso a componentes críticos del sistema instalados localmente e infraestructura de TI no relacionada con el juego dentro de un lugar de juego
Integridad	Proteger contra la modificación o destrucción indebida de información e incluye garantizar el no repudio y la autenticidad de la información.

Término	Descripciones
Internet	Un sistema interconectado de redes que conecta computadoras de todo el mundo a través de TCP/IP.
Dirección de protocolo de Internet (dirección IP)	Número único de un equipo que se utiliza para determinar dónde deben entregarse los mensajes transmitidos en Internet. La dirección IP es análoga a un número de casa para el correo postal ordinario.
Sistema de detección de intrusos/Sistema de prevención de intrusiones (IDS/IPS)	Un sistema que inspecciona toda la actividad de red entrante y saliente e identifica patrones sospechosos que pueden indicar un ataque a la red o al sistema por parte de alguien que intenta ingresar 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 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 está dedicado a transmitir datos.
No conformidad mayor	Se ha identificado una falla fundamental (sistemática) que afecta a varios controles de GIS y significa que no se pueden cumplir las políticas de seguridad 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 mayor; • Cualquier no conformidad que resulte en el probable envío de un producto no conforme. Una condición que puede resultar en la falla o reducir materialmente la usabilidad de los productos o servicios para su propósito previsto; o • 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 garantizar 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 "Man-in-the-Middle"	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	Una medida de seguridad diseñada para establecer la autenticidad de un mensaje por medio de un autenticador dentro de la transmisión derivado de ciertos elementos predeterminados del propio mensaje.
Código de autenticación de mensajes (MAC)	Una suma de comprobación criptográfica en los datos que utiliza una clave simétrica para detectar modificaciones accidentales e intencionadas de los datos.
No conformidad menor	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

Término	Descripciones
	en la falla del sistema o reduzca su capacidad para garantizar procesos o productos controlados. Puede ser: • Una falla en alguna parte del sistema en relación con un control; o • Un solo lapso observado en el seguimiento de un elemento del sistema.
Código móvil	Código ejecutable que se mueve de una computadora a otra, incluido el código legítimo y el código malicioso, como los virus informáticos.
Autenticación multifactor (MFA)	Tipo de autenticación que utiliza dos o más de las siguientes opciones para comprobar la identidad de un usuario: • Información conocida solo por 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)	El 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 señalar por su posible mejora para cumplir con las mejores prácticas de la industria.
Contraseña	Una 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 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 de entrada o salida físico de un módulo que proporciona acceso al módulo para señales físicas, representado 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 y lo procesa y reenvía. Esto cierra efectivamente el camino recto entre las redes internas y externas. Dificultar que un atacante obtenga direcciones internas y otros detalles de la red interna.
Protocolo	Un 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 del juego.
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 las redes. Un enrutador utiliza la dirección de red configurada por software para tomar decisiones de reenvío.

Término	Descripciones
Protocolo de comunicación segura	Un protocolo de comunicación que proporciona la confidencialidad, la autenticación y la protección de la integridad del contenido adecuadas.
Área de servidor segura	Sala de servidores de TI, sala de telecomunicaciones y otros espacios dedicados en un lugar de juego que albergan componentes críticos del sistema e infraestructura de TI no relacionada con juegos.
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.

Datos confidenciales	Información que debe manejarse de manera segura, incluidos, entre otros, 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;
	• Contabilidad e información de eventos significativos relacionados con los componentes críticos del sistema del GPE;
	• Semillas del GNA 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 clientes, instrumentos de apuestas y cualquier otra transacción de juego;
	• Transferencias de fondos hacia y desde cuentas de clientes, cuentas de pago electrónico y con fines de juego;
	• Paquetes de software dentro del GPE;
	• Cualquier dato de ubicación relacionado con la actividad de los empleados o clientes (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 fiscal, 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) que deba mantenerse confidencial; y
	• Cualquier otro dato considerado sensible por el Organismo Regulador o la Empresa del Juego.

Servidor	Una instancia en ejecución de software que es capaz de aceptar solicitudes de clientes y la computadora 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 las empresas de juegos. Los ejemplos incluyen consultores de TI, proveedores de servicios administrados, plataformas de software como servicio (SaaS) y 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 Shell (Shellcode)	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 garantía de información de un sistema.

Término	Descripciones
Verificación de firma	Garantizar mediante firma electrónica la comprobación de que cualquier paquete de software es una copia auténtica del software creado por su fabricante y, en su caso, una copia exacta del software certificado por el Laboratorio de Pruebas Independiente (ITL).
Protocolo simple de administración de red (SNMP)	Protocolo que se utiliza para configurar, ver y, en general, administrar dispositivos en red. Las impresoras en red, los conmutadores, etc. a menudo implementan este protocolo de forma predeterminada.
Ingeniería social	Un intento de engañar a alguien para que revele información (por ejemplo, una contraseña) que puede usarse para atacar sistemas o redes. Los ataques de ingeniería social incluyen intrusiones no técnicas en un GPE utilizando información adquirida a través de la interacción humana y se basan en trucos que se aprovechan de que un individuo no esté familiarizado con la tecnología y los protocolos emergentes.
Código fuente	Una lista de texto de comandos que se compilarán o ensamblarán en un programa informático ejecutable.
Protocolo sin estado	Un esquema de comunicaciones que trata cada solicitud como una transacción independiente que no está relacionada con ninguna solicitud anterior, de modo que la comunicación consta de pares independientes de solicitudes y respuestas.
Interruptor	Conecta dispositivos en una red 802.3. Un conmutador reenvía datos a su destino mediante la dirección MAC incrustada en cada paquete.
Administrador del sistema	La(s) persona(s) responsable(s) de mantener el funcionamiento estable del GPE (incluida la infraestructura de software y hardware y el software de aplicación).
Controles técnicos	Los mecanismos de seguridad implementados dentro de los sistemas y la infraestructura del entorno de producción de juego (GPE) 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 la denegación de servicio; la posibilidad de que una fuente de amenaza explote con éxito una vulnerabilidad en particular; cualquier peligro potencial para una red que alguien o algo pueda identificar como vulnerable y, por lo tanto, tratar de explotar.
Marca de tiempo	Registro del valor actual de la fecha y 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)	El conjunto de protocolos de comunicaciones utilizados para conectar hosts en Internet.
Acceso no autorizado	Una persona obtiene acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso.
Protocolo de datagramas de usuario (UDP)	Un protocolo de transporte que no garantiza la entrega. Por lo tanto, es más rápido, pero menos confiable.
Control de versiones	El método por el cual se verifica en su evolución que los componentes críticos del sistema aprobados están funcionando 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, generalmente con intenciones maliciosas, que se ejecuta y se propaga modificando otros programas o archivos.
Escaneador de Virus	Software utilizado para prevenir, detectar y eliminar virus informáticos, incluidos malware, gusanos y troyanos.
Vulnerabilidad	Software, hardware u otras debilidades en una red o sistema que pueden proporcionar una "puerta" para introducir una amenaza.

Término	Descripciones
Protocolo equivalente por cable (WEP)	Un algoritmo fácilmente roto y, por lo tanto, obsoleto 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 dispositivos de red inalámbrica. Un WAP se usa 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 de 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.