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 – Publicado el 30 de septiembre 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 confidencialidad, integridad, disponibilidad, y contabilidad 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 de juego, 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 está basado 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 confidencialidad, integridad, disponibilidad, y contabilidad 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

La 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.

a. Entrevista: Tipo de método de evaluación caracterizado por el proceso de mantener conversaciones con personas o grupos dentro de un proveedor 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 comprobar, inspeccionar, revisar, observar, estudiar o analizar uno o más objetos de evaluación para facilitar la comprensión, lograr una aclaración u obtener pruebas.
c. Prueba: Tipo de método de evaluación caracterizado por el proceso de ejercer uno o más objetos de auditoría en condiciones específicas para comparar el comportamiento real con el esperado.

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 de este módulo, 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.

NOTA: 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, incluyendo, entre otros, la revisión de documentación, entrevistas, evaluación de controles, evaluación del plan de respuesta a incidentes del GIS y evaluación de riesgos.

2.4. Frecuencia de auditoría

Las auditorías de controles de LGIS deben ser realizadas por una ISF con la “frecuencia de auditoría” indicada en el GLI-GSF-1. Esto puede incluir auditorías adicionales solicitadas por el organismo regulador o la empresa de juego, centradas específicamente en cambios críticos dentro del GPE que podrían afectar a la seguridad del GPE, que podrían permitir el acceso a datos sensibles y/o componentes críticos del sistema, o cualquier otro cambio que afecte al flujo de datos o a la postura de seguridad.

NOTA: El organismo regulador o la empresa de juego también pueden solicitar que se realice un análisis de vulnerabilidades o pruebas de seguridad técnica del juego (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 para "Informes de auditoría" como 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.

NOTA: 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	Los procedimientos de verificación deben basarse en evaluaciones de riesgos y especificar claramente las herramientas, el personal responsable y los requisitos de documentación.
LGIS-1.1.3	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; y e. Identidad de la persona iniciando el procedimiento de verificación, cuando se realiza a pedido.
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 puede ser verificado 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, incluyendo, como mínimo, la separación de funciones, las líneas de responsabilidad y los controles de acceso.
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; c. Iniciar, autorizar o aprobar entradas en libros mayores generales o subsidiarios; y 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-4.1.4	Los cables dentro del área segura del servidor y los gabinetes de datos deben mantenerse adecuadamente y protegerse tanto de los riesgos ambientales como de posibles interferencias.
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-4.2.2	Cuando la cobertura de vigilancia no sea viable, la empresa de juegos de azar podrá considerar la posibilidad de permitir controles compensatorios, como registros de acceso restringido con tarjeta magnética.
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, tarjetas magnéticas, tarjetas de proximidad, tarjetas con chip integrado) 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 definido por la evaluación de riesgos; 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; iii. Los procedimientos utilizados para proteger la red cuando dichos dispositivos/quioscos están en uso; y 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 remoto; b. Nombre del programador autorizado o representante del proveedor de servicios; c. Motivo del acceso remoto; 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 implícita.
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 (por ejemplo, autenticación 802.1X, filtrado MAC, etc.).
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.
Controles administrativos	Políticas, procedimientos y pautas implementadas por una empresa de juegos para administrar su GISMS.
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
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 GIS.
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.
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.

Término	Descripciones
	• 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 servicio 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. • 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.
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.
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.
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.

Término	Descripciones
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 confidencialidad, integridad, disponibilidad, y contabilidad.
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 de juego, 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.
Sistemas de Juego	Componentes críticos del sistema que están relacionados con cualquier norma técnica y/o requisito reglamentario aplicable a las actividades de juego.
Incidente de GIS	Un evento que pone en peligro real o potencialmente la confidencialidad, disponibilidad, integridad, o contabilidad de un GPE o de los datos confidenciales que el GPE procesa, almacena o transmite, o que constituya una violación o una amenaza inminente de violación de las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable. Algunos ejemplos de incidentes notificables de GIS son, entre otros: • Acceso no autorizado a datos sensibles o componentes críticos del sistema. • Ejecución de código malicioso o infección por ransomware dentro del GPE. • Pérdida, robo o divulgación no autorizada de información de identificación personal. • Cortes o interrupciones del sistema que afecten a la integridad o disponibilidad de las operaciones de juego durante un período definido (por ejemplo, más de 15 minutos). • Detección de alteración, manipulación o intento de comprometer el software o hardware de juego. • Intentos de inicio de sesión fallidos repetidos o sistemáticos que indiquen un ataque de fuerza bruta. • Compromiso o uso indebido de credenciales administrativas o certificados de seguridad. • Cambios en la configuración de seguridad que fueron realizados al margen de los procesos de gestión de cambios autorizados.
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
Política de GIS	Un documento que describe la estructura de gestión de la seguridad, asigna claramente las responsabilidades en materia de seguridad y establece las bases necesarias para medir de forma fiable los avances y el cumplimiento.
Personal de tecnología de la información (personal de TI)	Personal que tiene acceso a componentes críticos del sistema instalados localmente y a infraestructura informática no relacionada con el juego dentro de un local de juego.
Integridad	Proteger contra la modificación o destrucción indebida de la información e incluir garantizar la no repudiación y autenticidad de la información.

Término	Descripciones
Clave	Un valor utilizado para controlar funciones criptográficas, como descifrado, cifrado, descifrado, firmas, hash, etc.
Seguridad por Capas	Un enfoque de defensa que utiliza múltiples protecciones independientes en todo un sistema, como cortafuegos, autenticación, cifrado y monitoreo, de modo que un atacante debe sortear varias capas antes de acceder a datos confidenciales o componentes críticos del sistema.
Malware	Un programa que se inserta en un sistema, generalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad, disponibilidad, y contabilidad de los datos, aplicaciones o sistema operativo de la víctima o de molestar o interrumpir a la víctima.
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.
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).
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.
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).
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 en el GPE.
Evaluación de Riesgo	Identificar, analizar y priorizar las amenazas y vulnerabilidades para las operaciones o activos de una empresa de juegos de azar, o para personas u otras entidades, que se derivan del deterioro de la confidencialidad, integridad, disponibilidad y responsabilidad de los datos confidenciales o de la fiabilidad, seguridad o capacidad del GPE.
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.

Término	Descripciones

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.
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).
Interruptor	Conecta dispositivos en una red IEEE 802.3. Un conmutador reenvía datos a su destino mediante la dirección MAC incrustada en cada paquete.
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.

Término	Descripciones
Acceso no autorizado	Una persona obtiene acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso.
Virus	Un programa autorreplicante, generalmente 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 introducir una amenaza.
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.
Estación de trabajo	Una interfaz para que el personal autorizado acceda a las funciones reguladas del GPE.