GLI®

MARCO DE SEGURIDAD DEL JUEGO

GLI-GSF-3

AUDITORÍA DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN DEL JUEGO (GIS) - CONTROLES DE PROVEEDORES

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 por sus siglas en inglés) 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 de GLI, GLI-GSF-3, establece los Controles de Seguridad de la Información del Juego (GIS) adicionales al GLI-GSF-1, que son necesarios para auditar específicamente a un Proveedor que integra una aplicación comercial u otra solución auxiliar en el GPE de una Empresa de Juegos que no afecta directamente a los componentes o actividades de juego regulados.
b. Este módulo está destinado a ser evaluado como un complemento del GLI-GSF-1, que proporciona los controles 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 del Juego de GLI (GLI-GSF) está disponible de forma gratuita a www.gaminglabs.com.

1.2. Proveedores 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 que tienen un papel en la supervisión o el funcionamiento de un GPE o en la prestación de servicios integrales a su función. A los efectos de este módulo, los proveedores se refieren a los proveedores de servicios que integran aplicaciones comerciales y otras soluciones auxiliares en el GPE de una empresa de juegos que no afectan directamente a los componentes o actividades de juego regulados. Para obtener información adicional, consulte la sección "Rol de gestión de datos confidenciales y empresas de juegos" del GLI-GSF-1.

NOTA: Tenga en cuenta que, al leer e implementar los Controles de GIS del GLI-GSF-1, el Proveedor asume el papel de la "Empresa de Juego", mientras que la Empresa de Juego asume el papel de "Organismo Regulador".

1.3. Entorno de producción de juegos (GPE)

Un GPE se refiere al entorno operativo donde las actividades de juego y los servicios relacionados se realizan, 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, como los juegos de casino, la lotería, las apuestas de eventos y los juegos interactivos. El GPE también abarca los sistemas de backend, las aplicaciones comerciales y la infraestructura que interactúan y/o respaldan las actividades de juego. 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 de juegos (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 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 es primordial para mantener la confianza pública en el sector. Por lo tanto, los casinos, loterías, operaciones de apuestas de eventos, operaciones de juegos interactivos y otras empresas de juegos deben establecer y mantener un marco claramente definido y documentado para lograr y preservar la confianza 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 basa 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 y/o Empresa de Juegos que desee implementar un conjunto completo de Controles de GIS que se aplicarán a los Proveedores junto con los Controles de GIS Comunes del GLI-GSF-1.

2. AUDITORÍAS DE CONTROLES DE GIS (VGIS) DE PROVEEDORES

2.1. Descripción general de la auditoría

La Auditoría de Controles de VGIS se realiza con la intención de identificar cualquier caso real o potencial de incumplimiento, vulnerabilidades o debilidades, y garantizar que la integridad, confidencialidad y disponibilidad de la información bajo el control de la Empresa de Juegos se conserve cuando la aplicación comercial de un Proveedor u otra solución auxiliar se integre en el GPE. 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 GIS detallada en el GLI-GSF-3 está en los controles específicos de seguridad de la información para que los proveedores los apliquen, además de los controles comunes de seguridad de la información para 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 VGIS Controls utiliza una variedad de métodos de evaluación que incluyen los siguientes métodos, cuyos resultados se utilizan para respaldar la determinación de la efectividad de Control VGIS a lo largo del tiempo. Puede encontrar información adicional sobre los "Métodos de auditoría" utilizados en una auditoría de proveedores de GIS en el GLI-GSF-1.

2.3. Tareas de auditoría

El Apéndice detalla los controles mínimos de VGIS 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 VGIS 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 según los requisitos reglamentarios y el alcance de la evaluación. La información sobre las actividades de auditoría de controles de VGIS de alto nivel se puede encontrar en la sección "Tareas de auditoría" en el GLI-GSF-1.

2.4. Frecuencia de auditoría

El Proveedor debe realizar una Auditoría de Controles de VGIS antes de integrar cada aplicación comercial u otra solución auxiliar en el GPE de una Empresa de Juego y entre cualquier cambio crítico que considere la Empresa de Juego o el Organismo Regulador. La expectativa es que un Proveedor solo necesitará obtener una Auditoría de Controles de VGIS anual para cada aplicación comercial u otra solución auxiliar, a menos que la Empresa de Juegos o el Organismo Regulador exijan lo contrario, ya que podrían requerir auditorías adicionales.

2.5. Informes de auditoría

Los resultados de una auditoría de controles de VGIS 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 VGIS debe cumplir con los requisitos de los "Informes de auditoría" que se especifican en el GLI-GSF-1.

2.6. Remediación

Si el informe de auditoría de controles de VGIS de la ISF recomienda la corrección, el Proveedor debe proporcionar a la Empresa de juegos y a la ISF, si así lo requiere, un plan de remediación y cualquier plan de mitigación de riesgos que detalle las acciones del Proveedor y el cronograma para implementar los pasos de corrección. Para obtener información adicional, consulte la sección "Remediación" del GLI-GSF-1.

2.7. Empresa de seguridad independiente (ISF)

La auditoría de controles de VGIS 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 la empresa de juegos o el organismo regulador especifiquen 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 DEL JUEGO (VGIS) DEL PROVEEDOR

Además de los controles de GIS especificados en el GLI-GSF-1 para Empresas de Juego GIG1 Gaming Enterprises, los siguientes controles GIS adicionales se aplican a la integración de la aplicación comercial de un proveedor u otra solución auxiliar en los GPE utilizados para cualquier forma de juego. Es posible que ciertos controles de GIS comunes especificados en GLI-GSF-1 para empresas de juego GIG1 que se relacionen específicamente con juegos regulados no sean aplicables a la aplicación comercial de un proveedor u otra solución auxiliar.

VGIS-1	Organización de proveedores
VGIS-1.1	**Privacidad del proveedor**
VGIS-1.1.1	El Proveedor debe demostrar el cumplimiento de los principios de "privacidad por diseño y por defecto" en la arquitectura, el desarrollo y el funcionamiento de todos los productos y servicios proporcionados a la Empresa de juego.
VGIS-1.1.2	El Proveedor debe proporcionar funcionalidades y documentación que respalden el cumplimiento por parte de la Empresa de juegos con las leyes de privacidad de datos pertinentes (por ejemplo, GDPR, CCPA), incluida la gestión del consentimiento y el cumplimiento de los derechos de los interesados.
VGIS-1.2	**Divulgación responsable**
VGIS-1.2.1	El Vendedor debe revelar cualquier vulnerabilidad de seguridad de sus productos y/o servicios a todas las Empresas de juego que los hayan comprado.
VGIS-1.2.2	El Proveedor debe establecer una política y un proceso asociado para tratar las divulgaciones responsables, que identifique dónde se deben realizar los informes y con qué rapidez se evaluarán y actuarán, si es necesario.
VGIS-1.3	**Colaboración y respuesta a incidentes de seguridad**
VGIS-1.3.1	El Proveedor debe haber establecido y documentado procesos para una colaboración efectiva con todas las Empresas de Juego afectadas durante cualquier incidente de seguridad que afecte a las aplicaciones comerciales y otras soluciones auxiliares proporcionadas.
VGIS-1.3.2	El Proveedor debe notificar a las Empresas de juego afectadas sin demora indebida tras la identificación y confirmación de un incidente de seguridad.
VGIS-1.3.3	El Proveedor debe haber establecido procesos para colaborar con las Empresas de juego involucradas durante los incidentes de seguridad que afecten el servicio prestado. Esto incluye la notificación oportuna, el intercambio de información y los esfuerzos coordinados de respuesta y recuperación.
VGIS-1.3.4	El Proveedor debe proporcionar actualizaciones oportunas y precisas, que incluyen: a. Naturaleza y alcance del incidente; b. Sistemas o datos afectados; c. Causa conocida o sospechada; d. Acciones de mitigación en curso; y e. Acciones recomendadas por los usuarios.
VGIS-1.3.5	El Proveedor debe coordinarse activamente con Gaming Enterprise para: a. Contener el incidente b. Restaurar los servicios afectados c. Apoyar la investigación forense si es necesario; y d. Evite la recurrencia a través de acciones correctivas.
VGIS-2	**Gestión de cuentas y privilegios**
VGIS-2.1	**Registros de actividad de cuentas y privilegios**
VGIS-2.1.1	El Proveedor debe asegurarse de que todas las actividades relacionadas con la cuenta o las actividades relacionadas con los privilegios, incluida la creación, modificación y eliminación o eliminación de cuentas y privilegios, se registren y supervisen por completo con el fin de respaldar las auditorías e investigaciones periódicas.

VGIS-2.1.2	En los casos en que el Proveedor inicie actividades relacionadas con la cuenta o con privilegios, el sistema debe: a. Generar alertas en tiempo real a los contactos de seguridad designados por la empresa de juegos; b. Generar registros de eventos en tiempo real que cumplan con los controles de accesibilidad y transferencia de registros requeridos; c. Registrar registros detallados, incluida la marca de tiempo, el usuario o sistema iniciador, la naturaleza del cambio y las cuentas afectadas; d. Asegurar de que todos los registros sean a prueba de manipulaciones y se conserven de acuerdo con las políticas de retención de registros y auditorías de Gaming Enterprise.
VGIS-2.2	**Control de cuentas y privilegios**
VGIS-2.2.1	El Proveedor está obligado a proporcionar a la Empresa de juegos la capacidad de habilitar, deshabilitar y eliminar cuentas de usuario para acceder a las aplicaciones comerciales del Proveedor y otras soluciones auxiliares, y a otorgar y revocar privilegios, a discreción de la Empresa de juegos.
VGIS-2.2.2	La funcionalidad para habilitar o deshabilitar cuentas de usuario y para otorgar y revocar privilegios debe estar disponible para la empresa de juego en todo momento, lo que garantiza que puedan administrar el acceso y los privilegios en función de los requisitos operativos, de seguridad o de cumplimiento sin la intervención o demora del Proveedor.
VGIS-2.2.3	Cuando se le solicite, el Proveedor debe mantener la capacidad técnica para integrarse con los sistemas automatizados de la empresa de juego para la activación y desactivación de cuentas en tiempo real a través de protocolos estándar de la industria compatibles con las herramientas de aprovisionamiento y desaprovisionamiento generalmente disponibles.
VGIS-2.3	**Cuentas elevadas**
VGIS-2.3.1	Un proveedor que solicite acceso elevado al GPE de una empresa de juegos debe seguir un proceso de aprobación en tiempo real.
VGIS-2.3.2	El Proveedor no debe acceder directamente al GPE de la Empresa de Juegos sin autorización previa.
VGIS-2.3.3	Todo acceso debe cumplir con los procedimientos de aprobación definidos por la empresa de juego o utilizar métodos preaprobados que garanticen que la empresa de juegos conserve el control total, incluida la capacidad de revocar el acceso en cualquier momento.
VGIS-2.3.4	El Proveedor debe asegurarse de que todos los intentos de acceso y actividades dentro del GPE de la Empresa de juegos se registren en detalle y estén disponibles a pedido y se transfieran a la Empresa de juego.
VGIS-2.3.5	En los casos en que se utilicen soluciones de software como servicio (SaaS) basadas en la nube, el proveedor debe asegurarse de que los acuerdos contractuales incluyan disposiciones para auditorías de terceros para verificar el cumplimiento de las mejores prácticas de la industria.
VGIS-2.4	**Controles de acceso basados en roles**
VGIS-2.4.1	Los controles de acceso basados en roles deben implementarse y ser lo suficientemente granulares como para admitir funciones administrativas segmentadas (por ejemplo, el aprovisionamiento de usuarios no debe requerir derechos de administrador completos).
VGIS-2.4.2	La empresa de juego debe tener la capacidad técnica para configurar permisos por rol, que luego se pueden aplicar a grupos o usuarios.
VGIS-2.4.3	Los roles predeterminados son aceptables cuando los permisos para el rol son visibles para la empresa de juego con fines de auditoría. Es aceptable mostrar "Todos" para el rol de administrador de nivel superior (por ejemplo, superusuario, administrador global).
VGIS-2.5	**Eventos de cuenta y privilegios**
VGIS-2.5.1	El proveedor debe asegurarse de que los siguientes eventos se registran completamente. Este nivel de detalle es necesario para respaldar la auditoría, el análisis forense y el monitoreo del cumplimiento, y llena el vacío cuando se realizan auditorías de permisos puntuales (mensuales, trimestrales, etc.). a. Todos los eventos relacionados con la cuenta. Por ejemplo, si un sistema está configurado para bloquear una cuenta después de tres intentos fallidos de inicio de sesión, los registros deben reflejar toda la actividad relacionada, debe haber tres eventos de inicio de sesión fallidos distintos registrados, seguidos de un evento de bloqueo de cuenta separado registrado, con un total de cuatro entradas registradas; y b. Todos los eventos relacionados con privilegios. Por ejemplo, si un usuario concede permisos a un rol y posteriormente quita ese permiso, debe haber dos eventos registrados que muestren qué permisos se modificaron por rol.

VGIS-2.6	**Autenticación de usuario**
VGIS-2.6.1	Cuando se le solicite, el Proveedor debe mantener la capacidad técnica para: a. Integrar con los sistemas de inicio de sesión único de la empresa de juego a través de protocolos estándar de la industria compatibles con los sistemas generalmente disponibles para inicio de sesión único (SSO). b. Aplicar la autenticación multifactor a través de métodos estándar de la industria suficientemente sólidos (notificación push, TOTP, token de hardware, no SMS).
VGIS-2.6.2	Cada intento exitoso y fallido de cambiar una contraseña de cuenta, PIN u otro secreto utilizado para la autenticación debe registrarse y contener lo siguiente: a. Fecha y hora del evento; b. Nombre de host o dirección IP del cliente donde se inició el evento. Tenga en cuenta que, en algunos casos, la correlación de eventos de "inicio de sesión correcto" puede servir para cumplir con este control; c. Nombre de host, dirección IP u otro identificador único del sistema donde se produjo el cambio de cuenta. Tenga en cuenta que en determinados escenarios de equilibrio de carga, normalmente en el entorno local, el servidor donde se produjo el cambio debe ser identificable. Este control no se aplica a los sistemas SaaS de terceros en los que el sistema o el inquilino son identificables a través de otros métodos; d. Resultado del evento (Exitoso o Fallido); e. Identificador único de la cuenta de destino (la cuenta a la que se aplica el cambio de contraseña); y f. Identificador único de la cuenta iniciada (la cuenta que cambió la contraseña de la cuenta de destino).
VGIS-3	**Transferencia de registros y accesibilidad**
VGIS-3.1	**Generación y retención de registros**
VGIS-3.1.1	Cuando los registros sean generados por las aplicaciones comerciales del Proveedor u otras soluciones auxiliares, el Proveedor debe asegurarse de que estos registros se conserven de forma segura y sean fácilmente accesibles para la Empresa de Juegos a pedido para respaldar los requisitos de investigación forense o auditoría.
VGIS-3.2	**Capacidad de transferencia e integridad**
VGIS-3.2.1	Cuando se le solicite, el Proveedor debe mantener la capacidad técnica para transferir registros al sistema de registro centralizado de la Empresa de juegos o una solución equivalente, de manera oportuna y en un formato estándar de la industria compatible con las herramientas de monitoreo y respuesta a incidentes generalmente disponibles.
VGIS-3.2.2	Todas las transferencias de registros deben realizarse a través de canales seguros utilizando protocolos de cifrado estándar de la industria para mantener la confidencialidad e integridad de los datos en tránsito.
VGIS-3.2.3	Los registros transferidos deben estar completos, sin alteraciones y en un formato estructurado que conserve la integridad de la marca de tiempo, los identificadores del sistema de origen y los detalles de eventos necesarios para la trazabilidad y la auditoría.
VGIS-3.2.4	Los registros transferidos deben ser conciliables con un informe del sistema nativo para admitir comprobaciones de integridad para el muestreo o las pruebas de rendimiento completas.
VGIS-4	**Gestión de la cadena de suministro**
VGIS-4.1	**Plan de gestión de riesgos de la cadena de suministro**
VGIS-4.1.1	El Proveedor debe implementar y mantener un Plan de Gestión de Riesgos de la Cadena de Suministro (SCRM) actualizado, completo y documentado para garantizar la integridad, seguridad y confiabilidad de todos los sistemas, componentes y servicios proporcionados a una Empresa del Juego en virtud de un acuerdo.
VGIS-4.1.2	El Plan SCRM debe describir las políticas, procedimientos, roles, responsabilidades y procesos utilizados para identificar, evaluar, mitigar y monitorear los riesgos de la cadena de suministro a lo largo del ciclo de vida del producto o servicio.
VGIS-4.1.3	El Proveedor debe establecer, mantener y revisar periódicamente las políticas y procedimientos formales que respaldan la ejecución del Plan SCRM. Estos documentos deben ponerse a disposición de la Empresa de Juego previa solicitud con fines de supervisión y verificación de cumplimiento.

VGIS-4.2	**Evaluación y revisión de riesgos de la cadena de suministro**
VGIS-4.2.1	El Proveedor debe realizar evaluaciones y revisiones periódicas de riesgos de todas las entidades de la cadena de suministro, incluidos los subcontratistas, los proveedores de servicios y otros proveedores externos.
VGIS-4.2.2	Estas evaluaciones y revisiones de riesgos realizadas por el Proveedor deben evaluar los riesgos asociados con cada proveedor o contratista y el sistema, componente del sistema o servicio específico que brindan.
VGIS-4.2.3	El Proveedor debe tomar las medidas adecuadas para mitigar los riesgos identificados de acuerdo con las mejores prácticas de la industria y los requisitos contractuales.
VGIS-4.3	**Políticas y procedimientos contra la falsificación**
VGIS-4.3.1	El Proveedor debe desarrollar, documentar e implementar políticas y procedimientos antifalsificación diseñados para detectar, prevenir y responder a la introducción de componentes falsificados en el sistema.
VGIS-4.3.2	Las políticas y procedimientos antifalsificación implementados deben incluir métodos para la verificación de componentes, la validación de proveedores, la respuesta a incidentes y la presentación de informes.
VGIS-4.4	**Mapeo y análisis de la cadena de suministro**
VGIS-4.4.1	El proveedor debe realizar un mapeo y análisis exhaustivos de la cadena de suministro de software, incluida la identificación y documentación de todos los componentes de software (propietarios, de código abierto y de terceros), sus fuentes, dependencias y relaciones.
VGIS-4.4.2	El proveedor debe garantizar la transparencia y la trazabilidad en toda la cadena de suministro y mantener este mapeo durante todo el ciclo de vida del sistema, componente o servicio.
VGIS-5	**Desarrollo e implementación de software seguro**
VGIS-5.1	**Implementaciones controladas**
VGIS-5.1.2	El Proveedor no debe realizar ninguna implementación de software automatizada en el GPE de la Empresa de juego sin la programación previa, la aprobación explícita y el registro por parte de la Empresa de juego.
VGIS-5.1.3	Todos los eventos de implementación deben ser rastreables y estar sujetos al programa de gestión de cambios de la empresa de juego.
VGIS-5.2	**Codificación segura e integración continua/canalizaciones de implementación continua**
VGIS-5.2.1	El Proveedor debe seguir estándares de codificación seguros (por ejemplo, OWASP), que deben aplicarse de manera consistente durante todo el proceso de desarrollo.
VGIS-5.2.2	El proveedor debe realizar revisiones rigurosas del código, así como integrar herramientas de análisis de código estático y dinámico en la canalización de CI/CD (integración continua/implementación continua) para detectar y remediar vulnerabilidades.
VGIS-5.2.3	Las canalizaciones de CI/CD del proveedor deben estar protegidas con controles sólidos, que incluyen: a. Control de acceso y registro de auditoría para repositorios de código b. Entornos de compilación seguros y gestión de artefactos c. Directivas de administración de cambios y acceso a la implementación d. Protección contra modificaciones no autorizadas de la lógica de canalización
VGIS-5.3	**Integridad del software**
VGIS-5.3.1	Todas las versiones de software deben estar firmadas digitalmente por el Proveedor utilizando técnicas criptográficas para garantizar la autenticidad, evitar la manipulación y permitir la verificación del origen.
VGIS-5.3.2	El proveedor debe implementar mecanismos de validación de hash criptográfico y suma de comprobación durante las fases de empaquetado, distribución e implementación para garantizar la integridad de los componentes de software.
VGIS-5.3.3	El Proveedor debe emplear herramientas de verificación de integridad para detectar modificaciones no autorizadas en los componentes de software. Cualquier desviación del estado esperado debe desencadenar alertas y procedimientos de respuesta a incidentes.
VGIS-5.3.4	El Proveedor debe respaldar o implementar directamente la lista blanca de aplicaciones para garantizar que solo se ejecuten los componentes de software autorizados y validados dentro del GPE.
VGIS-5.4	**Aislamiento de funciones**
VGIS-5.4.1	Las funciones de seguridad deben aislarse lógica y físicamente de las funciones que no son de seguridad, lo que garantiza que las operaciones confidenciales (por ejemplo, autenticación, procesos criptográficos, auditoría) estén protegidas contra el compromiso.

VGIS-5.4.2	El proveedor debe garantizar una separación clara entre la funcionalidad orientada al usuario (por ejemplo, interfaces de usuario, interacción de juegos) y la funcionalidad de administración del sistema (por ejemplo, herramientas administrativas, paneles de configuración) para evitar el uso indebido de privilegios y reducir las superficies de ataque.
VGIS-5.5	**Requisitos de seguridad y modelado de amenazas**
VGIS-5.5.1	Los requisitos de seguridad deben ser definidos por el proveedor desde el principio, junto con los requisitos funcionales. Esto incluye el cumplimiento de las regulaciones relevantes (por ejemplo, las leyes de privacidad de datos), la adhesión a las mejores prácticas de la industria y las políticas de seguridad internas.
VGIS-5.5.2	El proveedor debe realizar el modelado de amenazas en las primeras etapas de desarrollo y mantenerlo durante todo el ciclo de vida del software. El proveedor debe identificar y evaluar posibles vectores de ataque e implementar mitigaciones de diseño adecuadas para abordarlos.
VGIS-5.6	**Principios de diseño seguro y gestión de la configuración**
VGIS-5.6.1	El Proveedor debe aplicar principios de diseño seguro reconocidos, que incluyen, entre otros: a. Principio de privilegio mínimo: Los derechos de acceso deben limitarse al mínimo necesario para su funcionamiento. b. Defensa en profundidad: Se deben implementar múltiples capas de controles para mitigar el riesgo en varios niveles. c. Fallar de forma segura: el software debe manejar las fallas de manera segura y controlada sin exponer datos confidenciales o funcionalidades. d. Simplicidad en el diseño: El diseño de software debe minimizar la complejidad para reducir el riesgo de vulnerabilidades y facilitar el mantenimiento.
VGIS-5.6.2	El proveedor debe aplicar una gestión de configuración segura en todos los entornos de implementación, incluidos el desarrollo, las pruebas, el ensayo y la producción. Estas configuraciones deben administrarse, controlarse por versiones y revisarse periódicamente para verificar el cumplimiento de los estándares de seguridad.
VGIS-5.7	**Configuración y conectividad del firewall**
VGIS-5.7.1	El Proveedor debe garantizar y respaldar el funcionamiento del producto detrás de un firewall (cortafuegos) basado en host o en red.
VGIS-5.7.2	Para los servicios que escuchan conexiones entrantes, el Proveedor debe proporcionar detalles para que el puerto, el protocolo y la aplicación de destino (por ejemplo, HTTP, SSL, MS-SQL) se permitan a través del firewall de la empresa de juego. Los detalles de la fuente deben proporcionarse como guía (por ejemplo, clientes de Internet con navegador web, clientes internos con software desarrollado por el Proveedor).
VGIS-5.7.3	Para el software que inicia conexiones salientes, el proveedor debe proporcionar detalles para el puerto, el protocolo y la aplicación de destino (por ejemplo, HTTP, SSL, MS-SQL) que se permitirán a través del firewall de la empresa de juego. Los detalles del destino deben proporcionarse como guía (por ejemplo, FQDN o rango de IP del entorno en la nube/SaaS del Proveedor, ubicación del servicio de escucha instalado proporcionado por el Proveedor e implementado en el GPE de la Empresa de Juegos). No se aceptan rangos de IP de destino demasiado amplios donde pueden residir otros servicios (por ejemplo, rangos de IP compartidos en un entorno de nube como AWS, Azure, GCP).
VGIS-6	**Pruebas de seguridad técnica (GTS) del juego de proveedores**
VGIS-6.1	**Metodología de prueba**
VGIS-6.1.1	El Proveedor debe realizar las Pruebas GTS del Proveedor de acuerdo con las metodologías y requisitos descritos en el GLI-GSF-2.
VGIS-6.1.2	Las pruebas de GTS del proveedor deben incluir la evaluación de las aplicaciones comerciales y / o servicios auxiliares en busca de vulnerabilidades, configuraciones incorrectas y rutas de acceso no autorizadas.
VGIS-6.2	**Ajuste del alcance basado en el riesgo**
VGIS-6.2.1	El alcance de las pruebas de GTS del proveedor puede ajustarse en función del tamaño, el contexto y la naturaleza de las aplicaciones comerciales y/o los servicios auxiliares que se integran en el GPE de la empresa de juegos.
VGIS-6.2.2	Los ajustes al alcance deben considerar el impacto potencial, las implicaciones de seguridad y el nivel de riesgo que las aplicaciones comerciales y/o los servicios auxiliares presentan para la integridad y el funcionamiento del GPE.

VGIS-6.2.3	Cualquier modificación en el alcance de las pruebas de GTS del Proveedor requiere una revisión y aprobación previas por parte de la empresa de juego.

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.
Registro de auditoría	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 responsabilidad durante un período determinado.
Autenticación	Verificar la identidad de un usuario, proceso, paquete de software o dispositivo, a menudo como requisito previo para permitir el acceso a los recursos en el GPE
Disponibilidad	Garantizar el acceso y el uso oportunos y confiables de la información.
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
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. • 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.

Término	Descripciones
	• 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, incluidos web, aplicaciones, bases de datos, autenticación, correo, proxy, protocolo de tiempo de red (NTP) y servicio de nombres de dominio (DNS). • Dispositivos de usuario final, 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 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.
Empresa de juego	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 del 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 del juego (GISMS)	Un sistema de gestión definido y documentado que consiste en un conjunto de políticas, procesos y sistemas para gestionar los riesgos de los datos, 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.

Término	Descripciones
Integridad	Proteger contra la modificación o destrucción indebida de información e incluye garantizar el no repudio y la autenticidad de la información.
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).
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.
Riesgo	La probabilidad de que una amenaza tenga éxito en su ataque contra una red o sistema.

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 de 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 patrocinadores, 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 del cliente 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

Término	Descripciones
	de servicios en la nube. Los proveedores y vendedores externos también se consideran proveedores de servicios.
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.
Acceso no autorizado	Una persona obtiene acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso.
Proveedores	Proveedores de servicios que integran aplicaciones comerciales y otras soluciones auxiliares en el GPE de una empresa de juegos que no afectan directamente a los componentes o actividades de juego regulados.