GLI®

MARCO DE SEGURIDAD DEL JUEGO

GLI-GSF-5

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

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 de GLI, GLI-GSF-5, 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 en línea, utilizando un sitio web de juego, una aplicación móvil, u otra plataforma digital, para ofrecer juegos interactivos, juegos de estudio en vivo, lotería por Internet, apuestas de eventos en línea o cualquier otra forma de juego en línea.
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 en línea y los servicios relacionados se llevan a cabo, gestionan 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 juegos en línea, como juegos interactivos (iGaming), lotería interactiva (iLottery), apuestas de eventos en línea y juegos de estudio en vivo. El GPE también abarca los sistemas de backend, las aplicaciones comerciales y la infraestructura que interactúan y / o respaldan las actividades del juego en línea. Las características clave de un GPE se describen en la sección "Entorno de producción del juego (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 del juego en línea es primordial para mantener la confianza del público en el sector. Por lo tanto, las empresas de juegos que ofrecen juegos en línea deben establecer y mantener un marco claramente definido y documentado para lograr y preservar la confianza pública en sus operaciones. El objetivo es alinear la GIS de tal manera que las operaciones de juego puedan funcionar como otras operaciones de comercio electrónico para garantizar un entorno seguro y estable con las características seguras de las operaciones en industrias paralelas.

1.6. Normas y directrices de seguridad consultadas

Cada módulo del GLI-GSF 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 en línea junto con los controles de GIS comunes del GLI-GSF-1.

2. AUDITORÍAS DE CONTROLES DE GIS EN LÍNEA (OGIS)

2.1. Descripción general de la auditoría

La Auditoría de Controles de OGIS 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-5 está en los controles específicos de seguridad de la información para los juegos en línea 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 apoyo del GLI-GSF.

2.2. Métodos de auditoría

Una auditoría de controles de OGIS en línea 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 OGIS en línea 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 OGIS en línea 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 OGIS necesarios. Los controles de GIS en línea 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.

NOTA: La información sobre las actividades de auditoría de controles de GIS en línea de alto nivel 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 OGIS 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 OGIS en línea 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 OGIS en línea 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 OGIS en línea 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 OGIS en línea debe ser realizada por personas con calificaciones suficientes, lo que significa que la 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 DEL JUEGO EN LÍNEA (OGIS)

Además de los controles de GIS comunes especificados en el GLI-GSF-1 para las empresas de juego GIG3, los siguientes controles de GIS adicionales se aplican a los GPE de las empresas de juego que ofrecen juegos en línea.

OGIS-1	Verificación de firmas de programas de control críticos
OGIS-1.1	**Procedimiento de verificación de firmas y registro**
OGIS-1.1.1	Las firmas de los Programas de Control Crítico se obtendrán de la GPE a través de un procedimiento de verificación de firmas, que deberá ejecutarse bajo las siguientes condiciones: a. Al instalar o actualizar cualquier Programa de Control Crítico; b. Al encender el sistema o recuperarse de un estado de apagado; c. Como mínimo, una vez cada 24 horas durante las operaciones normales; y d. Bajo pedido (bajo demanda).
OGIS-1.1.2	El procedimiento de verificación de firmas debe incluir uno o más pasos analíticos para comparar las firmas actuales de los Programas de Control Crítico en el GPE con las firmas de las versiones aprobadas actuales.
OGIS-1.2	**Registro de auditoría de verificación**
OGIS-1.2.1	El resultado del procedimiento de verificación de firmas debe registrarse en un registro de auditoría de verificación, que comprende parte de los datos confidenciales que deben recuperarse en caso de desastre o falla del equipo o software.
OGIS-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. Identificación de cada Programa de Control Crítico verificado; c. Los resultados de firma esperados y generados, incluida la indicación de cualquier error de programa o discrepancia de firma; y d. Cuando se realiza a petición, el ID de la cuenta de usuario que inició el procedimiento de verificación;
OGIS-1.2.3	El Organismo Regulador debe poder acceder al registro de auditoría de verificación en un formato que permita el análisis de cada verificación por parte del Organismo Regulador.
OGIS-1.3	**Error de verificación**
OGIS-1.3.1	Cualquier falla en la verificación de la firma de cualquier Programa de Control Crítico debe requerir una notificación de la falla de verificación que se comunicará a la Empresa de Juegos.
OGIS-1.3.2	Cuando lo requiera el Organismo Regulador, la Empresa de Juegos debe informar al Organismo Regulador de la falla en la verificación de la firma y las acciones correctivas tomadas sin demora indebida.
OGIS-2	**Administración de Back Office**
OGIS-2.1	**Aplicación de autenticación de factores (MFA)**
OGIS-2.1.1	Las aplicaciones de administración de back office deben admitir la aplicación de la autenticación multifactorial (MFA) para todas las cuentas con privilegios utilizadas por personas para acceder a las aplicaciones, siempre que sea posible. Esto incluye cuentas administrativas, operativas, de sistema y de soporte con permisos elevados.
OGIS-2.1.2	Cuando se aplica la autenticación de MFA, el MFA debe usar al menos dos factores de autenticación distintos (por ejemplo, contraseña y token de hardware) para reducir el riesgo de acceso no autorizado debido a credenciales comprometidas.
OGIS-2.1.3	Cuando no sea posible implementar la autenticación multifactorial (por ejemplo, en cuentas de servicio), las cuentas con privilegios deben contar con controles compensatorios, como autenticación sólida, gestión de cuentas con privilegios, controles de acceso condicional y monitoreo adicional.
OGIS-2.2	**Supervisión de acceso de soporte de proveedores**
OGIS-2.2.1	Todo el acceso de los proveedores a las aplicaciones de administración de back office, ya sea remoto o in situ, con fines de mantenimiento, resolución de problemas o soporte debe ser estrictamente controlado, monitoreado y registrado por la empresa de juego.
OGIS-2.2.2	El acceso de proveedores solo debe otorgarse de forma temporal, según sea necesario, a través de canales de comunicación seguros.
OGIS-2.2.3	Todas las actividades realizadas por los proveedores durante dicho acceso deben registrarse íntegramente y ser auditables para garantizar la contabilidad y facilitar la monitorización, el análisis y la revisión forense.

OGIS-2.2.4	Todos los cambios en el acceso de los proveedores, incluyendo adiciones, modificaciones o eliminaciones, deben documentarse y registrarse formalmente para mantener un registro auditable de las actividades de gestión de acceso.
OGIS-2.2.5	El GPE debe incluir un mecanismo para revocar inmediatamente el acceso de los proveedores en caso de un incidente relacionado con el GIS, garantizando la rápida mitigación de los posibles riesgos operativos o de seguridad.
OGIS-2.3	**Controles de acceso basado en roles y privilegios mínimos (RBAC)**
OGIS-2.3.1	Las aplicaciones de administración de back office deben implementar controles de acceso basados en roles (RBAC) para asignar permisos en función de las responsabilidades. Los cambios en el RBAC deben documentarse y registrarse.
OGIS-2.3.2	El acceso debe seguir el principio de privilegios mínimos, asegurando que los usuarios tengan solo los permisos mínimos necesarios para realizar sus funciones.
OGIS-2.3.3	Las aplicaciones de administración de back office deben aplicar una segregación de funciones para evitar que la misma persona realice tareas conflictivas (por ejemplo, iniciar y aprobar transacciones).
OGIS-2.4	**Restricciones de acceso a la red**
OGIS-2.4.1	El acceso a las aplicaciones de administración de back office debe restringirse a redes confiables y autorizadas utilizando e implementando al menos uno de los siguientes controles para hacer cumplir esta restricción: listas blancas de IP, cortafuegos y segmentación de red, o acceso seguro a redes privadas virtuales (VPN). a. Se debe denegar explícitamente el acceso a las redes públicas y a los dispositivos no confiables. b. Se debe denegar implícitamente el acceso a todo el tráfico que no esté explícitamente autorizado. c. Las soluciones de confianza cero deben verificar continuamente la fiabilidad de los usuarios y los dispositivos antes de concederles acceso, asegurándose de que no se concede ninguna confianza implícita basada en la ubicación de la red u otros factores supuestos. d. Cuando la implementación de los controles anteriores no sea factible debido a la configuración del producto, se deben aplicar y documentar controles compensatorios adicionales.
OGIS-2.4.2	Los controles de acceso a la red deben revisarse y actualizarse periódicamente para garantizar la alineación continua con la postura de seguridad de la empresa de juegos.
OGIS-2.5	**Gestión de sesiones y cuentas**
OGIS-2.5.1	Las aplicaciones de administración de back office deben configurarse para prohibir los inicios de sesión simultáneos desde la misma cuenta de usuario en varios dispositivos o sesiones.
OGIS-2.5.2	Cuando sea técnicamente posible, las sesiones activas existentes deben cerrarse cuando se intente iniciar sesión por duplicado, con el fin de evitar el acceso simultáneo no autorizado y proteger la integridad de la cuenta.
OGIS-3	**Integridad del lado del servidor y seguridad de programación**
OGIS-3.1	**Validación del lado del servidor de la lógica de juego**
OGIS-3.1.1	Todas las transiciones de estado y lógica de juego críticas (por ejemplo, puntuación, actualizaciones de saldo, resolución de ganancias/pérdidas) deben validarse en el lado del servidor, independientemente de la entrada del cliente.
OGIS-3.1.2	Las entradas recibidas del sitio web de juego, la aplicación móvil u otra plataforma digital deben verificarse para verificar su integridad, autenticación y coherencia lógica antes de aplicar cualquier cambio de estado.
OGIS-3.2	**Control de ejecución y restricciones de código externo**
OGIS-3.2.1	La empresa de juegos debe implementar y mantener mecanismos sólidos diseñados para evitar la ejecución de código potencialmente dañino o no autorizado introducido a través de dispositivos móviles, medios extraíbles u otras fuentes externas.
OGIS-3.2.2	La empresa de juegos debe restringir la ejecución en los servidores críticos para que solo se ejecuten aplicaciones aprobadas y verificadas, bloqueando la ejecución de cualquier otro código no aprobado o no autorizado (por ejemplo, la implementación de una lista blanca de aplicaciones que solo permita la ejecución de aplicaciones de software preaprobadas o incluidas en la 'lista blanca' en un sistema).
OGIS-3.2.3	La empresa de juegos debe aplicar políticas que deshabiliten o limiten la capacidad de ejecutar código desde dispositivos externos o que no sean de confianza, incluida la desactivación de las funciones de ejecución automática y la restricción de la ejecución de scripts.

OGIS-3.3	**Aplicación de políticas**
OGIS-3.3.1	La empresa de juegos debe establecer y hacer cumplir las políticas que rigen el uso de dispositivos móviles y medios externos en los servidores que ejecutan programas de control crítico (por ejemplo, solo los dispositivos móviles gestionados pueden conectarse a la red y las unidades USB están bloqueadas en los servidores críticos). Esto puede incluir la gestión de dispositivos móviles (MDM), controles de acceso a la red o restricciones a nivel de servidor para evitar conexiones o transferencias de datos no autorizadas.
OGIS-3.3.2	La Empresa de juegos debe restringir o prohibir la conexión o el uso de dispositivos móviles y medios externos no autorizados para evitar la introducción de código dañino o no confiable.
OGIS-3.3.3	La empresa de juegos debe definir procedimientos y métodos seguros para introducir cualquier código, software o actualizaciones externas para garantizar la integridad y el cumplimiento de los estándares de seguridad.
OGIS-3.3.4	La empresa de juegos debe establecer requisitos para la autenticación, el escaneo y la validación del dispositivo antes de permitir cualquier medio o código externo en los componentes críticos del sistema.
OGIS-3.4	**Monitoreo de GPE y respuesta a incidentes de GIS**
OGIS-3.4.1	Se deben implementar mecanismos de monitoreo continuo para detectar, alertar y registrar cualquier intento de ejecución de código no autorizado, lo que permite una respuesta oportuna, análisis e investigación forense de posibles incidentes de GIS.
OGIS-3.4.2	La empresa de juegos debe contar con procedimientos para abordar de inmediato cualquier incidente de GIS relacionado con el código móvil o las amenazas ejecutables externas.
OGIS-3.5	**Seguridad en la nube y en entornos virtualizados**
OGIS-3.5.1	Cada instancia de servidor implementada dentro de un entorno virtualizado o en la nube debe estar dedicada a una única función crítica (por ejemplo, el servidor de la base de datos no debe alojar los servicios web o de aplicaciones). Este enfoque garantiza una separación lógica de funciones, limita el radio de ocurrencia de posibles incidentes de seguridad y se alinea con el principio de privilegio mínimo.
OGIS-3.5.2	La empresa de juegos debe implementar controles técnicos y administrativos para hacer cumplir la separación de roles entre instancias de servidor aislando funciones. Esto incluye el uso de máquinas virtuales, contenedores o servicios distintos para cada función (por ejemplo, base de datos, aplicación, servidor web) y la aplicación de configuraciones, controles de acceso y monitorización para cada instancia.
OGIS-4	**Mecanismos de protección de aplicaciones**
OGIS-4.1	**Comunicaciones seguras en aplicaciones móviles**
OGIS-4.1.1	Las aplicaciones móviles deben garantizar una comunicación segura entre el cliente y el servidor. Esto se puede lograr mediante la fijación de certificados SSL/TLS o medidas equivalentes, como la monitorización de la transparencia de los certificados o los marcos de fijación dinámica, que proporcionan una protección comparable contra los ataques 'Man-In-The-Middle' (hombre en el medio) y, al mismo tiempo, permiten una gestión segura de los certificados o las claves de cifrado.
OGIS-4.1.2	Las aplicaciones móviles deben diseñarse para finalizar las conexiones de red inmediatamente si el certificado o la clave de encriptación anclados no coinciden con el valor esperado.
OGIS-4.1.3	Todos los fallos en la validación de certificados o claves de cifrado deben registrarse con fines de monitorización, análisis e investigación forense, garantizando la trazabilidad de los incidentes GIS y los posibles riesgos para el sistema.
OGIS-4.2	**Detección de jailbreak/raíz en dispositivos móviles**
OGIS-4.2.1	Como parte de una estrategia de defensa por capas, las aplicaciones móviles pueden implementar la detección de jailbreak (iOS) y la detección de raíz (Android) para evitar la ejecución en dispositivos comprometidos. La detección debe cubrir técnicas, herramientas y anomalías del sistema comunes indicativas de manipulación.
OGIS-4.2.2	Si se determina que un dispositivo móvil está arraigado o liberado, la aplicación debe restringir el acceso a las características confidenciales o finalizar la operación.
OGIS-4.3	**Ofuscación de código para aplicaciones móviles**
OGIS-4.3.1	El código base de la aplicación móvil debe implementar la ofuscación del código para protegerlo contra la ingeniería inversa. Esto incluye, entre otras cosas: a. Renombrar clases, variables y métodos con identificadores no descriptivos; b. Modificar los flujos de control para que la lógica del programa sea más difícil de seguir; y c. Aplicar el cifrado de cadenas u ocultar recursos críticos.
OGIS-4.3.2	El proceso de ofuscación de código debe integrarse en la canalización de compilación automatizada para garantizar que cada compilación de producción se ofusque correctamente antes del lanzamiento.

OGIS-4.3.3	Se deben implementar mecanismos de detección de manipulaciones para alertar al personal autorizado si la aplicación móvil se modifica después de su distribución, garantizando así la integridad a lo largo de todo el ciclo de vida del software.
OGIS-4.4	**Detección y prevención de ataques de relleno de contraseñas**
OGIS-4.4.1	La empresa de juegos debe implementar mecanismos para detectar patrones consistentes con el relleno de contraseñas, como intentos de inicio de sesión de gran volumen utilizando credenciales variadas desde una sola dirección IP o dispositivo.
OGIS-4.4.2	Las medidas preventivas deben aplicarse en los terminales de autenticación (p.ej. los desafíos de CAPTCHA, la limitación de velocidad, las políticas de bloqueo de cuentas y la lógica de detección de relleno de credenciales, etc.).
OGIS-4.5	**Soluciones de mitigación de bots**
OGIS-4.5.1	El GPE debe integrar una solución de mitigación de bots para detectar y bloquear el tráfico automatizado que intenta realizar acciones abusivas, fraudulentas o no autorizadas.
OGIS-4.5.2	Las soluciones de mitigación de bots deben incluir análisis de comportamiento, huellas dactilares de dispositivos y mecanismos de desafío-respuesta para diferenciar entre usuarios humanos y scripts automatizados.
OGIS-4.6	**Seguridad de API**
OGIS-4.6.1	Todas las API que admiten el sitio web de juego, la aplicación móvil u otras plataformas digitales deben cumplir con las 10 mejores prácticas de seguridad de API de OWASP, incluida la autenticación, la limitación de velocidad, la validación de datos y el manejo de errores.
OGIS-4.6.2	La empresa de juegos debe realizar regularmente pruebas de seguridad de la API, incluso en la fase de desarrollo (por ejemplo, pruebas de penetración, análisis estático/dinámico) e implementar puertas de enlace de API o firewalls de aplicaciones web (WAF) para hacer cumplir las políticas de seguridad de la API y monitorear el tráfico en tiempo real.
OGIS-4.7	**Arquitectura de seguridad**
OGIS-4.7.1	Los segmentos de red que comprenden la infraestructura del sitio web de juego, la aplicación móvil u otra plataforma digital deben estar aislados entre sí y solo permitir la comunicación necesaria en protocolos y hosts específicos.
OGIS-4.7.2	La comunicación entre segmentos se limitará explícitamente a los protocolos, hosts y servicios necesarios para el funcionamiento operativo.
OGIS-4.7.3	En una red de confianza cero, todo el tráfico entre segmentos debe autenticarse, autorizarse y supervisarse continuamente para evitar el acceso no autorizado y el movimiento lateral dentro de la red.
OGIS-4.7.4	El sitio web de juego, la aplicación móvil u otra plataforma digital deben estar protegidos por un WAF o un control equivalente que proporcione una protección comparable contra los ataques basados en la web, incluidos, entre otros, los ataques de inyección, los scripts entre sitios y otras amenazas comunes de la capa de aplicación.
OGIS-4.7.5	El WAF o control equivalente debe monitorearse regularmente en busca de eventos de interés y actualizarse para garantizar que los últimos vectores de ataque estén configurados para ser monitoreados.
OGIS-5	**Controles de protección contra denegación de servicio distribuido (DDoS)**
OGIS-5.1	**Limitación y control de velocidad multicapa**
OGIS-5.1.1	La limitación de velocidad debe aplicarse en múltiples niveles de la arquitectura GPE para identificar y restringir los patrones de solicitudes abusivas y mitigar la degradación del servicio: a. Nivel de red: los cortafuegos y los controladores de entrada deben aplicar límites a las conexiones o paquetes por fuente (por ejemplo, por dirección IP). b. Nivel de la puerta de enlace API: las puertas de enlace API deben, siempre que sea posible, limitar el número de llamadas por cliente, incorporando mecanismos de gestión de ráfagas y retroceso. c. Nivel de aplicación: la lógica de la aplicación debe detectar y suprimir el uso excesivo o abusivo de puntos finales específicos para evitar el agotamiento de los recursos.
OGIS-5.1.2	La limitación de velocidad debe adaptarse a los cambios en los patrones de tráfico y la carga del sistema, y todas las infracciones de los límites definidos deben registrarse con fines de monitorización, análisis y análisis forense.

OGIS-5.2	Ofuscación de IP y mitigación de DDoS
OGIS-5.2.1	Las direcciones IP públicas de los servidores de juegos, las API, los paneles administrativos y otros componentes críticos del sistema deben ocultarse para evitar que la infraestructura sea objeto de ataques directos. Este ocultamiento puede lograrse, entre otros, mediante: a. Proxies inversos, redes de distribución de contenidos (CDN) o equilibradores de carga basados en la nube (por ejemplo, colocando una CDN delante de un servidor de juegos para gestionar las solicitudes mientras se oculta la dirección IP del servidor de origen; y b. Traducción de direcciones de red (NAT) y redes superpuestas (por ejemplo, utilizando direcciones IP privadas combinadas con NAT, o implementando redes superpuestas definidas por software, para enmascarar la verdadera infraestructura de origen, la ubicación y el direccionamiento de los servidores backend.
OGIS-5.2.2	Los servicios de protección contra DDoS de terceros deben integrarse en el GPE para mejorar la resiliencia y mantener la disponibilidad. La integración debe proporcionar las siguientes capacidades: a. Detectar y absorber ataques volumétricos, de protocolo y de capa de aplicación (por ejemplo, identificando y bloqueando automáticamente las solicitudes excesivas del Protocolo de Transferencia de Hipertexto (HTTP) dirigidas a una API); b. Garantizar que el tráfico malicioso se filtre en sentido ascendente antes de llegar al GPE (por ejemplo, utilizando centros de depuración para limpiar el tráfico); c. Mantener la continuidad del negocio mediante la conmutación automática por error y las redes periféricas globales (por ejemplo, redirigiendo el tráfico a nodos periféricos alternativos si un nodo regional está siendo atacado); y d. Validar los acuerdos de nivel de servicio (SLA) y los procedimientos de respuesta del GIS con los proveedores de servicios (por ejemplo, probando periódicamente la conmutación por error y los tiempos de respuesta según los SLA contractuales).

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 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
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.
Aplicación de administración de back office	Un sistema de software seguro y centralizado utilizado por las empresas de juegos y los organismos reguladores para administrar, monitorear y respaldar las funciones operativas, financieras, de cumplimiento y de servicio al cliente de un GPE, como la verificación de la identidad, la prevención del blanqueo de capitales y los sistemas de información reglamentaria.
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 Crítico, 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 la GPE.

Término	Descripciones
	• 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 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 la 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.
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.

Término	Descripciones
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.
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 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 la confidencialidad, integridad, disponibilidad, y contabilidad.
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 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 son relativos a cualquier estándar técnico aplicable y/o requisito reglamentario para las actividades de juego.
Puerta de Enlace	Cualquier dispositivo, sistema o aplicación de software que pueda realizar la función de traducir datos de un formato a otro. La característica clave de una puerta de enlace es que convierte el formato de los datos, no los datos en sí.
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.

Término	Descripciones
	• 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
Integridad	Proteger contra la modificación o destrucción indebida de información e incluye garantizar el no repudio y la autenticidad de la información.
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.
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.
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 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. También conocido como ataque 'En Ruta'.
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.
Código móvil	Código ejecutable que se mueve de una computadora a otra, incluido el código legítimo y el código malicioso, como los virus informáticos.
Microservicio	Una pequeña pieza de software independiente que realiza una función específica dentro de un sistema más grande. Cada microservicio se ejecuta por separado, se comunica con los demás a través de conexiones seguras y se puede actualizar o sustituir sin interrumpir el funcionamiento del sistema completo.
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, WAPs, y teléfonos, dispositivos de red VoIP, puntos de acceso inalámbricos, dispositivos de red y otros dispositivos de seguridad.
Contraseña	Una cadena de caracteres (letras, números y otros símbolos) que se usa para autenticar una identidad o para verificar la autorización de acceso.

Término	Descripciones
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.
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 de los juegos de azar.
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.

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 RNG y cualquier otra información que afecte los resultados de los juegos y las apuestas;
	• Claves de cifrado, donde la implementación elegida requiere la transmisión de claves;
	• Números de validación asociados con cuentas de 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 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").

Término	Descripciones
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).
Controles técnicos	Los mecanismos de seguridad implementados dentro de los sistemas y la infraestructura del Entorno de Producción del Juego para proteger contra el acceso no autorizado, 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.
Acceso no autorizado	Una persona obtiene acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso.
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.
Vulnerabilidad	Software, hardware u otras debilidades en una red o sistema que pueden proporcionar una "puerta" para introducir una amenaza.