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 BORRADOR – Publicado el 22 de agosto de 2025

Contenido

1. INTRODUCCIÓN 3

1.1. DECLARACIÓN GENERAL 3

1.2. ROL DE GESTIÓN DE DATOS CONFIDENCIALES Y EMPRESAS DE JUEGOS 3

1.3. ENTORNO DE PRODUCCIÓN DEL JUEGO (GPE) 3

1.4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE JUEGOS (GISMS) 3

1.5. PROPÓSITO DEL MARCO 3

1.6. NORMAS Y DIRECTRICES DE SEGURIDAD CONSULTADAS 4

1.7. ADOPCIÓN Y OBSERVANCIA 4

2. AUDITORÍAS DE CONTROLES DE GIS EN LÍNEA 5

2.1. DESCRIPCIÓN GENERAL DE LA AUDITORÍA 5

2.2. MÉTODOS DE AUDITORÍA 5

2.3. TAREAS DE AUDITORÍA 5

2.4. FRECUENCIA DE AUDITORÍA 5

2.5. INFORMES DE AUDITORÍA 6

2.6. REMEDIACIÓN 6

2.7. EMPRESA DE SEGURIDAD INDEPENDIENTE (ISF) 6

APÉNDICE: CONTROLES DE SEGURIDAD DE LA INFORMACIÓN (GIS) DE JUEGO EN LÍNEA . 7

DEFINICIONES DE TÉRMINOS 11

BORD

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 en línea, juegos de estudio en vivo, lotería por Internet, apuestas de eventos en línea o cualquier otra forma de juego interactivo.
b. Este módulo está destinado a ser evaluado como un complemento del GLI-GSF-1, que proporciona los controles de GIS comunes necesarios para auditar el GISMS de una empresa de juegos.
c. Este módulo se puede utilizar junto con el GLI-GSF-2, que proporciona un punto de referencia para realizar evaluaciones de seguridad técnica de juegos (GTS) del GPE de una empresa de juegos.
d. Dependiendo del tipo de empresa de juegos, también pueden aplicarse módulos adicionales de GLI-GSF.

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

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

Garantizar la seguridad de un GPE es una responsabilidad colectiva que abarca las múltiples entidades que componen la Empresa de Juegos, como el operador y sus proveedores, fabricantes, vendedores, proveedores de servicios y otras entidades que tienen un papel en la supervisión o el funcionamiento de un GPE o en la prestación de servicios integrales a su función. Cada entidad desempeña un papel crucial en el mantenimiento de la integridad, disponibilidad y confidencialidad del entorno, especialmente cuando se trata de datos confidenciales. Para obtener información adicional, consulte la sección "Rol de gestión de datos confidenciales y empresas de juegos" del GLI-GSF-1.

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

1.3. Entorno de producción del juego (GPE)

Un GPE se refiere al entorno operativo en el que las actividades de juego 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, el software y los procesos necesarios para facilitar diversas formas de juegos en línea, como juegos interactivos, lotería interactiva, 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.

PAOR

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

1.7. Adopción y observancia

Este módulo del GLI-GSF puede ser adoptado en su totalidad o en parte por cualquier organismo regulador que desee implementar un conjunto completo de controles de GIS que se aplicarán a los juegos en línea junto con los controles de GIS comunes del GLI-GSF-1.

RA OR

Derechos de autor © 2025 Gaming Laboratories International, LLC

Todos los derechos reservados.

2. AUDITORÍAS DE CONTROLES DE GIS EN LÍNEA

2.1. Descripción general de la auditoría

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

NOTA: El enfoque de la guía de GIS detallada en el GLI-GSF-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 GIS 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 GIS en línea a lo largo del tiempo. Se puede encontrar información adicional sobre los "Métodos de auditoría" en el GLI-GSF-1.

2.3. Tareas de auditoría

El Apéndice detalla los controles de GIS en línea mínimos con más detalle. Los usuarios de este documento son dirigidos al Apéndice, así como al Apéndice del GLI-GSF-1 para asegurarse de que no se pasen por alto los controles de GIS necesarios. Los controles de 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. 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.

2.4. Frecuencia de auditoría

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

a. Despliegue de nuevas plataformas
    i. Integración de servidores o agregadores de juegos remotos nuevos o muy modificados, controladores de jackpots, sistemas de administración de cuentas de usuarios, motores de apuestas de eventos y otros sistemas de juegos en línea
    ii. Lanzamiento de nuevas verticales de juego (por ejemplo, apuestas de eventos, juegos de estudio en vivo)
    iii. Expansión de la plataforma a sitios web de juego, aplicaciones móviles, televisores inteligentes o consolas
b. Cambios en la infraestructura y la arquitectura del backend
    i. Migración a un nuevo proveedor de nube o alojamiento
    ii. Adopción de modelos de contenedorización, microservicios o sin servidor
    iii. Despliegue de nuevos centros de datos (especialmente interjurisdiccionales)
c. Modificaciones al almacenamiento y manejo de datos confidenciales
    i. Cambios en el almacenamiento, el registro, el cifrado o la retención de datos confidenciales
    ii. Cambios en la residencia de datos confidenciales (por ejemplo, mover el almacenamiento primario de datos confidenciales de una ubicación a otra)
d. Principales actualizaciones de la base de código o de la plataforma
    i. Actualizaciones significativas de los componentes críticos del sistema
    ii. Uso de nuevos marcos de desarrollo o lenguajes de programación
    iii. Integración de funciones basadas en IA (por ejemplo, análisis de comportamiento, detección de fraudes)

BORRADOR

e. Cambios en los sistemas de pago o transacciones financieras
    i. Integración de nuevos procesadores de pagos, billeteras o API bancarias
    ii. Introducción de métodos de pago alternativos
    iii. Cambios en los mecanismos de retiro, depósito o pago
    iv. Ajuste a la lógica de las transacciones financieras en todo el sistema
        f. Cambios en la identificación de usuarios y la detección de ubicación
    i. Introducción de nuevos procesos de verificación de identidad (KYC) y métodos de detección de ubicación
    ii. Cambios en las políticas de credenciales de autenticación, autenticación multifactor (MFA) y fuentes de datos de ubicación (por ejemplo, Wi-Fi, GSM, GPS)
    iii. Integración con proveedores de verificación de identidad de terceros y proveedores de detección de ubicación de terceros
g. Desencadenadores de respuesta a incidentes
    i. Cualquier violación de datos, compromiso de servicio o evento de fraude
    ii. Detección de malware, software de trampas o actividad de colusión
h. Cualquier otro cambio que el Organismo Regulador considere crítico

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

2.5. Informes de auditoría

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

2.6. Remediación

Si el informe de auditoría de controles de GIS 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. Para obtener información adicional, consulte la sección "Remediación" del GLI-GSF-1.

2.7. Empresa de seguridad independiente (ISF)

La auditoría de controles de GIS 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.

BORD

Derechos de autor © 2025 Gaming Laboratories International, LLC

Todos los derechos reservados.

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: a. Operar independientemente de cualquier proceso o software de seguridad dentro de la GPE; y b. 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 de los Programas de Control Crítico.
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; 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	MFA debe aplicarse a todas las cuentas privilegiadas que accedan a la aplicación de administración de Back Office. Esto incluye cuentas administrativas, operativas y de soporte técnico con permisos elevados.
OGIS-2.1.2	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-2.2	**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 solo debe otorgarse de forma temporal, según sea necesario, a través de canales seguros, y la actividad debe ser totalmente auditable.
OGIS-2.3	**Control de acceso basado en roles y privilegios mínimos**
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 laborales de los usuarios.
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.

RAOR

OGIS-2.3.3	Se debe hacer cumplir la 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 mediante listas blancas de IP, firewalls y segmentación de red.
OGIS-2.4.2	Se debe denegar explícitamente el acceso a las redes públicas y a los dispositivos que no son de confianza.
OGIS-2.4.3	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 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 deben finalizarse si se intenta un inicio de sesión duplicado.
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 solo a aplicaciones aprobadas y verificadas, bloqueando todo el resto del código para que no se ejecute en servidores críticos.
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 donde operan los programas de control crítico.
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 y respuesta a incidentes**
OGIS-3.4.1	Se debe implementar un monitoreo continuo para detectar cualquier intento de ejecución de código no autorizado.
OGIS-3.4.2	La empresa de juegos debe contar con procedimientos para abordar de inmediato cualquier evento de seguridad 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. 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. 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 supervisión específicos de la carga de trabajo.
OGIS-4	**Mecanismos de protección de aplicaciones**

DRAFT

OGIS-4.1	**Fijación SSL en aplicaciones móviles**
OGIS-4.1.1	Las aplicaciones móviles deben implementar la fijación SSL para garantizar una comunicación segura entre el cliente y el servidor.
OGIS-4.1.2	Las aplicaciones móviles deben diseñarse para finalizar las conexiones de red inmediatamente si el certificado o la clave anclados no coinciden.
OGIS-4.1.3	Los errores de validación de certificados deben registrarse con fines forenses y de supervisión.
OGIS-4.2	**Detección de jailbreak/raíz en dispositivos móviles**
OGIS-4.2.1	Las aplicaciones móviles deben 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 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	La base de código de la aplicación móvil debe usar técnicas de ofuscación de código para dificultar la ingeniería inversa del binario alterando los nombres de clase, variable y método, y reestructurando los flujos de control.
OGIS-4.3.2	El proceso de ofuscación debe incluirse en la canalización de compilación automatizada para garantizar que cada compilación de producción se ofusque correctamente antes del lanzamiento, y los mecanismos de detección de alteraciones deben alertar si la aplicación móvil se ha modificado después de la distribución.
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, incluidos los desafíos de CAPTCHA, la limitación de velocidad, las políticas de bloqueo de cuentas y la lógica de detección de relleno de credenciales, deben aplicarse en los puntos finales de autenticación.
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.
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 o la plataforma digital 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	El sitio web de juego, la aplicación móvil u otra plataforma digital deben estar protegidos por un WAF o equivalente.
OGIS-4.7.3	El WAF o 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	Se debe aplicar la limitación de velocidad en varios niveles para limitar los patrones de solicitud abusivos y mitigar la degradación del servicio:

DRAFT

	a. Nivel de red: los firewalls y los controladores de entrada deben limitar las conexiones o los paquetes por IP. b. Nivel de puerta de enlace de API: limite las llamadas a la API por cliente, con mecanismos de manejo de ráfagas y de retroceso. c. Nivel de aplicación: aplique lógica para detectar y suprimir el uso excesivo o el abuso de puntos finales específicos.
OGIS-5.1.2	La limitación de velocidad debe ser adaptativa y registrar las infracciones para su análisis.
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 de administración y otros componentes críticos del sistema deben ofuscarse mediante: a. Proxies inversos, redes de entrega de contenido (CDN) o equilibradores de carga en la nube; y b. Traducción de direcciones de red (NAT) y superposición de redes para enmascarar la verdadera infraestructura de origen.
OGIS-5.2.2	Los servicios de protección DDoS de terceros deben integrarse para: a. Detectar y absorber ataques volumétricos, de protocolo y de capa de aplicación; b. Asegúrarse de que la depuración del tráfico se realice más arriba antes de llegar al GPE; c. Mantener la continuidad del negocio a través de la conmutación automática por error y las redes perimetrales globales; y d. Validar los acuerdos de nivel de servicio (SLA) y los procedimientos de respuesta a incidentes con los proveedores de servicios.

BOR D

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.
Biometría	Una entrada de identificación biológica, como huellas dactilares, patrones de retina, datos de reconocimiento facial o huellas de voz
Puente	Divide las redes para reducir el tráfico general de la red. Un puente permite o impide que los datos pasen a través de él mediante la lectura de la dirección MAC.
Aplicaciones empresariales	Aplicaciones que funcionan como un servicio compartido para que los usuarios recopilen, procesen, mantengan, usen, compartan, difundan o eliminen datos confidenciales dentro del GPE con fines de auditoría de cumplimiento y respuesta a incidentes de seguridad
Plan de continuidad del negocio y recuperación ante desastres	Un plan para procesar aplicaciones críticas y evitar la pérdida de datos en caso de una falla importante de hardware o software o destrucción de instalaciones.
Envenenamiento de caché	Un ataque en el que el atacante inserta datos corruptos en la base de datos de caché del Servicio de nombres de dominio (DNS).
Tecnología de las comunicaciones	Cualquier método utilizado y los componentes empleados para facilitar la transmisión y recepción de información, incluida la transmisión y recepción por sistemas que utilizan redes de datos por cable, inalámbricas, por cable, de radio, microondas, luz, fibra óptica, satélite o informática, incluidas Internet e intranets.
Cumple	Se consideró que la política y la evidencia observadas cumplían plenamente con el GLI-GSF.
Confidencialidad	Preservar las restricciones autorizadas sobre el acceso y la divulgación de la información, incluidos los medios para proteger la privacidad personal y la información de propiedad.
Plan de contingencia	Política y procedimientos de gestión diseñados para mantener o restaurar las operaciones de juego, posiblemente en una ubicación alternativa, en caso de emergencias, fallas del sistema o desastres.

PAOR

Derechos de autor © 2025 Gaming Laboratories International, LLC

Todos los derechos reservados.

Término	Descripciones
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. • Componentes que generan, transmiten o procesan números aleatorios utilizados para determinar el resultado de juegos y eventos. • Componentes que almacenan los resultados o el estado actual del juego, la apuesta o los fondos disponibles de un cliente. • Puntos de entrada y salida de los componentes anteriores, incluidos otros sistemas que se comunican directamente con los componentes críticos del sistema. • Tecnología y redes de comunicaciones que transmiten datos confidenciales, incluidos los equipos de comunicación de red (NCE) y los controles de seguridad de la red. • Componentes que proporcionan servicios de seguridad, incluidos servidores de autenticación, servidores de control de acceso, sistemas de gestión de eventos e información de seguridad (SIEM), sistemas de seguridad física, sistemas de vigilancia, sistemas de autenticación multifactor (MFA), sistemas antimalware/antivirus. • Componentes que facilitan la segmentación, incluidos los controles de seguridad de red internos. • Componentes de virtualización como máquinas virtuales, conmutadores/enrutadores virtuales, dispositivos virtuales, aplicaciones/escritorios virtuales e hipervisores. • Infraestructura y componentes en la nube, tanto externos como locales, e incluyendo instancias de contenedores o imágenes, nubes privadas virtuales, administración de identidades y accesos basada en la nube, componentes que residen en las instalaciones o en la nube, mallas de servicios con aplicaciones en contenedores y herramientas de orquestación de contenedores. • Tipos de servidores que incluyen web, aplicación, base de datos, autenticación, correo, proxy, protocolo de tiempo de red (NTP) y sistema de nombres de dominio (DNS). • Dispositivos de terminales de usuario, como computadoras, computadoras portátiles, estaciones de trabajo, estaciones de trabajo administrativas, tabletas y dispositivos móviles. • 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).

RAOR

Derechos de autor © 2025 Gaming Laboratories International, LLC

Todos los derechos reservados.

Término	Descripciones
	• 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.
Módulo criptográfico	Hardware, software, firmware o combinación de los mismos que implementan funciones criptográficas como cifrado, descifrado, firmas, hash y administración de claves. El propósito principal de un módulo criptográfico es proporcionar un procesamiento y almacenamiento seguros de claves y operaciones.
Integridad de datos	La propiedad de que los datos son precisos y consistentes y no se han alterado de manera no autorizada en el almacenamiento, durante el procesamiento y mientras están en tránsito.
Denegación de servicio distribuida (DDOS)	Un tipo de ataque en el que se utilizan múltiples sistemas comprometidos, generalmente infectados con un programa de software destructivo, para apuntar a un solo sistema. Las víctimas de un ataque DDOS consisten tanto en el sistema objetivo final como en todos los sistemas utilizados y controlados maliciosamente por el pirata informático en el ataque distribuido.
Dominio	Un grupo de computadoras y dispositivos en una red que se administran como una unidad con reglas y procedimientos comunes.
Servicio de nombres de dominio (DNS)	La base de datos de Internet distribuida globalmente que (entre otras cosas) asigna los nombres de las máquinas a los números IP y viceversa.
Protocolo de configuración dinámica de host (DHCP)	Un servicio de red que permite a los dispositivos solicitar una configuración desde un punto central. Primero se transmite una solicitud a través del segmento de red, luego cualquier servidor responde a esa máquina específica con una dirección, cuánto tiempo es válida esa dirección y otros detalles pertinentes.
Ancho de banda efectivo	La cantidad de datos que realmente se pueden transferir a través de una red por unidad de tiempo. El ancho de banda efectivo a través de Internet suele ser considerablemente menor que el ancho de banda de cualquiera de los enlaces constituyentes.
Encriptación	La conversión de datos en una forma, llamada texto cifrado, que no puede ser fácilmente entendida por personas no autorizadas. Cuando el cifrado no sea posible debido a una limitación tecnológica o de rendimiento, se deben implementar otras medidas de protección razonables en su lugar y revisarlas caso por caso.
Clave de cifrado	Una clave que se ha cifrado para ocultar el valor del texto sin formato subyacente.
Aplicaciones expuestas externamente	Aplicaciones que son públicas y detectables a través del reconocimiento y el escaneo de red desde la Internet pública fuera de la red de la empresa. Esto no se aplica a las aplicaciones destinadas al uso de los usuarios.
Activos empresariales expuestos externamente	Activos que son públicos y detectables a través del reconocimiento del Sistema de nombres de dominio y el escaneo de red desde la Internet pública fuera de la red de la empresa. Esto no se aplica a los activos destinados al uso del usuario.
Cortafuegos	Un componente de un sistema informático o red que está diseñado para bloquear el acceso o el tráfico no autorizados al mismo tiempo que permite la comunicación externa.
Empresa de juegos	Un operador y cualquier proveedor, fabricante, vendedor, proveedor de servicios y/u otras entidades que tengan un papel en la supervisión del funcionamiento de un GPE o en la prestación de servicios integrales a su función, incluida la gestión de datos confidenciales.

BORRADOR

Derechos de autor © 2025 Gaming Laboratories International, LLC

Todos los derechos reservados.

Término	Descripciones
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.
Sistema de juego	Componente crítico del sistema en relación con cualquier estándar técnico aplicable y/o requisito reglamentario para las actividades de juego.
Entrada	Cualquier dispositivo, sistema o aplicación de software que pueda realizar la función de traducir datos de un formato a otro. La característica clave de una puerta de enlace es que convierte el formato de los datos, no los datos en sí.
Política de GIS	Un documento que delinea la estructura de gestión de la seguridad y asigna claramente las responsabilidades de seguridad y sienta las bases necesarias para medir de manera confiable el progreso y el cumplimiento.
Incidente de GIS	Un suceso que ponga en peligro real o potencialmente la integridad, confidencialidad o disponibilidad de un GPE o de los datos confidenciales que el GPE procesa, almacena o transmite o que constituye una violación o amenaza inminente de violación de las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable.
Plan de respuesta a incidentes de GIS	La documentación de un conjunto predeterminado de instrucciones o procedimientos cuando se encuentra un ciberataque malicioso contra el GPE de una empresa de juegos
Membresía de grupo	Un método para organizar las cuentas de usuario en una sola unidad (por puesto de trabajo) mediante el cual el acceso a las funciones del sistema puede modificarse a nivel de unidad y los cambios surten efecto para todas las cuentas de usuario asignadas a la unidad.
Protocolo de transporte de hipertexto (HTTP)	El protocolo subyacente utilizado para definir cómo se formatean y transmiten los mensajes, y qué acciones deben realizar los servidores y navegadores en respuesta a varios comandos.
Concentrador	Conecta dispositivos en una red de par trenzado. Un concentrador no realiza ninguna tarea además de la regeneración de señales.
Integridad	Proteger contra la modificación o destrucción indebida de información e incluye garantizar el no repudio y la autenticidad de la información.
Internet	Un sistema interconectado de redes que conecta computadoras de todo el mundo a través de TCP/IP.
Dirección de protocolo de Internet (dirección IP)	Número único de un equipo que se utiliza para determinar dónde deben entregarse los mensajes transmitidos en Internet. La dirección IP es análoga a un número de casa para el correo postal ordinario.
Sistema de detección de intrusos/Sistema de prevención de intrusiones (IDS/IPS)	Un sistema que inspecciona toda la actividad de red entrante y saliente e identifica patrones sospechosos que pueden indicar un ataque a la red o al sistema por parte de alguien que intenta ingresar o comprometer un sistema. Utilizada en seguridad informática, la detección de intrusiones se refiere al proceso de monitorear las actividades de la computadora y la red y analizar esos eventos para buscar signos de intrusión en el GPE.
Seguridad del IP (IPSec)	Un conjunto de protocolos para proteger las comunicaciones de Protocolo de Internet (IP) mediante la autenticación y el cifrado de cada paquete IP de un flujo de datos. IPsec también incluye protocolos para establecer la

BORRADO

Término	Descripciones
	autenticación mutua entre agentes al comienzo de la sesión y la negociación de claves de cifrado que se utilizarán durante la sesión.
Kerberos	Un protocolo de autenticación de red diseñado para proporcionar una autenticación segura para aplicaciones cliente/servidor mediante el cifrado de clave secreta.
Clave	Un valor utilizado para controlar funciones criptográficas, como descifrado, cifrado, descifrado, firmas, hash, etc.
Gestión de claves	Actividades que implican el manejo de claves de cifrado y otros parámetros de seguridad relacionados (por ejemplo, contraseñas) durante todo el ciclo de vida de las claves, incluida su generación, almacenamiento, establecimiento, entrada y salida, y puesta a cero.
Utilización de enlaces	El porcentaje de tiempo que un enlace de comunicaciones está dedicado a transmitir datos.
No conformidad mayor	Se ha identificado una falla fundamental (sistemática) que afecta a varios controles de GIS y significa que no se pueden cumplir las políticas de seguridad generales. Puede ser: • Una serie de no conformidades menores contra un control pueden representar una falla total del sistema y, por lo tanto, considerarse una no conformidad mayor; • Cualquier no conformidad que resulte en el probable envío de un producto no conforme. Una condición que puede resultar en la falla o reducir materialmente la usabilidad de los productos o servicios para su propósito previsto; o • Una no conformidad que el juicio y la experiencia indican es probable que resulte en la falla del sistema o que reduzca materialmente su capacidad para garantizar procesos y productos controlados.
Disfunción	Cuando un componente crítico del sistema no funciona según lo previsto.
Malware	Un programa que se inserta en un sistema, generalmente de forma encubierta, con la intención de comprometer la integridad, confidencialidad o disponibilidad de los datos, aplicaciones o sistema operativo de la víctima o de molestar o interrumpir a la víctima.
Ataque "Man-in-the-Middle"	Un ataque en el que el atacante transmite en secreto y posiblemente altera la comunicación entre dos partes que creen que se están comunicando directamente entre sí.
Autenticación de mensajes	Una medida de seguridad diseñada para establecer la autenticidad de un mensaje por medio de un autenticador dentro de la transmisión derivado de ciertos elementos predeterminados del propio mensaje.
Código de autenticación de mensajes (MAC)	Una suma de comprobación criptográfica en los datos que utiliza una clave simétrica para detectar modificaciones accidentales e intencionadas de los datos.
No conformidad menor	Un control de GIS no se ha abordado o no cumple con el GLI-GSF (no sistemático) y ese juicio y experiencia indican que no es probable que resulte en la falla del sistema o reduzca su capacidad para garantizar procesos o productos controlados. Puede ser: • Una falla en alguna parte del sistema en relación con un control; o • Un solo lapso observado en el seguimiento de un elemento del sistema.
Código móvil	Código ejecutable que se mueve de una computadora a otra, incluido el código legítimo y el código malicioso, como los virus informáticos.
Autenticación multifactor (MFA)	Tipo de autenticación que utiliza dos o más de las siguientes opciones para comprobar la identidad de un usuario: • Información conocida solo por el usuario (por ejemplo, una contraseña, PIN o respuestas a preguntas de seguridad); • Un artículo poseído por un usuario (por ejemplo, un token electrónico, un token físico o una tarjeta de identificación); y • Los datos biométricos de un usuario (por ejemplo, huellas dactilares, patrones de retina, datos de reconocimiento facial o huellas de voz).

PROOF

Derechos de autor © 2025 Gaming Laboratories International, LLC

Todos los derechos reservados.

Término	Descripciones
Equipo de comunicación de red (NCE)	Tecnología de comunicaciones que controla la comunicación de datos en un sistema, incluidos, entre otros, NIC, cables, conmutadores, puentes, concentradores, enrutadores, puntos de acceso inalámbricos y teléfonos, dispositivos de red VoIP, puntos de acceso inalámbricos, dispositivos de red y otros dispositivos de seguridad.
Tarjeta de interfaz de red (NIC)	El mecanismo por el cual los terminales y sistemas se conectan a la red. Las NIC pueden ser tarjetas de expansión complementarias, tarjetas PCMCIA o interfaces integradas.
Observación	Un hallazgo que vale la pena señalar por su posible mejora para cumplir con las mejores prácticas de la industria.
Contraseña	Una cadena de caracteres (letras, números y otros símbolos) que se usa para autenticar una identidad o para verificar la autorización de acceso.
Información de identificación personal (PII)	Datos confidenciales que podrían usarse para identificar a una persona en particular. Los ejemplos incluyen un nombre legal, fecha de nacimiento, lugar de nacimiento, número de identificación gubernamental (número de seguro social, número de identificación del contribuyente, número de pasaporte o equivalente), información financiera personal (números de instrumentos de crédito o débito, números de cuentas bancarias, etc.) u otra información personal si lo define el Organismo Regulador.
Número de identificación personal (PIN)	Un código numérico asociado a un individuo y que permite el acceso seguro a un dominio, cuenta, red, sistema, etc.
Controles físicos y ambientales	Las medidas implementadas para proteger los activos físicos, las instalaciones y las condiciones ambientales que albergan los sistemas y la infraestructura del entorno de producción de juegos.
Puerto	Un punto de entrada o salida físico de un módulo que proporciona acceso al módulo para señales físicas, representado por flujos de información lógica (los puertos separados físicamente no comparten el mismo pin o cable físico).
Proxy	Una aplicación que "rompe" la conexión entre el cliente y el servidor. El proxy acepta ciertos tipos de tráfico que entran o salen de una red y lo procesa y reenvía. Esto cierra efectivamente el camino recto entre las redes internas y externas. Dificultar que un atacante obtenga direcciones internas y otros detalles de la red interna.
Protocolo	Un conjunto de reglas y convenciones que especifica el intercambio de información entre dispositivos, a través de una red u otros medios.
Organismo regulador	El organismo gubernamental o equivalente que regula o controla las operaciones de los juegos de azar.
Acceso remoto	Cualquier acceso desde fuera del sistema o de la red del sistema, incluido cualquier acceso desde otras redes dentro del mismo sitio o lugar.
Riesgo	La probabilidad de que una amenaza tenga éxito en su ataque contra una red o sistema.
Enrutador	Conecta las redes. Un enrutador utiliza la dirección de red configurada por software para tomar decisiones de reenvío.
Protocolo de comunicación segura	Un protocolo de comunicación que proporciona la confidencialidad, la autenticación y la protección de la integridad del contenido adecuadas.
Shell seguro (SSH)	Permite tunelizar cualquier otro protocolo de forma segura.
Certificado de seguridad	Información, a menudo almacenada como un archivo de texto que utiliza el protocolo Transport Socket Layer (TSL) para establecer una conexión segura. Para que se cree una conexión TSL, ambos lados deben tener un certificado de seguridad válido.

PROOF

Derechos de autor © 2025 Gaming Laboratories International, LLC

Todos los derechos reservados.

Término	Descripciones

Datos confidenciales	Información que debe manejarse de manera segura, incluidos, entre otros, según corresponda:
	• Registros de auditoría y bases de datos del sistema que registran la información utilizada para determinar el resultado, el pago, el canje y el seguimiento de la información del usuario;
	• Contabilidad e información de eventos significativos relacionados con los componentes críticos del sistema del GPE;
	• Semillas 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").
Proveedores de servicios	Entidades que ofrecen plataformas, software y servicios a las empresas de juegos. Los ejemplos incluyen consultores de TI, proveedores de servicios administrados, plataformas de software como servicio (SaaS) y proveedores de servicios en la nube. Los proveedores y vendedores externos también se consideran proveedores de servicios.
Identificador de conjunto de servicios (SSID)	Un nombre que identifica una LAN inalámbrica 802.11 en particular.
Código Shell (Shellcode)	Un pequeño fragmento de código utilizado como carga útil en la explotación de la seguridad. Shellcode explota la vulnerabilidad y permite a un atacante la capacidad de reducir la garantía de información de un sistema.
Verificación de firma	Garantizar mediante firma electrónica la comprobación de que cualquier paquete de software es una copia auténtica del software creado por su fabricante y, en su caso, una copia exacta del software certificado por el Laboratorio de Pruebas Independiente (ITL).
Protocolo simple de administración de red (SNMP)	Protocolo que se utiliza para configurar, ver y, en general, administrar dispositivos en red. Las impresoras en red, los conmutadores, etc. a menudo implementan este protocolo de forma predeterminada.
Ingeniería social	Un intento de engañar a alguien para que revele información (por ejemplo, una contraseña) que puede usarse para atacar sistemas o redes. Los ataques de ingeniería social incluyen intrusiones no técnicas en un GPE utilizando

BORRADOR

Derechos de autor © 2025 Gaming Laboratories International, LLC

Todos los derechos reservados.

Término	Descripciones
	información adquirida a través de la interacción humana y se basan en trucos que se aprovechan de que un individuo no esté familiarizado con la tecnología y los protocolos emergentes.
Código fuente	Una lista de texto de comandos que se compilarán o ensamblarán en un programa informático ejecutable.
Protocolo sin estado	Un esquema de comunicaciones que trata cada solicitud como una transacción independiente que no está relacionada con ninguna solicitud anterior, de modo que la comunicación consta de pares independientes de solicitudes y respuestas.
Interruptor	Conecta dispositivos en una red 802.3. Un conmutador reenvía datos a su destino mediante la dirección MAC incrustada en cada paquete.
Administrador del sistema	La(s) persona(s) responsable(s) de mantener el funcionamiento estable del GPE (incluida la infraestructura de software y hardware y el software de aplicación).
Controles técnicos	Los mecanismos de seguridad implementados dentro de los sistemas y la infraestructura del Entorno de Producción 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.
Marca de tiempo	Registro del valor actual de la fecha y hora que se agrega a un mensaje en el momento en que se crea el mensaje.
Protocolo de control de transmisión/Protocolo de Internet (TCP/IP)	El conjunto de protocolos de comunicaciones utilizados para conectar hosts en Internet.
Acceso no autorizado	Una persona obtiene acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso.
Protocolo de datagramas de usuario (UDP)	Un protocolo de transporte que no garantiza la entrega. Por lo tanto, es más rápido, pero menos confiable.
Control de versiones	El método por el cual se verifica que los componentes críticos del sistema aprobados en evolución están funcionando en un estado aprobado.
Red privada virtual (VPN)	Una red lógica que se establece sobre una red física existente y que normalmente no incluye todos los nodos presentes en la red física.
Virus	Un programa autorreplicante, generalmente con intenciones maliciosas, que se ejecuta y se propaga modificando otros programas o archivos.
Virus Scanner	Software utilizado para prevenir, detectar y eliminar virus informáticos, incluidos malware, gusanos y troyanos.
Vulnerabilidad	Software, hardware u otras debilidades en una red o sistema que pueden proporcionar una "puerta" para introducir una amenaza.
Punto de acceso inalámbrico (WAP)	Proporciona capacidades de red a dispositivos de red inalámbrica. Un WAP se usa a menudo para conectarse a una red cableada, actuando así como un enlace entre las partes cableadas e inalámbricas de la red.
Wi-Fi	La tecnología estándar de red de área local inalámbrica (WLAN) para conectar computadoras y dispositivos electrónicos entre sí y/o a Internet.

BORRADOR