GLI®

MARCO DE SEGURIDAD DEL JUEGO

GLI-GSF-2

EVALUACIÓN DE SEGURIDAD TÉCNICA DEL JUEGO (GTS)

Versión 1.0 – Publicado el 7 de febrero de 2025

Contenido

Derechos de autor © 2025 Gaming Labs International, LLC

Todos los derechos reservados.

1. INTRODUCCIÓN

1.1. Comunicado general

La integridad y precisión del funcionamiento 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 Firma de Seguridad Independiente (ISF) calificada para realizar evaluaciones de seguridad de juego como una adición esencial a las pruebas y certificación de los Componentes Críticos del Sistema de un GPE por parte de un Laboratorio de Pruebas Independiente (ITL).

a. Este módulo del Marco de Seguridad del Juego GLI, GLI-GSF-2 establece un punto de referencia para la realización de evaluaciones de la Seguridad Técnica del Juego (GTS) del GPE de una Empresa de Juegos.
b. Estas Pruebas GTS se aplican a las GPE utilizadas para todas las formas de juego, como los juegos de casino, la lotería, las apuestas de eventos y los juegos interactivos.
c. Este módulo se puede utilizar junto con el GLI-GSF-1, el cual proporciona los Controles Comunes de Seguridad de la Información del Juego (GIS) necesarios para auditar el Sistema de Gestión de la Seguridad de la Información del Juego (GISMS) de una empresa del juego
d. Dependiendo del tipo de empresa de juegos, también se pueden aplicar módulos adicionales de GLI-GSF.

NOTA: Todo el marco de seguridad para juegos GLI (GLI-GSF) está disponible de forma gratuita en www.gaminglabs.com.

1.2. Empresa de juegos y rol de gestión de datos confidenciales

Garantizar la seguridad de una GPE es una responsabilidad colectiva que abarca las múltiples entidades que componen la Empresa de Juegos, como el operador y sus proveedores, fabricantes, vendedores, prestadores de servicios y otras entidades que tienen un papel en la supervisión o el funcionamiento de una GPE o en la prestación de servicios integrales para 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 sensibles, que como mínimo consisten en lo siguiente, según corresponda:

a. 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;
b. Información contable y de eventos Significativos relacionados con los componentes críticos del sistema de la GPE;
c. Semillas RNG y cualquier otra información que afecte los resultados de los juegos y las apuestas;
d. Claves de cifrado, donde la implementación elegida requiere la transmisión de claves;
e. Números de validación asociados con cuentas de usuarios, instrumentos de apuestas y cualquier otra transacción de juego;
f. Transferencias de fondos hacia y desde cuentas de usuarios, cuentas de pago electrónico y con fines de juego;
g. Paquetes de software dentro de la GPE;
h. Cualquier dato de ubicación relacionado con la actividad de los empleados o usuarios (por ejemplo, gestión de cuentas, juegos en línea, etc.);
i. Cualquiera de la siguiente información registrada para cualquier empleado o cliente:
    i. Número de identificación gubernamental (número de seguro social, número de identificación del contribuyente, número de pasaporte o equivalente);
    ii. Información financiera personal (números de instrumentos de crédito o débito, números de cuentas bancarias, etc.);
    iii. Credenciales de autenticación en relación con cualquier cuenta de usuario o cuenta de usuario;
    iv. Cualquier otra información de identificación personal (PII, por sus siglas en inglés) que deba mantenerse confidencial; y
j. Cualquier otro dato que el Organismo Regulador o la Empresa de Juegos considere sensible.

NOTA: Este documento no tiene la intención de definir qué entidades son responsables de asegurar la GIS. Es responsabilidad de las múltiples entidades que componen la Empresa de Juegos de Azar ponerse de acuerdo sobre la responsabilidad.

1.3. Entorno de producción de juegos (GPE)

Un GPE se refiere al entorno operativo donde se realizan, administran y entregan a los usuarios las actividades de juego y los servicios relacionados en vivo o en tiempo real. Abarca la infraestructura física y virtual, los sistemas, el software y los procesos necesarios para facilitar diversas formas de juego, como los juegos de casino, la lotería, las apuestas de eventos y los juegos interactivos. El GPE también abarca los sistemas de backend, las aplicaciones empresariales y la infraestructura que interactúan y/o respaldan las actividades de juego. Las características clave de un GPE incluyen:

a. Componentes críticos del sistema: Esto incluye los dispositivos de red, servidores, dispositivos informáticos, componentes virtuales, hardware y plataformas de software que respaldan la ejecución de actividades de juego, como dispositivos de juego, mesas de juego, sistemas de juego, sistemas de lotería, sistemas de apuestas de eventos y sistemas o aplicaciones de juego interactivo.
b. Módulos criptográficos: Los módulos criptográficos utilizados dentro del GPE son responsables de las funciones criptográficas, incluido el cifrado y descifrado de datos confidenciales, utilizando algoritmos que cumplen con los estándares actuales aceptados por la industria, como ISO/IEC 19790, FIPS 140-2 o equivalentes.
c. Procesamiento de transacciones: El GPE procesa las transacciones monetarias relacionadas con las actividades de juego, incluidas las apuestas, los pagos, los depósitos, los retiros y las transacciones financieras con los clientes.
d. Medidas de seguridad: Se implementan sólidas medidas de seguridad para salvaguardar la integridad, confidencialidad y disponibilidad de los componentes críticos del sistema, los datos confidenciales, las transacciones financieras y la información de los usuarios contra el acceso no autorizado, el fraude, la manipulación y las amenazas cibernéticas.
e. Gestión de riesgos: El GPE emplea prácticas de gestión de riesgos para identificar, evaluar, mitigar y monitorear los riesgos asociados con las operaciones de juego, incluidos los riesgos operativos, los riesgos financieros, los riesgos regulatorios y los riesgos tecnológicos.
f. Operación continua: Un GPE generalmente opera las 24 horas del día, los 7 días de la semana para satisfacer la demanda de los clientes y maximizar la generación de ingresos. Esto requiere alta disponibilidad, confiabilidad y resiliencia de la infraestructura y los sistemas para minimizar el tiempo de inactividad y las interrupciones.
g. Monitoreo y control: Existen mecanismos de monitoreo, vigilancia y control en tiempo real para supervisar las actividades de juego, detectar anomalías, garantizar el cumplimiento de las reglas y regulaciones y responder con prontitud a incidentes de la GIS, fraude u otros problemas.
h. Cumplimiento regulatorio: El cumplimiento de las regulaciones de juego, los requisitos de licencia y los estándares de la industria es esencial en un GPE para garantizar el juego limpio, la protección de los usuarios, las prácticas de juego responsable y el cumplimiento de las obligaciones legales y reglamentarias.

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, lo que implica la identificación de riesgos de la GIS, la implementación de controles y salvaguardas adecuados, el monitoreo y la evaluación continuos de las medidas de seguridad y la mejora continua para adaptarse a las amenazas cambiantes y los requisitos de cumplimiento.

1.5. Propósito del marco

Garantizar la seguridad e integridad de las actividades de juego es primordial para mantener la confianza del público en el sector. Por lo tanto, los casinos, loterías, operaciones de apuestas de eventos, operaciones de juegos interactivos y otras empresas de juegos deben establecer y mantener un marco claramente definido y documentado para lograr y preservar la confianza del público 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.

Derechos de autor © 2025 Gaming Labs International, LLC

Todos los derechos reservados.

1.6. Normas y directrices de seguridad consultadas

Cada módulo de la GLI-GSF está basado en estándares y directrices de seguridad de uso común que proporcionan una base aceptada por la industria para desarrollar prácticas efectivas de gestión de la 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 de la GLI-GSF puede ser adoptado en su totalidad o en parte por cualquier Organismo Regulador que desee aplicar un conjunto completo de Metodologías de Ensayo de la GTS.

2. EVALUACIONES DE LA GTS

2.1. Resumen de la evaluación

La evaluación de la GTS se lleva a cabo 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 juego. Esta metodología se basa en gran medida en la seguridad por capas para reducir el riesgo para los sistemas informáticos y de red, proporcionando redundancia y reforzando el modelo de seguridad general, ya que se deben vulnerar varias capas de seguridad antes de acceder a un almacén de datos confidencial.

NOTA: El enfoque de la guía GTS detallada en el GLI-GSF-2 está en las pruebas técnicas de seguridad para juegos, otros métodos de evaluación se discuten en los módulos de soporte del GLI-GSF.

2.2. Métodos de evaluación

Una evaluación la GTS utiliza una serie de métodos de evaluación, entre los que se incluyen los siguientes métodos, cuyos resultados se utilizan para respaldar la determinación de la seguridad de un GPE:

a. Entrevista: Un tipo de método de evaluación caracterizado por el proceso de llevar a cabo discusiones con individuos o grupos dentro de una empresa de juegos 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 verificar, inspeccionar, revisar, observar, estudiar o analizar uno o más objetos de evaluación para facilitar la comprensión, lograr aclaraciones u obtener evidencia.
c. Prueba: Un tipo de método de evaluación caracterizado por el proceso de ejercitar uno o más objetos de evaluación bajo condiciones específicas para comparar el comportamiento real con el esperado.

2.3. Tareas de evaluación

A continuación se presentan las actividades de evaluación de la GTS de alto nivel sugeridas. En el Apéndice se detallan los requisitos mínimos de pruebas de la GTS con más detalle. Se dirige a los usuarios de este documento al Apéndice para asegurarse de que no se pase por alto ninguna prueba de la GTS necesaria. Las pruebas de la GTS enumeradas en el Apéndice no son exhaustivas y se pueden incluir pruebas de la GTS adicionales en función de los requisitos reglamentarios y el alcance de la evaluación de la GTS. Estas evaluaciones de la GTS deben abarcar más que escaneos automatizados e incorporar técnicas manuales de pruebas de penetración.

2.3.1. Evaluación de vulnerabilidades

La ISF realiza una evaluación de vulnerabilidades de los sistemas, sitios web de Internet, aplicaciones móviles, redes internas, externas e inalámbricas de la Empresa de Juegos con la intención de identificar vulnerabilidades o vulnerabilidades potenciales de dispositivos, sistemas y aplicaciones que transfieren, almacenan o procesan datos confidenciales conectados o presentes en las redes. Las evaluaciones de vulnerabilidad incluyen la identificación y cuantificación pasiva de los riesgos potenciales dentro del GPE.

2.3.2. Prueba de penetración

La ISF realiza una prueba de penetración de los sistemas, sitios web de Internet, aplicaciones móviles y redes internas, externas e inalámbricas de la Empresa de Juegos para confirmar si las vulnerabilidades identificadas de los dispositivos, sistemas y aplicaciones son susceptibles de ser comprometidas. El simple hecho de ejecutar un escaneo de vulnerabilidades y proporcionar esos resultados no es suficiente para cumplir con los requisitos de la prueba de penetración. Debe haber alguna forma de verificación y/o explotación manual. Las pruebas de penetración incluyen:

a. Evaluar la seguridad de los entornos externos e internos del GPE.
b. Identificar las debilidades que podrían ser explotadas por los atacantes para obtener acceso no autorizado, interrumpir las operaciones o exfiltrar datos confidenciales.

c. Simulación de posibles escenarios de ataque para comprender el impacto de las vulnerabilidades en la postura de seguridad del GPE.
d. Validar los hallazgos de las evaluaciones de vulnerabilidad a través de técnicas de prueba manuales.

2.3.3. Evaluaciones de riesgos

La ISF realiza una evaluación de riesgos para identificar posibles amenazas y vulnerabilidades, así como no conformidades a cualquier prueba de la GTS aplicable que pueden no estar explícitamente enumeradas en el GLI-GSF, pero que se observaron durante la auditoría y pueden constituir un riesgo. La ISF debe utilizar un sistema de puntuación apropiado para la seguridad del juego (por ejemplo, CVSS, ISO/IEC 31010, etc.) para asignar niveles de gravedad (crítica,alto riesgo, riesgo medio, o riesgo bajo) a amenazas, vulnerabilidades y no conformidades, permitiendo la priorización de respuestas y recursos según el nivel de gravedad. El sistema de puntuación utilizado por la ISF debe ser identificado en el informe de evaluación de la GTS.

2.4. Frecuencia de evaluación

2.4.1. Evaluación inicial

La Empresa de Juegos de Azar debe tener una evaluación de la GTS realizada por una ISF dentro de los noventa días posteriores al inicio de las operaciones de juego dentro de esa jurisdicción, a menos que el Organismo Regulador haya aconsejado lo contrario. Cualquier aplazamiento de esta evaluación de la GTS solicitado por la Empresa de Juegos, junto con un calendario de evaluaciones actualizado, debe ser autorizado por el Organismo Regulador.

NOTA: Se recomienda que los organismos reguladores permitan flexibilidad en los horarios de evaluación de la GTS de las empresas de juegos de azar multijurisdiccionales para permitir la consolidación de las evaluaciones de varias jurisdicciones en un programa común.

2.4.2. Evaluación anual

La Empresa de Juegos de Azar debe, por regla general, tener otra evaluación de la GTS realizada por una ISF dentro de los doce meses posteriores a la evaluación de la GTS anterior, a menos que el organismo regulador haya aconsejado lo contrario. Cualquier aplazamiento de esta evaluación solicitado por la Empresa de Juegos, junto con un calendario de evaluaciones actualizado, debe ser autorizado por el Organismo Regulador.

NOTA: Se recomienda que los organismos reguladores permitan flexibilidad en los horarios de evaluación de la GTS de las empresas de juegos de azar multijurisdiccionales para permitir la consolidación de las evaluaciones de varias jurisdicciones en un programa común.

2.4.3. Evaluaciones adicionales

La Empresa de Juegos debe, por regla general, tener evaluaciones de la GTS adicionales realizadas por una ISF después de cualquier cambio crítico dentro del GPE, como actualizaciones y modificaciones de infraestructura o aplicaciones, o la instalación de nuevos Componentes Críticos del Sistema. La determinación de lo que constituye un cambio "crítico" se basa en el proceso de evaluación de riesgos de la empresa de juegos, la configuración específica del GPE y los requisitos del organismo regulador. Sin embargo, cualquier cambio que pueda afectar a la seguridad del GPE o permitir el acceso a datos confidenciales y/o componentes críticos del sistema puede ser considerado "crítico" por la Empresa de juego.

2.5. Informes de evaluación

Los resultados de una evaluación de la GTS identificarán para las empresas de juego aquellas áreas de las operaciones en las que se debe considerar la mejora y recomendarán estrategias para mejorar esas áreas. El informe de evaluación de la GTS debe presentarse al organismo regulador a más tardar noventa días después de que se haya completado la evaluación de la GTS, a menos que el organismo regulador haya aconsejado lo contrario. El informe de evaluación de la GTS debe incluir todo lo siguiente:

a. Resumen ejecutivo:

i. El nombre y la información de contacto de la Empresa de Juegos;
ii. Una breve descripción del modelo de negocio de la empresa de juegos, las actividades de juego ofrecidas, los proveedores de servicios utilizados, la ubicación, el número de empleados, el sitio web, las certificaciones y una descripción de alto nivel de la infraestructura de informática (incluidos los centros de datos, los servicios en la nube, etc.)

b. Detalles de la evaluación de la GTS:
i. El nombre de la ISF, la afiliación de la empresa, la información de contacto y las calificaciones y experiencia de las personas que llevaron a cabo la evaluación de la GTS;
ii. La(s) fecha(s) de la evaluación de la GTS, incluida la fecha de solicitud, la fecha de inicio, la fecha de finalización y la fecha del informe;

c. Alcance de la evaluación de la GTS:
i. Una descripción general de alto nivel de las pruebas realizadas, especificando los entornos (por ejemplo, desarrollo, producción) y los tipos de sistemas probados (por ejemplo, aplicaciones web, redes, bases de datos, sistemas operativos).
ii. Identificación de los componentes críticos del sistema y los activos revisados, detallando cómo se seleccionaron estos componentes y activos como parte de la evaluación de la GTS.
iii. Herramientas y técnicas específicas utilizadas durante la evaluación de la GTS, incluidos los nombres de los programas, las versiones y los sitios web oficiales de las herramientas empleadas.

d. Metodología:
i. Una descripción detallada de la metodología de la prueba de penetración o el marco de evaluación de vulnerabilidades aplicado (por ejemplo, OWASP, OSSTMM).
ii. Cualquier limitación o exclusión en la evaluación de la GTS, con justificaciones (por ejemplo, ciertos sistemas estaban fuera del alcance debido a requisitos comerciales).

e. Pruebas recopiladas:
i. Documentación revisada, incluidos los nombres, las fechas y las versiones.
ii. Personal entrevistado, con roles, ubicaciones, nombres, fechas y versiones de las entrevistas.
iii. Pruebas (p.ej. capturas de pantalla, registros) que ilustren claramente las vulnerabilidades identificadas, incluidos los comandos y las herramientas utilizados para detectar estos problemas.
iv. Técnicas de muestreo utilizadas para verificar la postura de seguridad, incluido el tamaño y la naturaleza de la muestra.

f. Hallazgos y resultados:
i. Un resumen de cada vulnerabilidad descubierta, clasificadas por gravedad (por ejemplo, crítica, alto riesgo, riesgo medio, riesgo bajo).
ii. Una explicación detallada de cada vulnerabilidad, respaldada por pruebas (por ejemplo, capturas de pantalla, registros).
iii. Una evaluación del impacto o riesgo potencial asociado con cada vulnerabilidad identificada, teniendo en cuenta el entorno específico de la empresa de juegos.
iv. Pasos de corrección recomendados para cada vulnerabilidad identificada, con niveles de prioridad y plazos sugeridos para la mitigación.
v. La respuesta de la empresa de juego a los hallazgos y resultados, incluidas las medidas correctoras recomendadas.

2.6. Remediación

Si el informe de evaluación de la GTS de la ISF recomienda la remediación, la Empresa de Juegos de Azar debe proporcionar al organismo regulador y a la ISF, si es requerido por 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 corrección.

a. Cada vulnerabilidad debe abordarse a través del proceso de corrección de la empresa de juegos, lo que incluye:
i. Acciones tomadas para determinar el alcance de la vulnerabilidad específica y contenerla.
ii. Investigación de la causa raíz para determinar las causas más básicas de la vulnerabilidad.
iii. Acciones tomadas para corregir la vulnerabilidad y, en respuesta a la causa raíz, eliminar la recurrencia de la vulnerabilidad.

b. Las medidas correctivas para abordar cada vulnerabilidad crítica o de alto riesgo identificada deben llevarse a cabo de inmediato y el organismo regulador y la ISF, si es requerido por el organismo regulador,

deben ser notificados de las acciones tomadas dentro de los treinta días, a menos que el organismo regulador especifique lo contrario. Sio es requerido por el organismo regulador, la ISF debe realizar una evaluación de seguimiento dentro de un plazo razonable espewcificado en el plan de remediación para confirmar las acciones tomadas, evaluar su efectividad y determinar si las vulnerabilidades se han resuelto.

c. Los pasos de remediación para abordar cada vulnerabilidad identificada como riesgo medio o riesgo bajo deben ser documentados y enviados por la Empresa de Juegos al organismo regulador y a la ISF, si es requerido por el organismo regulador, para su revisión en un plazo de treinta días, a menos que el organismo regulador especifique lo contrario. Si las acciones se consideran satisfactorias, se les dará seguimiento en la próxima evaluación programada.

d. Una vez que se hayan tomado las medidas correctivas, la Empresa de Juegos proporcionará al organismo regulador y a la ISF, si es requerido por el organismo regulador, la documentación que evidencie la finalización.

e. La Empresa de Juegos de Azar debe mantener registros de corrección, incluidas pruebas objetivas, durante al menos cinco años, a menos que el organismo regulador especifique lo contrario.

2.7. Empresa de Seguridad Independiente (ISF)

La evaluación de la GTS debe ser llevada a cabo por individuos con suficientes calificaciones, lo que significa que la ISF debe contratar a individuos suficientemente calificados, competentes y experimentados. A menos que el organismo regulador especifique lo contrario, estas personas deben:

a. Tener una formación académica pertinente o, de otro modo, proporcionar cualificaciones pertinentes para evaluar los GPE;

b. Obtener y mantener certificaciones suficientes para demostrar competencia y experiencia como profesional de seguridad calificado por juntas de certificación reconocidas, ya sea a nivel nacional o internacional. Las siguientes certificaciones pueden demostrar la idoneidad para completar la evaluación de la GTS:
   i. Profesional Certificado en Seguridad Ofensiva (OSCP)
   ii. Hacker Ético Certificado (CEH)
   iii. Certificaciones de Certificación Global de Aseguramiento de la Información (GIAC), Probador de Penetración Certificado por GIAC (GPEN), Probador de Penetración de Aplicaciones Web GIAC (GWAPT), Investigador de Exploits y Probador de Penetración Avanzado GIAC (GXPN).
   iv. Autoridad Nacional de Ciberseguridad (NCSC), Certificación del Servicio de Verificación de Salud de la informática (CHECK).
   v. Tiger Scheme: Probador de seguridad senior, probador de seguridad calificado
   vi. Proveedor de escaneo aprobado (ASV)

c. Tener al menos cinco años de experiencia en la realización de evaluaciones de la GTS en la industria del juego o, cuando sea aceptable para el organismo regulador, otra experiencia relevante en evaluaciones de seguridad de una industria similar; y

d. Cumplir con cualquier otro requisito prescrito por el organismo regulador.

NOTA: Nada de lo aquí contenido tiene la intención de prohibir que el personal cualificado del organismo regulador actúe como una ISF, siempre que sean independientes de la Empresa de Juego que se está evaluando.

3. ANÁLISIS DE VULNERABILIDADES RECURRENTES

3.1. Cadencia de los escaneos

A menos que el organismo regulador especifique lo contrario, los escaneos de vulnerabilidades de red internos y externos deben realizarse al menos trimestralmente y después de cualquier cambio crítico en el GPE. Cualquier aplazamiento de los escaneos de vulnerabilidad que solicite la empresa de juego, junto con un calendario actualizado, deberá ser autorizado por el Organismo Regulador.

NOTA: Se recomienda que los organismos reguladores permitan flexibilidad para la programación de escaneos de vulnerabilidades de las empresas de juegos de azar multijurisdiccionales a fin de permitir la consolidación de los análisis de vulnerabilidades de varias jurisdicciones en un horario común.

3.2. Requisitos del escáner

Los escáneres de vulnerabilidades deben utilizarse para probar e identificar las vulnerabilidades de los dispositivos de red interna, las aplicaciones y las defensas del perímetro de la red, así como el cumplimiento del plan y los estándares de seguridad. Los escáneres de vulnerabilidades deben tener la capacidad de manejar las siguientes tareas mínimas:

a. No disruptivo: el escáner debe configurarse para evitar métodos de prueba disruptivos que podrían causar bloqueos del sistema, reinicios o interferir con los servicios de red, como el servicio de nombres de dominio (DNS), el enrutamiento o la conmutación.
b. Detección de hosts: El escáner debe identificar con precisión los sistemas en vivo, incluidos aquellos que no responden a las solicitudes de eco ("ping") estándar del Protocolo de Mensajes de Control de Internet (ICMP).
c. Detección de servicios: El escáner debe realizar un escaneo exhaustivo de puertos en todos los puertos del Protocolo de Control de Transmisión (TCP) y puertos comunes del Protocolo de Datagramas de Usuario (UDP), lo que garantiza una cobertura completa de servicios como protocolos de autenticación, servidores de bases de datos y otros componentes de infraestructura crítica.
d. Huellas digitales del sistema operativo y del servicio: el escáner debe identificar con precisión los sistemas operativos y las versiones del servicio para ayudar a priorizar los esfuerzos de corrección de forma eficaz.
e. Independencia de la plataforma: El escaneo debe ser compatible con todas las plataformas de uso común, lo que garantiza una amplia aplicabilidad.
f. Precisión: El escáner debe informar de las vulnerabilidades confirmadas y potenciales con un alto nivel de certeza, garantizando que incluso los riesgos potenciales se tengan en cuenta en las determinaciones de cumplimiento.
g. Consideración del equilibrador de carga: En entornos que utilizan equilibradores de carga, el analizador debe tener en cuenta las posibles incoherencias de configuración y asegurarse de que todas las direcciones IP relevantes se analizan adecuadamente.
h. Requisitos específicos de los componentes: El escáner debe ser capaz de detectar vulnerabilidades en varios componentes, lo que garantiza una cobertura completa de todos los riesgos de seguridad potenciales. Los componentes clave incluyen:
    i. Firewalls y enrutadores: busque vulnerabilidades y problemas de configuración que puedan comprometer la seguridad de la red.
    ii. Sistemas operativos: Detecte vulnerabilidades conocidas y asegúrese de que los sistemas estén adecuadamente parcheados.
    iii. Servidores de bases de datos: Identifique cualquier acceso abierto desde Internet y detecte vulnerabilidades conocidas.
    iv. Servidores web: Pruebe si hay vulnerabilidades y problemas de configuración, incluida la exploración de directorios.
    v. Servidores de aplicaciones: Detectan la presencia de vulnerabilidades en los servidores de aplicaciones y sus configuraciones.
    vi. Scripts web comunes: identifique vulnerabilidades en scripts como CGI, ASP y PHP.
    vii. Cuentas integradas: Detecte cuentas y contraseñas predeterminadas, informando de cualquier vulnerabilidad de este tipo.
    viii. Servidores DNS: Detecte vulnerabilidades, incluidos problemas con las transferencias de zona DNS.
    ix. Servidores de correo: identifique las vulnerabilidades específicas de las configuraciones de los servidores de correo.
    x. Componentes de virtualización: detecte vulnerabilidades en hosts virtuales, máquinas e hipervisores.
    xi. Aplicaciones web: Detecte vulnerabilidades como la inyección de código SQL y el scripting entre sitios (XSS), especialmente en aplicaciones web personalizadas.
    xii. Otras aplicaciones: Escanee en busca de vulnerabilidades en varias aplicaciones, como transmisión de medios o servidores proxy.
    xiii. Servicios comunes: identifique vulnerabilidades en servicios como el uso compartido de archivos

y el correo electrónico.

xiv. Puntos de acceso inalámbricos (WAPs): Detecta vulnerabilidades y configuraciones incorrectas en redes inalámbricas.

xv. Puertas traseras/malware: identifique la presencia de software malicioso como rootkits y troyanos.

xvi. SL/TLS: Detecte protocolos y configuraciones criptográficas inseguros, garantizando el cumplimiento de estándares de criptografía sólidos.

xvii. Protocolos de acuerdo de clave anónimos: identifique y denuncie el uso de protocolos criptográficos inseguros que carecen de autenticación del servidor.

xviii. Acceso remoto: Detecte configuraciones de software de acceso remoto inseguras que podrían comprometer el entorno.

3.3. Tareas de escaneo

Los escaneos de vulnerabilidades internas deben realizarse desde una perspectiva de análisis con credenciales. Los escaneos de vulnerabilidades externas pueden realizarse desde una perspectiva de exploración sin credenciales.

3.4. Identificación de vulnerabilidades

Se debe establecer un proceso para identificar las vulnerabilidades de seguridad, utilizando fuentes externas acreditadas para obtener información sobre vulnerabilidades de seguridad, y utilizar un sistema de puntuación adecuado para la seguridad de los juegos (por ejemplo, CVSS, ISO/IEC 31010, etc.), para asignar un nivel de gravedad del riesgo (crítico, alto riesgo, riesgo medio o riesgo bajo) a las vulnerabilidades de seguridad recién descubiertas. El sistema de puntuación utilizado debe identificarse en los resultados del escaneo.

3.5. Resultados del escaneo

La Empresa de Juegos debe presentar la verificación de los escaneos de vulnerabilidad al organismo regulador e incluir un plan de remediación y cualquier plan de mitigación de riesgos para aquellas vulnerabilidades que no se puedan resolver. Si es requerido por el organismo regulador, los nuevos esaceneos deben realizarse hasta que cada vulnerabilidad crítica o de alto riesgo se resuelva y/o sea aceptada a través de un programa formal de aceptación de riesgos. Todas las vulnerabilidades verificadas deben ser corregidas por la Empresa de Juegos y documentadas en un informe proporcionado al organismo regulador.

3.6. Calificaciones de escaneo

Los escaneos de vulnerabilidad trimestrales deben ser realizados por una ISF, personal cualificado del organismo regulador actuando como una ISF, o a través de un empleado cualificado de la Empresa de Juegos actuando como una ISF, que esté separado, en términos organizacionales, de la función que implementa los cambios en el GPE.

Derechos de autor © 2025 Gaming Labs International, LLC

Todos los derechos reservados.

APÉNDICE: PRUEBAS DE SEGURIDAD TÉCNICA PARA JUEGOS (GTS)

A. Metodologías de pruebas de la GTS

Las pruebas de la GTS deben consistir en una evaluación de la seguridad del GPE por medio de una simulación de ataque por parte de una ISF siguiendo metodologías conocidas de evaluación de vulnerabilidades y pruebas de penetración según lo prescrito por el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM), el Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP), el Estándar de Ejecución de Pruebas de Penetración (PTES), la Guía Técnica del Instituto Nacional de Estándares y Tecnología (NIST) para Pruebas y Evaluación de Seguridad de la Información (SP800-115), y otras especificaciones según sea necesario. Estas metodologías garantizan que la información recopilada a lo largo de las pruebas de la GTS sea lo suficientemente detallada como para evaluar con precisión las áreas de exposición al riesgo y su posible impacto en el GPE.

NOTA: Se espera que las pruebas relacionadas con la seguridad de la red, el sistema y el servidor se realicen en el GPE en vivo. Para evitar cualquier interrupción de los servicios en vivo, las pruebas relacionadas con la seguridad de las aplicaciones se pueden realizar en un entorno que no sea de producción (por ejemplo, un entorno de desarrollo, un entorno de pruebas, etc.) que refleja de cerca la configuración del GPE para garantizar resultados precisos.

A.1. Pruebas de caja blanca

Las pruebas de caja blanca se llevan a cabo con pleno conocimiento de la arquitectura interna del GPE, incluido el acceso al código fuente, las configuraciones de red y la documentación detallada. Este enfoque permite un examen exhaustivo del funcionamiento interno del sistema, lo que permite la identificación de vulnerabilidades que pueden no ser evidentes a través de pruebas externas.

A.2. Pruebas de caja gris

Las pruebas de caja gris combinan elementos de las pruebas de caja blanca y las pruebas de caja negra. La ISF tiene un conocimiento parcial de la estructura interna del GPE, lo que a menudo refleja la perspectiva de un usuario con privilegios elevados pero no con acceso administrativo completo. Este enfoque simula un escenario en el que un atacante tiene algún conocimiento interno y tiene como objetivo probar los controles de GIS con una perspectiva semiprivilegiada.

A.3. Pruebas de caja negra

Las pruebas de caja negra se realizan sin ningún conocimiento previo de la arquitectura interna del GPE. La ISF se acerca al sistema como lo haría un atacante externo, intentando identificar y explotar vulnerabilidades sin ninguna información interna. Este tipo de pruebas son cruciales para simular escenarios de ataque del mundo real.

B. Evaluaciones de vulnerabilidades

La evaluación de vulnerabilidades es un proceso crítico para identificar vulnerabilidades utilizando bases de datos de vulnerabilidades actualizadas, que podrían explotarse posteriormente durante las pruebas de penetración mediante la realización de consultas básicas relacionadas con los servicios que se ejecutan en los sistemas desde los que es posible acceder a datos confidenciales. Dadas las limitadas ventanas de prueba, la ISF debe tener plena visibilidad y la capacidad de eludir cierta protección, incluidos todos los servicios de mejora de la seguridad del proveedor de servicios (por ejemplo, redes de entrega de contenido, inspección profunda de paquetes, protección contra denegación de servicio, firewalls de aplicaciones web, etc.) para permitir una evaluación más precisa y completa mediante la eliminación de obstáculos que de otro modo podrían enmascarar vulnerabilidades. Las evaluaciones de vulnerabilidades se pueden realizar mediante escáneres de vulnerabilidades automatizados.

B.1. Evaluación de vulnerabilidades de la capa interna de la red

El objetivo de la evaluación de vulnerabilidades de la capa interna de la red es identificar las debilidades de seguridad dentro de la infraestructura interna del GPE. Esta evaluación de vulnerabilidades tiene como objetivo descubrir vulnerabilidades que podrían ser explotadas por amenazas internas, cuentas comprometidas o

atacantes que han obtenido acceso a la red interna a través de violaciones externas o movimiento lateral.

a. Los objetivos de esta evaluación de vulnerabilidades son los sistemas internos, que incluyen:
   i. Servidores dentro de la DMZ o LAN.
   ii. Estaciones de trabajo y otros dispositivos de red conectados al GPE.
   iii. Aplicaciones y servicios que manejan datos confidenciales u operaciones críticas.
b. La ISF debe realizar una serie de actividades diseñadas para identificar y mapear la red interna, enumerar los sistemas y descubrir las debilidades de seguridad:
   i. Relevamiento de red: Un mapeo completo de la red interna para detectar hosts en vivo, arquitectura de red y dispositivos conectados. Esta fase ayuda a definir la superficie de ataque interna.
   ii. Escaneo de puertos: Identificación de puertos abiertos en sistemas internos, revelando servicios potencialmente expuestos que los atacantes pueden explotar.
   iii. Identificación del sistema (enumeración): detección de sistemas operativos, tipos de dispositivos y servicios que se ejecutan en la red. Esto incluye la identificación de todos los dispositivos y sistemas de infraestructura crítica en el entorno interno.
   iv. Enumeración de servicios: recopilación de información detallada sobre servicios y aplicaciones en ejecución para comprender sus versiones, configuraciones y vulnerabilidades asociadas.
   v. Análisis sin credenciales: estos escaneos de vulnerabilidades simulan un atacante sin acceso interno ni credenciales de autenticación válidas. Se utilizan para identificar puertos abiertos, servicios y vulnerabilidades básicas visibles para cualquier persona que obtenga acceso a la red.
   vi. Análisis con credenciales: Estos escaneos de vulnerabilidades utilizan credenciales de autenticación válidas para realizar una inspección más exhaustiva de los sistemas internos. Se utilizan para revelar información más detallada sobre los niveles de parches, las debilidades de la configuración, los controles de GIS faltantes y los permisos inadecuados, lo que proporciona un análisis más completo de los posibles vectores de ataque.
   vii. Validación de hallazgos y eliminación de falsos positivos: La ISF debe intentar validar los hallazgos de los escaneos de vulnerabilidades para garantizar que los problemas informados sean precisos. Esto incluye la verificación manual de los detalles de la vulnerabilidad para confirmar su legitimidad y la eliminación de falsos positivos de los resultados, lo que garantiza que solo se informen los riesgos reales y procesables.
c. Para garantizar una cobertura completa, la ISF debe evaluar diferentes capas de la red y la pila tecnológica, incluida la seguridad a nivel de host, a nivel de red y a nivel de aplicación:
   i. Escaneo de puertos y servicios: La ISF escaneará todos los sistemas y estaciones de trabajo para identificar los puertos abiertos y los servicios en ejecución que pueden proporcionar puntos de entrada para los atacantes.
   ii. Pruebas de VLAN de capa 2: La ISF debe evaluar la configuración de las VLAN, asegurándose de que estén correctamente segmentadas y protegidas. Esto incluye pruebas de subredes o dispositivos no deseados que comparten el mismo dominio de difusión.
   iii. Pruebas de red de capa 3: La ISF debe evaluar las VLAN que se conectan a zonas públicas o a la DMZ de Internet, asegurando que no haya una exposición inadecuada de los sistemas internos a amenazas externas.
   iv. Enumeración completa de vulnerabilidades: La ISF debe enumerar todas las computadoras internas y dispositivos de red para proporcionar un inventario detallado de las vulnerabilidades presentes en la red. Esto incluye tanto los sistemas activos como los componentes de infraestructura pasivos, como conmutadores, enrutadores y firewalls.
d. El uso del análisis con credenciales proporciona una visión más profunda de las configuraciones internas y la postura de seguridad. Para las exploraciones se puede utilizar un enfoque de muestreo del 20%-30% del inventario del GPE, centrándose en los sistemas de alto riesgo o en los que manejan datos sensibles. El análisis con credenciales evalúa configuraciones como:
   i. Permisos de usuario: Garantizar que los controles de acceso se apliquen correctamente y que no se otorguen privilegios excesivos a usuarios no administrativos.
   ii. Gestión de parches: Identificación de sistemas a los que les faltan parches o actualizaciones de seguridad críticos.
   iii. Debilidades de configuración: Revelar errores de configuración que pueden exponer datos confidenciales o permitir el acceso no autorizado.

B.2. Evaluación de vulnerabilidades de la capa externa de la red

El objetivo de la evaluación de vulnerabilidades de la capa externa de la red es identificar las debilidades de seguridad dentro de la infraestructura externa del GPE. Esta evaluación de vulnerabilidades de la capa externa de la red tiene como objetivo descubrir vulnerabilidades que podrían ser explotadas por amenazas externas, usuarios no autorizados o atacantes dirigidos a sistemas de acceso público.

a. Los objetivos de esta evaluación de vulnerabilidades de la capa externa de la red son los sistemas orientados hacia el exterior, que incluyen:
    i. Servidores y dispositivos accesibles a través de direcciones IP públicas.
    ii. Aplicaciones y servicios expuestos a internet que manejan o transmiten datos sensibles.
    iii. Firewalls y dispositivos de red orientados al público que protegen el entorno interno del GPE.
b. La ISF debe realizar una serie de actividades diseñadas para identificar y mapear la red externa, enumerar los sistemas expuestos y descubrir las debilidades de seguridad:
    i. Resondeo de red: Un mapeo completo de la red externa para detectar hosts en vivo, arquitectura de red y dispositivos conectados. Esta fase ayuda a definir la superficie de ataque externa.
    ii. Escaneo de puertos: Identificación de puertos abiertos en sistemas externos, revelando servicios potencialmente expuestos que los atacantes pueden explotar.
    iii. Identificación del sistema (enumeración): detección de sistemas operativos, tipos de dispositivos y servicios que se ejecutan en la red externa. Esto incluye la identificación de todos los dispositivos y sistemas de infraestructura crítica expuestos a Internet.
    iv. Enumeración de servicios: recopilación de información detallada sobre servicios y aplicaciones en ejecución para comprender sus versiones, configuraciones y vulnerabilidades asociadas;
    v. Análisis sin credenciales: estos escaneos de vulnerabilidades simulan un atacante sin acceso interno ni credenciales de auitenticación válidas. Se utilizan para identificar puertos abiertos, servicios y vulnerabilidades básicas visibles para cualquier persona que obtenga acceso a la red.
    vi. Validación de hallazgos y eliminación de falsos positivos: La ISF debe intentar validar los hallazgos de los escaneos de vulnerabilidades para garantizar que los problemas informados sean precisos. Esto incluye la verificación manual de los detalles de la vulnerabilidad para confirmar su legitimidad y la eliminación de falsos positivos de los resultados, lo que garantiza que solo se informen los riesgos reales y procesables.
c. Dadas las limitadas ventanas de prueba, la ISF debe tener plena visibilidad y la capacidad de eludir cierta protección, incluidos todos los servicios de mejora de la seguridad del proveedor de servicios (por ejemplo, redes de entrega de contenido, inspección profunda de paquetes, protección contra denegación de servicio, firewalls de aplicaciones web, etc.) para permitir una evaluación más precisa y completa mediante la eliminación de obstáculos que de otro modo podrían enmascarar vulnerabilidades. Esto garantiza que la postura de seguridad del GPE se evalúe con precisión y que no se pasen por alto vulnerabilidades críticas.

B.3. Evaluación de vulnerabilidades de la capa de aplicaciones

El objetivo de la evaluación de vulnerabilidades de la capa de aplicaciones es identificar las debilidades de seguridad en las aplicaciones web, móviles y de escritorio asociadas con el GPE. Esta evaluación de vulnerabilidades de la capa de aplicaciones utiliza principalmente métodos de escaneo automatizados, complementados con la validación manual para garantizar la precisión. Las posibles debilidades de seguridad pueden incluir fallas en la validación de entradas, autenticación, administración de sesiones y otras áreas comunes de preocupación.

a. Los objetivos de esta evaluación de vulnerabilidades de la capa de aplicaciones son las aplicaciones expuestas a usuarios externos (B2C) y los portales administrativos internos (B2B) como parte del GPE, que incluyen:
    i. Aplicaciones públicas a las que pueden acceder usuarios y usuarios externos.
    ii. Servicios web, API y otros componentes integrales de las operaciones del GPE.
    iii. Integraciones de empresa a empresa (B2B), como fuentes de datos para cuotas, datos de partidos y resultados; Estos servicios deben ser seguros para evitar el acceso no autorizado y las violaciones de datos.
    iv. Portales de gestión de back-office utilizados por socios, afiliados u operadores.
b. La ISF debe realizar una serie de actividades diseñadas para identificar y mapear la estructura, incluyendo todas las URL accesibles y puntos de entrada, y descubrir las debilidades de seguridad.

c. La ISF debe utilizar herramientas automatizadas estándar de la industria para escanear las aplicaciones en busca de vulnerabilidades. Estas herramientas están diseñadas para detectar una amplia gama de problemas de seguridad comunes, incluidas vulnerabilidades de inyección (p.ej. inyección de SQL, Cross-Site Scripting (XSS), inyección de comandos), fallas de autenticación y administración de sesiones, configuraciones incorrectas de seguridad y componentes y librerías de aplicaciones desactualizados:
d. Después del escaneo automatizado, la ISF debe validar manualmente los hallazgos para garantizar la precisión y eliminar los falsos positivos. Este paso confirma que solo se informan las vulnerabilidades genuinas, lo que proporciona una descripción general confiable de la posición de seguridad de la aplicación

C. Pruebas de penetración

Las pruebas de penetración son un proceso crítico para evaluar la seguridad del GPE mediante la simulación de la perspectiva de un atacante mediante la identificación y explotación de vulnerabilidades que podrían comprometer la confidencialidad, integridad y disponibilidad del GPE. Las pruebas de penetración permiten a la ISF validar las vulnerabilidades identificadas durante los escaneos de vulnerabilidades y evaluar la eficacia de los controles de GIS existentes en escenarios de ataque del mundo real.

C.1. Prueba de penetración de la capa interna de la red

El objetivo de la prueba de penetración de la capa interna de la red es explotar las vulnerabilidades identificadas dentro de la infraestructura interna del GPE. Esta prueba de penetración de la capa interna de la red simula un atacante que ya se ha afianzado en la red interna. El objetivo de esta prueba de penetración de la capa interna de la red es descubrir vulnerabilidades que podrían ser explotadas por amenazas internas, cuentas comprometidas o atacantes que han violado el perímetro externo.

a. Los objetivos de esta prueba de penetración de la capa interna de la red son los sistemas internos, que incluyen:
    i. Servidores dentro de la DMZ o LAN.
    ii. Estaciones de trabajo y otros dispositivos de red conectados al GPE.
    iii. Aplicaciones y servicios que manejan datos confidenciales u operaciones críticas.
b. Durante la prueba de penetración de la capa interna de la red, la ISF debe realizar las siguientes actividades clave:
    i. Reconocimiento y recopilación de información:
        1. Relevamiento de redes: mapeo de la red interna para identificar hosts en vivo, arquitectura de red y dispositivos conectados, definiendo la superficie de ataque interna.
        2. Identificación del sistema (enumeración): identificación de los sistemas operativos, los tipos de dispositivos y los servicios que se ejecutan en la red, centrándose en los componentes críticos de la infraestructura.
    ii. Escaneo de red interna:
        1. Escaneo de puertos: Identificación de puertos abiertos en sistemas internos para detectar posibles puntos de entrada.
        2. Enumeración de servicios: recopilación de información detallada sobre los servicios en ejecución para evaluar sus configuraciones y las vulnerabilidades asociadas.
    iii. Identificación de vulnerabilidades:
        1. Análisis de vulnerabilidades internas: Hacer coincidir los sistemas y servicios identificados con las vulnerabilidades conocidas para resaltar los parches faltantes, las configuraciones incorrectas y los fallos de software.
        2. Revisión de la configuración y el control de acceso: evaluación de los permisos de los usuarios, los controles de acceso y las configuraciones del sistema para identificar posibles brechas de seguridad.
    iv. Simulación de ataque:
        1. Intentos iniciales de explotación: Intentar explotar las vulnerabilidades identificadas para obtener acceso no autorizado dentro de la red interna.
        2. Escalada de privilegios y movimiento lateral: Pruebas de oportunidades para escalar privilegios y moverse lateralmente dentro de la red para acceder a sistemas y datos adicionales.
    v. Pruebas de segmentación y aislamiento:

1. Efectividad de VLAN: evaluación de qué tan bien las VLAN y la segmentación evitan infracciones y limitan el movimiento lateral.
2. Medidas de aislamiento: Evaluar las técnicas de aislamiento para garantizar que contengan eficazmente las amenazas y restrinjan el acceso no autorizado.

vi. Validación del control de acceso:

1. Restricción de movimiento lateral: Garantizar que los controles de acceso estén configurados para evitar movimientos laterales no autorizados dentro de la red.
2. Protección de sistemas críticos: Verificación de que los controles de acceso bloquean eficazmente el acceso no autorizado a los sistemas clave

C.2. Prueba de penetración de la capa externa de la red

El objetivo de la prueba de penetración de la capa externa de la red es explotar las vulnerabilidades identificadas dentro de la infraestructura externa del GPE. Esta prueba de penetración de la capa externa de la red simula un ataque por parte de un actor de amenazas externo que intenta infringir el GPE a través de sus sistemas externos. El objetivo de esta prueba de penetración de la capa externa de la red es descubrir vulnerabilidades que podrían ser explotadas por atacantes externos para obtener acceso no autorizado, interrumpir operaciones o exfiltrar datos confidenciales.

a. Los objetivos de esta prueba de penetración de la capa externa de la red son los sistemas orientados hacia el exterior, que incluyen:
   i. Servidores y dispositivos accesibles a través de direcciones IP públicas.
   ii. Aplicaciones y servicios expuestos a internet que manejan o transmiten datos sensibles.
   iii. Firewalls y dispositivos de red orientados al público que protegen el entorno interno del GPE.

b. Durante la prueba de penetración de la capa externa de la red, la ISF debe realizar las siguientes actividades clave:
   i. Reconocimiento y recopilación de información:
      1. Descubrimiento basado en dominios: Identificación de información disponible públicamente relacionada con el GPE, incluidos nombres de dominio, direcciones IP y servicios asociados.
      2. Perfiles de red: mapeo de la superficie de ataque externa, incluida la identificación de la topología de red, los servicios activos y los posibles puntos de entrada.
   ii. Escaneo de redes externas:
      1. Escaneo de puertos: Identificación de puertos abiertos en sistemas externos para detectar posibles puntos de entrada.
      2. Enumeración de servicios: recopilación de información detallada sobre los servicios expuestos, como versiones y configuraciones de software, para evaluar posibles vulnerabilidades.
   iii. Identificación de vulnerabilidades:
      1. Análisis de vulnerabilidades: comparación de los sistemas y servicios descubiertos con las bases de datos de vulnerabilidades actualizadas para identificar debilidades explotables.
      2. Revisión de configuraciones y parches: evaluación de las configuraciones del sistema en busca de debilidades de seguridad, como software obsoleto, configuraciones débiles o servicios expuestos.
   iv. Simulación de ataque:
      1. Intentos iniciales de explotación: Intentar explotar las vulnerabilidades identificadas para obtener acceso no autorizado a sistemas externos.
      2. Escalada de privilegios: si se obtiene acceso inicial, intentar escalar privilegios para obtener niveles más altos de acceso.
      3. Pruebas de movimiento lateral: Pruebas de oportunidades de movimiento lateral que podrían permitir a un atacante adentrarse más en la red desde el sistema externo comprometido.
   v. Pruebas de derivación:
      1. Evaluación de la defensa perimetral: Probar la eficacia de las defensas perimetrales, incluidos los firewalls de aplicaciones web (WAF), intentando eludirlos.

Derechos de autor © 2025 Gaming Labs International, LLC

Todos los derechos reservados.

2. Ataques sofisticados simulados: Simulación de técnicas de ataque avanzadas para evaluar qué tan bien se mantienen las medidas de seguridad frente a amenazas sofisticadas.

C.3. Prueba de penetración de la capa de aplicación

El objetivo de la prueba de penetración de la capa de aplicación es explotar las vulnerabilidades identificadas en todos los tipos de aplicaciones asociadas con el GPE, incluidas las aplicaciones web, las aplicaciones móviles y las aplicaciones de escritorio. Esta prueba de penetración de la capa de aplicación simula escenarios de ataque del mundo real para evaluar la resistencia de la aplicación contra el acceso no autorizado, las filtraciones de datos y otras actividades maliciosas. La prueba de penetración de la capa de aplicación implica un enfoque estructurado, que incluye el escaneo automatizado como paso preliminar, seguido de pruebas manuales en profundidad de las áreas de seguridad principales para explorar y validar las vulnerabilidades de seguridad. Las pruebas de penetración de la capa de aplicación seguirán las Guías de Pruebas de Seguridad de OWASP aplicables y evaluarán las aplicaciones para el OWASP Top 10.

a. Los objetivos de esta prueba de penetración de la capa de aplicación son las aplicaciones expuestas a usuarios externos (B2C) y los portales administrativos internos (B2B) como parte del GPE, que incluyen:
   i. Aplicaciones públicas a las que pueden acceder usuarios y usuarios externos.
   ii. Servicios web, API y otros componentes integrales de las operaciones del GPE.
   iii. Integraciones de empresa a empresa (B2B), como fuentes de datos para cuotas, datos de partidos y resultados; Estos servicios deben ser seguros para evitar el acceso no autorizado y las violaciones de datos.
   iv. Portales de gestión de back-office utilizados por socios, afiliados u operadores.
b. Durante la prueba de penetración de la capa de aplicación, la ISF debe realizar las siguientes actividades clave:
   i. Reconocimiento y recopilación de información:
      1. Generación de perfiles de aplicaciones: recopile información detallada sobre la arquitectura de la aplicación, incluidos los lenguajes de programación, los marcos, las tecnologías de bases de datos, los protocolos de comunicación de back-end, las librerías de terceros y los controles de GIS.
      2. Ingeniería inversa: descompile la aplicación para examinar el código fuente, las API y los componentes de terceros en busca de secretos codificados, exposición de datos confidenciales o configuraciones inseguras.
   ii. Pruebas de autenticación:
      1. Aplicación de la política de credenciales: revise la política de credenciales de la aplicación y asegúrese de que aplica los requisitos de complejidad (longitud, caracteres y rotación periódica).
      2. Seguridad del almacenamiento de credenciales: evalúe la seguridad de los mecanismos de almacenamiento de credenciales, asegurándose de que se cifran y salen correctamente.
      3. Evaluación de la autenticación multifactor (MFA): evalúe la seguridad, la eficacia y la implementación adecuada de la MFA y pruebe las posibles técnicas de omisión.
      4. Resistencia a los ataques de fuerza bruta: pruebe la resistencia contra los ataques de fuerza bruta, incluido el bloqueo de cuentas y las implementaciones de CAPTCHA.
      5. Autenticación basada en tokens: pruebe la seguridad de los tokens de autenticación (JWT, tokens OAuth) utilizados por la aplicación para interactuar con los servicios de backend.
   iii. Validación de autorización:
      1. Pruebas de control de acceso basado en roles (RBAC): pruebe la aplicación de roles en toda la aplicación, asegurándose de que los usuarios con diferentes niveles de permisos solo puedan acceder a las áreas, funciones y datos autorizados apropiados para sus roles.
      2. Pruebas de escalada de privilegios: pruebe las vulnerabilidades de escalada de privilegios, incluida la escalada horizontal y vertical mediante la explotación de los puntos finales de la API, la funcionalidad de la aplicación o las configuraciones de backend inseguras.
      3. Pruebas de omisión de autorización: intente eludir los controles de autorización mediante

la manipulación de URL, la manipulación de parámetros o referencias directas a objetos. Intente acceder a áreas no autorizadas utilizando diferentes niveles de privilegios.

iv. Pruebas de gestión de sesiones:
   1. Revisión de manejo de sesiones: recopile y analice las cookies de sesión, los encabezados y los tokens del lado del servidor para detectar posibles usos indebidos o configuraciones incorrectas.
   2. Verificación de la seguridad del token de sesión: verifique la seguridad del token de sesión, incluida la aleatoriedad, la unicidad y la protección contra la exposición a través de parámetros de URL o cookies inseguras. Asegúrese de que los tokens caduquen correctamente, no se reutilicen y se manejen correctamente al cerrar la sesión.
   3. Evaluación de la caducidad de la sesión y del tiempo de espera: evalúe la caducidad de la sesión y los mecanismos de tiempo de espera para garantizar que las sesiones se finalicen correctamente después de la inactividad o el cierre de sesión.
   4. Pruebas de vulnerabilidades de secuestro de sesión: pruebe las vulnerabilidades de secuestro de sesión, como la captura de cookies de sesión o la explotación de vulnerabilidades de fijación de sesión.
   5. Implementación de atributos de cookies seguras: asegúrese de que los atributos de cookies seguras estén en su lugar, como las marcas HttpOnly y Secure.

v. Validación de entrada y ataques de inyección:
   1. Revisión de validación de entrada: asegúrese de que los campos de entrada del usuario (como nombre de usuario, contraseña, campos de búsqueda, etc.) estén debidamente validados para evitar vulnerabilidades comunes de las aplicaciones.
   2. Ataques de inyección: Pruebe la aplicación en busca de vulnerabilidades que podrían permitir a un atacante inyectar código malicioso, SQL, comandos, scripts e inyección LDAP (por ejemplo, JavaScript o cargas útiles maliciosas), dentro de la aplicación y sus interacciones con los servicios de backend.
   3. Evaluación de la gestión de la carga de archivos: evalúe la gestión de la carga de archivos para asegurarse de que solo se aceptan y procesan de forma segura los tipos de archivos permitidos, y de que se validan el tamaño y el contenido de los archivos. Asegúrese de que las cargas de archivos restrinjan los tipos de archivo y validen las entradas, evitando la ejecución remota de código.
   4. Pruebas de validación del lado del cliente: omita los mecanismos de validación del lado del cliente y evalúe si se está aplicando la validación adecuada del lado del servidor.

vi. Manejo de errores y divulgación de información:
   1. Evaluación de la sensibilidad de los mensajes de error: Evalúe si los mensajes de error revelan datos confidenciales sobre el funcionamiento interno de la aplicación que podrían ayudar a un atacante a planificar nuevos ataques (por ejemplo, seguimientos de pila, errores SQL).
   2. Identificación de fugas de información: identifique los casos en los que los datos confidenciales se exponen inadvertidamente a través de encabezados del Protocolo de Transporte Hypertext (HTTP), mensajes de error u otros canales de comunicación.
   3. Pruebas de control de errores inesperados: pruebe cómo la aplicación maneja los errores inesperados y si los datos confidenciales o los detalles del sistema se exponen durante estos errores.

vii. Integración y seguridad de API:
   1. Evaluación de API: evalúe la seguridad de los servicios web y las API utilizados en el GPE, asegurándose de que autentiquen correctamente a los usuarios, validen las entradas y eviten el acceso no autorizado.
   2. Pruebas de autenticación basadas en tokens: Pruebe la seguridad de los tokens OAuth u otros mecanismos de autenticación de API, garantizando los procesos adecuados de manejo y revocación.
   3. Evaluación de limitación de velocidad: evalúe la implementación de mecanismos de limitación de velocidad para evitar abusos y ataques de denegación de servicio de distribución (DoS).

viii. Configuración y endurecimiento seguros:
   1. Evaluación de comunicaciones seguras: Verifique el uso de HTTPS con estándares de cifrado modernos (TLS 1.2 o superior) en todos los canales de comunicación entre el cliente y el servidor.

2. Pruebas de seguridad de datos en tránsito: pruebe si los datos transmitidos entre la aplicación y los servicios de backend están cifrados mediante un cifrado fuerte (TLS 1.2+).
3. Ataques Man-in-the-Middle (MITM): pruebe la vulnerabilidad de la aplicación a los ataques MITM, asegurándose de que el tráfico no pueda ser interceptado o modificado por un atacante. Asegúrese de que los certificados estén validados.
4. Revisión de exposición mínima del servicio: confirme que no se estén ejecutando servicios innecesarios ni puertos abiertos en el servidor que puedan aumentar la superficie de ataque.
5. Evaluación de anclaje de certificados: compruebe que la aplicación implementa el anclaje de certificados para evitar el uso de certificados falsificados durante la comunicación con el servidor back-end.

ix. Pruebas de almacenamiento de datos local:
1. Pruebas de almacenamiento de datos inseguro: pruebe los datos confidenciales almacenados de forma insegura en el dispositivo, incluidas las credenciales de autenticación codificadas, PII, los tokens y las cookies de sesión almacenadas en texto sin formato o en formatos cifrados débilmente.
2. Verificación de permisos de archivos y directorios: Verifique que los permisos de archivos estén configurados correctamente, asegurándose de que solo los usuarios autorizados puedan acceder a los archivos críticos.

x. Gestión de parches y pruebas de actualización:
1. Mecanismo de actualización segura: asegúrese de que las actualizaciones se entreguen de forma segura y verifique la integridad de los paquetes de actualización.
2. Aplicación de parches: Pruebe si los parches críticos se aplican rápidamente a la aplicación y sus dependencias.

xi. Pruebas de lógica de aplicaciones y flujo de trabajo:
1. Pruebas de fallas en el procesamiento de transacciones: Pruebe si hay fallas en el procesamiento de transacciones, como pagos insuficientes, pagos excesivos o manipulación de montos de transacciones.
2. Evaluación de la manipulación del flujo de trabajo: Evalúe si los flujos de trabajo se pueden omitir o manipular, lo que permite a los usuarios realizar acciones no autorizadas u omitir pasos críticos.
3. Pruebas de abuso de funcionalidad: pruebe escenarios de abuso de funcionalidad en los que las funciones legítimas se pueden utilizar indebidamente para acciones no deseadas, como la reutilización de códigos promocionales o la explotación de mecanismos de reembolso.
4. Validación de la precisión de las apuestas y los pagos: Valida que la aplicación procesa las apuestas de forma precisa y segura y refleja los saldos de los usuarios, las ganancias y el historial de transacciones.
5. Seguridad de la API de apuestas de eventos: asegúrese de que las API que entregan datos de partidos, resultados o cuotas sean seguras y no puedan ser manipuladas.
6. Pruebas de seguridad de saldos de usuarios: Pruebe la precisión y seguridad de los saldos de los usuarios, asegurándose de que los depósitos, retiros, apuestas y ganancias se reflejen correctamente.
7. Validación de bonos y ofertas promocionales: Valide la implementación de ofertas promocionales y de bonos, asegurándose de que no puedan ser abusados, pasados por alto o manipulados a través de fallas lógicas.
8. Prevención de repeticiones de transacciones: asegúrese de que las repeticiones o reintentos de transacciones (como volver a realizar una apuesta) no puedan dar lugar a transacciones duplicadas o ganancias no autorizadas.
9. Evaluación de detección de cuentas múltiples: evalúe la capacidad de la aplicación para detectar y prevenir el uso de varias cuentas para manipular probabilidades, explotar bonificaciones o participar en colusión.

xii. Componentes y librerías de terceros:
1. Seguridad de librerías de terceros: revise y evalúe la integridad y la seguridad de las librerías y dependencias de terceros utilizadas por la aplicación utilizada por la aplicación, asegurándose de que estén actualizadas y libres de vulnerabilidades conocidas.
2. Uso inseguro de API: pruebe el uso inadecuado de API, como implementaciones

inseguras de autenticación biométrica, cámara, micrófono y otras funciones del dispositivo.

3. Gestión de dependencias: Analice las librerías de terceros utilizadas dentro de la aplicación, comprobando si hay componentes obsoletos o vulnerables que puedan comprometer la seguridad de la aplicación.

c. Para probar aplicaciones que se ejecutan desde un servidor (aplicaciones web), la ISF debe realizar las siguientes actividades de prueba adicionales:

i. Recopilación de información pública:

1. Recopilación pasiva de información: recopile información sobre la aplicación mediante métodos no intrusivos, como Google dorking, para descubrir datos de acceso público.
2. Perfiles tecnológicos: Realice búsquedas de WHOIS, enumeración de DNS y huellas digitales de tecnología para recopilar detalles sobre la infraestructura y los servicios de la aplicación.

ii. Manejo entre sitios:

1. Pruebas de secuencias de comandos entre sitios (XSS): pruebe los campos de entrada y los parámetros de URL para XSS y otros ataques relacionados con la entrada, asegurándose de que las entradas estén correctamente desinfectadas y codificadas. Verifique que los datos presentados a los usuarios estén correctamente desinfectados y codificados para mitigar XSS y otros ataques relacionados con la salida.
2. Evaluación de falsificación de solicitudes entre sitios (CSRF): evalúe la resistencia de la aplicación frente a ataques CSRF, garantizando el uso adecuado de tokens anti-CSRF para protegerse contra solicitudes no autorizadas.

iii. Uso del encabezado de seguridad:

1. Implementación de encabezados de seguridad: Garantice la implementación correcta de encabezados de seguridad esenciales como la Política de seguridad de contenido (CSP) y la seguridad estricta de transporte (HSTS) para protegerse contra vulnerabilidades web comunes.
2. Configuración del encabezado de seguridad: compruebe que los encabezados de seguridad adicionales, como X-Content-Type-Options, estén configurados correctamente para evitar el rastreo de tipos MIME y otros ataques.

d. Para probar las aplicaciones que se instalan en el dispositivo de un usuario (aplicaciones móviles y aplicaciones de escritorio), la ISF debe realizar las siguientes actividades de prueba adicionales:

i. Resistencia a la manipulación:

1. Seguridad binaria: Examine los binarios de la aplicación en busca de debilidades, asegurándose de que los datos confidenciales no se almacenen en formatos inseguros ni se incrusten en la aplicación.
2. Técnicas de ofuscación: Verifique que el código de la aplicación esté ofuscado para evitar la ingeniería inversa y la manipulación del código por parte de actores malintencionados.
3. Mecanismos antimanipulación: Pruebe la presencia de mecanismos antimanipulación que impidan o detecten cambios no autorizados en los archivos binarios o de configuración de la aplicación.
4. Autoprotección de la aplicación: compruebe si la aplicación puede detectar la manipulación o la presencia de depuradores y evitar que actores maliciosos modifiquen la aplicación en tiempo real.
5. Protección contra reversión: asegúrese de que la aplicación evite que los atacantes reviertan a una versión vulnerable.

ii. Seguridad de los datos sensibles y las comunicaciones:

1. Almacenamiento en caché de datos y archivos temporales: asegúrese de que los datos confidenciales no se almacenen en caché de forma insegura ni se dejen en archivos temporales después de cerrar la aplicación.
2. Uso del portapapeles: Verifique que los datos confidenciales no se almacenen involuntariamente ni se pueda acceder a ellos a través del portapapeles (por ejemplo, copiar contraseñas o información de tarjetas de crédito).
3. Ataques de comunicación entre procesos (IPC): Compruebe si hay vulnerabilidades en la forma en que la aplicación se comunica con otros procesos, asegurándose de que no se puedan inyectar datos no autorizados.

iii. Salvaguardas de memoria:
   1. Vulnerabilidades de desbordamiento de búfer: pruebe las vulnerabilidades de desbordamiento de búfer que podrían conducir a la ejecución remota de código.
   2. Daños en la memoria: asegúrese de que las protecciones de memoria, como la prevención de ejecución de datos (DEP) y la aleatorización del diseño del espacio de direcciones (ASLR), estén en su lugar.

iv. Protecciones de virtualización y depuración:
   1. Detección de máquinas virtuales: asegúrese de que la aplicación pueda detectar y evitar que se ejecute en un entorno virtualizado, lo que podría usarse para manipular o aplicar ingeniería inversa al software.
   2. Antidepuración: pruebe la presencia de técnicas antidepuración que impidan el uso de herramientas de depuración para aplicar ingeniería inversa a la aplicación.

v. Tareas adicionales de prueba de aplicaciones móviles:
   1. Análisis de metadatos de la App Store: Identifique la plataforma de la aplicación (iOS/Android) y revise la ficha de la tienda de aplicaciones, el historial de versiones, la información del desarrollador y los permisos solicitados por la aplicación durante la instalación.
   2. Seguridad del llavero/almacén de claves: pruebe si los datos confidenciales se almacenan de forma segura mediante el almacén de claves de Android o el llavero de iOS, asegurándose de que se GISan los estándares criptográficos adecuados.
   3. Jailbreaking/Root Detection: Verifique que la aplicación pueda detectar y responder a la ejecución en un entorno con jailbreak (iOS) o rooteado (Android), limitando el acceso a funciones críticas.

D. Evaluaciones de seguridad de la nube y los contenedores

La evaluación de seguridad de la nube y los contenedores garantiza la implementación, la gestión y el funcionamiento seguros de los entornos en la nube y en contenedores dentro del entorno de producción de juegos (GPE). Esta evaluación de seguridad de la nube y los contenedores se centra en la seguridad de los componentes basados en la nube, las aplicaciones en contenedores y los marcos de orquestación de soporte para minimizar los riesgos y mejorar la resiliencia de la seguridad.

D.1. Evaluación de seguridad de la nube

El objetivo de la evaluación de seguridad de la nube es garantizar la gestión segura de los componentes basados en la nube dentro del GPE, garantizando que los controles GIS y configuraciones de seguridad específicos de la nube se implementen y gestionen correctamente. Durante la evaluación de seguridad de la nube, la ISF debe realizar las siguientes actividades clave:

a. Controles de acceso: verifique que las políticas de acceso apliquen el principio de privilegios mínimos y que se implementen métodos de autenticación sólidos, como la autenticación multifactor, para las cuentas críticas.
b. Gestión de cuentas: evalúe los procesos de creación, gestión y desactivación de cuentas. Asegúrese de que los roles y permisos estén definidos correctamente y de que las cuentas inactivas o innecesarias se eliminen de inmediato.
c. Registro y supervisión: confirme que todas las acciones críticas, como el acceso a datos confidenciales y los cambios de configuración, se registran y almacenan de forma segura. Asegúrese de que existan mecanismos de supervisión y alerta para detectar y responder a posibles incidentes de seguridad.
d. Configuración de seguridad: Revise las configuraciones de red y recursos para garantizar la segmentación, el aislamiento y el control del tráfico adecuados. Verifique que los datos confidenciales estén cifrados y que las claves de cifrado se administren de forma segura.
e. Revisión de reglas y políticas de firewall: asegúrese de que los firewalls específicos de la nube (por ejemplo, grupos de seguridad, políticas de firewall nativas de la nube) estén configurados correctamente para restringir el acceso en función del privilegio mínimo.
f. Aislamiento de servicios y aplicaciones: revise la segmentación de los servicios y aplicaciones en la nube, asegurándose de que estén correctamente aislados entre sí para minimizar el riesgo de movimiento lateral por parte de los atacantes.

Derechos de autor © 2025 Gaming Labs International, LLC

Todos los derechos reservados.

D.2. Evaluación de la seguridad de los contenedores

El objetivo de la evaluación de seguridad de contenedores es evaluar la postura de seguridad de los GPE que utilizan tecnología basada en contenedores (por ejemplo, Kubernetes) mediante la identificación de vulnerabilidades, configuraciones incorrectas y amenazas potenciales para garantizar la integridad, confidencialidad y disponibilidad de las aplicaciones y los datos. Durante la evaluación de seguridad de contenedores, la ISF debe realizar las siguientes actividades clave

a. Configuración del contenedor:
   i. Gestión segura de imágenes: asegúrese de que las imágenes de los contenedores procedan de fuentes fiables, se analizen periódicamente en busca de vulnerabilidades y se minimicen para reducir las superficies de ataque.
   ii. Endurecimiento de la configuración: Verifique que los contenedores estén configurados de acuerdo con las mejores prácticas, con los servicios innecesarios deshabilitados y los límites de recursos aplicados.
b. Seguridad de orquestación:
   i. Seguridad del clúster: evalúe la seguridad de la plataforma de orquestación, incluidas las configuraciones del plano de control, la seguridad de los nodos y el aislamiento de la carga de trabajo.
   ii. Control de acceso: revise la configuración de RBAC para garantizar las asignaciones de permisos adecuadas y el acceso administrativo restringido.
   iii. Políticas de red: evalúe la segmentación de la red y el control del tráfico dentro del entorno de contenedores para garantizar una comunicación segura y restringida.
c. Seguridad en tiempo de ejecución:
   i. Supervisión y detección de amenazas: implemente y revise la supervisión del comportamiento del tiempo de ejecución de los contenedores para detectar anomalías y responder a las amenazas.
   ii. Administración de parches: asegúrese de que las imágenes de los contenedores se actualicen con los parches de seguridad más recientes y de que no se implementen imágenes obsoletas.
d. Seguridad de la cadena de suministro:
   i. Gestión de dependencias: supervise y gestione bibliotecas y dependencias de terceros para reducir el riesgo de ataques a la cadena de suministro.
   ii. Seguridad de la canalización: proteja la canalización de CI/CD para garantizar que solo se implemente el código verificado y seguro.

E. Evaluaciones y pruebas adicionales

E.1. Evaluación de la seguridad del cortafuegos

El objetivo de la evaluación de seguridad del cortafuegos (firewall) es identificar las posibles debilidades en las configuraciones, los conjuntos de reglas y las prácticas de administración del firewall. Esta evaluación de seguridad del cortafuegos garantiza que el firewall esté configurado y administrado adecuadamente para prevenir eficazmente el acceso no autorizado y mitigar las amenazas de seguridad, en línea con las políticas de GIS de la Empresa de Juego y las mejores prácticas de la industria. Durante la evaluación de seguridad del cortafuegos, la ISF debe realizar las siguientes actividades clave:

a. Análisis de la arquitectura de red:
   i. Comprensión del entorno: Comprender a fondo la arquitectura de red del GPE, incluidos los activos que el firewall debe proteger y las amenazas potenciales a esos activos.
   ii. Identificación de fallas de diseño: Evaluación de la ubicación del firewall dentro de la red para identificar cualquier falla o vulnerabilidad de diseño en su implementación actual en comparación con las mejores prácticas de la industria.
b. Revisión del conjunto de reglas:
   i. Reglas de privilegios mínimos: asegúrese de que las reglas estén configuradas de acuerdo con el principio de privilegios mínimos.
   ii. Restricción de conexión: confirme que las conexiones entrantes y salientes están restringidas solo a los servicios necesarios.

iii. Traducción de direcciones de red (NAT): Verifique que NAT esté implementada correctamente.
iv. Bloqueo de protocolos: asegúrese de que todos los protocolos desconocidos o indefinidos estén bloqueados.
v. Presencia de regla de limpieza: confirme la presencia de una regla de "limpieza" para manejar el tráfico no especificado.
vi. Revisión de la documentación de las reglas: Revise y confirme que las reglas estén debidamente documentadas y que las reglas temporales estén deshabilitadas o eliminadas cuando ya no sean necesarias.

c. Revisión de los ajustes de configuración:
i. Configuración de acceso no autorizado: identifique cualquier ajuste de configuración que pueda permitir el acceso no autorizado o comprometer la seguridad de los sistemas protegidos por el firewall.
ii. Cumplimiento de la política de firewall: verifique que la configuración del firewall se alinee con las políticas de GIS de la Empresa de Juego y las mejores prácticas de la industria.

d. Revisión de la consola de administración central:
i. Control de acceso: asegúrese de que solo el personal autorizado pueda acceder a la consola de administración del firewall y de que los controles de acceso se apliquen correctamente.
ii. Protección de la consola: Confirme que la consola de administración está adecuadamente protegida contra el acceso no autorizado, incluido el uso de protocolos cifrados para la administración remota.

e. Registro, auditoría y supervisión:
i. Configuración de registro: asegúrese de que el registro esté habilitado para eventos de seguridad (por ejemplo, inicios de sesión fallidos) y que los registros de auditoría estén configurados para capturar datos relevantes.
ii. Administración de registros: confirme que los registros de auditoría se escriben en una ubicación central, se realiza una copia de seguridad periódica y se revisan periódicamente para detectar actividades sospechosas.
iii. Supervisión y alertas: Verifique que se hayan implementado mecanismos de alerta para proporcionar visibilidad en tiempo real de posibles incidentes de seguridad.

f. Gestión de parches:
i. Implementación de parches: Confirme que existe un sistema para probar parches antes de implementarlos en firewalls de producción, y que todos los parches relacionados con la seguridad se aplican con prontitud.
ii. Revisión de parches: Evalúe si el firmware y el software del firewall están actualizados y en línea con las mejores prácticas de seguridad.

g. Seguridad de acceso remoto:
i. Seguridad del protocolo: asegúrese de que los protocolos innecesarios para acceder al firewall estén deshabilitados y que el acceso remoto solo se permita a través de protocolos seguros y cifrados.
ii. Restricciones de acceso: Verifique que el acceso remoto al firewall esté restringido a redes de confianza y direcciones IP específicas.
iii. Filtrado de tráfico: confirme que el filtrado de tráfico está configurado correctamente para controlar el flujo de datos entre los entornos en la nube y entre las infraestructuras en la nube y en las instalaciones.

h. Seguridad de la red virtual:
i. Segmentación de red: evalúe la segmentación dentro de las redes virtuales, asegurándose de que los datos confidenciales y los servicios críticos estén aislados de áreas menos seguras.
ii. Gestión del tráfico entre entornos: Garantice la gestión segura del tráfico entre diferentes entornos en la nube, así como entre los sistemas en la nube y en las instalaciones, centrándose en el cifrado y la protección de la integridad de los datos.

i. Integración de la gestión de identidades y accesos (IAM):
i. Políticas de control de acceso: asegúrese de que las políticas de IAM estén integradas con los firewalls en la nube para aplicar un control de acceso estricto y un acceso basado en roles.
ii. Autenticación multifactor (MFA): verifique que se aplique MFA para acceder a las configuraciones de firewall en la nube y las consolas de administración.

j. Automatización y orquestación:

i. Automatización de la configuración: evalúe el uso de herramientas de automatización para administrar y aplicar las reglas y configuraciones de firewall en entornos de nube, lo que garantiza la coherencia y reduce los errores humanos.
ii. Cumplimiento de políticas: confirme que se han implementado comprobaciones de cumplimiento automatizadas para garantizar que las configuraciones de firewall permanezcan alineadas con las políticas de GIS y las mejores prácticas.

E.2. Evaluación de seguridad de las bases de datos

El objetivo de la evaluación de la seguridad de las bases de datos es garantizar que las bases de datos, que almacenan datos confidenciales como PII, datos de transacciones financieras y datos relacionados con los juegos, estén seguras contra el acceso no autorizado y cumplan con las mejores prácticas y los estándares regulatorios aplicables. La evaluación de seguridad de las bases de datos incluye la revisión de los mecanismos de cifrado y la seguridad general del entorno de la base de datos, incluidas las protecciones de datos en reposo y datos en tránsito. La evaluación de seguridad de las bases de datos sigue las directrices de OWASP para el almacenamiento criptográfico y otros estándares de la industria, lo que garantiza la seguridad y confidencialidad de los datos confidenciales del GPE. Durante la Evaluación de Seguridad de las Bases de Datos, la ISF debe realizar las siguientes actividades clave:

a. Revisión de la documentación: La documentación del proceso se solicita a la Empresa de Juego y se analiza para verificar su integridad y alineación con las mejores prácticas.
   i. Revisión de la configuración:
      1. Línea base de configuración segura: verifique la configuración general del entorno de base de datos para asegurarse de que los servicios, los puertos y las cuentas de usuario estén configurados de forma segura. Busque cualquier servicio innecesario que pueda aumentar la superficie de ataque.
      2. Procedimientos de copia de seguridad y recuperación: Revise cómo se administran las copias de seguridad y asegúrese de que estén cifradas y almacenadas de forma segura. Los procedimientos de copia de seguridad y recuperación deben incluir el cifrado durante el tránsito y el almacenamiento.
      3. Configuración de auditoría y registro: verifique que la auditoría esté habilitada para acciones críticas como el acceso a datos confidenciales, cambios de configuración e intentos de escalada de privilegios. Asegúrese de que los registros de auditoría se almacenen de forma segura y se revisen periódicamente.
      4. Métodos de cifrado de datos: Evalúe si el cifrado de datos en reposo y datos en tránsito se aplica correctamente, utilizando algoritmos de cifrado estándar de la industria (por ejemplo, AES-256).
   ii. Control de acceso y autenticación:
      1. Control de acceso basado en roles (RBAC): revise las políticas de control de acceso para asegurarse de que solo los usuarios autorizados tengan acceso a las bases de datos confidenciales. Confirme que los roles de usuario se asignan en función del principio de privilegios mínimos.
      2. Autenticación multifactor (MFA): asegúrese de que las cuentas de bases de datos críticas, como los administradores, estén protegidas con la autenticación multifactor.
      3. Administración de cuentas de usuario: evalúe los procesos para crear, administrar y desactivar cuentas de usuario de la base de datos, asegurándose de que las cuentas inactivas o innecesarias se eliminen o deshabiliten.
   iii. Análisis y aplicación de parches de vulnerabilidades:
      1. Análisis regulares de vulnerabilidades: Asegúrese de que los escaneos de vulnerabilidades se realicen con regularidad para detectar y abordar las vulnerabilidades del software de la base de datos, los parches obsoletos y los errores de configuración.
      2. Administración de parches: Verifique que los parches críticos se apliquen con prontitud y que las versiones obsoletas de la base de datos se retiren o se protejan correctamente.
      3. Endurecimiento de la base de datos: Revise las medidas de refuerzo de seguridad adoptadas para evitar vulnerabilidades comunes de la base de datos, como ataques de inyección SQL y configuraciones incorrectas.
   iv. Protección de datos y controles de privacidad:
      1. Enmascaramiento de datos y tokenización: asegúrese de que el enmascaramiento de

datos se aplique a entornos que no sean de producción, especialmente para bases de datos que contengan datos confidenciales.

2. Supervisión de la actividad de la base de datos (DAM): asegúrese de que las herramientas de supervisión de la actividad de la base de datos estén en su lugar para detectar comportamientos anómalos o intentos de acceso no autorizados.
3. Gestión de claves de cifrado:
4. Almacenamiento de claves y controles de acceso: asegúrese de que las claves de cifrado se almacenen y protejan de forma segura mediante un módulo de plataforma segura (TPM) o un módulo de seguridad de hardware (HSM), y que el acceso esté estrictamente controlado y registrado.
5. Rotación y caducidad de claves: revise las políticas y los procedimientos para la rotación, caducidad y revocación de claves, asegurándose de que los ciclos de vida de las claves se gestionen de forma segura.

v. Seguridad y aislamiento de la red:

1. Segmentación de bases de datos: asegúrese de que las bases de datos estén correctamente segmentadas desde segmentos de red menos seguros. El acceso debe restringirse en función de la lista blanca de IP y la zonificación de la red.
2. Configuración del cortafuegos: Confirme que los cortafuegos están instalados para evitar el acceso no autorizado a los servidores de bases de datos y que se utilizan protocolos seguros para la comunicación entre la base de datos y los servidores de aplicaciones.
3. Comunicación cifrada: Verifique que toda la comunicación entre la base de datos y los clientes o aplicaciones esté cifrada mediante TLS/SSL.

b. Entrevista y demostración en vivo: Se realiza una entrevista en video con el administrador de la base de datos (DBA), quien demuestra las configuraciones y consultas en vivo en el sistema de la base de datos, lo que permite la verificación de los controles de GIS en acción.

i. Verificación de la configuración: Durante la entrevista, verifique visualmente las configuraciones en la base de datos para asegurarse de que los controles de cifrado y GIS coincidan con la documentación.
ii. Demostración de cifrado: Solicite al DBA que demuestre cómo se almacenan y se accede a los datos cifrados, asegurándose de que los datos confidenciales estén cifrados correctamente y cumplan con los requisitos reglamentarios.
iii. Verificación de almacenamiento de contraseñas: asegúrese de que el DBA ejecute consultas que muestren cómo se almacenan las contraseñas (hash y sal) y verifique que los registros más antiguos también sigan los protocolos de cifrado adecuados.
iv. Cifrado de datos y controles de acceso: Revise y confirme el cifrado de PII, como nombres legales, números de identificación gubernamental (números de seguro social, números de identificación de contribuyentes, números de pasaporte o equivalentes) e información financiera personal (números de instrumentos de crédito o débito, números de cuentas bancarias, etc.), asegurándose de que todos los campos confidenciales estén cifrados.

E.3. Evaluación de la Seguridad de Ingeniería Social

El objetivo de la Evaluación de la Seguridad de Ingeniería Social es poner a prueba el elemento humano de la seguridad del GPE, identificando las vulnerabilidades que podrían explotarse mediante la manipulación en lugar de por medios técnicos. Esta evaluación de Seguridad de Ingeniería Social ayuda a identificar las debilidades en el comportamiento humano y la seguridad física que podrían dar lugar a infracciones, lo que garantiza un enfoque más holístico para proteger el GPE. Durante la Evaluación de Seguridad de Ingeniería Social, la ISF debe realizar las siguientes actividades clave:

a. Comportamiento humano:

i. Campañas de phishing: simule ataques de phishing dirigidos para evaluar la eficacia de la formación de los empleados y la capacidad del GPE para detectar y denunciar correos electrónicos sospechosos.
ii. Vishing y pretextos: Realice intentos de ingeniería social basados en el teléfono para extraer datos confidenciales u obtener acceso no autorizado haciéndose pasar por entidades de confianza.

iii. Spear Phishing: Ataques de phishing personalizados dirigidos a objetivos de alto valor dentro de la Empresa de Juego para probar la solidez de las protecciones de cuentas de acceso ejecutivo y privilegiado.

b. Seguridad Física:
   i. Intentos de intrusión física: Pruebe las medidas de seguridad física intentando obtener acceso no autorizado a áreas restringidas dentro del GPE, evaluando la efectividad de los protocolos de seguridad.
   ii. Compromiso del dispositivo: Intentar colocar dispositivos no autorizados dentro de la instalación para interceptar comunicaciones o exfiltrar datos, evaluando los controles de GIS físicos implementados.
   iii. Clonación de credenciales de acceso: Pruebe la resistencia de los controles de acceso físico intentando clonar las credenciales de acceso de los empleados y obtener acceso a áreas seguras.

E.4. Evaluación de seguridad inalámbrica

El objetivo de la Evaluación de Seguridad Inalámbrica es evaluar la seguridad y confiabilidad de la infraestructura inalámbrica dentro de la GPE. La Evaluación de Seguridad Inalámbrica se centra en la identificación de vulnerabilidades, configuraciones incorrectas y debilidades en las redes inalámbricas que podrían conducir a accesos no autorizados, interceptación de datos u otras formas de explotación. Garantiza que las redes inalámbricas que soportan el GPE sean seguras, resistentes y se gestionen correctamente de acuerdo con las mejores prácticas de seguridad. La Evaluación de Seguridad Inalámbrica implica un enfoque estructurado, que combina escaneo activo y pasivo, revisiones de configuración y pruebas de vulnerabilidad.

a. Los objetivos de la Evaluación de Seguridad Inalámbrica son los puntos de acceso inalámbrico (WAP), las redes inalámbricas y cualquier infraestructura inalámbrica asociada dentro del GPE, que incluyen:
   i. Redes de cara al público utilizadas por usuarios, visitantes o contratistas.
   ii. Redes inalámbricas internas utilizadas por los empleados con fines administrativos u operativos.
   iii. Redes de invitados y acceso inalámbrico segregado para uso no crítico.
   iv. Dispositivos inalámbricos utilizados para operaciones internas, como terminales de mano, tabletas u otros dispositivos móviles que se conectan a la infraestructura inalámbrica de la GPE.
b. Durante la Evaluación de Seguridad Inalámbrica, la ISF debe realizar las siguientes actividades clave:
   i. Reconocimiento y recopilación de información:
      1. Mapeo de puntos de acceso inalámbricos: mapee todos los WAP en la red GPE para identificar todos los dispositivos que transmiten o se conectan a la infraestructura inalámbrica.
      2. Topografía de red: escanee las redes inalámbricas para identificar identificadores de conjuntos de servicios (SSID), dispositivos conectados a la red y puntos de acceso que transmiten dentro del entorno.
      3. Detección de puntos de acceso no autorizados: identifique los puntos de acceso no autorizados o no autorizados que puedan haberse agregado a la red de forma maliciosa o errónea.
   ii. Revisión de configuración y seguridad:
      1. Cifrado y controles de acceso: Asegúrese de que los protocolos de cifrado seguros, como WPA3 o WPA2 con AES, estén en uso en todas las redes inalámbricas y que los protocolos de cifrado heredados (por ejemplo, WEP) estén deshabilitados. Revise los controles de acceso para garantizar la segmentación adecuada de las redes de invitados, públicas e internas.
      2. Administración de SSID: Evalúe si los SSID se están transmitiendo innecesariamente y asegúrese de que los SSID ocultos estén configurados para redes críticas.
      3. Autenticación y autorización: Asegúrese de que los mecanismos de autenticación (por ejemplo, 802.1x) se implementen y apliquen correctamente, evitando que dispositivos o usuarios no autorizados accedan a redes confidenciales. Verifique el uso correcto de los portales cautivos y las claves previamente compartidas, cuando corresponda.
      4. Segmentación de red: Revise la segmentación entre redes públicas, de invitados e internas para asegurarse de que el acceso a los sistemas críticos esté restringido y supervisado.

5. Identificación de vulnerabilidades: identifique las vulnerabilidades frente a las bases de datos de vulnerabilidades actualizadas, incluido cualquier firmware sin parches en dispositivos inalámbricos.

iii. Detección y monitoreo de intrusiones:
   1. Detección de puntos de acceso no autorizados: asegúrese de que los sistemas estén en su lugar para detectar y alertar a los administradores sobre dispositivos inalámbricos no autorizados o puntos de acceso no autorizados. Implemente un monitoreo continuo para detectar cualquier actividad inusual en las redes inalámbricas.
   2. Sistema de detección de intrusiones inalámbricas/Sistema de prevención de intrusiones (IDS/IPS): Evalúe la eficacia de cualquier IDS o IPS inalámbrico para identificar y prevenir ataques como la desautenticación, la interferencia o los ataques de intermediario MITM.

iv. Pruebas inalámbricas activas y pasivas:
   1. Pruebas pasivas: Para entornos inalámbricos de alto tráfico, se utilizan métodos de escaneo pasivo para monitorear y analizar el tráfico inalámbrico sin interactuar con la red.
   2. Pruebas activas: En áreas seguras o de poco tráfico, se deben realizar métodos de prueba activos (por ejemplo, intento de conexión, explotación de vulnerabilidades o captura de protocolo de enlace) para evaluar la resistencia de la infraestructura inalámbrica.
   3. Prueba de sangrado: evalúe el alcance de la señal inalámbrica para asegurarse de que no se filtre fuera del área de cobertura prevista, lo que podría exponer la red a los atacantes.

v. Rendimiento de la red inalámbrica y cobertura de la señal:
   1. Mapeo de cobertura de señal: evalúe la ubicación y la intensidad de la señal de los puntos de acceso inalámbricos para garantizar que la señal inalámbrica no se extienda más allá del perímetro seguro. Garantizar una cobertura coherente y fiable dentro de las zonas previstas, como las zonas operativas clave dentro del GPE.
   2. Evaluación del rendimiento: pruebe la capacidad de la red inalámbrica para manejar cargas de tráfico máximas sin degradar el rendimiento o la seguridad.

vi. Actualizaciones de firmware: asegúrese de que todos los puntos de acceso inalámbricos y la infraestructura relacionada ejecuten firmware actualizado para protegerse contra vulnerabilidades conocidas.

vii. Políticas de redes inalámbricas:
   1. Asegúrese de que la red inalámbrica cumpla con las políticas de seguridad de la organización, los estándares de la industria del juego y las regulaciones pertinentes (por ejemplo, PCI DSS, GDPR, etc.).
   2. Confirme que las redes públicas y de invitados sigan un conjunto separado de políticas para evitar cualquier superposición o acceso no autorizado a redes internas críticas.

viii. Registro y auditoría: Verifique que los mecanismos de registro estén habilitados en todos los puntos de acceso y que los registros de auditoría de acceso se almacenen de forma segura y se revisen periódicamente para detectar signos de actividad no autorizada.

ix. Seguridad física: Confirme que los dispositivos de red inalámbrica (por ejemplo, puntos de acceso y controladores) estén protegidos físicamente, con acceso restringido solo al personal autorizado.

E.5. Evaluación de la seguridad del código fuente

El objetivo de la evaluación de la seguridad del código fuente es detectar vulnerabilidades de seguridad, incluidos los problemas comunes y las amenazas más complejas específicas del GPE, mediante la revisión manual y el uso de herramientas automatizadas. Durante la Evaluación de Seguridad del código fuente, la ISF debe realizar las siguientes actividades clave:

a. Escaneo de código automatizado: Las herramientas automatizadas se utilizan para escanear el código fuente en busca de vulnerabilidades conocidas y patrones de código que puedan indicar fallas de seguridad.
b. Revisión manual del código: Se realiza una inspección manual en profundidad en áreas críticas como el manejo de transacciones, la lógica del juego y los sistemas de autenticación.
c. Autenticación y autorización: Garantice mecanismos seguros para la autenticación de usuarios y el control de acceso. Verifique la solidez de la autenticación multifactor (MFA) y los sistemas de gestión de sesiones para evitar el acceso no autorizado.

d. Validación de entrada y codificación de salida: valide todas las entradas del usuario para asegurarse de que se desinfectan correctamente para evitar vulnerabilidades comunes como la inyección de código SQL y el scripting entre sitios (XSS). Asegúrese de que los datos de salida estén codificados de forma segura antes de devolverlos a los usuarios.
e. Manejo de datos confidenciales: evalúe cómo se manejan los datos confidenciales, como la información de identificación personal (PII, por sus siglas en inglés) y la información de pago, lo que garantiza el cifrado de los datos tanto en tránsito como en reposo. Evalúe la administración de las claves de cifrado para evitar la exposición.
f. Manejo y registro de errores: Revise los procedimientos de manejo de errores para asegurarse de que los datos confidenciales, así como información del sistema no se divulgue a través de mensajes de error. Los registros de auditoría deben estar debidamente protegidos y evitar registrar datos confidenciales, como las credenciales de autenticación.
g. Seguridad de la lógica del juego: Analice la implementación de la lógica central del juego, incluidos los mecanismos del generador de números aleatorios (RNG), para garantizar la equidad y la integridad. Las implementaciones seguras de RNG son cruciales para evitar la manipulación de los resultados del juego.
h. Librerías y dependencias de terceros: asegúrese de que todas las librerías externas utilizadas en la aplicación estén actualizadas y libres de vulnerabilidades conocidas. Audite periódicamente las dependencias como parte del ciclo de vida de desarrollo seguro.

E.6. Prueba de simulación adversarial

El objetivo de la Prueba de Simulación Adversarial es mejorar la postura de seguridad del GPE mediante la simulación de escenarios de ataque sofisticados del mundo real en todo el espectro de posibles vectores de ataque, centrándose en los aspectos digitales y físicos de la seguridad. La Prueba de Simulación Adversarial está diseñada para poner a prueba la resistencia del GPE frente a una serie de tácticas, técnicas y procedimientos avanzados utilizados por los atacantes del mundo real. El objetivo de la Prueba de Simulación Adversarial es evaluar la capacidad del GPE para detectar, responder y mitigar las técnicas de ataque avanzadas que determinados actores de amenazas podrían emplear. Esta prueba cubre lo siguiente:

a. A diferencia de las pruebas de penetración tradicionales, la Prueba de Simulación Adversarial limita a un adversario persistente y altamente calificado que busca romper las defensas del GPE utilizando cualquier medio necesario.
b. Durante la la Prueba de Simulación Adversarial, la ISF debe realizar las siguientes actividades clave:
    i. Inteligencia de código abierto (OSINT) y recopilación de información:
        1. Información disponible públicamente: Recopile y analice información disponible públicamente sobre la Empresa de juegos, su infraestructura, empleados y socios.
        2. Registro de dominio e información de DNS: recopile datos de registros de WHOIS, búsquedas de DNS y detalles de registro de dominio para identificar posibles vectores de ataque relacionados con la administración de dominios.
        3. Perfiles de redes sociales: Analice las cuentas de redes sociales de los empleados clave para recopilar información que podría aprovecharse en ataques de ingeniería social.
        4. Documentación de acceso público: busque documentos de acceso público, como PDF, presentaciones e informes, que puedan contener nombres de empleados, procesos internos u otros datos confidenciales.
        5. Búsquedas de filtraciones y filtraciones de datos: investigue si se ha expuesto algún dato confidencial relacionado con la empresa en violaciones anteriores, incluidas credenciales de autenticación y PII.
        6. Huella técnica: Identificar la infraestructura, los servicios y las tecnologías externas utilizados por el GPE a través de técnicas de reconocimiento pasivo, como la captura de pancartas, las consultas de los motores de búsqueda (por ejemplo, Google Dorking) y las bases de datos de seguridad pública.
        7. Relaciones con terceros: Investigue las asociaciones, los proveedores y los servicios de terceros utilizados por la empresa de juegos para identificar posibles vulnerabilidades de la cadena de suministro.
    ii. Ataques de red avanzados:
        1. Movimiento lateral: simule un atacante interno que ha obtenido acceso inicial, probando la capacidad de moverse lateralmente a través de la red para acceder componentes críticos del sistema.

2. Mecanismos de persistencia: Pruebe las defensas del GPE contra los atacantes que intentan establecer una persistencia a largo plazo dentro de la red, asegurando la detección y eliminación de puntos de apoyo maliciosos.
3. Exfiltración de datos: simule los métodos que un atacante podría usar para exfiltrar datos confidenciales del GPE, probando la eficacia de las medidas de prevención de pérdida de datos (DLP).
4. Reconocimiento avanzado: Realice detección y reconocimiento de red sigilosos para mapear la red interna e identificar activos y sistemas clave para ataques dirigidos.
5. Pruebas de comando y control (C2): Establezca y mantenga la comunicación con los sistemas comprometidos utilizando varias técnicas C2 para probar las capacidades de detección de la Empresa de Juego.
6. Escalada de privilegios: pruebe la capacidad del GPE de escalar privilegios desde el acceso de nivel inferior hasta el acceso administrativo o raíz, aprovechando las configuraciones incorrectas o las vulnerabilidades del sistema.
7. Volcado y reutilización de credenciales: intente extraer y reutilizar credenciales de autenticación de sistemas comprometidos para infiltrarse aún más en la red o acceder a datos confidenciales.

iii. Evaluación de Respuesta a Incidentes:

1. Detección y alerta: Evalúe la eficacia de los sistemas de monitoreo y alerta del GPE en la detección de actividades de ataque sofisticadas, asegurando una respuesta oportuna.
2. Respuesta y contención: Evalúe la velocidad y eficiencia del equipo de respuesta a incidentes en la contención y mitigación de las amenazas simuladas, centrándose en minimizar el impacto.
3. Análisis posterior al incidente: Revise la capacidad para realizar un análisis exhaustivo posterior al incidente, implementar las lecciones aprendidas y mejorar las defensas de seguridad para prevenir futuros incidentes.

c. Los resultados de la la la Prueba de Simulación Adversarial proporcionarán a la Empresa de Juego una comprensión detallada de cómo se comportan sus defensas de seguridad frente a escenarios de ataque avanzados. Los hallazgos informarán sobre las mejoras estratégicas de seguridad y reforzarán la importancia de una estrategia de defensa proactiva y estratificada, que garantice que el GPE siga siendo sólida contra las amenazas emergentes.

Derechos de autor © 2025 Gaming Labs International, LLC

Todos los derechos reservados.

DEFINICIONES DE TÉRMINOS

Término	Descripciones
Acceso	Posibilidad de hacer uso de cualquier recurso del GPE.
Control de acceso	El proceso de otorgar o denegar solicitudes específicas para obtener y usar datos confidenciales y servicios relacionados específicos de un sistema; y para entrar en instalaciones físicas específicas que albergan infraestructuras críticas de redes o sistemas.
Estándares de cifrado avanzados (AES)	Cifrado de bloque simétrico que puede cifrar (cifrar) y descifrar (descifrar) información.
Algoritmo	Un conjunto finito de instrucciones inequívocas realizadas en una secuencia prescrita para lograr un objetivo, especialmente una regla o procedimiento matemático utilizado para calcular un resultado deseado. Los algoritmos son la base de la mayoría de la programación informática.
Aplicación	Software informático diseñado para ayudar a un usuario a realizar una tarea específica.
Registro de Auditoría	Un registro auditable de acciones, eventos o cambios dentro de un GPE, que captura detalles como actividades de usuarios, intentos de acceso, alteraciones y operaciones del sistema para garantizar la seguridad, el cumplimiento y la responsabilidad durante un periodo 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 del GPE
Credenciales de autenticación	Cualquier contraseña, autenticación multifactor, certificados digitales, PIN, datos biométricos, preguntas y respuestas de seguridad y cualquier otro método de acceso a la cuenta (por ejemplo, deslizamiento magnético, tarjetas de proximidad, tarjetas con chip integrado).
Disponibilidad	Garantizar el acceso oportuno y fiable a la información y su utilización.
Copia de seguridad	Una copia de los archivos y programas realizados para facilitar la recuperación si es necesario.
Biometría	Una entrada de identificación biológica, como huellas dactilares, patrones de retina, datos de reconocimiento facial o huellas de voz
Puente	Divide las redes para reducir el tráfico general de la red. Un puente permite o evita que los datos pasen a través de él mediante la lectura de la dirección MAC.
Aplicaciones de Negocio	Aplicaciones que funcionan como un servicio compartido para que los usuarios recopilen, procesen, mantengan, utilicen, compartan, difundan o eliminen datos confidenciales dentro de la GPE con fines de auditoría de cumplimiento y respuesta a incidentes de seguridad
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 alámbricas, inalámbricas, de cable, de radio, de microondas, de luz, de fibra óptica, de satélite o informáticas, incluidas Internet y las intranets.
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 comportamientos relacionados con cualquier norma técnica 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 a las operaciones de juegos o del sistema.
Componente crítico del sistema	Cualquier hardware, software, programas de control críticos, tecnología de comunicaciones, otros equipos o componentes implementados en un GPE para permitir la participación de los usuarios en los juegos, y cuyo fallo o compromiso pueda provocar la pérdida de los derechos de los usuarios, ingresos gubernamentales o acceso no autorizado a los datos utilizados para

Término	Descripciones
	generar informes para el Organismo Regulador. Ejemplos de componentes críticos del sistema incluyen, pero no se limitan a: • Componentes que registran, almacenan, procesan, comparten, transmiten o recuperan datos confidenciales. • Componentes que podrían afectar a la seguridad de los datos confidenciales o al 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 usuario. • Puntos de entrada y salida de los componentes anteriores, incluidos otros sistemas que se comunican directamente con los componentes críticos del sistema. • Tecnología de comunicaciones y redes que transmiten datos confidenciales, incluidos los equipos de comunicación de red (NCE) y los controles de seguridad de 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 internos de la red. • 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, que incluyen instancias de contenedores o imágenes, nubes privadas virtuales, administración de identidades y accesos basada en la nube, componentes que residen en las instalaciones o en la nube, mallas de servicios con aplicaciones en contenedores y herramientas de orquestación de contenedores. • Tipos de servidores, incluidos web, aplicaciones, bases de datos, autenticación, correo, proxy, protocolo de tiempo de red (NTP) y servicio de nombres de dominio (DNS). • Dispositivos de usuario final, como ordenadores, 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 administración de la configuración de software o para la implementación de objetos en el GPE o en componentes que pueden afectar al GPE. • Redes y sistemas corporativos que interactúan con el GPE y desde los cuales los atacantes podrían usar para moverse lateralmente hacia el GPE (por ejemplo, las redes de los casinos corporativos y las redes corporativas de los operadores en línea). • Cualquier otro componente que el Organismo Regulador o la Empresa de Juegos de Azar consideren crítico para la GPE
Módulo criptográfico	Hardware, software, firmware o combinación de los mismos que implementan funciones criptográficas como cifrado, descifrado, firmas, hash y administración de claves. El objetivo principal de un módulo criptográfico es proporcionar un procesamiento y almacenamiento seguros de claves y operaciones.

Término	Descripciones
Integridad de los datos	La propiedad de que los datos son precisos y coherentes y no se han alterado de forma no autorizada en el almacenamiento, durante el procesamiento y mientras están en tránsito.
Denegación de servicio Distribuido (DDoS)	Un tipo de ataque en el que se utilizan múltiples sistemas comprometidos, generalmente infectados con un programa de software destructivo, para atacar 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 nombres de máquinas a números IP y viceversa.
Encriptación	La conversión de datos en un formulario, llamado texto cifrado, que no puede ser fácilmente entendido por personas no autorizadas. Cuando el cifrado no sea posible debido a una limitación de la tecnología o del rendimiento, se deben implementar otras medidas de protección razonables en su lugar y revisarse caso por caso.
Clave de cifrado	Una clave que se ha cifrado para disfrazar 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 y al mismo tiempo permitir la comunicación con el exterior.
Empresa de juegos	Un operador y cualquier proveedor, fabricante, vendedor, prestador de servicios y/u otras entidades que tengan una función en la supervisión del funcionamiento de un GPE, o que presten servicios integrales para su función, incluida la gestión de datos confidenciales.
Seguridad de la información de los juegos (GIS)	Proteger los datos confidenciales y los componentes críticos del sistema contra el acceso, el uso, la divulgación, la interrupción, la modificación o la destrucción no autorizados con el fin de proporcionar integridad, confidencialidad y disponibilidad.
Sistema de gestión de seguridad de la información del juego (GISMS)	Un sistema de gestión definido y documentado que consta de un conjunto de políticas, procesos y sistemas para gestionar los riesgos para los datos confidenciales, los activos y los componentes críticos del sistema de una empresa de juegos dentro de un GPE, con el objetivo de garantizar niveles aceptables de riesgo GIS.
Entorno de producción de juegos (GPE)	El entorno operativo donde las actividades de juego y los servicios relacionados se realizan, administran y entregan a los usuarios 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 gestionar datos confidenciales, así como los sistemas y la infraestructura de backend que interactúan y/o apoyan 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 GIS	Un suceso que real o potencialmente pone en peligro la integridad, confidencialidad o disponibilidad de un GPE o 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, las políticas o procedimientos de GIS o las políticas de uso aceptable.
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 exploradores en respuesta a varios comandos.
Concentrador	Conecta dispositivos en una red de par trenzado. Un hub no realiza ninguna tarea además de la regeneración de señales.
Integridad	Proteger contra la modificación o destrucción indebida de la información e incluye garantizar el no repudio y la autenticidad de la información.

Término	Descripciones
Internet	Un sistema interconectado de redes que conecta computadoras de todo el mundo a través de TCP / IP.
Dirección de protocolo de Internet (dirección IP)	Número único de un equipo que se utiliza para determinar dónde se deben entregar los mensajes transmitidos por 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 de alguien que intenta entrar 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.
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.
Malfuncionamiento	Cuando un componente crítico del sistema no funciona según lo previsto.
Malware	Un programa que se inserta en un sistema, generalmente de forma encubierta, con la intención de comprometer la integridad, confidencialidad o disponibilidad de los datos, las aplicaciones o el sistema operativo de la víctima, o de molestar o interrumpir a la víctima.
Ataque Man-In-The-Middle (MITM)	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	Medida de seguridad diseñada para establecer la autenticidad de un mensaje por medio de un autenticador dentro de la transmisión derivada de ciertos elementos predeterminados del propio mensaje.
Código de autenticación de mensajes (MAC)	Suma de comprobación criptográfica de los datos que utiliza una clave simétrica para detectar modificaciones accidentales e intencionadas de los datos.
Autenticación multifactor (MFA)	Un tipo de autenticación que utiliza dos o más de los siguientes para verificar la identidad de un usuario: • Información que solo conoce el usuario (por ejemplo, una contraseña, PIN o respuestas a preguntas de seguridad); • Un artículo poseído por un usuario (por ejemplo, un token electrónico, un token físico o una tarjeta de identificación); y • Los datos biométricos de un usuario (por ejemplo, huellas dactilares, patrones de retina, datos de reconocimiento facial o huellas de voz).
Equipo de comunicación de red (NCE)	Tecnología de comunicaciones que controla la comunicación de datos en un sistema, incluidos, entre otros, NIC, cables, conmutadores, puentes, concentradores, enrutadores, puntos de acceso inalámbricos y teléfonos, dispositivos de red VoIP, puntos de acceso inalámbricos, dispositivos de red y otros dispositivos de seguridad.
Tarjeta de interfaz de red (NIC)	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 digno de mención para su posible mejora con el fin de cumplir las mejores prácticas del sector.
Contraseña	Cadena de caracteres (letras, números y otros símbolos) que se utiliza para autenticar una identidad o para verificar la autorización de acceso.
Información de identificación personal (PII)	Datos sensibles que podrían utilizarse 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

Término	Descripciones
	crédito o débito, números de cuentas bancarias, etc.) u otra información personal si así lo define el Organismo Regulador.
Número de identificación personal (PIN)	Un código numérico asociado a un individuo y que permite el acceso seguro a un dominio, cuenta, red, sistema, etc.
Puerto	Un punto físico de entrada o salida de un módulo que proporciona acceso al módulo para señales físicas, representadas 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 entra o sale de una red y lo procesa y lo reenvía. Esto cierra efectivamente el camino recto entre las redes internas y externas. Lo que dificulta 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 redes entre sí. Un enrutador (router) utiliza la dirección de red configurada por software para tomar decisiones de reenvío.
Datos confidenciales	Información que debe manejarse de manera segura, incluidas, entre otras, según corresponda: a. 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; b. Información contable y de eventos Significativos relacionados con los componentes críticos del sistema del GPE; c. semillas RNG y cualquier otra información que afecte los resultados de los juegos y las apuestas; d. Claves de cifrado, donde la implementación elegida requiere la transmisión de claves; e. Números de validación asociados con cuentas de usuarios, instrumentos de apuestas y cualquier otra transacción de juego; f. Transferencias de fondos hacia y desde cuentas de usuarios, cuentas de pago electrónico y con fines de juego; g. Paquetes de software dentro del GPE; h. Cualquier dato de ubicación relacionado con la actividad de los empleados o usuarios (por ejemplo, gestión de cuentas, juegos en línea, etc.); i. Cualquiera de la siguiente información registrada para cualquier empleado o cliente: • 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.); • Credenciales de autenticación en relación con cualquier cuenta de usuario o cuenta de usuario; • Cualquier otra información de identificación personal (PII, por sus siglas en inglés) que deba mantenerse confidencial; y j. Cualquier otro dato que el Organismo Regulador o la Empresa de Juegos considere sensible.
Servidor	Una instancia en ejecución de software que es capaz de aceptar solicitudes de clientes y el equipo que ejecuta dicho software. Los servidores operan dentro de una arquitectura cliente-servidor, en la que los "servidores" son

Término	Descripciones
	programas informáticos que se ejecutan para atender las solicitudes de otros programas ("clientes").
Proveedores de servicios	Entidades que ofrecen plataformas, software y servicios a empresas de juegos. Algunos ejemplos son los consultores de TI, los proveedores de servicios gestionados, las plataformas de software como servicio (SaaS) y los proveedores de servicios en la nube. Los proveedores y vendedores externos también se consideran proveedores de servicios.
Identificador de conjunto de servicios (SSID)	Nombre que identifica una LAN inalámbrica 802.11 determinada.
Ingeniería Social	Un intento de engañar a alguien para que revele información (por ejemplo, una contraseña) que puede usarse para atacar sistemas o redes. Los ataques de ingeniería social incluyen intrusiones no técnicas en un GPE utilizando información adquirida a través de la interacción humana y se basan en trucos que se aprovechan de que una persona no está familiarizada 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.
Interruptor	Conecta dispositivos en una red 802.3. Un switch reenvía los datos a su destino mediante la dirección MAC incrustada en cada paquete.
Amenaza	Cualquier circunstancia o evento con el potencial de afectar negativamente las operaciones de la red (incluida la misión, las funciones, la imagen o la reputación), los activos o las personas a través de un sistema a través del acceso no autorizado, la destrucción, la divulgación, la modificación de la información y / o la denegación de servicio; la posibilidad de que una fuente de amenaza explote con éxito una vulnerabilidad concreta; cualquier peligro potencial para una red que alguien o algo pueda identificar como vulnerable y, por lo tanto, tratar de explotar.
Protocolo de control de transmisión/Protocolo de Internet (TCP/IP)	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.
Virus	Un programa autorreplicante, normalmente 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" a la introducción de una amenaza.
Protocolo equivalente por cable (WEP)	Un algoritmo fácilmente rompible y, por lo tanto, obsoleto para proteger las redes inalámbricas IEEE 802.11. Originalmente estaba destinado a permitir el mismo nivel de protección que una conexión por cable, pero pronto se descubrieron fallas después de su adopción que lo hicieron apenas mejor que ninguna protección.
Punto de acceso inalámbrico (WAP)	Proporciona capacidades de red a los dispositivos de red inalámbrica. Un WAP se utiliza a menudo para conectarse a una red cableada, actuando así como enlace entre las partes cableadas e inalámbricas de la red.
Wi-Fi	La tecnología estándar de red de área local inalámbrica (WLAN) para conectar computadoras y dispositivos electrónicos entre sí y/o a Internet.
Acceso protegido Wi-Fi (WPA)	El sucesor de WEP. Su autenticación se puede romper en ciertas circunstancias, pero las frases de contraseña suficientemente complejas son lo suficientemente seguras para la mayoría de los usos.
Estación de trabajo	Una interfaz para que el personal autorizado acceda a las funciones reguladas de la GPE.