GLI®

MARCO DE SEGURIDAD DEL JUEGO

GLI-GSF-1

AUDITORÍA DE CONTROLES COMUNES DE SEGURIDAD DE LA INFORMACIÓN DEL JUEGO (GIS)

Versión 1.0 BORRADOR – Publicado el 19 de abril de 2024

Contenido

1. INTRODUCCIÓN

1.1. Declaración General

La integridad y precisión del funcionamiento de un entorno de producción del juego (GPE por sus siglas en inglés) depende en gran medida de los procedimientos operativos, configuraciones e infraestructura de la red. Con las amenazas cada vez más emergentes para las operaciones de juego, los organismos reguladores dependen en gran medida de la experiencia de una empresa de seguridad independiente (ISF) calificada para realizar evaluaciones de seguridad de juego como una adición esencial a las pruebas y certificación de los componentes críticos del sistema de un GPE por parte de un laboratorio de pruebas independiente (ITL). Este módulo del Marco de Seguridad del Juego de GLI (GLI-GSF-1) establece los controles comunes de seguridad de la información del juego (GIS por sus siglas en inglés) necesarios para auditar el Sistema de Gestión de Seguridad de la Información del Juego (GISMS) de una Organización de Juego para garantizar una gestión eficaz de la seguridad en el GPE de una Organización de Juego. Estos controles comunes de GIS se aplican a las GPE utilizadas para todas las formas de juego, como los juegos de casino, lotería, apuestas de eventos y juegos interactivos. Dependiendo del tipo de Organización de Juego, también se pueden aplicar módulos adicionales del GLI-GSF. Además, el GLI-GSF-2 *[que se publicará para comentarios en un futuro próximo]* proporcionará la orientación necesaria para realizar evaluaciones de Seguridad Técnica de Juegos (GTS) de la GPE de una Organización de Juegos.

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

1.2. Entorno de Producción del Juego (GPE)

Un GPE se refiere al entorno operativo donde se realizan, administran y entregan las actividades de juego y los servicios relacionados a los clientes en vivo o en tiempo real. Abarca la infraestructura física y virtual, los sistemas, el software y los procesos necesarios para facilitar diversas formas de juego, incluidos (entre otros): juegos de casino, lotería, apuestas de eventos y juegos interactivos. La GPE también abarca los sistemas de la oficina auxiliar (backend) y la infraestructura que interactúan y/o respaldan las actividades de juego. Las características clave de una GPE incluyen:

a. Componentes críticos del sistema: Esto incluye las plataformas de hardware y software que respaldan la ejecución de actividades de juego, como dispositivos de juego, mesas de juego, sistemas de juego, sistemas de apuestas y sistemas o aplicaciones de juego interactivos.
b. Procesamiento de transacciones: La GPE procesa las transacciones monetarias relacionadas con las actividades de juego, incluidas las apuestas, pagos, depósitos, retiros y transacciones financieras con los clientes.
c. Medidas de seguridad: Se implementan medidas de seguridad sólidas para salvaguardar la seguridad, integridad, confidencialidad y disponibilidad de los componentes críticos del sistema, datos confidenciales, transacciones financieras e información de los usuarios contra el acceso no autorizado, fraude, manipulación y amenazas cibernéticas.
d. Gestión de riesgos: La 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, riesgos financieros, riesgos regulatorios y riesgos tecnológicos.
e. 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 una alta disponibilidad, confiabilidad y resiliencia de la infraestructura y los sistemas para minimizar el tiempo de inactividad y las interrupciones.
f. 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 rápidamente a incidentes GIS, fraude u otros problemas.
g. Cumplimiento normativo: El cumplimiento de las regulaciones de juego, los requisitos de licencia y los estándares de la industria es esencial en una GPE para garantizar el juego limpio, la protección de los clientes, las prácticas de juego responsable y el cumplimiento de las obligaciones legales y reglamentarias.

1.3. 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, activos y componentes críticos del sistema de una Organización de juego dentro de su GPE contra el acceso, divulgación, alteración o destrucción no autorizados. Abarca políticas, procedimientos, controles y prácticas de gestión de riesgos específicamente adaptadas a los desafíos únicos y requisitos regulatorios de la industria del juego, lo que implica la identificación de riesgos SIG, 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.

1.4. 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 organizaciones de juegos deben establecer y mantener un marco claramente definido y documentado para lograr y preservar la confianza pública en sus operaciones. El objetivo es alinear los 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.

2. AUDITORÍAS DE GISMS

2.1. Visión General de la Auditoría

La auditoría GISMS se realiza con la intención de identificar cualquier caso real o potencial de incumplimiento, vulnerabilidad o debilidad, y garantizar que se preserve la confidencialidad, integridad y disponibilidad de la información bajo el control de la Organización de juego. Este enfoque se basa en gran medida en la seguridad por capas para reducir el riesgo para los sistemas informáticos y de red. El enfoque por capas proporciona redundancia y refuerza el modelo de seguridad general, ya que se deben vulnerar varias capas de seguridad antes de acceder a un almacén de datos crítico.

NOTA: El enfoque de la guía GIS detallada en el GLI-GSF-1 se centra en los controles comunes de seguridad de la información del juego, otros métodos de evaluación se discuten en los módulos de soporte del GLI-GSF.

2.2. Métodos de Auditoría

Una auditoría GISMS utiliza una serie de métodos de evaluación, incluidos los siguientes métodos, cuyos resultados se utilizan para respaldar la determinación de la eficacia del control GIS a lo largo del tiempo:

a. Entrevista: Un tipo de método de evaluación que se caracteriza por el proceso de llevar a cabo discusiones con individuos o grupos dentro de una Organización de Juegos para facilitar la comprensión, lograr aclaraciones o conducir a la localización de pruebas.
b. Examinar: Tipo de método de evaluación que se caracteriza 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: Tipo de método de evaluación que se caracteriza por el proceso de ejercitar uno o más objetos de auditoría en condiciones especificadas para comparar el comportamiento real con el esperado.

2.3. Tareas de Auditoría

A continuación se presentan las actividades de auditoría de alto nivel sugeridas. En el Apéndice se detallan los requisitos mínimos de control común GIS con más detalle. Se dirige a los usuarios de este documento al Apéndice para asegurarse de que no se pase por alto ningún control GIS necesario. Los controles GIS enumerados en el Apéndice no son exhaustivos y pueden incluirse controles GIS adicionales en función de los requisitos reglamentarios y el alcance de la evaluación.

2.3.1. Revisión de la Documentación Presentada

En primer lugar, la ISF evalúa los controles GIS existentes de la Organización de Juegos mediante la recopilación y revisión de la documentación pertinente para comprender y evaluar mejor los aspectos pertinentes de la GPE en relación con el GIS general, y para determinar si la documentación complementa adecuadamente los controles técnicos. Un ejemplo de parte de la documentación que se espera que se revise incluye, pero no se limita a:

a. Política GIS
b. Acceso de usuarios
c. Procedimientos de desarrollo y pruebas
d. Acuerdo de Nivel de Servicio
e. Política de uso de los servicios de red
f. Controles de detección, prevención y recuperación para protegerse contra código malintencionado
g. Política de copia de seguridad de datos
h. Procedimientos establecidos para que los medios se eliminen de forma segura
i. Procedimientos para el manejo y almacenamiento de información (para proteger la información de la divulgación no autorizada o el uso indebido)
j. Programa de Gestión del Cambio
k. Procedimientos para monitorear el uso de los medios de procesamiento de información
l. Políticas, planes operativos y procedimientos para las actividades de teletrabajo
m. Política sobre el uso de controles criptográficos
n. Diagrama de red

2.3.2. Entrevistas con Personal Clave

Después de recopilar y revisar la documentación relevante, la ISF entrevista al personal clave (usuarios, administradores y gerencia) para identificar prácticas no documentadas y obtener retroalimentación. Como parte del proceso de entrevistas, la ISF discute las prácticas reales en uso y a lo largo de las otras fases de la evaluación, la ISF identifica los procedimientos en uso basados en los resultados técnicos de la evaluación. Esta información permite a la ISF identificar brechas de procedimiento e identificar buenas prácticas que no están completamente documentadas en las políticas y procedimientos formales. Además, el ISF mide el nivel de conocimiento de los usuarios durante las entrevistas para determinar si los usuarios ajenos a la función de TI tienen un nivel adecuado de comprensión de los GIS y su papel en la protección de la información y otros activos críticos. Se entrevistará como mínimo a las siguientes personas clave responsables de establecer la política de GIS y de aplicarla.

a. Persona con la responsabilidad general de la operación de juego
b. Oficial de cumplimiento
c. Responsable de seguridad de la información
d. Personal operativo
e. Desarrolladores de software

2.3.3. Evaluación de Controles Administrativos

La ISF realiza pruebas y evaluaciones para evaluar la eficacia y la idoneidad de estas medidas administrativas para mitigar los riesgos y garantizar el cumplimiento de los requisitos de seguridad. Por lo general, esta evaluación aborda los siguientes temas:

a. Políticas, normas y directrices
b. Seguridad Organizacional
c. Gestión de Operaciones
d. Actualización de parches y administración
e. Monitoreo del acceso y uso del sistema
f. Procedimientos de gestión de cambios
g. Clasificación y Control de Activos
h. Planes de contingencia

i. Respuesta a incidentes GIS

2.3.4. Evaluación de Controles Técnicos

La ISF realiza pruebas y evaluaciones para evaluar la eficacia y la idoneidad de estas salvaguardas técnicas para mitigar los riesgos y proteger los datos confidenciales. Por lo general, esta evaluación aborda los siguientes temas:

a. Diseño de Infraestructura
b. Topografía de Redes / Pruebas de Penetración
c. Seguridad de redes y comunicaciones
d. Controles de acceso lógico
e. Seguridad de los sistemas operativos (SO)
f. Controles de software malintencionado
g. Diseño y configuración de bases de datos
h. Controles criptográficos
i. Monitoreo del sistema
j. Informes y registro
k. Controles de desarrollo del sistema

2.3.5. Evaluación de Controles Físicos y Ambientales

La ISF realiza pruebas y evaluaciones para evaluar la eficacia y la idoneidad de estos controles en la protección contra amenazas físicas, peligros ambientales y acceso no autorizado a áreas sensibles. Por lo general, esta evaluación aborda los siguientes temas:

a. Ubicación y seguridad de las instalaciones
b. Seguridad perimetral
c. Controles de acceso
d. Seguridad de los equipos
e. Detección de intrusos
f. Sistemas de alarma
g. Sistemas de vigilancia
h. Calefacción, ventilación y aire acondicionado
i. Sistemas de energía
j. Cableado de alimentación y comunicaciones
k. Detección y extinción de incendios
l. Respuesta a emergencias

2.3.6. Evaluación de Riesgos

La ISF realiza una evaluación de riesgos para identificar problemas de no conformidad con cualquier control aplicable, y cualquier amenaza y vulnerabilidad potencial que no se enumere explícitamente en el GLI-GSF, pero que se observó durante la auditoría y puede constituir un riesgo.

2.4. Frecuencia de Auditoría

2.4.1. Auditoría Inicial

La Organización de Juegos debe tener una auditoría GISMS realizada por una ISF dentro de los noventa días posteriores al inicio de las operaciones de juego de la Organización de Juegos dentro de esa jurisdicción, a menos que el organismo regulador haya aconsejado lo contrario. Cualquier aplazamiento de esta auditoría según lo solicitado por la Organización del Juego, junto con un cronograma de auditoría actualizado, será autorizado por el organismo regulador.

NOTA: Se recomienda que los organismos reguladores permitan flexibilidad para los cronogramas de auditoría de las organizaciones de juego multijurisdiccionales para permitir la consolidación de las auditorías de múltiples jurisdicciones en un cronograma común.

2.4.2. Auditoría Anual

La Organización de Juegos debe, por regla general, tener otra auditoría GISMS realizada por una ISF dentro de los doce meses posteriores a la auditoría GISMS anterior, a menos que el organismo regulador haya aconsejado lo contrario. Cualquier aplazamiento de esta auditoría según lo solicitado por la Organización del Juego, junto con un cronograma de auditoría actualizado, será autorizado por el organismo regulador.

NOTA: Se recomienda que los organismos reguladores permitan flexibilidad para los cronogramas de auditoría de las organizaciones de juego multijurisdiccionales para permitir la consolidación de las auditorías de múltiples jurisdicciones en un cronograma común.

2.4.3. Auditorías Adicionales

Es posible que se necesiten auditorías GISMS adicionales con mayor frecuencia en función de la crtiticidad de los cambios dentro de la GPE, como los cambios que pueden afectar o proporcionar acceso a datos confidenciales y/o componentes críticos del sistema.

2.5. Informes de Auditoría de GISMS

Los resultados de una auditoría del SGSI determinarán para la administración las areas de las operaciones en las que se debe considerar la posibilidad de mejorar y recomendarán estrategias para mejorar esas areas. El informe de auditoría del GISMS debe presentarse al organismo regulador a más tardar sesenta días después de que se haya completado la auditoría del GISMS. El informe de auditoría del SGSI debe incluir todo lo siguiente:

a. El nombre y una breve historia de la Organización de Juego, mencionando su modelo de negocio y las actividades de juego ofrecidas o utilizadas por terceros, así como la ubicación, número de empleados, sitio web, certificaciones reales, descripción de alto nivel de la infraestructura, incluido el centro de datos, etc.
b. El nombre de la ISF, afiliación de la empresa, información de contacto y calificaciones y experiencia de las personas que llevaron a cabo la auditoría;
c. La(s) fecha(s) de la auditoría, incluida la fecha de solicitud, fecha de inicio, fecha de finalización, fecha del informe y fecha de vencimiento;
d. El alcance de la auditoría, que incluye:
    i. Una visión general de alto nivel del trabajo realizado y del entorno de control en funcionamiento;
    ii. Los controles con los que se llevó a cabo la auditoría;
    iii. Los componentes críticos del sistema que se revisaron
    iv. Cómo se identificaron los componentes críticos del sistema y si la auditoría incluyó aplicaciones, redes, bases de datos y/o sistemas operativos;
    v. Una indicación de las condiciones de la auditoría, incluidos los controles excluidos de la auditoría y las razones de su exclusión;
e. El enfoque de auditoría, que incluye preguntas basadas en la indagación, observación, pruebas, personas clave entrevistadas;
f. Evidencia obtenida durante la auditoría para corroborar los resultados de la auditoría, incluyendo:
    i. Los documentos que fueron revisados, incluyendo versión y fechas, personal entrevistado,.
    ii. Los nombres, fechas y versiones de la documentación revisada;
    iii. Los nombres, funciones y ubicaciones del personal entrevistado;
    iv. Los lugares visitados;
    v. Los detalles de los recorridos realizados;
    vi. Las muestras revisadas para verificar el cumplimiento;
g. Los resultados de la auditoría, indicando para cada control su estado como conforme, observación, no conformidad menor o no conformidad mayor;
h. Hallazgos, que incluyen:
    i. Una explicación de las no conformidades identificadas;

ii. Evidencia que respalde y describa las no conformidades;
iii. Impacto o impacto potencial de las no conformidades;
iv. Medidas correctivas recomendadas para abordar las no conformidades existentes y realizar mejoras;

i. La respuesta de la Organización de Juegos a los hallazgos y las medidas correctivas recomendadas, incluidas las fechas de resolución y las personas responsables; y

j. Otros factores relevantes, como si los GISMS cumplen o han sido auditados con otros requisitos (e.g. ISO/IEC 27001, WLA-SCS, NIST-CSF, etc.)

2.6. Acciones Correctivas

Si el informe de auditoría GISMS de la ISF recomienda una acción correctiva, la Organización de Juegos debe proporcionar a la ISF y al organismo regulador un plan de remediación y cualquier plan de mitigación de riesgos que detalle las acciones y el cronograma de la Organización de Juegos para implementar la acción correctiva.

a. Las no conformidades se abordarán a través del proceso de acción correctiva de la Organización del juego, que incluye:
   i. Medidas adoptadas para determinar el alcance de la no conformidad específica y contenerla.
   ii. Investigación de la causa raíz para determinar las causas más básicas de la no conformidad.
   iii. Acciones tomadas para corregir la no conformidad y, en respuesta a la causa raíz, eliminar la recurrencia de la no conformidad.
b. Las acciones correctivas para abordar las no conformidades importantes identificadas se llevarán a cabo de inmediato y se notificará a la ISF y al organismo regulador de las acciones tomadas dentro de los treinta días, a menos que el organismo regulador especifique lo contrario. La ISF realizará una auditoría de seguimiento en un plazo de noventa días para confirmar las acciones tomadas, evaluar su eficacia y determinar si las no conformidades han sido resueltas.
c. Las acciones correctivas para abordar las no conformidades menores identificadas deberán ser documentadas y enviadas por la Organización de Juegos a la ISF y al 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 auditoría programada.
d. Una vez que se hayan tomado las medidas correctivas, la Organización de Juegos proporcionará a la ISF y al organismo regulador la documentación que evidencie la finalización.
e. La Organización de Juegos debe mantener registros de acciones correctivas, incluyendo evidencia objetiva, durante al menos tres años, a menos que el organismo regulador especifique lo contrario.

2.7. Empresa de Seguridad Independiente (ISF)

La auditoría GISMS será realizada por personas con calificaciones suficientes, lo que significa que la ISF contratará a personas suficientemente calificadas, competentes y experimentadas. Estas personas deberán:

a. Tener una formación académica pertinente o proporcionar de otra manera las cualificaciones pertinentes para evaluar a las 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 auditoría GISMS:
   i. Auditor Líder ISO/IEC 27001;
   ii. Auditor Certificado de Sistemas de Información (CISA);
   iii. Gerente Certificado de Seguridad de la Información (CISM);
   iv. Profesional Certificado en Seguridad de Sistemas de Información (CISSP);
c. Tener al menos cinco años de experiencia en la realización de auditorías GISMS dentro de la industria del juego; y
d. Cumplir con cualquier otro requisito prescrito por el organismo regulador.

APÉNDICE: CONTROLES DE SEGURIDAD DE LA INFORMACIÓN DE JUEGO (GIS)

A. Adopción de Controles de Seguridad Críticos de CIS

Para establecer una línea de base clara y razonable para los controles comunes de GIS, el GLI-GSF incorpora por referencia los siguientes controles de los Controles de Seguridad Críticos del Centro para la Seguridad de Internet (CIS), Versión 8, que deben ser cumplidos por cada Organización de Juego (Empresa).

NOTA: El documento completo de controles críticos de seguridad del CIS está disponible de forma gratuita en www.cisecurity.org.

1	**Inventario y Control de Activos Empresariales**
1.1	Establecer y Mantener un Inventario Detallado de Activos Empresariales
1.2	Abordar los Activos no Autorizados
2	**Inventario y Control de Activos de Software**
2.1	Establecer y Mantener un Inventario de Software
2.2	Asegúrese de que el Software Autorizado sea Compatible Actualmente
2.3	Abordar el Software no Autorizado
3	**Protección de Datos**
3.1	Establecer y Mantener un Proceso de Gestión de Datos
3.2	Establecer y Mantener un Inventario de Datos
3.4	Aplicar la Retención de Datos
3.5	Eliminar los Datos de Forma Segura
3.6	Cifrar los Datos en los Terminales de los Usuarios
3.7	Establecer y Mantener un Esquema de Clasificación de Datos
3.9	Cifrar Datos en Medios Extraíbles
3.10	Cifrar Datos Confidenciales en Tránsito
3.11	Cifrar Datos Confidenciales en Reposo
3.14	Registrar el Acceso a Datos Confidenciales
4	**Configuración Segura de Activos y Software de la Empresa**
4.1	Establecer y Mantener un Proceso de Configuración Seguro
4.2	Establecer y Mantener un Proceso de Configuración Seguro para la Infraestructura de Red
4.3	Configurar el Bloqueo Automático de Sesiones en Activos Empresariales
4.4	Implementar y Administrar un Firewall en los Servidores
4.6	Gestionar de Forma Segura los Activos y el Software de la Empresa
4.7	Administrar Cuentas Predeterminadas en Activos y Software de la Empresa
4.8	Desinstalar o Deshabilitar Servicios Innecesarios en los Activos y el Software de la Empresa
4.9	Configuración de Servidores DNS de Confianza en Activos Empresariales
4.10	Aplicar el Bloqueo Automático de Dispositivos en Dispositivos Portátiles de Terminal de Usuario
5	**Gestión de Cuentas**
5.1	Establecer y Mantener un Inventario de Cuentas
5.2	Usar Contraseñas Únicas
5.3	Desactivar Cuentas Inactivas

5.4	Restringir los Privilegios de Administrador a Cuentas de Administrador Dedicadas
5.5	Establecer y Mantener un Inventario de Cuentas de Servicio
5.6	Centralizar la Gestión de Cuentas
6	**Gestión del Control de Acceso**
6.1	Establecer un Proceso de Concesión de Acceso
6.2	Establecer un Proceso de Revocación de Acceso
6.3	Requerir MFA para Aplicaciones Expuestas Externamente
6.4	Requerir MFA para el Acceso Remoto a la Red
6.5	Requerir MFA para el Acceso Administrativo
6.7	Centralizar el Control de Acceso
6.8	Definir y Mantener el Control de Acceso Basado en Roles
7	**Gestión Continua de Vulnerabilidades**
7.1	Establecer y Mantener un Proceso de Gestión de Vulnerabilidades
7.2	Establecer y Mantener un Proceso de Corrección
7.3	Realizar una Gestión Automatizada de Parches del Sistema Operativo
7.4	Realizar una Gestión Automatizada de Parches de Aplicaciones
7.5	Realizar Análisis Automatizados de Vulnerabilidades de los Activos Internos de la Empresa
7.6	Realizar Análisis Automatizados de Vulnerabilidades de Activos Empresariales Expuestos Externamente
7.7	Corrección de Vulnerabilidades Detectadas
8	**Gestión de Registros de Auditoría**
8.1	Establecer y Mantener un Proceso de Gestión de Registros de Auditoría
8.2	Recopilación de Registros de Auditoría
8.3	Garantizar un Almacenamiento Adecuado de los Registros de Auditoría
8.4	Estandarizar la Sincronización Horaria
8.5	Recopilar Registros de Auditoría Detallados
8.9	Centralizar los Registros de Auditoría
8.10	Conservar Registros de Auditoría
8.11	Realizar Revisiones de Registros de Auditoría
8.12	Recopilación de Registros de Proveedores de Servicios
9	**Protecciones de Correo Electrónico y Navegador Web**
9.1	Asegúrese de Usar Solo Navegadores y Clientes de Correo Electrónico Totalmente Compatibles
9.2	Usar Servicios de Filtrado de DNS
9.7	Implementar y Mantener Protecciones Antimalware para Servidores de Correo Electrónico
10	**Defensas Contra Malware**
10.1	Implementación y Mantenimiento de Software Antimalware
10.2	Configurar Actualizaciones Automáticas de Firmas Antimalware
10.6	Administrar de Forma Centralizada el Software Antimalware
10.7	Usar Software Antimalware Basado en el Comportamiento
11	**Recuperación de Datos**
11.1	Establecer y Mantener un Proceso de Recuperación de Datos
11.2	Realizar Copias de Seguridad Automatizadas

11.3	Proteger los Datos de Recuperación
11.4	Establecer y Mantener una Instancia Aislada de Datos de Recuperación
11.5	Recuperación de Datos de Prueba
12	**Gestión de la Infraestructura de Red**
12.1	Asegúrese de que la Infraestructura de Red esté Actualizada
12.2	Establecer y Mantener una Arquitectura de Red Segura
12.3	Gestionar de Forma Segura la Infraestructura de Red
12.4	Establecer y Mantener Diagrama(s) de Arquitectura
12.6	Uso de Protocolos Seguros de Gestión de Red y Comunicación
13	**Monitoreo y Defensa de Redes**
13.1	Centralizar las Alertas de Eventos de Seguridad
13.2	Implementar una Solución de Detección de Intrusiones Basada en Host
13.3	Implementar una Solución de Detección de Intrusiones en la Red
13.4	Realizar Filtrado de Tráfico Entre Segmentos de Red
13.7	Implementar una Solución de Prevención de Intrusiones Basada en Host
13.8	Implementar una Solución de Prevención de Intrusiones en la Red
13.9	Implementar el Control de Acceso a Nivel de Puerto
13.10	Realizar Filtrado de la Capa de Aplicación
14	**Capacitación en Habilidades y Concienciación en Seguridad**
14.1	Establecer y Mantener un Programa de Concienciación Sobre Seguridad
14.2	Capacitar a los Miembros de la Fuerza Laboral para que Reconozcan los Ataques de Ingeniería Social
14.3	Capacitar a los Miembros de la Fuerza Laboral Sobre las Mejores Prácticas de Autenticación
14.4	Capacitar a la Fuerza Laboral Sobre las Mejores Prácticas de Manejo de Datos
14.6	Capacitar a los Miembros de la Fuerza Laboral Sobre el Reconocimiento y la Notificación de Incidentes de Seguridad
14.9	Llevar a Cabo una Formación en Materia de Seguridad y Formación en Habilidades Específicas para Cada Función
15	**Gestión de Proveedores de Servicios**
15.1	Establecer y Mantener un Inventario de Proveedores de Servicios
15.2	Establecer y Mantener una Política de Gestión de Proveedores de Servicios
15.3	Clasificar Proveedores de Servicios
15.4	Asegúrese de que los Contratos de los Proveedores de Servicios Incluyan Requisitos de Seguridad
15.5	Evaluar a los Proveedores de Servicios
15.6	Supervisar a los Proveedores de Servicios
15.7	Retirar de Forma Segura a los Proveedores de Servicios
16	**Seguridad del Software de la Aplicación**
16.1	Establecer y Mantener un Proceso Seguro de Desarrollo de Aplicaciones
16.2	Establecer y Mantener un Proceso para Aceptar y Abordar las Vulnerabilidades del Software
16.3	Realizar un Análisis de la Causa Raíz de las Vulnerabilidades de Seguridad
16.4	Establecer y Administrar un Inventario de Componentes de Software de Terceros
16.5	Utilizar Componentes de Software de Terceros Actualizados y de Confianza
16.6	Establecer y Mantener un Sistema y un Proceso de Clasificación de Severidad para las Vulnerabilidades de las Aplicaciones

16.8	Sistemas de Producción y no Producción Separados
16.9	Capacitar a los Desarrolladores en Conceptos de Seguridad de Aplicaciones y Codificación Segura
16.12	Implementación de Comprobaciones de Seguridad a Nivel de Código
16.13	Realizar Pruebas de Penetración de Aplicaciones
17	**Gestión de la Respuesta a Incidentes**
17.1	Designar Personal para Gestionar los Incidentes
17.2	Establecer y Mantener Información de Contacto para Informar Incidentes de Seguridad
17.3	Establecer y Mantener un Proceso Empresarial para Informar de Incidentes
17.4	Establecer y Mantener un Proceso de Respuesta a Incidentes
17.5	Asignar Roles y Responsabilidades Clave
17.6	Definir Mecanismos de Comunicación Durante la Respuesta a Incidentes
17.7	Realizar Ejercicios Rutinarios de Respuesta a Incidentes
17.8	Realizar Revisiones Posteriores al Incidente
17.9	Establecer y Mantener Límites de Incidentes de Seguridad
18	**Pruebas de Penetración**
18.1	Establecer y Mantener un Programa de Pruebas de Penetración
18.2	Realizar Pruebas Periódicas de Penetración Externa
18.3	Corregir los Resultados de las Pruebas de Penetración
18.4	Validar las Medidas de Seguridad
18.5	Realizar Pruebas Periódicas de Penetración Interna

B. Controles Comunes Adicionales de GIS

Además de los controles de seguridad críticos de CIS adoptados anteriormente, los siguientes controles comunes GIS adicionales se aplican a los GPE utilizados para todas las formas de juego.

[Se incluirá en el próximo período de comentarios]

DEFINICIONES DE TÉRMINOS

Término	Descripciones
Acceso	Posibilidad de hacer uso de cualquier recurso de la 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.
Protocolo de resolución de direcciones (ARP)	Protocolo utilizado para traducir direcciones IP en direcciones MAC para admitir la comunicación en una red de área local inalámbrica o cableada.
Controles administrativos	Políticas, procedimientos y directrices implementados por una Organización de Juegos para gestionar sus GISMS.
Estándares de cifrado avanzados (AES)	Cifrado de bloques simétricos 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.
Auditoría	Un registro que muestra quién ha accedido a un sistema y qué operaciones ha realizado el usuario durante un período determinado.
Autenticación	Verificar la identidad de un usuario, proceso, paquete de software o dispositivo, a menudo como requisito previo para permitir el acceso a los recursos de la GPE
Copia de seguridad	Una copia de los archivos y programas realizados para facilitar la recuperación si es necesario.
Biometría	Un dato de identificación biológica, como huellas dactilares o patrones de retina.
Puente	Divide las redes para reducir el tráfico general de la red. Un puente permite o impide que los datos pasen a través de él mediante la lectura de la dirección MAC.
Plan de Continuidad del Negocio y Recuperación ante Desastres	Un plan para procesar aplicaciones críticas y prevenir la pérdida de datos en caso de una falla importante de hardware o software o la destrucción de las instalaciones.
Envenenamiento de caché	Un ataque en el que el atacante inserta datos corruptos en la base de datos de caché del Servicio de nombres de dominio (DNS).
Tecnología de las Comunicaciones	Cualquier método utilizado, y los componentes empleados, para facilitar la transmisión y recepción de información, incluida la transmisión y recepción por sistemas que utilizan redes alámbricas, inalámbricas, por cable, de radio, de microondas, de luz, de fibra óptica, de satélite o de datos informáticos, incluidas Internet e intranets.
Cumple	Se consideró que la política y las pruebas examinadas cumplían plenamente con el GLI-GSF.
Plan de contingencia	Política y procedimientos de administración diseñados para mantener o restaurar las operaciones de juego, posiblemente en una ubicación alternativa, en caso de emergencias, fallas del sistema o desastres.
Componente crítico del sistema	Cualquier hardware, software, tecnología de comunicaciones, otros equipos o componentes implementados en una GPE para permitir la participación de los usuarios en los juegos, y cuya falla o compromiso pueda conducir a la pérdida de los derechos de los usuarios, ingresos gubernamentales o acceso no autorizado a los datos utilizados para generar informes para el organismo regulador. Ejemplos de componentes críticos del sistema incluyen, pero no se limitan a:

Término	Descripciones
	• Componentes que registran, almacenan, procesan, comparten, transmiten o recuperan datos sensibles. • 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. • 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 los juegos o a las operaciones del sistema. • Puntos de entrada y salida de los componentes anteriores, incluidos otros sistemas que se comunican directamente con los componentes críticos del sistema. • Tecnología de las comunicaciones y redes que transmiten datos sensibles. • Redes y sistemas corporativos que interactúan con la GPE y desde los cuales los atacantes podrían usar para moverse lateralmente hacia la GPE, incluidas las redes de los casinos corporativos y las redes corporativas de los operadores en línea.
Integridad de los datos	La propiedad de que los datos son precisos y coherentes y no han sido alterados de manera no autorizada durante el almacenamiento, durante el procesamiento y mientras están en tránsito.
Denegación de servicio distribuido (DDoS)	Un tipo de ataque en el que se utilizan varios 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 hacker en el ataque distribuido.
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.
Dominio	Un grupo de equipos y dispositivos en una red que se administran como una unidad con reglas y procedimientos comunes.
Protocolo de configuración dinámica de host (DHCP)	Un servicio de red que permite a los dispositivos solicitar una configuración desde un punto central. Primero, una solicitud se transmite a través del segmento de red, luego los servidores responden a esa máquina específica con una dirección, por cuánto tiempo es válida esa dirección y otros detalles pertinentes.
Ancho de banda efectivo	La cantidad de datos que realmente se pueden transferir a través de una red por unidad de tiempo. El ancho de banda efectivo a través de Internet suele ser considerablemente menor que el ancho de banda de cualquiera de los enlaces constituyentes.
Encriptación	La conversión de datos en un formulario, llamado texto cifrado, que no puede ser fácilmente entendido por personas no autorizadas.
Clave de cifrado	Una clave criptográfica que se ha cifrado para ocultar el valor del texto sin formato subyacente.
Cortafuegos	Un componente de un sistema informático o red que está diseñado para bloquear el acceso o el tráfico no autorizados y, al mismo tiempo, permitir la comunicación externa.
Seguridad de la información de juego (GIS)	Proteger los datos confidenciales y los componentes críticos del sistema contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados con el fin de proporcionar integridad, confidencialidad y disponibilidad.

Término	Descripciones
Sistema de gestión de seguridad de la información del juego (GISMS)	Un sistema de gestión definido y documentado que consiste en un conjunto de políticas, procesos y sistemas para gestionar los riesgos de los datos de la organización, con el objetivo de garantizar niveles aceptables de riesgo GIS.
Portal	Cualquier dispositivo, sistema o aplicación de software que pueda realizar la función de traducir datos de un formato a otro. La característica clave de un portal de enlace es que convierte el formato de los datos, no los datos en sí.
Política de GIS	Un documento que delinea la estructura de gestión de la seguridad y asigna claramente las responsabilidades de seguridad y sienta las bases necesarias para medir de forma fiable el progreso y el cumplimiento.
Incidente GIS	Un suceso que real o potencialmente pone en peligro la confidencialidad, integridad o disponibilidad de una GPE o de los datos confidenciales que la GPE procesa, almacena o transmite, o que constituye una violación o amenaza inminente de violación de las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable.
Plan de respuesta a incidentes GIS	La documentación de un conjunto predeterminado de instrucciones o procedimientos cuando se encuentra un ciberataque malicioso contra el GPE de una organización de juegos
Pertenencia a grupos	Un método de organización de cuentas de usuario en una sola unidad (por puesto de trabajo) mediante el cual el acceso a las funciones del sistema puede modificarse a nivel de unidad y los cambios surten efecto para todas las cuentas de usuario asignadas a la unidad.
Algoritmo hash	Función que convierte una cadena de datos en una salida de cadena alfanumérica de longitud fija.
Protocolo de transporte de hipertexto (HTTP)	El protocolo subyacente utilizado para definir cómo se formatean y transmiten los mensajes, y qué acciones deben realizar los servidores y navegadores en respuesta a varios comandos.
Concentrador (hub)	Conecta dispositivos en una red de par trenzado. Una hub no realiza ninguna tarea además de la regeneración de señales.
Sistema de detección de intrusos/Sistema de prevención de intrusiones (IDS/IPS)	Un sistema que inspecciona toda la actividad de la red entrante y saliente e identifica patrones sospechosos que pueden indicar un ataque a la red o al sistema por parte de alguien que intenta entrar en un sistema o ponerlo en peligro. 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 su sistema.
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.
Seguridad IP (IPSec)	Un conjunto de protocolos para proteger las comunicaciones de Protocolo de Internet (IP) mediante la autenticación y el cifrado de cada paquete IP de un flujo de datos. IPsec también incluye protocolos para establecer la autenticación mutua entre los agentes al inicio de la sesión y la negociación de las claves criptográficas que se utilizarán durante la sesión.
Kerberos	Protocolo de autenticación de red diseñado para proporcionar una autenticación sólida para aplicaciones cliente/servidor mediante criptografía de clave secreta.
Clave	Valor utilizado para controlar las operaciones criptográficas, como el descifrado, cifrado, generación de firmas o verificación de firmas.
Gestión de claves	Actividades que impliquen el manejo de claves criptográficas 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.

Término	Descripciones
Utilización de enlaces	El porcentaje de tiempo que un enlace de comunicaciones está involucrado en la transmisión de datos.
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.
Malware	Un programa que se inserta en un sistema, generalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad 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"	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.
No conformidad mayor (MaNC)	Se ha identificado una falla fundamental (sistemática) que afecta a varios controles y significa que no se pueden cumplir las políticas generales de seguridad. Puede ser: • Una serie de no conformidades menores contra un control pueden representar una falla total del sistema y, por lo tanto, considerarse una no conformidad mayor; o • Cualquier no conformidad que resulte en el probable envío de un producto no conforme. Una condición que puede resultar en la falla o reducir materialmente la usabilidad de los productos o servicios para su propósito previsto; o • Es probable que una no conformidad que el juicio y la experiencia indiquen resulte en la falla del sistema o reduzca materialmente su capacidad para asegurar procesos y productos controlados. Hasta que se resuelva, un problema de este tipo normalmente significará que la Organización de Juego no cumple con el GLI-GSF.
Autenticación de mensajes	Medida de seguridad destinada a establecer la autenticidad de un mensaje por medio de un autenticador dentro de la transmisión derivada de ciertos elementos predeterminados del propio mensaje.
No conformidad menor (MiNC)	Un control no se ha abordado o no cumple con el GLI-GSF (no sistemático) y que el juicio y la experiencia indican que no es probable que resulte en la falla del sistema o reduzca su capacidad para asegurar procesos o productos controlados. Puede ser: • Una falla en alguna parte del sistema en relación con un control; o • Un solo lapso observado en el seguimiento de un elemento del sistema. Un curso de acción para remediar esto debe proporcionarse con un cronograma apropiado.
Código móvil	Código ejecutable que se mueve de un equipo a otro, incluyendo tanto código legítimo como código malicioso como virus informáticos.
Autenticación multifactor (MFA)	Un tipo de autenticación que utiliza dos o más de los siguientes elementos para verificar la identidad de un usuario: • Información conocida solo por el usuario (por ejemplo, una contraseña, un patrón 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, reconocimiento facial o de voz).
Equipos de comunicación de red (NCE)	Uno o más dispositivos que controlan la comunicación de datos en un sistema, incluidos, entre otros, cables, conmutadores, puentes, concentradores, enrutadores, puntos de acceso inalámbricos y teléfonos.
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.

Término	Descripciones
Observación (OBS)	Existe una política, pero no cumple plenamente con el GLI-GSF o la evidencia de respaldo (o la falta de ella) planteó posibles preocupaciones. Cualquier problema que pueda convertirse en una no conformidad si no se trata hasta la próxima auditoría se marca con este estado.
Oportunidades de Mejora (OFI)	Estas oportunidades ayudan a mejorar el sistema en su conjunto o los procesos nombrados. Sin embargo, si se deben mejorar ciertos aspectos que generalmente cumplen con los requisitos del GLI-GSF, entonces se marcan con este estado.
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 confidenciales que podrían usarse para identificar a un usuario en particular. Los ejemplos incluyen un nombre legal, fecha de nacimiento, lugar de nacimiento, número de seguro social (o número de identificación gubernamental equivalente), número de licencia de conducir, número de pasaporte, dirección residencial, número de teléfono, dirección de correo electrónico, número de instrumento de débito, número de tarjeta de crédito, número de cuenta bancaria u otra información personal si lo define el organismo regulador.
Número de identificación personal (PIN)	Un código numérico asociado a un individuo y que permite el acceso seguro a un dominio, cuenta, red, sistema, etc.
Controles Físicos y Ambientales	Las medidas implementadas para proteger los activos físicos, las instalaciones y las condiciones ambientales que albergan los sistemas e infraestructura del Entorno de Producción del Juego.
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 entran o salen de una red, 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	Conjunto de reglas y convenciones que especifican el intercambio de información entre dispositivos, a través de una red u otro medio.
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 utiliza la dirección de red configurada por software para tomar decisiones de reenvío.
Protocolo de comunicación segura	Un protocolo de comunicación que proporciona la confidencialidad, autenticación y protección de la integridad del contenido adecuadas.
Secure Shell (SSH)	Permite tunelizar cualquier otro protocolo de forma segura.
Certificado de seguridad	Información, a menudo almacenada como un archivo de texto que utiliza el protocolo Transport Socket Layer (TSL) para establecer una conexión segura. Para que se cree una conexión TSL, ambas partes deben tener un certificado de seguridad válido.
Datos confidenciales	Información como PII, datos de juego, números de validación, credenciales de autenticación, PIN, contraseñas, semillas y claves seguras, y otros datos que se manejarán de manera segura.
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 programas informáticos que se ejecutan para atender las solicitudes de otros programas ("clientes").

Término	Descripciones
Identificador de conjunto de servicios (SSID)	Nombre que identifica una LAN inalámbrica 802.11 determinada.
Código de shell	Un pequeño fragmento de código utilizado como carga útil en la explotación de la seguridad. Shellcode explota la vulnerabilidad y permite a un atacante la capacidad de reducir la seguridad de la información de un sistema.
Protocolo simple de administración de red (SNMP)	Protocolo utilizado para configurar, ver y, en general, administrar dispositivos en red. Las impresoras en red, conmutadores, etc. a menudo implementan este protocolo de forma predeterminada.
Ingeniería Social	Un intento de engañar a alguien para que revele información (por ejemplo, una contraseña) que puede usarse para atacar sistemas o redes. Los ataques de ingeniería social incluyen intrusiones no técnicas en un GPE utilizando información adquirida a través de la interacción humana y se basan en trucos que se aprovechan de que un individuo no esté familiarizado con la tecnología y los protocolos emergentes.
Código fuente	Texto de la lista de comandos que se compilarán o ensamblarán en un programa informático ejecutable.
Protocolo sin estado	Un esquema de comunicaciones que trata cada solicitud como una transacción independiente que no está relacionada con ninguna solicitud anterior, de modo que la comunicación consta de pares independientes de solicitudes y respuestas.
Interruptor	Conecta dispositivos en una red 802.3. Un interruptor reenvía los datos a su destino mediante la dirección MAC incrustada en cada paquete.
Administrador de Sistemas	La(s) persona(s) responsable(s) de mantener el funcionamiento estable de la GPE (incluida la infraestructura de software y hardware y el software de aplicación).
Controles técnicos	Los mecanismos de seguridad implementados dentro de los sistemas y la infraestructura del entorno de producción del juego para proteger contra el acceso no autorizado, violaciones de datos y otras amenazas de seguridad.
Amenaza	Cualquier circunstancia o evento con el potencial de afectar negativamente las operaciones de la red (incluida la misión, funciones, imagen o reputación), activos o personas a través de un sistema mediante el acceso no autorizado, la destrucción, divulgación, modificación de la información y/o denegación de servicio; la posibilidad de que una fuente de amenaza explote con éxito una vulnerabilidad en particular; cualquier peligro potencial para una red que alguien o algo pueda identificar como vulnerable y, por lo tanto, tratar de explotar.
Sello de tiempo	Un registro del valor actual de la fecha y la hora que se agrega a un mensaje en el momento en que se crea el mensaje.
Protocolo de control de transmisión/Protocolo de Internet (TCP/IP)	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.
Verificación	Garantizar, mediante la comprobación de la firma electrónica, que cualquier paquete de software es una copia auténtica del software creado por su fabricante y, en su caso, una copia exacta del software certificada por el Laboratorio de Pruebas Independiente (ITL por sus siglas en inglés).
Control de versiones	El método por el cual se verifica que los componentes críticos del sistema aprobados en evolución funcionan en un estado aprobado.
Red privada virtual (VPN)	Una red lógica que se establece sobre una red física existente y que normalmente no incluye todos los nodos presentes en la red física.
Virus	Un programa autorreplicante, normalmente con intenciones maliciosas, que se ejecuta y se propaga modificando otros programas o archivos.

Término	Descripciones
Escáner de virus	Software utilizado para prevenir, detectar y eliminar virus informáticos, incluidos malware, gusanos y troyanos.
Vulnerabilidad	Software, hardware u otras debilidades en una red o sistema que pueden proporcionar una "puerta" a la introducción de una amenaza.
Apuesta	Cualquier compromiso de créditos o dinero por parte del cliente que tenga un impacto en el resultado del juego.
Protocolo equivalente por cable (WEP)	Un algoritmo que se rompe fácilmente y, por lo tanto, está en desuso 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 determinadas circunstancias, pero las frases de contraseña suficientemente complejas son lo suficientemente seguras para la mayoría de los usos.