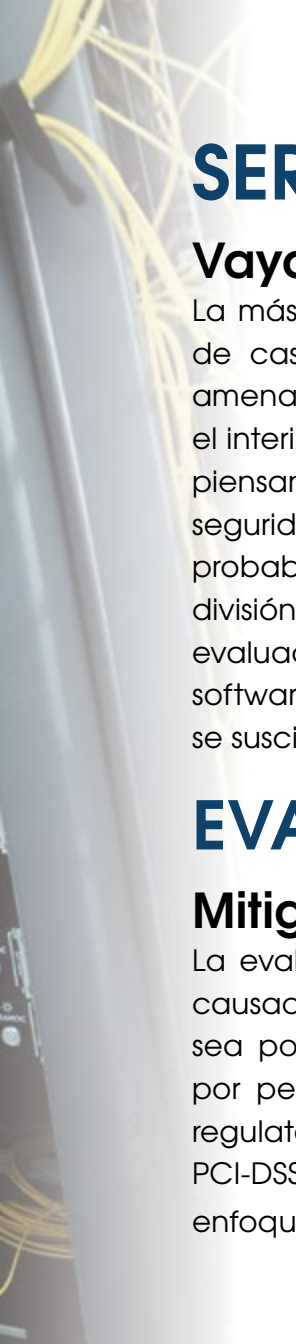

GLI®
SERVICIOS DE CAMPO
Protegiendo la Seguridad antes de que las amenazas se presenten



SERVICIOS DE CAMPO

Vaya más allá de lo superficial

La más peligrosa suposición que pueden hacer los reguladores y operadores de casino es que sus sistemas informáticos son seguros. Sin embargo, las amenazas a la seguridad pueden surgir en cualquier momento, tanto desde el interior como desde el exterior de su casino. La mayoría de las personas solo piensan en los hackers informáticos cuando ocurren incidentes vinculados a la seguridad, como violaciones externas, pero las estadísticas indican que es más probable que las amenazas provengan desde el interior de la organización. La división Bulletproof Solutions de Gaming Laboratories International (GLI®) ofrece evaluaciones de riesgos para redes, inspecciones a los sistemas y auditorías al software para identificar amenazas y reducir el riesgo antes de que los problemas se susciten.

EVALUACIÓN DE RIESGOS DE REDES

Mitigando su riesgo

La evaluación de redes puede ayudar a identificar los riesgos de seguridad causados por vulnerabilidades comunes de software, internas ó externas ya sea por amenazas que existen anónimamente en Internet o las generadas por personal interno. Este servicio difiere de las auditorías de cumplimiento regulatorio, como la llevada a cabo para la industria de las tarjetas de pago PCI-DSS, dado que únicamente se centra en criterios específicos y no en el enfoque holístico e integral de la gestión de seguridad.

Limitando la exposición innecesaria

Cualquier dispositivo conectado a la red puede ser vulnerable, como lo son: los medios de almacenamiento de respaldos, impresoras multifuncionales, servidores de redes y teléfonos inteligentes solo por mencionar algunos. GLI verificará la seguridad de su operación exponiendo las debilidades mediante ataques informáticos reales, lo que garantiza que los controles de las redes funcionen en toda la organización. De acuerdo a los resultados obtenidos, nuestro equipo de expertos recomendará soluciones para mitigar el riesgo.

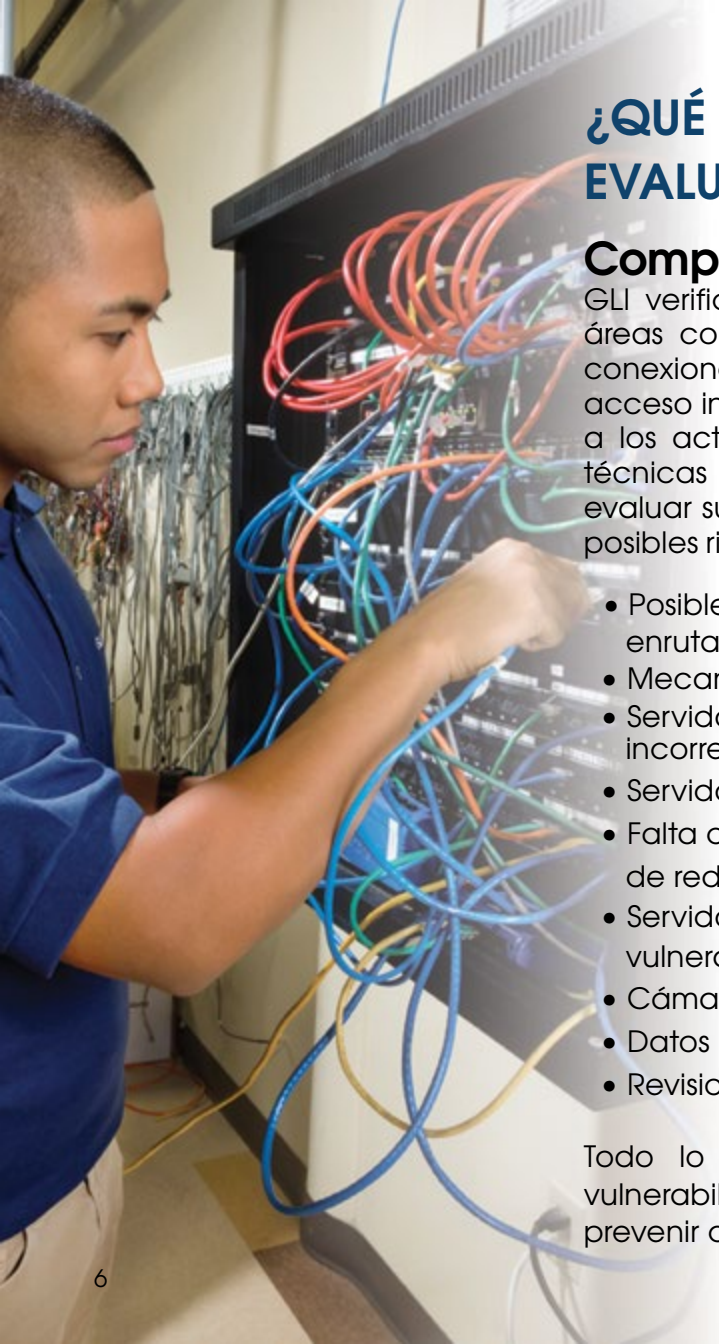
Después de realizar numerosas evaluaciones de riesgos de redes en múltiples casinos, nuestra experiencia ha identificado las vulnerabilidades más comunes que son las siguientes:

- Seguridad inalámbrica mal gestionada
- Controladores de dominios sin revisiones
- Deficiencia en la protección a las Bases de datos
- Servicios web no asegurados
- Cámaras de seguridad no protegidas

Manipulación de vulnerabilidades

Entonces, ¿qué implica esto para usted? Todo. La manipulación de vulnerabilidades puede permitir a un hacker aprovecharse de sus sistemas y poner en riesgo sus datos de distintas formas. Estas pueden incluir:

- Robo de información personal (p. ej., licencia de conducir o información de cuentas de jugadores)
- Manipulación de información de puntos de jugadores
- Control de los sistemas de cámaras de seguridad
- Control de los sistemas de redes
- Integridad comprometida de los sistemas de correo electrónico
- Integridad comprometida de los datos de recursos humanos



¿QUÉ SUCEDE DURANTE UNA EVALUACIÓN DE RIESGOS DE REDES?

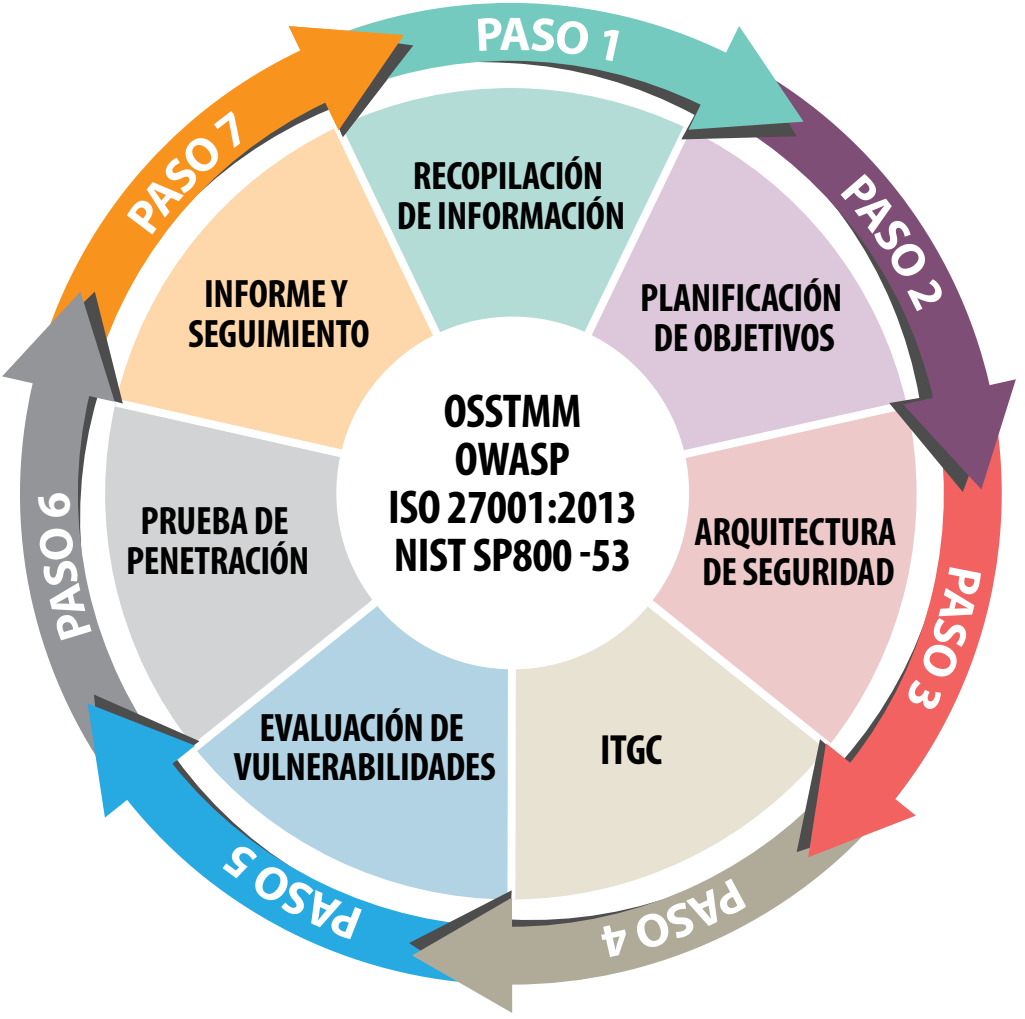
Comprendiendo los pesos y contrapesos

GLI verifica todas las áreas administrativas del sistema y áreas con accesibilidad a los jugadores para encontrar conexiones de redes abiertas y activas, así como puntos de acceso inalámbrico mal protegidos. Intentaremos acceder a los activos del casino mediante una combinación de técnicas y herramientas de software libre y comercial para evaluar su red, a fin de obtener un panorama claro de los posibles riesgos de redes que enfrenta su casino, entre ellos:

- Posible configuración inadecuada del cortafuegos y el enrutador en la arquitectura externa de la red
- Mecanismos de autenticación débiles
- Servidores de bases de datos configurados de forma incorrecta
- Servidores de archivos vulnerables
- Falta de revisión del protocolo simple de administración de red (SNMP)
- Servidores de dominio (DNS) y de correo electrónico vulnerables ó configurados de forma incorrecta
- Cámaras de seguridad IP vulnerables
- Datos de recursos humanos no protegidos
- Revisiones faltantes del proveedor

Todo lo anterior genera un informe que detalla las vulnerabilidades descubiertas y recomendaciones para prevenir dificultades a futuro.

EVALUACIÓN DE RIESGOS DE REDES



Identificando las amenazas antes de que ocurran

Las inspecciones a los sistemas, verifican que los archivos que están controlados y que se encuentran en un sistema en particular, coincidan con los que fueron ensayados anteriormente por un laboratorio de tercera parte independiente, también las inspecciones aseguran que estos archivos cumplan con un estándar en particular o un grupo de estándares jurisdiccionales. Se considera que los archivos están "controlados" después de analizar las funciones de dichos archivos con la participación del fabricante del sistema. A los archivos controlados se les otorga una firma exclusiva que permanece en la versión específica del mismo. Con las herramientas que se utilizaron originalmente para crear la firma, se genera y se verifica la firma ya en campo donde se usa el sistema en línea.

Manteniendo la honestidad del juego

Si la firma generada difiere de la carta de certificación, entonces uno de los archivos contiene una versión diferente a la presentada en dicha carta o los archivos se han sido modificados de alguna manera. Si se han modificado, los archivos se consideran "no certificados". Dependiendo de la función de cada archivo, los no certificados podrían poner en riesgo la integridad del sistema. Si todos los archivos coinciden con la carta de certificación, podemos constatar que el sistema fue probado en uno de los laboratorios de GLI.

ENSAYOS DE COMUNICACIONES

Garantizando que el juego es lo que se espera

No es posible que nos puedan vendar los ojos. Nuestros profesionales están capacitados para identificar las actividades sospechosas en todo el ciclo de vida de la implementación de los juegos. Los ensayos de comunicaciones se realizan en la sala del casino para garantizar que las máquinas de juegos de azar comunican la información de los contadores de forma correcta. Al mismo tiempo, estos ensayos también verifican que el sistema registre la información de manera adecuada.

Detectando las diferencias

Los inspectores de campo de GLI verifican el ingreso de billetes, el sistema "ticket-in/ticket-out" (TITO) y los créditos otorgados (solo en la máquina) para cada máquina que es ensayada. Los ensayos abarcan todos los juegos en la sala o una muestra aceptable de ellos y generalmente incluyen a todos los fabricantes, diferentes ubicaciones y diferentes monedas. Esta información se compara con el sistema en línea para garantizar que todos los registros se verificaron e ingresaron al sistema correctamente. Nuestros profesionales en ensayos se aseguran de que cada juego haga lo que se espera.

Si hay alguna discrepancia, la máquina o máquinas en cuestión vuelven a ensayarse para verificar la precisión y si la máquina falla por segunda vez, entonces la máquina de juego y el sistema en línea se analizarán en detalle para buscar discrepancias. Esta información se envía a las agencias pertinentes para su revisión.

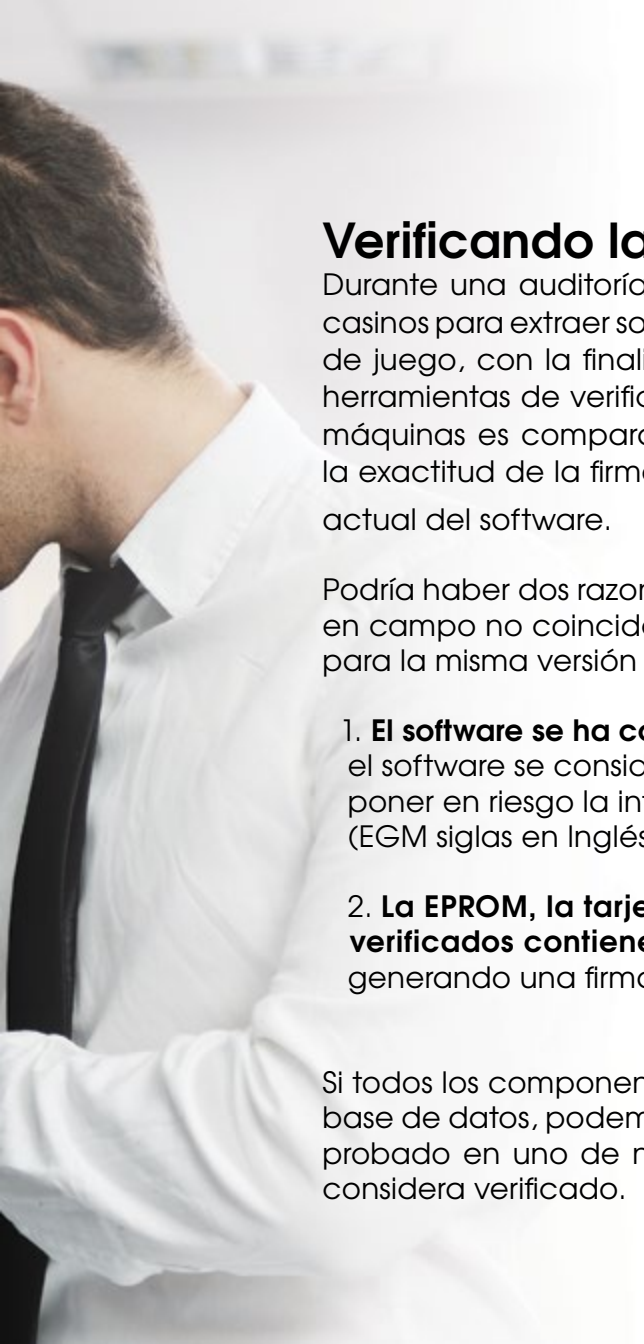
AUDITORÍAS DE SOFTWARE

Controlando el pulso del juego

Cuando GLI realiza una auditoría de software, el objetivo principal es verificar que cada componente del software crítico que se encuentra en una máquina en particular coincida con la misma versión que se ensayó en el laboratorio y que cumpla con un estándar en particular o un grupo de estándares jurisdiccionales. El software de juego se considera crítico tras analizar cómo controla el desempeño del juego y la funcionalidad del mismo.

Seguimiento de todas las partes móviles

Los componentes de software considerados importantes que deberían ensayarse incluyen los sistemas operativos (conocidos también como "programas principales"), que controlan a los contadores, la funcionalidad administrativa y los programas de juegos (conocidos también como "programas de personalidad"). Estos programas de personalidad controlan el desempeño del juego, su matemática y la información de la tabla de pagos. Otros componentes de software cuyos ensayos se consideran importantes en algunas jurisdicciones incluyen (sin carácter restrictivo) programas de comunicación, chips de BIOS, firmware de validadores de billetes y firmware de impresoras.



Verificando la exactitud

Durante una auditoría de software, GLI trabaja con el personal de los casinos para extraer software considerado importante de cada máquina de juego, con la finalidad de verificar su firma digital única, mediante herramientas de verificación de tercera parte. La firma obtenida en las máquinas es comparada con la base de datos de GLI para verificar la exactitud de la firma digital y para obtener el estado de aprobación actual del software.

Podría haber dos razones por las que una firma obtenida de un software en campo no coincide con la que registrada en nuestra base de datos para la misma versión del software:

1. **El software se ha corrompido o modificado.** Si este es el caso, el software se considera "no aprobado" y según su función, podría poner en riesgo la integridad de la máquina de juego electrónico (EGM siglas en Inglés).

2. **La EPROM, la tarjeta CF (Compact flash en Inglés) u otros medios verificados contienen las versiones incorrectas del software,** generando una firma incorrecta.

Si todos los componentes de software auditados coinciden con nuestra base de datos, podemos certificar que la EGM y todo su software se han probado en uno de nuestros laboratorios y por lo tanto el software se considera verificado.

INSPECCIÓN DE JUEGOS DE AZAR BASADOS EN EL SERVIDOR

Contenido para descargar, tecnología centralizada en el jugador, juegos basados en habilidades y mucho más

Las inspecciones de juegos basados en servidor consisten en investigar todos los servidores y sistemas informáticos relacionados con una red cerrada específica de área local (LAN). Solo se inspeccionará la funcionalidad. Para ello necesitaremos la siguiente información antes de realizar una inspección de juegos de azar basados en servidor:

- Tipo de fabricante del juego
- Versión específica del software instalado (o que se instalará)
- Equipos conectados en esa red específica
- Cantidad de juegos en la misma red

Adicionalmente, se realizarán ensayos de comunicaciones en por lo menos 10 juegos que se comunican directamente con el servidor.

INSPECCIÓN DE SERVIDORES

Optimizando su red en el casino

La inspección de servidores consiste en localizar y obtener una firma digital de los archivos controlados que se encuentran en el servidor ó en el conjunto de servidores. Los fabricantes deberán aplicar políticas al servidor para que no se permita la creación o eliminación de archivos adicionales en el servidor.

REVISIÓN FINAL

BULLETPROOF

Garantizando la calidad desde el principio hasta el fin

Toda la información obtenida durante la inspección se recopilará para una revisión final y un informe de inspección con los resultados será enviado al solicitante . El solicitante será responsable de hacer llegar los resultados a todas las partes interesadas.

GLI tiene el compromiso de ayudar a mantener seguros sus productos y equipos. Para obtener más información acerca de los servicios de campo Bulletproof Solutions, ensayos de redes o ensayos de penetración de redes, comuníquese con su representante de servicio al cliente local y consulte sobre la evaluación de riesgos de redes.

LOCACIONES EN TODO EL MUNDO

GLI®

MUCHO MÁS QUE SOLO ENSAYOS

GAMING LABORATORIES INTERNATIONAL®

SEDE MUNDIAL
600 Airport Road
Lakewood, NJ 08701 USA

T: 702.856.5822 Español
T: 732.942.3999 Inglés
F: 732.9420043

GLIespañol.com

El objetivo principal de GLI es ser el experto en cumplimiento y calidad global de confianza que nuestros clientes esperan, brindando un servicio de clase mundial y un valor inigualable.