SERIE DE ESTÁNDARES

GLI-21:

Sistemas Cliente - Servidor

Versión: 2.2

Fecha de Publicación: 6 de Septiembre de 2011

Esta página se dejo en blanco intencionalmente

ACERCA DE ESTE ESTÁNDAR

Este estándar ha sido producido por **Gaming Laboratories International, LLC** con el propósito de proporcionar certificaciones independientes a los fabricantes bajo este Estándar y cumplir con los requisitos establecidos en este documento.

El fabricante debe presentar el equipo con una petición de que sea certificado de acuerdo con este Estándar. Una vez certificado, **Gaming Laboratories International, LLC** suministrara un certificado de cumplimiento con evidencia de la certificación con este Estándar.

Esta página se dejo en blanco intencionalmente

Tabla de Contenido

Esta página se dejo en blanco intencionalmente

CAPITULO 1

1.0 VISIÓN GENERAL - ESTÁNDARES DE SISTEMAS CLIENTE - SERVIDOR

1.1 Introducción

1.1.1 Generalidades. **Gaming Laboratories International, LLC (GLI)** ha estado ensayando dispositivos de juegos desde el año 1989. A través de los años, hemos desarrollado una numerosa cantidad de estándares para jurisdicciones alrededor del mundo. En años recientes, muchas jurisdicciones han optado preguntar sobre los estándares técnicos de la industria sin tener que crear sus propios estándares. En adición, con la tecnología cambiante casi mensualmente, la nueva tecnología no se incorpora lo suficientemente rápido en los estándares existentes debido al largo proceso administrativo de crear regulaciones. Este documento, *Estándar 21 de GLI*, establecerá los estándares técnicos para los Sistemas Cliente-Servidor.

1.1.2 Historial Del Documento. Este documento es una composición de muchos estándares de alrededor del mundo. Algunos que GLI ha escrito y otros, como el Estándar Nacional de Australia y Nueva Zelandia, escrito por reguladores de la industria junto con laboratorios de ensayos y fabricantes de dispositivos de juegos. Nosotros hemos tomado cada de los documentos de estándares, combinando cada de las regulaciones exclusivas juntas, eliminando algunas regulaciones, y actualizando otras para que reflejen tanto el cambio en tecnología como el propósito de mantener un estándar objetivo y factual. A continuación, nosotros hemos listado dando crédito a las agencias cuyos documentos hemos repasado previo a escribir este estándar. Es la póliza de **Gaming Laboratories International, LLC** de actualizar este documento lo más a menudo posible, para que refleje los cambios de tecnología, procedimientos de ensayos o métodos para hacer fraude. Este documento será distribuido sin ningún costo a todos que lo soliciten. Este estándar y todos los otros pueden ser obtenidos descargando desde nuestro sitio web www.gaminglabs.com o escribiéndonos a:

Gaming Laboratories International, LLC
600 Airport Road
Lakewood, NJ 08701
(732) 942-3999 Tel
(732) 942-0043 Fax

1.2 Reconocimiento de otros Estándares Evaluados

1.2.1 Generalidades. Estos estándares han sido desarrollados evaluado y utilizando porciones de los documentos de las organizaciones listadas a continuación. Nosotros reconocemos a los reguladores que han ensamblado estos documentos y les agradecemos:

a) Oficina de Regulación de Juego de Queensland;
b) Departamento del Tesoro y Finanzas, División de Ingresos de Juego de Tasmania;
c) Oficina de Administración Financiera ACT ;
d) Departamento de Juegos y Carreras de Nueva Gales Del Sur;
e) Autoridad de Control de Casinos de Nueva Zelanda;
f) Departamento de Asuntos Internos, Juegos de Carreras y División de Censura de Nueva Zelanda;
g) Autoridad de Carreras y Juegos del Territorio de Norte;
h) Oficina del Comisionado de Licor y Juegos de Australia del Sur;
i) La Autoridad de Casinos y Juegos de Victoria;
j) Oficina de Juegos de Carreras y Licor del Oeste de Australia;
k) Oficina de Estándares De Sudáfrica;
l) La Junta de Control y Juego de Nevada;
m) Publicación Especial NIST 800-57 *Recomendaciones para Administraciones Claves – Parte 2: Buenas Prácticas para la Administración de Organizaciones Claves;*
n) Estándar Técnico Regulatorio 14 de Nevada; y
o) GSA G2S y S2S estándares de protocolos.

1.3 Propósito Del Estándar

1.3.1 Generalidades El propósito de este estándar técnico es lo siguiente:

a) Eliminar el criterio subjetivo en el análisis y certificación operacional de las terminales cliente de Juegos.

b) Solamente ensayar los criterios que impactan la credibilidad e integridad de la terminal cliente de juego tanto del punto de vista de colección de ingresos y como el punto de vista de juego del jugador.

c) Crear un estándar que asegure que los juegos basados en un servidor y soportados por un servidor son justos, seguros, y puedan ser auditables y operados correctamente.

d) Distinguir entre la política pública local y el criterio del Laboratorio. En GLI, nosotros creemos que es responsabilidad de cada jurisdicción local fijar su propia política pública con respecto al juego.

e) Reconocer que los ensayos no relacionados al juego (como ensayos de electricidad) no deben ser incorporados dentro de este estándar, sino dejados a Laboratorios especializados que se especializan en estos tipos de pruebas. Excepto donde se identifica específicamente en el estándar, las pruebas no son dirigidas a temas de salud o seguridad. Estos asuntos son responsabilidad del fabricante, comprador y operador del equipo.

f) Construir un estándar que pueda ser fácilmente cambiado o modificado para permitir nueva tecnología.

g) Construir un estándar que no especifique ningún método o algoritmo en particular. La intención es de permitir un amplio rango de métodos para ser utilizados en acorde a los estándares mientras que al mismo tiempo, apoyar el desarrollo de nuevos métodos.

1.3.2 Sin Limitación de Tecnología. Se debe tener precaución que este documento no sea leído de tal manera que limita la utilización de tecnología futura. Este documento no debe ser interpretado de manera que si la tecnología no está mencionada, entonces no es permitida.
Totalmente lo contrario, cuando alguna tecnología nueva es desarrollada, nosotros repasaremos este estándar, realizaremos cambios e incorporaremos nuevos estándares mínimos para la nueva tecnología.

1.4 Otros Documentos que Pueden Aplicar

Generalidades Por favor consulte nuestro sitio web www.gaminglabs.com por una lista completa de otros Estándares GLI disponibles, que también podrían aplicar.

1.5 Definición De Sistemas Cliente-Servidor

1.5.1 Generalidades. Un Sistema Cliente-Servidor (CSS, por sus siglas en inglés) puede ser definido separadamente ya sea como un Sistema de Juego Basado en Servidor (SBGS, por sus siglas en inglés) o un Sistema de Juego Respaldado por el Servidor (SSGS, por sus siglas en inglés). Ambos pueden ser definidos como la combinación de un Servidor Central, Dispositivos de Juego y todos los componentes de interfaz que funcionan colectivamente con el propósito de enlazar los dispositivos de juego con el servidor central para desempeñar una serie de funciones relacionadas con el juego, las cuales pueden incluir, pero no están limitadas a:

a) Descargar la lógica del juego a los Dispositivos de Juego;
b) Generación de Números Aleatorios en el Servidor Central;
c) Configuraciones del juego en el terminal ligero.

NOTA: La red de comunicaciones puede estar contenida en un solo lugar (LAN, por sus siglas en Inglés) o sobre una red de área amplia (WAN, por sus siglas en Inglés) a través de la cual un servidor en un solo lugar respalda dispositivos de juego en múltiples sitios.

1.5.1.1 Definición del Sistema de Juego Basado en Servidor (SBGS). La combinación de un servidor y terminales dispositivos de juego en donde el contenido completo o la porción integral del juego residen en el servidor. Este sistema trabaja colectivamente en una modalidad en la cual el dispositivo de juego no será capaz de funcionar cuando esté desconectado del sistema.

1.5.1.2 Definición del Sistema de Juego Respaldado por el Servidor (SSGS). La combinación de un servidor y un dispositivo(s) de juego que en su conjunto permiten la transferencia del programa de control completo y contenidos de juego a los dispositivos de juego con el propósito de descargar programas de control y otros recursos de software al dispositivo de juego intermitentemente. Los dispositivos de juego conectadas al sistema son capaces de operar independientemente del sistema una vez que el proceso de descarga ha sido completado. Esta configuración abarca casos donde el sistema puede tomar el control de los dispositivos

periféricos o equipos asociados considerados típicamente como parte de un dispositivo de juego convencional como un verificador de billetes o una impresora. En un Juego Respaldado por el Sistema, el resultado del juego es determinado por los dispositivos de juego conectadas al sistema y no por el sistema en sí. El dispositivo de juego es capaz de seguir funcionando aun si es desconectado del sistema.

1.6 Fases de los Ensayos

1.6.1 Generalidades. Las sumisiones CSS al Laboratorio de Pruebas serán realizadas en dos fases:

a) Dentro del entorno del laboratorio, y
b) En-sitio, luego de la instalación inicial del sistema para asegurar la configuración apropiada de las aplicaciones de seguridad.

NOTA: En adición a las pruebas en-sitio del sistema, el laboratorio debe proveer entrenamiento en esta nueva tecnología al regulador local, recomendar procedimientos de auditoría de campo, y asistencia con la compilación de controles internos, en caso de ser requeridos.

CAPITULO 2

2.0 REQUISITOS PARA LA COMUNICACIÓN

2.1 Introducción

2.1.1 Generalidades. Este capítulo se refiere a las comunicaciones entre el Servidor(es) de los Sistemas Cliente-Servidor (CSS), todos los componentes de interfaz y los dispositivos de juego utilizados en un ambiente de Sistemas Cliente-Servidor (CSS).

2.1.2 Protocolo de Comunicación. Cada componente de un Sistema Cliente-Servidor (CSS) debe funcionar como indica el protocolo de comunicación implementado. Todos los protocolos deben utilizar técnicas de comunicación que cuenten con una apropiada detección de errores y/o mecanismos de recuperación, los cuales son diseñados para prevenir intentos de manipulación. GLI recomienda firmemente un método de encriptación con semilla o algoritmos seguros. Cualquier otro método alternativo que se use será revisado caso por caso, con la aprobación del regulador.

2.1.3 Perdida de Comunicación. Para un Servidor de Juego Basado en Servidor (SBGS), un terminal debe ser considerado como no disponible si las comunicaciones del servidor o parte del sistema del dispositivo de juego se han interrumpido. Si un juego está en progreso, debe ser provisto un mecanismo para que el juego vuelva al punto donde se encontraba cuando la comunicación se perdió. Alternativamente, en un ambiente multi-jugador, una pérdida de la comunicación puede resultar en la cancelación del juego y la devolución de las apuestas a los jugadores.

En el caso de que los Dispositivos de Juego que hayan perdido la comunicación con el servidor, el Sistema Cliente-Servidor (CSS) deben proveer un medio, como el pago manual, para que los jugadores puedan cobrar los créditos indicados en el dispositivo de juego Basado en el Servidor en el momento en el que la comunicación fue interrumpida.

2.2 Sistema de Seguridad

2.2.1 Generalidades. En el evento de que el Sistema Cliente-Servidor (CSS) sea utilizado en conjunto con otros sistemas de red (networks) todas las comunicaciones, incluido el Acceso Remoto, deben pasar a través de por lo menos un firewall al nivel de aplicación aprobado y no tendrá la facilidad de permitir una ruta de red alterna. Si existe una ruta de red alterna para propósitos de redundancia, esta también debe pasar a través de por lo menos un firewall a nivel de aplicación.

NOTA: Cada Sistema Cliente-Servidor (CSS) sometido al Laboratorio de Pruebas será examinado cuidadosamente para asegurar que la configuración de campo propuesta es segura. El Laboratorio de Pruebas puede incluir recomendaciones de seguridad adicionales en la certificación final y entrenamiento de sitio a los reguladores, si es solicitado.

2.2.2 Registros de Auditoría de Firewall. La aplicación de Firewall debe mantener un registro de auditoría de la siguiente información y debe desactivar todas las comunicaciones y generar un evento de error si el registro de auditoría se llena:

a) Todos los cambios de configuración del firewall;
b) Todos los intentos de conexión con éxito o fallidos a través del firewall; y
c) Direcciones IP de inicio y destino, Número de Puerto y Direcciones MAC.

NOTA: Por favor tome nota, un parámetro configurable de 'intento de conexión fallido' puede ser utilizado para negar solicitudes de conexión adicionales cuando el umbral predefinido sea excedido. El administrador del sistema también debe ser notificado.

2.3 Acceso Remoto

2.3.1 Generalidades. Acceso Remoto es definido como cualquier acceso al sistema desde afuera del sistema de red confiable. El Acceso Remoto, donde sea permitido, deberá autentificar todo el sistema de cómputo basado en las configuraciones autorizadas del Sistema Cliente-Servidor (CSS) o aplicación de firewall que establezca una conexión con el Sistema Cliente-Servidor (CSS). La seguridad del Acceso Remoto será revisada caso por caso, en conjunto con la

tecnología actual y la autorización de la agencia regulatoria local. Los siguientes son requerimientos adicionales:

a) No autorizada la funcionalidad de administración remota de usuarios (agregar usuarios, cambio de permisos, etc.);
b) Acceso no autorizado a cualquier base de datos aparte del acceso de información usando funciones existentes; y
c) Acceso no autorizado al sistema operativo.

NOTE: GLI reconoce que el fabricante del sistema puede, según se necesite, acceder remotamente al Sistema Cliente-Servidor (CSS) y a sus componentes asociados con el propósito de dar servicio al producto y al cliente, si esto es permitido.

2.3.2 Auditoría de Acceso Remoto. El servidor del Sistema Cliente-Servidor (CSS) debe mantener un registro de actividad ya sea automáticamente, o permitiendo el ingreso manual de dicho registro describiendo toda información de Acceso Remoto que incluya:

a) Nombre de acceso;
b) Tiempo y fecha de cuando la conexión fue realizada;
c) Duración de la conexión; y
d) Actividad mientras esta registrado, incluyendo el acceso a áreas especificas y cambios que fueron realizados.

2.4 Comunicaciones de Red de Área Amplia

2.4.1 Generalidades. Las comunicaciones de Red de Área Amplia (WAN, por sus siglas en inglés) dentro del Sistema Cliente-Servidor (CSS) serán permitidas siempre que cumplan con las siguientes características:

a) La(s) jurisdicciones dentro del cual el Sistema Cliente-Servidor (CSS) opera no prohíban específicamente el uso del enlace de múltiples sitios;
b) Las comunicaciones sobre la Red de Área Amplia (WAN) sean seguras contra intrusiones, interferencias y espionajes a través de técnicas como por ejemplo el uso de Redes Privadas Virtuales (VPN, por sus siglas en inglés), encriptación, autentificaciones, etc.; y

c) Solo se utilicen sobre la Red de Área Amplia (WAN) funciones documentadas en el protocolo de comunicaciones utilizado. El protocolo deberá ser presentado al laboratorio de pruebas. La documentación del protocolo puede estar en partes múltiples como por ejemplo mecanismo de entrega y formatos de mensajes, etc.

CAPITULO 3

3.0 REQUISITOS DEL SERVIDOR CSS

3.1 Introducción

3.1.1 Generalidades. Esta sección cubre los elementos comunes de las operaciones "entre bastidores" de un Sistema Cliente-Servidor (CSS). El servidor(es) de juego puede ser localizado localmente, dentro de un solo establecimiento o instalación o puede ser localizado remotamente fuera del establecimiento a través de una Red de Área Amplia (WAN). En el caso donde un servidor del Sistema Cliente-Servidor (CSS) también realice tareas como las requeridas por otros sistemas, (por ejemplo, Sistemas de Monitoreo y Control En Línea, Sistemas de Validación de Boletos, etc.) esas porciones no aplicarán al documento de GLI-21 y podrían tener que ser evaluados con los estándares apropiados.

3.2 Servidores Múltiples

3.2.1 ***Generalidades***. Un Sistema Cliente-Servidor (CSS) puede en realidad estar hecho de una colección de servidores por razones de balanceo de cargas, redundancia o funcionalidad. Por ejemplo, podría haber dos o más servidores de juegos, un servidor financiero, servidor de monitoreo, servidor de descargas, etc. El sistema como conjunto, el cual podría ser una colección de tales servidores, debe reunir todos los requisitos de esta especificación pero no necesariamente cada servidor.

3.3 Operación General y Seguridad del Servidor

3.3.1 ***Generalidades***. Para un Sistema de Juego Basado en el Servidor, el Servidor de Juego deberá generar y transmitir datos de control, configuración e información a los Dispositivos de Juego, dependiendo de la actual implementación, como por ejemplo:

a) Movimiento de créditos,

b) Números Aleatorios,

c) Componentes del resultado de juego, como por ejemplo, bolas, naipes o posiciones de parada de rieles,
d) Resultados del juego actual, o
e) Actualización de los contadores de créditos para juegos ganados.

Para un Sistema de Juego Respaldado por el Servidor, el Servidor del Juego no participara en ningún proceso de determinación de juego, por ejemplo las funciones primarias serán la descarga de programas de control y otros recursos de software, o proveer comandos e instrucciones de control que puedan cambiar la configuración del software que ya ha sido descargado en el dispositivo de juego, en forma intermitente.

3.3.2 ***Seguridad***. Los servidores deben estar alojados en un cuarto de cómputo seguro o gabinetes asegurados con candado fuera de las terminales del jugador.

3.3.3 ***Protección contra Intrusiones***. Los servidores deben tener suficiente protección física/Lógica contra accesos no autorizados. Idealmente, el sistema requerirá proveer el acceso en conjunto pero no separados de la autoridad reguladora y el fabricante.

3.3.4 ***Requisitos del Acceso a la Configuración***. El menú de configuración/instalación del elemento de interfaz del CSS no debe estar disponible al menos que se utilice un método de acceso autorizado que es seguro.

3.3.5 ***Programación del Servidor***. No habrá medios disponibles para que un operador lleve a cabo una programación en el servidor en cualquier configuración, por ejemplo, el operador no podrá ejecutar un comando SQL para modificar la base de datos. Sin embargo es aceptable que los Administradores de la Red realicen un mantenimiento autorizado a la infraestructura de la red con derechos de acceso suficientes que incluyan el uso de comandos SQL que se encontraban previamente alojados en el sistema.

3.3.6 ***Protección contra Virus***. Es recomendable que todos los servidores y dispositivos del cliente deben contar con una protección contra virus adecuada donde sea aplicable.

3.3.7 ***Protección contra Copias***. Una protección contra copias, para prevenir la proliferación no autorizada o modificación del software, para servidores o clientes, puede ser implementada siempre y cuando que:

a) El método de protección contra copias este totalmente documentado y presentado al Laboratorio de Pruebas, quien verificara que la protección funciona como ha sido descrita; y
b) Cualquier dispositivo envuelto en hacer cumplir la protección contra copias puede ser verificado individualmente por la metodología descrita en la sección 3.7.2.

3.4 Comunicación Ethernet Inalámbrica

3.4.1 ***Generalidades***. Si se usara una solución de comunicaciones Ethernet inalámbrica, esta debe cumplir con las partes aplicables del estándar GLI-26 ‘Sistemas de Juegos Inalámbrico”.

3.5 Falla del Sistema

3.5.1 Generalidades. El CSS deberá ser diseñado para proteger la integridad de los datos importantes en la eventualidad de una falla. Los registros de auditoría, base de datos del sistema y cualquier otro dato importante debe ser almacenado utilizando métodos de protección razonables. Si se utilizan discos duros como medio de almacenamiento, se debe asegurar la integridad de los datos en el evento de una falla del disco. Los métodos aceptables incluirán, pero no estarán limitados a, múltiples discos duros en una configuración aceptable RAID, o replica/duplicado de datos entre dos o más discos duros. El método utilizado deberá proporcionar también un soporte abierto para copias de seguridad y restablecimiento. La implementación del esquema de copia de seguridad deberá ocurrir al menos una vez todos los idas, aunque todos los métodos deberán ser revisados caso por caso por el laboratorio de pruebas.

3.5.2 Requisitos para la Recuperación. En el evento de una falla catastrófica, cuando el CSS no pueda ser reiniciado de ninguna otra forma, deberá ser posible volver a cargar la base de datos desde el último punto de copia de seguridad viable y recuperar totalmente los contenidos de esa copia de seguridad; se recomienda que consista de al menos la siguiente información, donde sea aplicable:

a) Eventos significantes,

b) Información de auditoría,

c) Información del sitio especifico como la configuración del juego, cuentas de seguridad, etc.

3.6 Auto Monitoreo

3.6.1 Generalidades. El CSS debe implementar el auto monitoreo de todos los elementos de interfaz críticos (por ejemplo: servidores centrales, dispositivos de red, Firewall, enlaces a terceros, etc.) y tendrán la habilidad de notificar efectivamente al administrador del sistema de esta condición, siempre que la condición no sea catastrófica. El CSS deberá realizar esta operación con una frecuencia de al menos una vez cada 24 horas. La implementación de los esquemas de auto monitoreo serán revisados caso por caso por el laboratorio de pruebas. Adicionalmente, todos los elementos de interfaz críticos serán revisados caso por caso y se podría requerir la adopción de nuevas medidas por el sistema dependiendo de la severidad de la falla.

3.7 Verificación del Software del CSS

3.7.1 Componentes Controlados del Servidor

a) ***Generalidades***. Cada componente del CSS debe contar con un método para ser verificado a través de un proceso de verificación de tercer partido. El proceso de verificación de tercer partido no debe incluir ningún proceso o software de seguridad proporcionado por el sistema operativo o fabricante. Una validación secundaria puede usar software disponible comercialmente por el fabricante del sistema como parte de cualquier verificación secundaria:

b) El CSS debe ser capaz de verificar que todos los programas de control contenidos en el servidor o porción del sistema son copias autenticas de los componentes aprobados tanto automáticamente por lo menos una vez cada 24 horas y a pedido. El método de validación debe proporcionar por lo menos 128 bits de resolución o debe ser una comparación de bite a bite y debe prevenir la ejecución de cualquier componente del programa de control si se determina que el componente es invalido. Si se detecta un error, el sistema debe proveer una notificación visual del programa inválido. Un componente de programa del mecanismo de verificación debe estar alojado y ser cargado seguramente desde un medio no alterable. Un reporte debe estar disponible que

detalle el resultado de cada ejecución automática del mecanismo de validación y debe identificar cualquier componente del programa inválido.

3.7.2 Verificación de Dispositivos que no pueden ser Interrogados. Los dispositivos del programa que no pueden ser interrogados, como las tarjetas inteligentes, pueden ser utilizados siempre y cuando puedan ser verificados por la siguiente metodología:

a) Una prueba es enviada por un dispositivo idéntico, como por ejemplo una semilla de cálculo, a la cual el dispositivo debe responder con una suma de chequeo (checksum) de su espacio de programa total usando el valor de prueba.
b) El mecanismo de prueba y el medio que carga el software hacia el dispositivo es verificado por el laboratorio de pruebas y aprobado por el regulador.

Tales dispositivos, donde la exanimación del código fuente realizado por el laboratorio de pruebas muestra que un juego aprobado o el resultado monetario no pueden ser afectados, no deberán estar sujetos a estos requisitos.

3.7.3 Componentes Controlados de la Terminal Cliente

a) *Generalidades* Esta sección delineara los requerimientos del CSS cuando se descargue software, juegos y otros datos de configuración a las terminales cliente.
b) *Verificación de Integridad Independiente* El CSS debe proporcional la habilidad de conducir una verificación independiente de todos los componentes controlados aplicables alojados en el sistema.
    i. El proceso de verificación de tercer partido no debe incluir ningún proceso o software de seguridad proporcionado por el fabricante del sistema operativo, a no ser que el propósito sea de usarlo como un método de verificación secundario.

3.7.4 Verificación del Programa de Control. El CSS debe proporcionar la habilidad de autenticar todos los componentes controlados aplicables para los cuales reside una copia en el sistema a petición y una vez cada 24 horas y:

a) El CSS debe autenticar todos los archivos críticos incluyendo pero no limitado a ejecutables, datos, archivos del sistema operativo y otros archivos que podrían afectar el resultado del juego u operación para los cuales reside una copia en el sistema.

b) El CSS debe emplear un estándar de la industria de tercer partido de algoritmo de cifrado seguro (por ejemplo MD5, o SHA-1). Si se encuentra integrado, el fabricante debe estar preparado a demostrar el algoritmo elegido tanto al laboratorio de prueba como a la Comisión.

c) Un reporte debe estar disponible que detalle los resultados de la verificación de cada componente controlado verificado.

d) En el caso de una autenticación fallida, el CSS debe desactivar el componente controlado de una manera en que funcione seguidamente, incluyendo pero no limitado a la descarga, instalación y configuración del componente controlado hacia una terminal de cliente conectado no sea posible. El CSS también debe proporcionar un mecanismo de notificación de falla de autenticación a la Comisión.

3.8 Requisitos Del Historial Del Servidor

3.8.1 Generalidades. El servidor que respalda un Juego Basado en Servidor deberá proporcionar la siguiente información en pantalla:

a) Un historial completo del más reciente juego realizado y al menos nueve (9) juegos previos al juego más reciente por cada estación de jugador conectada al juego Basado en Servidor. La pantalla debe indicar el resultado del juego (o su representación equivalente), pasos intermedios del juego (tales como la secuencia de retención (hold) o retiro (draw) o una secuencia de doblado-abajo (double-down)), créditos disponibles, apuestas realizadas, créditos o monedas pagadas, y créditos cobrados. La capacidad para iniciar el historial del juego deberá estar disponible al jugador, para aquella información del historial asociada específicamente con el terminal de juego que inicio el historial del juego. La capacidad para iniciar el historial del juego para uno o todos los clientes que constituyen el Sistema de Juego Basado en Servidor debe estar disponible desde la porción de sistema o servidor del SBGS. El requisito para mostrar el historial del juego aplica a todos los programas del juego actualmente instalados en la porción de servidor del Juego basado en Servidor.

b) Un historial de transacciones completo para las transacciones realizadas en un sistema de apuestas sin dinero que incluya la transacción más reciente y las treinta y cuatro transacciones previas a la más reciente transacción por cada dispositivo de juego que incremento cualquiera de los contadores de entrada o salida del sistema de apuestas sin dinero. La capacidad de iniciar el historial de transacciones debe estar disponible en el

dispositivo de juego para aquel historial de transacción específicamente asociado con el terminal de juego que solicito la información del historial.

3.9 Librería de Datos Descargables

3.9.1 Generalidades. La Librería de Datos Descargables hace referencia al almacenamiento formal de todos los archivos de datos aprobados que pueden ser descargados al Dispositivo de Juego incluyendo el software de control y juego, programas periféricos, datos de configuración, etc.

3.9.2 Actualización de la Librería de Datos Descargables. Donde sea aplicable, la descarga de la Librería de Datos Descargables del CSS deberá ser únicamente escrita con un acceso seguro que sea controlado por el regulador, en cuyo caso el fabricante y/o el operador tendrán acceso a la Librería de Datos Descargables, siempre que este acceso no permita agregar nuevos archivos de datos descargables; o la Librería de Datos Descargables solo escribirá utilizando un método que sea aceptable por el Laboratorio de Pruebas y el Regulador.

3.9.3 Registro de Auditoría de la Librería de Datos Descargables. Cualquier cambio que sea haga a la Librería de Datos Descargables, incluyendo adición, cambio o eliminación de programas de juegos, debe ser almacenada en un registro de auditoría inalterable que incluirá:

a) Tiempo y fecha del acceso y/o evento;
b) Nombre de acceso (Log In);
c) Archivos de Datos Descargables agregados, cambiados, o removidos;

3.9.4 Registro de Auditoría de Actividad de Descarga. Cualquier registro de actividad entre el Servidor y el Dispositivo de Juego (Cliente) que involucre la descarga de la lógica del programa, el ajuste de las configuraciones del dispositivo de juego (cliente) o la activación de programas previamente descargados, deberán de ser almacenadas en un registro de auditoría inalterable que deberá incluir lo siguiente:

a) Los dispositivos de juego a los cuales se descargo el Programa de Juego y, si es aplicable, el programa al cual reemplazo;
b) Los dispositivos de juego sobre los que el Programa de Juego fue activado y el programa al cual reemplazo; y

c) Los valores de configuración del dispositivo antes y después de los cambios.

3.10 Descarga de Archivos de Datos del Dispositivo de Juego y Programas de Control

3.10.1 Generalidades. Este capítulo describirá los requisitos del CSS cuando descargue software, juegos y otros datos de configuración al Dispositivo de Juego, si el Servidor proporciona la funcionalidad de descarga de los programas de control y otros recursos de software, ya sea para un Sistema de Juego Basado en Servidor o un Sistema de Juego Respaldado por el Servidor.

3.10.2 Programa de Control. Esta sección describirá los estándares técnicos mínimos que deben ser cumplidos, cuando estos apliquen, cuando se descargue/active programas de control desde el servidor del SSGS al dispositivo de juego:

a) El Dispositivo de Juego y/o el Servidor SSGS deben tener un método para monitorear y reportar al Sistema de Monitoreo y Control (MCS por sus siglas en Ingles) todo acceso a las puertas externas durante un proceso interactivo de descarga del programa y/o activación del proceso. Si el SSGS no cuenta con la capacidad de monitorear el acceso de puertas durante el proceso interactivo de descarga del programa y/o activación del proceso, el reporte del laboratorio de pruebas deberá indicar esta circunstancia para que Controles Internos puedan ser desarrollados con el fin de asegurar la seguridad del dispositivo de juego, sobre todo con lo concerniente a los compartimientos de dinero en efectivo, donde aplique.

b) Antes de la ejecución del software actualizado, la terminal cliente debe estar en un estado inactivo (Idle) por cuatro minutos y el software satisfactoriamente autenticado como se define dentro la sección de verificación del programa de control de las regulaciones de juego.

c) Antes de que cualquier software sea añadido o removido de un dispositivo de juego, o estación cliente que sea parte del juego soportado por el sistema que puede resultar en la pérdida o cambio de la información de los contadores contables mandatorios, la información de un conjunto completo de información de contadores debe ser satisfactoriamente comunicado al sistema de contabilidad de las maquinas.

d) Será posible realizar un análisis forense del juego que puede incluir la observación de los datos del juego en el Servidor CSS y/o ser capaz de poner los datos de juego de regreso en otro dispositivo de juego para propósitos de exanimación.

3.11 Control de las Configuraciones del Dispositivo de Juego

3.11.1 Generalidades. Los Dispositivos de Juego utilizados en un entorno CSS que tengan configuraciones alterables que requieran Control Regulatorio, como es descrito en el estándar GLI-11 sección 1.5, pueden ser exonerados siempre y cuando se cumplan las regulaciones de esta sección.

3.11.2 Cambios de Configuración de la Tabla de Pagos/Denominación. Los Programas de Control del Dispositivo de Juego que ofrezcan múltiples tablas de pago y/o denominaciones que puedan ser configuradas a través del Servidor CSS no requerirán el Control Regulatorio para cambiar la tabla de pagos seleccionada, siempre que:

a) Todas las tablas de pagos que estén disponibles cumplan con el porcentaje de pago teórico y los requisitos de las probabilidades, donde aplique;
b) El Dispositivo de Juego y/o Servidor CSS mantengan los contadores de las Cantidades de Apuesta y las Cantidades Ganadas dentro de la Memoria Crítica para cada una de las tablas de pago que estén disponibles;
c) El Dispositivo de Juego mantenga los contadores de Contabilidad Principales en dólares y centavos o la denominación más baja disponible para la moneda local;
d) El juego este en un Estado de Inactividad cuando ocurra la actualización; y
e) El cambio no cause pagos o asignación de créditos incorrectos (por ejemplo para juegos que usan depósito de reservas de pago y aceptadores de monedas con una denominación fija).

3.11.3 Borrado de la Memoria Crítica del Dispositivo de Juego. El proceso de borrado de la memoria RAM en los Dispositivos de Juego a través del CSS debe utilizar un método seguro que pueda requerir del Control Regulatorio. Para los sistemas que no cumplan con esta regla, el regulador debe aprobar el método utilizado.

NOTA: El borrado de memoria crítica Non-RAM, u otra memoria, debe cumplir con los mismos requisitos mencionados aquí para la memoria RAM.

3.12 Descarga de Valores Aleatorios

3.12.1 <u>Generalidades</u>. El presente capítulo determina los elementos de un CSS que pueden ser utilizados para la generación de Valores Aleatorios, los cuales son subsecuentemente comunicados al Programa de Control del Dispositivo de Juego que es requerido para determinar los resultados del juego. La generación de Valores Aleatorios del Servidor CSS no incluye la generación de resultados del juego.
NOTA: Los sistemas que utilizan recursos limitados de recursos de juego (por ejemplo, sistemas electrónicos Pull-Tab) deben cumplir con el estándar GLI-14 de Sistemas Finitos de Raspar y Jalar Etiquetas, en adición a los estándares fijados en este documento, donde sea aplicable.

3.12.2 <u>Generador de Número Aleatorio (RNG).</u> En el caso que el CSS tenga la habilidad de descargar Valores Aleatorios al dispositivo de juego, el Generador de Numero Aleatorio (RNG) funcionará de acuerdo con el 99% de los niveles de confianza, como se indica dentro de los requisitos del RNG del estándar GLI-11 en la sección 3.3.

CAPITULO 4

4.0 REQUISITOS DEL DISPOSITIVO DE JUEGO DEL CSS

4.1 Introducción

4.1.1 <u>Generalidades</u>. Esta terminal es utilizada por el jugador para colocar sus apuestas, jugar los juegos ofrecidos y ganar premios (cuando aplique). La Terminal del Jugador puede recibir información del juego desde el servidor de juegos, en el caso de un Sistema de Juego Basado en Sistema o hacer su propia determinación en el caso de un Sistema de Juego Respaldado por el Sistema, y entonces mostrar información al jugador. El juego y otras funcionalidades pueden ser separados en partes, donde algunos componentes pueden ser generados dentro o fuera de la Terminal del Jugador (ejemplo, Terminales del Jugador que funcionan con un sistema). Donde sea aplicable, todas las terminales cliente deben conformar con todos los requerimientos de Dispositivos de Juego establecidos por la autoridad jurisdiccional requerida.

Glosario

Referencia	Definición
Servidor CSS	El 'anfitrión' (host) que es la fuente primaria del sistema de control e información.
Programa de Control	El programa de control es el software que opera las funciones del terminal de cliente, incluyendo las tablas de pago para el juego. El programa de control puede correr independientemente en el CSS o puede requerir información generada por el sistema para realizar las funciones de la terminal de cliente.
Memoria Critica	La memoria critica es usada para guardar/almacenar todos los datos que son considerados vitales para la operación continua de la terminal de cliente.
Firewall	Barrera de seguridad de la red (network). Un firewal es un dispositivo que guardia/cuida la entrada a una red privada y mantiene fuera el tráfico no autorizado o no deseado.
Contenidos del Juego	La descarga de cualquier dato, con excepción del programa de juego o valores aleatorios.
Datos del Juego	Los datos almacenados dentro de una memoria no volátil que refleja la contabilidad y eventos de seguridad que es especifico a la terminal de cliente individual, que incluye: 1) Reportes de errores. 2) Todos los contadores de caída (drop meters). 3) La historia del último juego (esto debe ser mantenido dentro de la historia de juego en caso que haya una disputa de jugador donde el supuesto problema tomo lugar antes y no fue reportado hasta después de actualizar el nuevo juego, una representación textual una alternativa aceptable). 4) Historial de los billetes. 5) Reportes da las transacciones electrónicas (cashless). 6) Reportes de auditoría para las transacciones del programa de juego de la terminal de cliente.
Programa de Juego	El programa de control que reside en el servidor CSS y/o la terminal de cliente.
Descarga de Datos de Librería	Una librería controlada por un regulador que reside en el servidor CSS que contiene el programa de juego complete y/o la parte del servidor con componentes críticos del programa de juego.
Estado inactivo	La terminal de cliente está en un estado inactive, incluyendo mientras el juego esta deshabilitado, cuando no hay actividad en el dispositivo, no créditos, y sin condiciones de error.
Elementos de Interface	Cada punto en las comunicaciones dentro del CSS que incluye al mínimo el servidor CSS, terminal de cliente y cualquier otro equipo que es usado para propósitos de transmitir datos.
Terminal de Cliente	Un elemento dentro de un CSS es una terminal de cliente. La terminal de cliente en una configuración apoyada por un servidor puede funcionar independientemente del servidor CSS luego de una actualización exitosa del programa de control o requiere contenido del juego que es producido por el servidor CSS para funcionar como configuración basada en el servidor.
Valores Aleatorios	Donde un generador de números aleatorios es guardado/almacenado en el servidor CSS y comunica los números aleatorios a la terminal de cliente que son requeridos para qué la terminal de cliente funcione, donde el programa de control de la terminal de cliente no es independiente del servidor CSS.
Control Regulatorio	Un método usado y solamente accesible por el regulador para asegurar la seguridad del CSS.
Sistema de Juego basado en el servidor (SBGS)	La combinación de un servidor y terminal(es) de cliente(s) en cual la porción integral o entera del contenido de juego reside en el servidor. Este sistema trabaja colectivamente de forma que la terminal de cliente no sea capaz de funcionar cuando este desconectada del sistema.
Sistema de Juego Apoyado por Servidor (SSGS)	La combinación de un servidor y terminal(es) de cliente(s) que juntos permiten transferir el programa de control entero y contenido del juego al la terminal(es) de cliente para el propósito de descargar los programas de control y otros recursos del software a la terminal de cliente convencional o terminal de cliente en forma intermitente. Las terminales de cliente conectadas al sistema son capaces de operar independientemente del sistema luego que el proceso de descarga ha sido completado. Esta configuración encierra casos donde el sistema puede tomar control de los dispositivos periféricos o equipo asociado típicamente considerado parte de una terminal de cliente convencional como un validador de billetes o una impresora. En un juego apoyado por el sistema, el resultado de juego es determinado por la terminal de cliente conectado al sistema y no por el sistema en sí. La terminal de

	cliente es capaz de funcionar si es desconectado desde el sistema.