SERIES DE ESTÁNDARES TÉCNICOS

GLI-26:

Estándar de Sistemas Inalámbricos

Versión: 2.0

Fecha de Publicación: 24 de Febrero del 2015

Esta página se dejo en blanco intencionalmente

SOBRE 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.

Un fabricante debe presentar equipo con una petición que sea certificado de acuerdo con este Estándar. A partir de la certificación, **Gaming Laboratories International, LLC**., suministrara un certificado evidenciando la certificación a este Estándar.

GLI-26 Sistemas Inalámbricos será un documento vivo el cual debe cambiar con la evolución de la tecnología y la tecnología de la red inalámbrica. GLI-26 no tiene por objeto reemplazar o invalidar cualquier documento actual o futuro en la Serie de Estándares de GLI. Como un ejemplo, las recomendaciones en GLI-26 no tienen por objeto circunvalar cualquier especificación en GLI-21 Sistemas Cliente Servidor y/o GLI-27 Buenas Prácticas en Seguridad de Redes, si la red en cuestión soporta funcionalidades de cliente-servidor y/o red por cable. Igualmente, para otros tipos de redes y el documento de estándares de GLI que se aplica específicamente a esas redes, el estándar específico tiene prioridad.

Esta página se dejo en blanco intencionalmente

Sistemas Inalámbricos

GLI-26 Versión 2.0

Historial de Revisiones

Para el historial de revisiones de este estándar, comuníquese con nuestra oficina.

Tabla de Contenidos

CAPÍTULO 1 ..... **7**

1.0 Visión General **7**

1.1 Introducción *7*
1.2 Reconocimiento de Otros Estándares Revisados *7*
1.3 Propósito del Estándar *8*
1.4 Otros Documentos que Pueden Aplicarse *9*
1.5 Fases de las Pruebas *9*

CAPÍTULO 2 ..... **10**

2.0 Requisitos de Dispositivo Inalámbrico **10**

2.1 Dispositivos Inalámbricos *10*
2.2 Puntos de Acceso Inalámbrico (WAP) *11*
2.3 Dispositivos de Conectividad Inalámbrica (WCD) *12*
2.4 Dispositivos de Cliente Inalámbrico *12*
2.5 Dispositivos de Sistema Inalámbrico *12*
2.6 Otros Dispositivos Inalámbricos *12*

CAPÍTULO 3 ..... **13**

3.0 REQUISITOS DE SOFTWARE PARA LOS COMPONENTES INALÁMBRICOS **13**

3.1 Dispositivos Inalámbricos - Requisitos de Software *13*
3.2 Cliente Inalámbrico - Software *13*
3.3 Cliente de Operador Inalámbrico - Software *15*
3.4 Cliente de Jugador Inalámbrico - Software *16*
3.5 Sistema de Juego Inalámbrico - Software *19*
3.6 Requisitos del Juego *22*
3.7 Requisitos del Generador de Números Aleatorios (RNG) *24*
3.8 Impuestos *24*

CAPÍTULO 4 ..... **25**

4.0 REQUISITOS DE SEGURIDAD DE LA RED INALÁMBRICA **25**

4.1 Requisitos de Encriptación y Autenticación Inalámbrica *25*
4.2 Protocolo de Comunicación Inalámbrica *26*

CAPÍTULO 5 ..... **30**

5.0 REQUISITOS DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN (ISS) **30**

5.1 Declaración General *30*
5.2 Política de Seguridad de Información *30*
5.3 Controles Administrativos *31*
5.4 Controles Técnicos *34*
5.5 Controles Físicos y Ambientales *38*

Glosario **40**

Ejemplo de la Red Inalámbrica **42**

CAPÍTULO 1

1.0 Visión General

1.1 Introducción

1.1.1 <u>Declaración General.</u> 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 26 de GLI*, establecerá los estándares técnicos para los Redes Inalámbricos.

1.1.2 <u>Historial del Documento.</u> A continuación, nosotros hemos listado dando crédito a las agencias cuyos documentos hemos repasado previo a escribir este estándar. Es la política 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 Revisados

1.2.1 <u>Declaración General</u>. Este Estándar fue desarrollado por medio de revisiones y utilizaciones de porciones del los documentos de las organizaciones que se indican a continuación. Reconocemos y le agradecemos a los reguladores que han compilado estos documentos:

a. Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
b. El Consejo del Estándar de Seguridad de la Industria de Carta de Pago de la Alianza Wi-Fi.
c. El Instituto Nacional de Estándares y Tecnología.
d. Las Redes ARUBA.

e. NETGEAR
f. Sistemas Cisco, Inc.
g. "IPsec Virtual Private Network Fundamentals" escrito por James Henry Carmouche (ISBN: 1587052075).
h. La Comisión de Juegos de Azar de Nevada y la Junta de Control de Juegos del Estado de Nevada.

1.3 Propósito del Estándar

1.3.1 <u>Declaración General.</u> El propósito de este Estándar Técnico es lo siguiente:

a. Eliminar criterios subjetivos en el análisis y la certificación de las Redes Inalámbricas de Área Local (WLAN).
b. Evaluar únicamente aquellos criterios que afectan la confidencialidad, credibilidad e integridad de las Redes Inalámbricas de Área Local.
c. Crear un Estándar que asegure que la seguridad del WLAN y/o Sistemas Wi-Fi en un ambiente de juegos es lo mas equivalente posible a la seguridad de un sistema por cable al establecer controles y guías para el diseño, implementación, y uso de las redes y dispositivos inalámbricos.
d. Distinguir entre la política pública local y el criterio del laboratorio. En GLI, consideramos que cada jurisdicción local debe fijar su propia política pública con respecto a la red inalámbrica.
e. Reconocer que las pruebas que no son relacionadas con los juegos (tales como la Certificación de Wi-Fi, las pruebas de Seguridad de Producto, y las pruebas Eléctricas) no deben incorporarse en este estándar, sino que deben derivarse a los laboratorios de pruebas correspondientes que se especialicen en esos tipos de pruebas. Excepto donde se indique específicamente en el estándar, las pruebas no están relacionados con cuestiones de salud o seguridad. Estas cuestiones son responsabilidad del fabricante, del comprador y del operador del equipo.
f. Desarrollar un estándar que pueda modificarse fácilmente para incorporar tecnología nueva.
g. Desarrollar un estándar que no especifique una tecnología en particular, método o algoritmo específico. El intento es permitir el uso de un rango amplio de métodos para ser utilizados para conformar el estándar y al mismo tiempo fomentar el desarrollo de métodos nuevos.

ANOTACIÓN: Debido a los cambios continuos y mejoramientos en las tecnologías inalámbricas y de red, la información en este documento se considera actual solamente a partir de fecha de publicación. Por lo tanto, es imperativo que las empresas continuamente revisen y actualicen sus políticas de control interno y sus procedimientos para asegurar que la red inalámbrica este segura y que las amenazas y vulnerabilidades se manejen como corresponde. Igualmente, la tecnología usada en los WLAN se revisara y actualizara como corresponde para asegurar que las características de seguridad más estrictas se han implementado. Los requisitos en este documento han sido desarrollados basados en un modelo de un WLAN centralizado en una red privada empresarial. En un modelo de WLAN centralizado, los requisitos de seguridad,

autenticación, y comunicación son controlados y manejados a través de un sistema o servidores de gestión para implementar una red más fuerte, segura, y verificable.

1.3.2 Sin Limitación de Tecnología. Se debe tener en cuenta que este estándar no debe entenderse de forma tal que limite el uso de tecnología futura. El documento no debe interpretarse de forma que si no se menciona la tecnología, implique que no esté permitida. Al contrario, a medida que se desarrolle tecnología nueva, revisaremos este estándar, realizaremos cambios e incorporaremos nuevos estándares mínimos para la tecnología nueva.

1.4 Otros Documentos que Pueden Aplicarse

1.4.1 Declaración General. Este documento tiene por objeto ser usado como un estándar suplementario que se aplica en adición a los estándares bases de GLI o los adoptados por la jurisdicción para el producto en los ensayos. Este estándar detallara los requisitos adicionales que se deben cumplir para operar cualquier dispositivo o sistema en una red inalámbrica. Por favor referir a nuestro sitio web http://www.gaminglabs.com para una lista completa de los Estándares de GLI.

1.4.2 Los Estándares Internos Mínimos de la Parte Interesada. La implementación de una Red Inalámbrica y/o un Sistema es un proyecto complejo, y por lo tanto requiere el desarrollo de procesos y procedimientos internos para asegurar que el sistema este configurado y opere con el nivel de seguridad y control necesario. Con ese fin, se espera que el operador de la red /parte interesada establezca un conjunto de Especificaciones Mínimas de Control Interno (MICS) para definir los requisitos internos para la creación, gestión, y manejo de la red inalámbrica en adición a los requisitos para el control interno de cualquier software y hardware de cliente del jugador/operador, y sus cuentas asociadas.

1.5 Fases de las Pruebas

1.5.1 Declaración General. Las presentaciones de un Sistema Inalámbrico al Laboratorio de Ensayos serán realizadas en dos fases:

a) Dentro del entorno del laboratorio; y
b) En el campo después de la instalación inicial del sistema para asegurar la configuración correcta de las aplicaciones de seguridad.

ANOTACIÓN: En adición a las pruebas del sistema/red inalámbrico en el campo, el laboratorio de pruebas debe proveer entrenamiento a los reguladores locales, recomendando procedimientos de auditoría en el campo, y asistencia con la compilación de controles internos, si se solicita.

CAPÍTULO 2

2.0 Requisitos de Dispositivo Inalámbrico

2.1 Dispositivos Inalámbricos

2.1.1 ***<u>Declaración General.</u>*** Los Dispositivos Inalámbricos se refieren a cualquier dispositivo que se comunica inalámbricamente a través de una red de área local o que tiene un impacto en una red inalámbrica. Esto incluye, pero no se limita a:

a. Un Punto de Acceso Inalámbrico (WAP) es un dispositivo que le permite a los dispositivos inalámbricos conectar a una red inalámbrica usando un transporte inalámbrico (por ejemplo: Wi-Fi).
b. Un Dispositivo de Conectividad Inalámbrica (WCD) es un dispositivo que provee el interfaz a través del cual una red inalámbrica se puede acceder por otro hardware dentro del establecimiento de juego de azar (por ejemplo: un adaptador de red inalámbrica en un computador (PC)).
c. Un Dispositivo de Cliente Inalámbrico es un dispositivo que convierte las comunicaciones desde el Sistema Inalámbrico a una forma entendible por un humano, y convierte las decisiones humanas a un formato de comunicación entendible por el Sistema Inalámbrico.

ANOTACIÓN: *Se recomienda que todos los Dispositivos Inalámbricos sean aprobados por el Laboratorio del Asegurador (o equivalente) para la seguridad de dispositivo, la resistencia a las oleadas de electricidad, el descargo electroestático, la interferencia magnética, y las condiciones extremas de ambiente. El laboratorio de ensayos NO debe formular cualquier constatación con respecto a las pruebas de Seguridad y EMC, ya que eso es la responsabilidad del fabricante de los elementos o los que compran los elementos. El laboratorio de ensayos no debe ensayar, ser responsable, ni formular una constatación en relación a estos asuntos.*

2.1.2 ***<u>Configuración</u>***. Todos los Dispositivos Inalámbricos se deben configurar como sigue:

a) Todas las funciones de la gestión de la red deben:
    i. Autenticar todos los usuarios en la red; y
    ii. Encriptar todas las comunicaciones de la gestión de la red.
b) Todo el software que se comunicara a través de la red inalámbrica debe implementar control de acceso de usuario con autenticación fuerte, como se defina en los MICS del operador. Cualquier acceso administrativo debe requerir un nivel adicional de control.
c) Si cualquier credencial es codificado permanentemente en un componente de la red inalámbrica, debe ser encriptado.
d) Comunicación en la red segura solo debe ser posible entre componentes inalámbricos aprobados que han sido registrados y autenticados como validos en la red. No se permitirá ninguna comunicación no autorizada a los componentes y/o puntos de acceso.

e) Cualquier componente que usa la red inalámbrica para comunicar debe cumplir con todos los requisitos de encriptación y autenticación indicados dentro de este estándar.

2.2 Puntos de Acceso Inalámbrico (WAP)

2.2.1 ***Declaración General.*** El Punto de Acceso Inalámbrico (WAP) transmite información entre el(los) dispositivo(s) inalámbrico(s) y el resto de la red. Todos los dispositivos que proveen uno o más WAPs deben:

a) Ser instalados en un área seguro, controlado, o inaccesible para permitir la restricción de acceso físico al dispositivo.
b) Ser construido de tal manera que sea resistente a daño físico al hardware o corrupción del firmware/software contenido por uso normal.
c) Asegurar todos los puertos físicos para prevenir acceso no autorizado a la red a través de conexión física al Punto de Acceso Inalámbrico. Todos los puertos/conexiones no usados deben ser bloqueados físicamente o el software deshabilitado.
d) Limitar el alcance de la red inalámbrica a un área aprobado. (Por ejemplo: Antenas Direccionales, Geocercas, etc.)

ANOTACIÓN: *Se recomienda que todos los WAPs sean certificados por la* Wi-Fi Alliance ®. *El laboratorio de ensayos NO debe formular cualquier constatación con respecto a las pruebas de Wi-Fi, ya que eso es la responsabilidad del fabricante de los elementos o los que compran los elementos. El laboratorio de ensayos no debe ensayar, ser responsable, ni formular una constatación en relación a estos asuntos.*

2.2.2 ***Configuración.*** Todos los Dispositivos WAP deben ser configurados como sigue:

a) El nombre de usuario y contraseña por defecto se debe cambiar de lo predeterminado por la fábrica a un valor seguro controlado de acuerdo a los MICS de la parte interesada.
b) La contraseña por defecto de la red se debe cambiar de lo predeterminado por la fábrica a un valor seguro controlado de acuerdo a los MICS de la parte interesada.
c) El "Identificador de Grupo de Servicio (SSID)" para el dispositivo se debe configurar como sigue:
    i. El valor se debe cambiar de lo predeterminado por la fábrica a un valor seguro.
    ii. El SSID no debe contener cualquier referencia al nombre del sitio, fabricante, o cualquier otra referencia que pueda ser fácilmente discernida.
d) Acceso a las funciones administrativas del dispositivo de Punto de Acceso Inalámbrico debe ser limitado a las conexiones desde el lado por cable de la red que utilizan un protocolo seguro con una cuenta de usuario privilegiada definida por los MICS de la parte interesada.

ANOTACIÓN: Protocolos y métodos alternos de gestión de la red serán examinados caso por caso.

2.3 Dispositivos de Conectividad Inalámbrica (WCD)

2.3.1 ***Declaración General.*** Todos los Dispositivos de Conectividad Inalámbrica (WCDs) deben tener la capacidad de ser configurados para cumplir con los requisitos de configuración indicados en la sección 2.1.2 de este documento.

ANOTACIÓN: Se recomienda que todos los WCDs sean certificados por la Wi-Fi Alliance ®. El laboratorio de ensayos NO debe formular cualquier constatación con respecto a las pruebas de Wi-Fi, ya que eso es la responsabilidad del fabricante de los elementos o los que compran los elementos. El laboratorio de ensayos no debe ensayar, ser responsable, ni formular una constatación en relación a estos asuntos.

2.4 Dispositivos de Cliente Inalámbrico

2.4.1 ***Declaración General.*** Un Dispositivo de Cliente Inalámbrico permite la conexión a, e interacción con, un sistema inalámbrico. Todos los dispositivos de hardware que permiten el uso de software de Cliente Inalámbrico deben ser compatibles con, o incorporar un, WCD.

2.4.2 ***Otros Requisitos.*** Todos los dispositivos de hardware propios desarrollados para soportar los juegos inalámbricos deben cumplir con los estándares Jurisdiccionales correspondientes para su uso previsto, además de los requisitos indicados en este documento. A falta de estándares Jurisdiccionales específicos, se debe usar GLI-11.

2.5 Dispositivos de Sistema Inalámbrico

2.5.1 ***Declaración General***. Cualquier componente de sistema que utilice comunicación inalámbrica para comunicarse con la red de juegos debe cumplir con los siguientes requisitos:

a) Ser compatible con, o incorporar un, WCD.
b) Estar localizado en un área seguro y controlado dentro de la instalación de juegos para que el acceso a los dispositivos del sistema sea limitado a personas autorizadas.

2.6 Otros Dispositivos Inalámbricos

2.6.1 ***Declaración General.*** Los periféricos inalámbricos incluyendo, pero no limitado a, los teclados, los ratones, los presentadores/punteros, los audífonos, y los dispositivos móviles (por ejemplo: los teléfonos o tabletas de los clientes usados para actividades no de juegos) se deben usar de acuerdo a los siguientes controles de seguridad:

a) Estos dispositivos no se deben usar para comunicar Información Delicada (ver la sección 4.2.2) a menos que cumplan con todos los requisitos de seguridad y encriptación de comunicación inalámbrica indicados en este documento.
b) Todas las operaciones de estos componentes deben ser usadas de acuerdo con los requisitos aplicables de este estándar técnico, y otros Estándares GLI aplicables

CAPÍTULO 3

3.0 REQUISITOS DE SOFTWARE PARA LOS COMPONENTES INALÁMBRICOS

3.1 Dispositivos Inalámbricos - Requisitos de Software

3.1.1 ***Identificación.*** Todo el software de dispositivo inalámbrico debe contener información suficiente para identificar el software y nivel de revisión de la información almacenada en el dispositivo Inalámbrico, el cual puede ser mostrado a través de una pantalla de visualización.

ANOTACIÓN: El proceso usado para identificar el software y el nivel re revisión será evaluada caso por caso.

3.1.2 ***Verificación Independiente del Programa de Control.*** Debe ser posible permitir una verificación de integridad independiente del software del dispositivo desde una fuente externa. Esto es requerido para todo el software que pueda afectar la integridad del sistema. Esto se debe lograr con ser autenticado por un dispositivo de terceros, o por permitir el retiro del medio para que pueda ser verificado externamente. Otros métodos deben ser evaluados caso por caso. Esta verificación de integridad proveerá una manera para la verificación del software en el campo para identificar y validar el programa. El laboratorio de ensayos, antes de certificar el dispositivo, debe evaluar el método de verificación de integridad.

3.1.3 ***Validación.*** El software utilizado en una red inalámbrica deben tener la capacidad de autenticar que todo el software siendo utilizado es válido y, en case de fallo de las rutinas de autenticación, cesar todas las operaciones de juego y mostrar un mensaje de error hasta ser corregido. Esta autenticación debe ocurrir cuando se instala le software, cada vez que el software se cargue para uso, cuando se inicie una sesión activa, y cuando se solicite por una cuenta de usuario autorizada definida en los MICS de la parte interesada.

ANOTACIÓN: Los mecanismos de verificación serán evaluados caso por caso y aprobados por el laboratorio de ensayos independiente basado en las prácticas de seguridad estándares de la industria.

3.2 Cliente Inalámbrico - Software

3.2.1 ***Declaración General.*** El software de Cliente Inalámbrico es cualquier software descargado a, o instalado en, un dispositivo que se usa para interactuar con un sistema asociado. Los dispositivos de Cliente de Operador Inalámbrico solamente son para las funciones de visualización e interacción. Todos los créditos, contadores, datos críticos, y lógica de programa deben ser implementados y ejecutados por el sistema asociado. Todo el software de Cliente Inalámbrico debe cumplir con los requisitos indicados en la Sección 3.1 de este documento en adición a los listados a continuación.

3.2.2 ***<u>Interacciones de Cliente-Servidor.</u>*** Los siguientes requisitos se aplican al Software de Cliente Inalámbrico y las interacciones del cliente-servidor:

a) El Software de Cliente Inalámbrico no debe automáticamente alterar ninguna regla de cortafuegos especificada por el cliente para los puertos abiertos que son bloqueados por un cortafuegos de hardware o software.
b) El Software de Cliente Inalámbrico no debe acceder ningún puerto (automáticamente o por pedirle al usuario a acceder manualmente) que no sea necesario para la comunicación entre el cliente y el servidor.
c) Si el software de Cliente Inalámbrico incluye funcionalidad adicional no relacionada al juego o no administrativa, esta funcionalidad adicional no debe alterar la integridad del software en cualquier manera.
d) El Software de Cliente Inalámbrico no debe poseer la capacidad de ignorar las configuraciones de volumen del Dispositivo de Cliente Inalámbrico.
e) Se recomienda que el auto-completar, al almacenamiento de contraseñas, u otros métodos que llenaran el campo de la contraseña sean deshabilitados para El Software de Cliente Inalámbrico.

3.2.3 ***<u>Área de Operación Limitada.</u>*** Conexión a, y uso de, una Red Inalámbrica para propósitos de juegos o administración debe ser limitado a un área especifico como indicado in los MICS de la parte interesada. Una vez que el dispositivo es retirado del área definido, inmediatamente se debe deshabilitar y cesar todas las operaciones de juego o administrativas.

3.2.4 ***<u>Verificación de Compatibilidad.</u>*** Durante cualquier instalación o inicialización y antes de establecer una sesión, el Software de Cliente usado en conjunto con el Sistema debe detectar cualquier incompatibilidad o limitación de recurso con el dispositivo en cual está instalado lo que impediría la operación correcta del software de Cliente Inalámbrico. Si alguna incompatibilidad o limitación de recurso es detectada el cliente y sistema deben

a) Notificar el usuario de cualquier incompatibilidad y/o limitación de recurso que impide la operación (por ejemplo: versión de software, incumplimiento de las especificaciones mínimas, etc...); y
b) Impedir cualquier actividad de juego o administrativa mientras exista la incompatibilidad o limitación de recurso.

3.2.5 ***<u>Contenido.</u>*** El Software de Cliente Inalámbrico no debe contener ninguna funcionalidad considerada maliciosa por el cuerpo regulatorio. Esto incluye, pero no es limitado a, extracciones/transferencias de archivo no autorizadas, modificaciones de dispositivo de jugador no autorizadas, el acceso no autorizado a cualquier información personal almacenada por el dispositivo (contactos, calendario, etc.), y el malware.

3.2.6 ***<u>Cookies.</u>*** Todas las cookies de nivel aplicación no deben contener ningún código malicioso.

3.2.7 ***Comunicaciones.*** Las comunicaciones entre el Dispositivo Inalámbrico y el sistema asociado deben ocurrir sobre una conexión de red segura que cumple con todos los requisitos indicados en el Capitulo 4 (Requisitos de Seguridad de la Red Inalámbrica) de este estándar.

3.2.8 ***Requisitos del Interfaz del Usuario.*** EL interfaz de usuario es definido como una aplicación o programa que el operador ve y/o interactúa con el software de cliente para comunicar sus acciones al sistema asociado. El Interfaz de Usuario debe cumplir con lo siguiente:

a) Cualquier cambio de tamaño o recubrimiento del Interfaz de Usuario se debe aplicar precisamente para mostrar la visualización, botones, o puntos táctiles/de clic revisados.
b) Las funciones de todos los botones, puntos táctiles, o puntos de clic representados en la interfaz de usuario deben ser indicados claramente dentro del área del botón, o el punto táctil/de clic y/o dentro del menú de ayuda. Ninguna funcionalidad debe estar disponible a través de cualquier botón o punto táctil/de clic que está escondido o no documentado en el dispositivo de cliente.
c) La visualización de las instrucciones e información debe ser adaptada para la interfaz de usuario. Por ejemplo, en casos donde el dispositivo del cliente de jugador usa tecnologías con una pantalla de visualización más pequeña, es aceptable presentar una versión abreviada de la información del juego accesible directamente dentro del juego y disponer la versión completa de la información del juego a través de otra manera, tal como una pantalla, menú de ayuda, u otro interfaz secundario que es fácilmente identificado en la pantalla visual del juego.

3.2.9 ***Entradas Simultáneas.*** El programa no deber ser afectado negativamente por la activación simultánea o secuencial de las varias entradas y salidas que puede, sea intencionalmente o no, causar malfuncionamientos o resultados inválidos.

3.3 Cliente de Operador Inalámbrico - Software

3.3.1 ***Declaración General.*** El software de Cliente de Operador Inalámbrico es utilizado por el personal del Local de Juegos para realizar funciones administrativas dentro de la propiedad (por ejemplo: Validación de Boletos, monitoreo de Estado, etc.). Todo el software de Cliente de Operador Inalámbrico debe cumplir con los requisitos indicados en la Sección 3.2 (Requisitos de Software – Dispositivos Inalámbricos) de este documento, en adición a los indicados a continuación.

3.3.2 ***Funcionalidad Requerida para el software de Cliente de Operador Inalámbrico.*** En adición a los requisitos jurisdiccionales aplicables para el sistema conectado, el software de Cliente de Operador Inalámbrico debe cumplir con lo siguiente:

a) Todas las opciones disponibles presentadas en el Cliente de Operador Inalámbrico deben estar atadas a la cuenta del operador conectado. Solamente el acceso disponible para la cuenta conectada estará disponible a través del Cliente de Operador Inalámbrico.
b) Los dispositivos de Cliente de Operador Inalámbrico no deben almacenar datos delicados o información de sistema.

ANOTACIÓN: A falta de reglas jurisdiccionales especificas, se debe aplicar GLI-13.

3.3.3 ***Sesiones de Operador.*** Una sesión de operador se defina como un plazo de tiempo durante el cual un operador u otro personal del Local de Juegos puede utilizar un dispositivo de Cliente de Operador Inalámbrico para realizar funciones administrativas en el campo de juegos en un dispositivo inalámbrico.

a) Una sesión de Operador Inalámbrico es iniciada cuando el operador se conecta a su cuenta controlada usando su nombre de usuario y contraseña a través de su propio dispositivo o un dispositivo proporcionado por la propiedad.
b) Al operador se le proporciona (o ha creado) un identificador electrónico, tal como un certificado digital o una descripción de cuenta, y una contraseña que será utilizada para iniciar una sesión.
c) Le seguridad de la cuenta de operador debe ser establecida de acuerdo con los estándares jurisdiccionales de sistema aplicables.

3.3.4 ***Inactividad de Sesión de Operador.*** El software de cliente de operador inalámbrico debe contar con un mecanismo que detecta la inactividad de sesión y termina una sesión cuando sea aplicable.

a) Si el dispositivo de Cliente de Operador Inalámbrico no recibe una entrada del operador dentro de 5 minutos, u otro periodo de tiempo definido por el regulador, la sesión debe expirar y requerir reactivación. El personal del Local de Juegos puede restablecer su sesión al restablecer su conexión con el sistema. Este proceso debe incluir, como mínimo, la entrada manual de la contraseña segura del operador u otros métodos aceptados.
b) Ninguna funcionalidad de operador adicional se permite hasta que una nueva sesión se establezca.

3.4 Cliente de Jugador Inalámbrico - Software

3.4.1 ***Declaración General.*** El software de Cliente de Jugador Inalámbrico es utilizado por un jugador para tomar parte in cualquier actividad de juego sobre una red inalámbrica. Todo el software de Cliente de Jugador Inalámbrico debe cumplir con los requisitos indicados en la Sección 3.2 de este documento, en adición a los indicados a continuación.

3.4.2 ***Funcionalidad Requerida para el software de Cliente de Jugador Inalámbrico.*** En adición a los requisitos jurisdiccionales aplicables para los Clientes de Sistema de Juego Basado en Servidor, el software de Cliente de Jugador Inalámbrico debe cumplir con lo siguiente:

a) Los dispositivos de Cliente de Jugador Inalámbrico no deben contener ninguna lógica utilizada para generar el resultado de cualquier juego. Todas las funciones criticas

incluyendo la generación de cualquier juego (y el retorno al jugador) deben ser generadas por el Sistema de Juego y ser independiente del Cliente de Jugador Inalámbrico.

b) Los dispositivos de Cliente de Jugador Inalámbrico no deben ser capaces de realizar actividad de juego si están desconectados del servidor de juego asociado.
c) Los dispositivos de Cliente de Jugador Inalámbrico no deben almacenar datos delicados o información de sistema.
d) El software de Cliente de Jugador Inalámbrico no debe ser capaz de transferir información a otro software de Cliente Inalámbrico que no sea de funciones de chat (por ejemplo: texto, voz, video, etc.) y archivos aprobados (por ejemplo: fotos de perfil de usuario, fotos, etc.).
e) El resultado del juego no debe ser afectado por el ancho de banda efectivo, la utilización del enlace, la tasa de error de bit u otra característica del canal de comunicación entre el Sistema de Juego y el Cliente de Jugador.

ANOTACIÓN: A falta de reglas jurisdiccionales especificas, se debe aplicar GLI-21.

3.4.3 ***Sesiones de Juego Inalámbricas.*** Una sesión de juego inalámbrica es definida como el plazo de tiempo durante cual un jugador puede participar en una actividad de juego. Una sesión de juego inalámbrica se puede establecer por uno de los siguientes métodos, según lo permitido por el operador:

a) ***Dispositivo Proporcionado por el Lugar de Juego.*** El jugador puede obtener un dispositivo de cliente inalámbrico del personal del casino después de completar el proceso necesario definido dentro del los MICS de la parte interesada.
b) ***Dispositivo Propio del Jugador.*** El jugador puede obtener/bajar una aplicación o paquete de software que contiene el software del cliente de jugador inalámbrico, o acceder la aplicación del cliente a través de un interfaz de navegador.
    i. El proceso de instalación del software de cliente debe incluir un proceso de validación que requiere validación de sistema de la instalación y enlaza la conexión del usuario final a una cuenta específica para la duración de la sesión.
    ii. Donde se usen cookies, al jugador se le debe informar de su uso después de la instalación. Cuando se requieren cookies para la jugada, la jugada no puede ocurrir si el Dispositivo de Cliente de Jugador Inalámbrico no las acepta.

3.4.4 ***Gestión de Sesión de Jugador.*** Una sesión de jugador se maneja por uno de los siguientes métodos, según lo permitido por el operador:

a) ***Cuenta de Jugador Establecida.*** El jugador debe entrar al sistema de juego usando su cuenta de jugador establecida.
    i. Las cuentas de jugador deben cumplir con los MICS de la parte interesada y con los requisitos definidos en las reglas y regulaciones para las cuentas de jugador de la jurisdicción. A falta de reglas jurisdiccionales especificas, se debe aplicar GLI-16 “Sistemas sin Dinero en Efectivo en los Casinos”.

ii. El jugador puede apostar los créditos actualmente presentes en su cuenta durante esta sesión de juego. Se pueden agregar y canjear créditos de su cuenta personal a través de los métodos estándares de depósitos y retiros de una cuenta de jugador establecidos por los MICS de la parte interesada.

b) ***Jugada de Invitado.*** El personal del Lugar de Juego inicializará el software de cliente en el dispositivo y establecerá una conexión con el sistema de juego usando un método seguro.
   i. Se pueden agregar créditos a la sesión de juego inalámbrico usando métodos definidos en los MICS de la parte interesada. Estos créditos estarán disponibles para jugar usando el dispositivo de cliente. El jugador puede aumentar sus créditos disponibles a través de este mismo proceso.
   ii. El jugador puede canjear el saldo de crédito en la sesión de juego inalámbrica al volver al punto original de la sesión o a través del personal del Lugar de Juego, quien le pagara el saldo de crédito según los métodos estándares de retiro establecidos por los MICS de la parte interesada.

ANOTACIÓN: Implementaciones alternas de manejo de sesión de jugador serán revisadas caso por caso.

3.4.5 <u>Inactividad de Sesión de Juego Inalámbrica.</u> El software de cliente de jugador inalámbrico debe contar con in mecanismo que detecte inactividad de sesión y termine una sesión de juego inalámbrico cuando sea aplicable.

a) Si el dispositivo de Cliente de Jugador Inalámbrico no recibe entrada del jugador dentro de 30 minutos, u otro periodo de tiempo definido por el regulador, la sesión de juego inalámbrico debe expirar y requerir reactivación.
b) Si ocurre dicha terminación, el dispositivo de Cliente de Jugador Inalámbrico debe mostrarle al jugador que la sesión ha expirado e informarle de los pasos necesarios para restablecer la sesión de juego.
   i. Para las sesiones de juego asociadas a cuentas de jugador, el jugador puede establecer una nueva sesión y continuar la jugada al restablecer su acceso al sistema. Este proceso debe incluir, como mínimo, el ingreso manual de la contraseña segura del jugador.
   ii. Para todas las otras sesiones de juego, el dispositivo se debe devolver al punto original de la sesión o al representante de la propiedad para reactivación.

3.4.6 <u>Historial Orientada al Jugador.</u> Una facilidad de 'repetir última jugada' debe ser proporcionada, ya sea como una reconstrucción o por descripción. La repetición debe claramente indicar que es una repetición del previo ciclo de juego entero, y debe proporcionar la información siguiente (como mínimo):

a) La fecha y hora de cuando empezó y/o terminó el juego;
b) La visualización asociada al resultado final del juego, ya sea gráficamente o a través de un mensaje de texto claro;

c) El total de crédito/dinero en efectivo del jugador al inicio y/o final de la jugada;
d) La cantidad total apostada;
e) El dinero en efectivo/créditos totales ganados para el premio (incluyendo los Premios Gordos Progresivos);
f) Los resultados de las elecciones de jugador involucradas en el resultado del juego;
g) Los resultados de las fases de juego intermedias, tales como las apuestas o juegos de facción; y
h) La cantidad de los premios promocionales recibidos (si corresponde).

3.5 Sistema de Juego Inalámbrico - Software

3.5.1 Funcionalidad Requerida.

a) El Sistema de Juego Inalámbrico debe cumplir con todos los requisitos jurisdiccionales aplicables para los Sistemas de Juego Basado en Servidor. A falta de reglas jurisdiccionales especificas, se debe aplicar GLI-21.
b) El Sistema de Juego Inalámbrico debe incorporar un componente de rastreo de ubicación que puede rastrear las ubicaciones de todos los dispositivos de cliente inalámbrico que están conectados al sistema y detectar cuando cualquier dispositivo ha sido transportado fuera del área permitida. Cuando los dispositivos se encuentran fuera del área permitida, el sistema debe deshabilitar cualquier actividad de juego actual o sesiones de operador asociadas con esos dispositivos.

3.5.2 Habilitar/Deshabilitar el Juego. Los siguientes requisitos se aplican a deshabilitar y volver a habilitar el juego en el Sistema de Juego Inalámbrico:

a) El Sistema de Juego Inalámbrico debe ser capaz de deshabilitar o habilitar todo juego a mando;
b) El Sistema de Juego Inalámbrico debe ser capaz de deshabilitar o habilitar juegos individuales a mando;
c) El Sistema de Juego Inalámbrico debe ser capaz de deshabilitar o habilitar sesiones de juego individuales a mando; y
d) Cuando se deshabilita cualquier juego en el Sistema de Juego Inalámbrico, una entrada se debe hacer en un registro de auditoría que incluye la razón por cualquier deshabilitar o habilitar.

3.5.3 Juego Actual. Cuando se deshabilita un juego o actividad de juego:

a) El juego no debe ser accesible al jugador después de que el juego del jugador ha terminado completamente.
b) Se le debe permitir al jugador terminar el juego actual (por ejemplo: rondas de bonificación, duplicar/arriesgar y otras facciones de juego relacionadas a la apuesta inicial deben ser terminadas completamente).
c) Si apuestas se han hecho basadas en eventos de la vida real pendientes:

i. Las pantallas de juego deben claramente definir lo que ocurre con las apuestas si la actividad de juego permanecerá deshabilitada y el evento de la vida real correspondiente es terminado, y el Sistema de Juego Inalámbrico debe ser capaz de devolver todas las apuestas a los jugadores, o resolver todas las apuestas, según sea apropiado.
ii. Las pantallas de juego deben claramente definir lo que ocurre con las apuestas si la actividad de juego se vuelva a habilitar antes de que el evento de la vida real correspondiente se termine, y el Sistema de Juego Inalámbrico debe ser capaz de devolver todas las apuestas a los jugadores, o dejar activas todas las apuestas, según sea apropiado.

3.5.4 ***Juegos Incompletos.*** Un juego es incompleto cuando el resultado del juego se queda sin resolver o el resultado no se puede ver correctamente por el jugador. Juegos incompletos puede ser resultado de:

a) Perdida de comunicaciones entre el Cliente de Jugador Inalámbrico y el sistema de juego;
b) Un reinicio del sistema;
c) Un reinicio o malfuncionamiento del Cliente de Jugador Inalámbrico;
d) Una terminación anormal del Software de Cliente; o
e) Un comando de deshabilitar-juego por el sistema durante la jugada.

3.5.5 ***Terminación de Juegos Incompletos.*** El Sistema de Juego Inalámbrico puede proporcionar un mecanismo para que el jugador pueda completar un juego incompleto. Un juego incompleto se debe resolver antes de permitirle al jugador participar en otra instancia del mismo juego.

a) Si el jugador tiene un juego incompleto, el Sistema de Juego Inalámbrico debe presentar el juego incompleto para ser completado cuando se reconecta o cuando una nueva sesión de jugador se establezca.

i. Cuando no se requiere entrada del jugador para completar el juego, el juego debe mostrar el resultado final según lo determinado por el Sistema de Juego Inalámbrico y las reglas del juego, y la cuenta del jugador se debe actualizar de acuerdo.
ii. Para juegos de un solo jugador y multi-etapa, cuando se requiere entrada del jugador para completar el juego, el juego deber traer el jugador al estado de juego inmediatamente antes de la interrupción y permitirle al jugador completar el juego; y
(*ANOTACIÓN: La adición de una bonificación o facción opcional, como duplicar o arriesgar, no hace que el juego sea multi-etapa.)*

iii. Para juegos multi-jugador, el juego debe mostrar el resultado final según lo determinado por las reglas y/o términos y condiciones del juego, y la cuenta del jugador se debe actualizar de acuerdo.

b) Las apuestas asociadas con un juego incompleto que se puede continuar se deben guardar por el Sistema de Juego Inalámbrico hasta que se complete el juego. Las cuentas de jugador deben incluir fondos guardados en juegos incompletos.

3.5.6 ***Cancelación de Juegos Incompletos.*** Las apuestas asociadas con un juego incompleto que se puede continuar, pero permanece sin decisión por un periodo de tiempo especificado por el cuerpo regulatorio, se puede anular y las apuestas se confiscan o se devuelven al jugador a condición de que:

a) Las reglas y/o los términos y condiciones del juego deben claramente definir como se manejan las apuestas cuando permanecen sin decisión después del periodo de tiempo especificado y el Sistema de Juego Inalámbrico debe ser capaz de devolver o confiscar las apuestas, según corresponda.
b) En el evento que el juego no se pueda continuar debido a una acción del Sistema de Juego Inalámbrico, todas las apuestas se deben devolver a los jugadores de ese juego.

3.5.7 ***Apagada y Recuperación.*** El Sistema de Juego Inalámbrico debe contar con las siguientes capacidades de apagada y recuperación:

a) El Sistema de Juego Inalámbrico debe ser capaz de realizar una apagada segura sin pérdida de información, y permitir el reinicio automático al encender solamente después de ejecutar los siguientes procedimientos como requisito mínimo:
    i. Rutina(s) de continuación de programa, incluyendo auto pruebas, ejecutan exitosamente.
    ii. Todos los componentes de programa de control críticos del Sistema de Juego Inalámbrico han sido autenticados usando un método aprobado (por ejemplo: CRC, MD5, SHA-1, etc.); y
    iii. Se ha establecido e igualmente autenticado la comunicación con todos los componentes necesarios para la operación del Sistema de Juego Inalámbrico.
b) El Sistema de Juego Inalámbrico debe ser capaz de identificar y correctamente manejar la situación donde reinicios principales han ocurrido en otros componentes de juego que afectan el resultado del juego, cantidad de pago, o los informes.
c) El Sistema de Juego Inalámbrico debe contar con la capacidad de restaurar el sistema desde el último respaldo.
d) El Sistema de Juego Inalámbrico debe ser capaz de recuperar toda la información critica desde el momento del último respaldo hasta el momento en que ocurrió la falla o el reinicio del Sistema de Juego Inalámbrico.

3.5.8 ***Malfuncionamiento.*** El Sistema de Juego Inalámbrico debe:

a) No ser afectado por el malfuncionamiento de los Dispositivos de Cliente de Jugador Inalámbrico aparte de para instituir los procedimientos de juegos incompletos de acuerdo con estos requisitos; y

b) Incluir un mecanismo para anular las apuestas y jugadas en el evento de un malfuncionamiento del Sistema de Juego Inalámbrico mismo si una recuperación completa no es posible.

3.5.9 Historial de Lado Administrativo. Para cada juego individual jugado, la siguiente información, en adición a lo requerido anteriormente en la Sección 3.4.6, se debe almacenar, mantener, y demostrar fácilmente por cada sesión del Sistema de Juego Inalámbrico para un periodo definido dentro de los MICS de la parte interesada:

a) ID único del jugador;
b) Contribuciones a los pozos de Premio Gordo Progresivo (si es aplicable);
c) Estado del juego (en progreso, finalizado, etc.);
d) El numero de la mesa (si es aplicable) donde se jugó el juego;
e) La tabla de pago usada; y
f) El identificador y versión del juego.

3.6 Requisitos del Juego

3.6.1 Declaración General. Todo el software del juego para ser utilizado junto con el sistema de juego inalámbrico debe cumplir con los requisitos indicados dentro de los requisitos aplicables de cada jurisdicción para los juegos, para asegurar la equidad del jugador. A falta de reglas jurisdiccionales especificas, se debe aplicar GLI-11.

3.6.2 Entre Pares (P2P). Cuartos de juego P2P son entornos que le ofrecen al jugador la oportunidad de apostar con y contra el uno al otro. En estos entornos, el operador normalmente no participa en el evento de apuestas como un participante (por ejemplo: juegos respaldados por la casa), pero normalmente proporciona el servicio de apuestas o entorno para el uso de sus jugadores, y toma una parte, tarifa, o porcentaje para el servicio. Los sistemas que ofrecen juegos P2P deben cumplir con lo siguiente, a menos que se especifique de otra manera, en adición a las reglas de juego aplicables anteriores:

a) Proporcionar un mecanismo para razonablemente detectar y prevenir la colusión de jugadores, software de jugador artificial, ventajas injustas, y la capacidad de influir el resultado de un juego o torneo;
b) Proporcionar advertencias de cómo los robots pueden afectar el juego, para que los jugadores puedan hacer una decisión informada de participar y proporcionar pasos para denunciar el posible uso de un jugador-robot;
c) No permitir que los jugadores autorizados ocupen más de una silla en cualquier mesa individual;
d) Proporcionarle a los jugadores autorizados la opción de participar en una mesa donde todos los jugadores han sido seleccionados aleatoriamente;
e) Informarle a los jugadores autorizados de la duración de tiempo que cada jugador ha estado sentado en una mesa en particular;
f) Indicar claramente a todos los jugadores autorizados en la mesa si cualquier jugador está

jugando con dinero de la casa (shills) o son jugadores de proposición; y

g) No debe usar software de jugador artificial para actuar como un jugador autorizado, excepto en los modos de jugada gratis o entrenamiento.

3.6.3 ***<u>Jugadores Computarizados.</u>*** Los siguientes requisitos se aplican al uso de jugadores computarizados en modos de jugada gratis o entrenamiento:

a) El software puede contar con el uso de Inteligencia Artificial (AI) para facilitar la jugada de los modos de demonstración, jugada gratis, o entrenamiento.
b) El uso de software AI debe ser claramente explicado en los menús de ayuda.
c) Todos los jugadores computarizados deben ser claramente marcados en las mesas para que los jugadores sepan cuales jugadores no son humanos.

3.6.4 ***<u>Concursos/Torneos.</u>*** Un evento organizado que le permite a un jugador comprar o ganar la oportunidad de participar in la jugada competitiva contra otros jugadores puede ser permitido si se cumplen las siguientes reglas:

a) Mientras habilitado para la jugada de torneo, la facción de torneo no debe aceptar dinero real de cualquier fuente, ni pagar dinero real en cualquier manera, pero debe utilizar créditos, puntos, o fichas específicas de torneo que no tiene valor en efectivo.
b) Las reglas del concurso/torneo de juego inalámbrico deben estar disponibles a un jugador registrado en la aplicación de cliente a través de la cual el concurso/torneo se está realizando. Las reglas deben incluir, como mínimo:
    i. Todas las condiciones que se deben cumplir por los jugadores para entrar al, y avanzar a través del, concurso/torneo.
    ii. Cualquier condición con respecto a entradas tardes o torneos completamente vacios y como se maneja la auto colocación ciega y/o la compra de entrada inicial.
    iii. Información especifica relacionada con cualquier concurso/torneo individual, incluyendo la cantidad de dinero colocado en el pozo del premio.
    iv. La distribución de fondos basado en resultados específicos.
    v. El nombre de la organización (o personas) que realizó el concurso/torneo de parte de, o conjunto con, el operador si es aplicable.

c) El resultado de cada concurso/torneo debe estar disponible en el software de cliente de juego inalámbrico para la revisión por los participantes. Posterior a ser publicados, los resultados de cada concurso/torneo están disponibles a pedido del establecimiento de juego. El registro incluye lo siguiente:
    i. Nombre del evento;
    ii. Fecha(s) del evento;
    iii. Número total de entradas;
    iv. Cantidad de cuotas de entrada;
    v. Total del pozo de premio; y
    vi. Cantidad pagada por cada categoría ganadora.

ANOTACIÓN: Para los concursos/torneos gratis (por ejemplo: el jugador registrado no paga una cuota de entrada), la información requerida por lo anterior se debe registrar excepto por el número de entradas, cantidad de cuotas de entrada, y el total del pozo de premio.

3.7 Requisitos del Generador de Números Aleatorios (RNG)

3.7.1 ***Declaración General.*** El generador de número aleatorio que se usara en conjunto con el sistema de juego inalámbrico debe ser criptográficamente fuerte en el momento de presentación y cumplir con los requisitos de aleatoriedad establecidos por la autoridad jurisdiccional solicitada. A falta de reglas jurisdiccionales especificas, se deben aplicar los requisitos de RNG de GLI-11.

3.8 Impuestos

3.8.1 ***Declaración General.*** El Sistema de Juego Inalámbrico debe soportar un mecanismo que es capaz de identificar todas las ganancias que están sujetas a los impuestos y proporcionar la información necesaria de acuerdo con los requisitos de impuestos de cada jurisdicción.

CAPÍTULO 4

4.0 REQUISITOS DE SEGURIDAD DE LA RED INALÁMBRICA

4.1 Requisitos de Encriptación y Autenticación Inalámbrica

4.1.1 ***<u>Declaración General.</u>*** Esta sección define los requisitos de encriptación y autenticación para la red inalámbrica siendo utilizada para comunicar información del juego. GLI requiere el uso de autenticación de usuario, autorización, y encriptación fuerte.

a) Todas las soluciones de WLAN (Red de Área Local Inalámbrica) deben proporcionar autenticación de múltiples factores al nivel de la red y del dispositivo.

   ANOTACIÓN: El laboratorio de ensayos examinará las metodologías de encriptación y autenticación segura caso por caso.

b) Si el router soporta autenticación WPA2, se deben habilitar como sigue:
   i. Todos los Puntos de Acceso deben ser configurados con el Modo Enterprise habilitado o con una llave fuerte compartida previamente.
   ii. Todos los Puntos de Acceso deben cumplir con el IEEE 802.11
c) Una contraseña u otro método seguro según lo definido en los MICS de la parte interesada debe ser habilitado para cada cliente que se conecte a la red.
d) Un método de respaldo para la autenticación inalámbrica fallida (por ejemplo: contraseñas olvidadas) debe ser por lo menos igual de fuerte al método principal. Este método de respaldo se debe detallar en los MICS de la parte interesada.
e) Estándares de Encriptación Avanzados (AES) o equivalente con un mínimo de encriptación de 256 bit se debe usar para soportar los servicios de integridad y confidencialidad.
f) La Llave Maestra Por Pares (PMK) utilizada debe contar con una vida de 24 horas o menos. Alternativamente, es aceptable que el PMK se cambie durante tiempo bajo de mantenimiento previamente programado como se describe en un documento de control interno.
g) La Llave Maestra Por Grupo (GMK) utilizada debe contar con una vida de 8 horas o menos.

4.1.2 ***<u>Privacidad Equivalente a Por Cable (WEP).</u>*** WEP no se debe usar.

ANOTACIÓN: Si no es posible para el fabricante implementar el protocolo WPA2, el laboratorio examinará le implementación de WEP como una encriptación y autenticación segura caso por caso.

4.2 Protocolo de Comunicación Inalámbrica

4.2.1 ***General.*** Cada red inalámbrica revisada por el laboratorio de ensayos independiente se examinará completamente para asegurar que la configuración de campo propuesta es segura. El laboratorio de ensayos independiente puede proporcionar recomendaciones de seguridad adicionales y proporcionare entrenamiento en el campo al operador de la red, si se solicita.

4.2.2 ***Datos Delicados.*** La comunicación de datos delicados debe ser segura contra espionaje, acceso, modificación, intrusión, o alteración sin autorización. Datos delicados incluyen, pero no se limitan a:

a) Semillas y resultados de RNG;
b) Llaves de encriptación, donde la implementación seleccionada requiere la transmisión de llaves;
c) PIN/Contraseñas;
d) Transferencia de fondos;
e) Información sobre el rastreo de jugador;
f) Paquetes de Descarga; y
g) Cualquier información que afecte el resultado del juego.

4.2.3 ***Protocolo(s) de Comunicación.*** Cada dispositivo debe ser evaluado caso por caso por los operadores de la red y por el laboratorio de ensayos independiente.

a) Cada componente de una red inalámbrica que comunica información del juego debe utilizar un protocolo de comunicaciones con encriptación y autenticación.
b) Cada componente de una red inalámbrica debe funcionar de acuerdo a su protocolo de comunicaciones implementado.
c) Los dispositivos que usan un transporte de comunicación no seguro (por ejemplo: Bluetooth) no se debe usar para cualquier función que afecta la jugada, la gestión de la cuenta del jugador, o cualquier otra función de juego critica.

4.2.4 ***Comunicación de Dispositivo Inalámbrico con Otros Sistemas.*** En el evento que los componentes de la porción inalámbrica de la red se utilicen en conjunción con otros sistemas de cable tradicionales; (por ejemplo: Sistemas de Monitoreo y Control En Línea, Sistemas de Validación de Tiquete, Sistemas Progresivos, etc.) las comunicaciones entre el dispositivo inalámbrico y la red tradicional deben cumplir con lo siguiente:

a) Todas las comunicaciones deben pasar a través de por lo menos un contrafuegos al nivel aplicación aprobado, y no proporcionar una ruta alternativa a menos que la ruta alternativa cumpla con los requisitos de este documento y cuenta con seguridad independiente (por ejemplo: llaves no iguales a las de otras redes), y
b) Todas las comunicaciones se deben realizar utilizando los métodos de autenticación y seguridad de red indicados en este estándar.

4.2.5 ***<u>Seguridad de Software de Red Inalámbrica.</u>*** Una red inalámbrica debe:

a) Implementar un método de seguridad que une los clientes y/o dispositivos al servidor, de tal manera que el software solo se puede usar por clientes y/o dispositivos autorizados.
b) Implementar un esquema de seguridad que utiliza llaves de seguridad metamórficas. En general, si se usan las llaves o semillas, no deben ser fuertemente codificadas y deben cambiar automáticamente, a través del tiempo, como una función del enlace de comunicación. Cada método debe ser revisado caso por caso por el operador de la red y el laboratorio de ensayos independiente.
c) Realizar autenticación mutua para asegurar que los clientes solo se comuniquen con las redes validas.
d) Validar los clientes y dispositivos a intervalos de tiempo predefinidos con por lo menos un método de autenticación como indicado anteriormente. Este intervalo de tiempo debe ser configurable basado en los requisitos del operador de la red.
e) Cerrar las sesiones activas si la autenticación de usuario ha superado el número de intentos fallidos. El número de intentos fallidos debe ser configurable basado en los requisitos del operador de la red/parte interesada.
f) Proporcionar un informe imprimible de los intentos de acceso a la red fallidos, incluyendo:
    i. Estampilla de hora y fecha,
    ii. Nombre del dispositivo, y
    iii. Identificador de hardware de todos los dispositivos solicitando acceso a la red.

4.2.6 ***<u>Métodos de Autenticación de la Red Inalámbrica.</u>*** Las comunicaciones entre los dispositivos en la red inalámbrica deben usar protocolos diseñados para asegurar, autenticar, y encriptar las redes inalámbricas. Uno de los siguientes protocolos de túneles encriptados debe ser utilizado para asegurar la comunicación de toda la información relacionada al juego sobre una red inalámbrica:

a) Protocolo de Autenticación Extensible Protegido (EAP Protegido o PEAP),
b) Protocolo de Autenticación Extensible – Seguridad de Capa de Transporte (EAP-TLS),
c) Protocolo de Autenticación Extensible - Seguridad de Capa de Transporte Tunelizado (EAP-TTLS),
d) Red Privada Virtual con L2TP/IPsec (VPN),
e) Protocolo Tunelizado Punto a Punto (PPTP), o
f) Capa de Sockets Seguros (SSL).

ANOTACIÓN: Estos métodos son autenticados contra los servidores LDAP, RADIUS, Kerberos o Microsoft Active Directory en adición a los bases de datos locales almacenados en el controlador de entrada segura. La implementación de cualquier otro método se evaluará caso por caso.

ANOTACIÓN Los esquemas de autenticación que usan la Infraestructura de Llave Publica deben requerir validación de certificado. Idealmente, en ambas direcciones (por ejemplo: certificados de cliente).

ANOTACIÓN: Métodos de autenticación y encriptación alternos se evaluaran caso por caso.

4.2.7 Fallas de Componente. La red inalámbrica debe contar con suficiente redundancia y modularidad para admitir la falla de un componente para prevenir la interrupción de las operaciones inalámbricas. Deben existir copias redundantes de cada registro de auditoría y base de datos de sistema, cuando sea aplicable, en el servidor inalámbrico con soporte abierto para los respaldos y la restauración. Esto incluye una red inalámbrica que cuenta con soporte para redundancia de conmutación por error. Una implementación de esquema de respaldo debe ocurrir en cumplimiento con la Política de Recuperación de Desastre, aunque todos los métodos se evaluaran caso por caso por el laboratorio de ensayos independiente.

4.2.8 Requisitos de Recuperación. En el evento de una falla catastrófica, cuando la red inalámbrica no se puede reiniciar de cualquier otra manera, debe ser posible volver a cargar el sistema desde el último punto de respaldo viable y completamente recuperar el contenido de ese respaldo. Los respaldos deben consistir de por lo menos la siguiente información, según corresponda:

a) Eventos significados,
b) Información de auditoría, y
c) Información especifica del lugar, como configuraciones únicas, cuentas de seguridad, etc.

4.2.9 Requisitos de Autorización de Usuario. El Sistema Inalámbrico debe implementar los siguientes requisitos de autorización de usuario:

a) Los sistemas inalámbricos deben utilizar un mecanismo seguro y controlado que es capaz de verificar que el dispositivo inalámbrico está siendo operado por una persona autorizada.
b) El mecanismo debe poder ser iniciado a pedido y regularmente.
c) Cualquier información de autorización comunicada por el dispositivo inalámbrico hacia el sistema para propósitos de identificación se debe obtener en el momento de la solicitud desde el sistema inalámbrico y no ser almacenado en el dispositivo de cliente inalámbrico.

ANOTACIÓN: Dispositivos estacionarios que no pueden ser movidos por el cliente pueden ser exento de estos requisitos caso por caso.

4.2.10 Conectividad. El sistema Inalámbrico debe proporcionar métodos para:

a) Inscribir y anular inscripción de los componentes;

b) Habilitar y deshabilitar componentes de sistema específicos;
c) Asegure que solamente los componentes de sistema inscritos y habilitados participen en el sistema de juego inalámbrico; y
d) Asegurar que la condición por defecto para todos los componentes debe ser no inscrito y deshabilitado.

CAPÍTULO 5

5.0 REQUISITOS DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN (ISS)

5.1 Declaración General

5.1.1 ***Declaración General.*** Para asegurar que los jugadores no estén expuestos a riesgos de seguridad innecesarios, estos requisitos de seguridad se aplican a los siguientes componentes críticos del Sistema Inalámbrico:

a) Los componentes del Sistema Inalámbrico que graban, almacenan, procesan, comparten, transmiten, o recuperan información delicada del jugador, por ejemplo: detalles de transacción, información de autenticación, saldos de cuenta de jugador;
b) Los componentes del Sistema Inalámbrico que generan, transmiten, o procesan números aleatorios usados para determinar el resultado de los juegos o eventos virtuales;
c) Los componentes del Sistema Inalámbrico que almacenan resultados o el estado actual de la apuesta de un jugador;
d) Los puntos de entrada y salida de los sistemas anteriores (otros sistemas que pueden comunicar directamente con sistemas críticos centrales); y
e) Las redes inalámbricas que transmiten información delicada del jugador.

5.2 Política de Seguridad de Información

5.2.1 ***Declaración General.*** Un documento de la política de seguridad de información debe estar en vigor para describir el enfoque del operador para gestionar le seguridad de información de seguridad y su implementación. La política de seguridad de información debe:

a) Contar con una estipulación que requiere una revisión cuando ocurren cambios al Sistema Inalámbrico o a los procesos del operador que alteran el perfil de riesgo del Sistema Inalámbrico;
b) Ser aprobado por la gerencia;
c) Ser comunicado a todos los empleados e partes externas relevantes;
d) Someterse a revisión a intervalos planificados; y
e) Delinear las responsabilidades del personal del operador y de cualquier tercero para la operación, servicio, y mantenimiento del Sistema Inalámbrico y/o sus componentes.

5.3 Controles Administrativos

5.3.1 ***<u>Seguridad de Recursos Humanos.</u>*** Las labores y responsabilidades de seguridad de los empleados deben estar definidas y documentadas de acuerdo a la política de seguridad de información.

a) Todos los empleados de la organización deben recibir entrenamiento de conocimiento de seguridad apropiado y actualizaciones regulares a las políticas y procedimientos organizativos según sea necesario para su función de trabajo.
b) Una política de control de acceso debe ser establecida, documentada, y revisada basada en los requisitos de seguridad y negocio para el acceso físico y lógico al Sistema Inalámbrico y/o sus componentes.
c) A los empleados solo se les debe proporcionar acceso a los servicios o facilidades a las que tienen autorización para usar.
d) La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares usando un proceso formal.
e) Los derechos de acceso de todos los empleados al Sistema Inalámbrico y/o sus componentes debe ser retirado cuando termina su empleo, contrato, o acuerdo, o ajustado en caso de cambio.

5.3.2 ***<u>Servicios de Terceros.</u>*** Las labores y responsabilidades de los proveedores de servicio de terceros deben estar definidas y documentadas de acuerdo a la política de seguridad de información.

a) Los acuerdos con proveedores de servicio de terceros involucrando acceder, procesar, comunicar, o gestionar el Sistema Inalámbrico y/o sus componentes, o agregar productos o servicios al Sistema Inalámbrico y/o sus componentes deben incorporar todos los requisitos de seguridad relevantes.
b) Los servicios, informes, y registros proporcionados por el tercero deben ser monitoreados y revisados por la gerencia por lo menos una vez al año.
c) Los cambios a la provisión de servicios, incluyendo mantener y mejorar las políticas, procedimientos, y controles de seguridad de información existentes, deben ser gestionados, teniendo en cuenta la criticidad de los sistemas y procesos de negocio implicados y la reevaluación de riesgos.
d) Los derechos de acceso de los proveedores de servicio de terceros al Sistema Inalámbrico y/o sus componentes deben ser retirados cuando se termina su contrato o acuerdo, o ajustado en caso de cambio.

5.3.3 ***<u>Gestión de Activos.</u>*** Todos los activos que almacenen, procesen, o comuniquen información controlada, incluyendo los que componen el entorno de operación del Sistema Inalámbrico y/o sus componentes, se deben contabilizar y tener un dueño nominado de acuerdo con la política de seguridad de información.

a) Un inventario de todos los activos que contienen artículos controlados se debe redactar y mantener.
b) Los activos se deben clasificar en términos de su criticidad, delicadez, y valor.

c) Cada activo debe tener un "dueño" designado el cual es responsable de asegurar que la información y los activos están apropiadamente clasificados, y de definir y periódicamente revisar las clasificaciones y restricciones de acceso.
d) Una política se debe incluir con respecto al uso aceptable de los activos asociados con el Sistema Inalámbrico y su entorno de operación.
e) Un procedimiento debe existir para retirar los activos de servicio y agregar nuevos activos.
f) Al equipamiento retirado de servicio se le debe sacar el medio de almacenamiento y deshacerlo de forma segura usando procedimientos documentados.
g) El medio de almacenamiento removible se debe deshacer de forma segura cuando ya no se necesita, usando procedimientos documentados.

5.3.4 ***Gestión de Llaves de Encriptación.*** La gestión de llaves de encriptación debe seguir procesos definidos de acuerdo con la política de seguridad de información.

a) Debe existir un proceso documentado para obtener o generar laves de encriptación.
b) Si las llaves de encriptación expiran, debe existir un proceso documentado para gestionar la expiración de las llaves de encriptación.
c) Debe existir un proceso documentado para revocar las llaves de encriptación.
d) Debe existir un proceso documentado para cambiar de forma segura el conjunto de llaves de encriptación actual.
e) Debe existir un proceso documentado para el almacenamiento de cualquier llave de encriptación.
f) Debe existir un método para recuperar la información encriptada con una llave de encriptación revocada o expirada para un periodo de tiempo definido después de que la llave queda invalida.

5.3.5 ***Ciclo Vital del Desarrollo de Software.*** La adquisición y desarrollo de software nuevo debe seguir unos procesos definidos de acuerdo con la política de seguridad de información.

a) El entorno de producción debe ser lógicamente y físicamente separada de los entornos de desarrollo y ensayos.
b) El personal de desarrollo se debe excluir de tener acceso de promover cambios al código en el entorno de producción.
c) Debe existir un método documentado para verificar que el software de prueba no se implemente en el entorno de producción.
d) Para prevenir la perdida de información de identificación personal, debe existir un método documentado para asegurar que los datos de producción sin procesar no se usen en los ensayos.
e) Toda la documentación relacionada al desarrollo de software y aplicación debe estar disponible y conservada para la duración del ciclo vital.

5.3.6 ***Control de Cambios.*** La implementación de cambios al hardware y software del Sistema Inalámbrico debe ser gestionada por el uso de procedimientos de control de cambio formales de acuerdo con la política de seguridad de información.

a) Lo procedimientos de control de cambio de programa deben ser adecuados para asegurar que solamente las versiones de programas correctamente aprobados y evaluados se implementen en el sistema inalámbrico de producción. Los controles de cambio de producción deben incluir:
    i. Un mecanismo o control de versión de software apropiado para todos los componentes de software;
    ii. Detalles de la razón por el cambio;
    iii. Detalles de la persona realizando el cambio;
    iv. Respaldos completos de las versiones previas del software;
    v. Una política dirigiéndose a los procedimientos de cambio de emergencia;
    vi. Procedimientos para las pruebas y migración de cambios;
    vii. Segregación de los deberes entre los desarrolladores, el equipo de control de calidad, el equipo de migración, y los usuarios; y
    viii. Procedimientos para asegurar que la documentación técnica y de usuario se actualice como resultado de un cambio.
b) Todos los parches se deben evaluar cuando posible en un sistema inalámbrico configurado idénticamente al sistema inalámbrico de destino. Bajo circunstancias donde la evaluación del parche no se puede realizar completamente a tiempo para cumplir con el cronograma para el nivel de severidad de la alerta, la evaluación del parche se debe gestionar con respecto a riesgo., ya sea por aislar o retirar el sistema inalámbrico no evaluado de la red o por aplicar el parche y evaluar después del hecho.

5.3.7 ***Gestión de Incidente.*** Un proceso para informar de los incidentes de seguridad de información y la respuesta de Gestión se debe documentar de acuerdo a la política de seguridad de información.

a) El proceso de gestión de incidente debe incluir una definición de que constituye un incidente de seguridad de información.
b) El proceso de gestión de incidente debe documentar como los incidentes de seguridad de información se informan a través de los canales de gestión apropiados.
c) El proceso de gestión de incidente debe abordar los procedimientos y responsabilidades de la Gerencia para asegura una respuesta rápida, efectiva, y ordenada a los incidentes de seguridad de información, incluyendo:
    i. Procedimientos para manejar diferentes tipos de incidente de seguridad de información;
    ii. Procedimientos para el análisis e identificación de la causa del incidente;
    iii. Comunicación con los afectados por el incidente;
    iv. Informar el incidente a la autoridad apropiada;
    v. Colecta de evidencia forense; y
    vi. Recuperación controlada de los incidentes de seguridad de información.

5.3.8 ***Continuidad de Negocio y Recuperación de Desastre.*** Un plan debe existir para recuperar las operaciones de juego en el evento que el sistema de juego de producción se vuelve inoperable.

a) El plan de recuperación de desastre debe abordar el método de almacenar información de cuenta de jugador y datos del juego para minimizar la perdida en el evento que el sistema de juego de producción se vuelve inoperable. Si replicación asincrónica se usa, el método para recuperar la información se debe describir o la perdida de información potencial se debe documentar.
b) El plan de recuperación de desastre debe delinear las circunstancias bajo cuales se debe invocar.
c) El plan de recuperación de desastre debe abordar el establecimiento de un sitio de recuperación físicamente separado del sitio de producción.
d) El plan de recuperación de desastre debe contener guías de recuperación que detallan los pasos técnicos requeridos para restablecer la funcionalidad de juego al sitio de recuperación.
e) El plan de continuidad de negocio debe abordar los procesos requeridos para resumir las operaciones administrativas de las actividades de juego después de la activación de la plataforma recuperada para un rango de escenarios apropiado para el contexto operacional del Sistema Inalámbrico.

5.4 Controles Técnicos

5.4.1 Auto Monitoreo.

a) El Sistema Inalámbrico debe implementar el auto monitoreo de componentes críticos (por ejemplo: anfitriones centrales, dispositivos de la red, contrafuegos, enlaces a terceros, etc.).
b) Un componente critico que falla las pruebas de auto monitoreo se debe retirar de servicio inmediatamente.
c) La red debe ser redundante para que después del paso b) anterior no resulte en una condición de negación de servicio.

5.4.2 Requisitos del Servicio de Nombre de Dominio (DNS).

a) El servidor principal usado para resolver las solicitudes de DNS usadas en asociación con el Sistema Inalámbrico deben estar localizadas físicamente en un centro de datos seguro.
b) El acceso lógico y físico al servidor principal DNS debe limitarse al personal autorizado.
c) Las transferencias de zona a servidores arbitrarios no se debe permitir.

5.4.3 Monitoreo.

a) Los relojes de todos los componentes del Sistema Inalámbrico deben estar sincronizados con una fuente de tiempo precisa acordada para asegurar el registro consistente. Distorsión del tiempo se debe revisar periódicamente.
b) Los registros de auditoría que graban las actividades del usuario, excepciones, y eventos de seguridad de información se deben producir y mantener por un periodo apropiado para asistir en las futuras investigaciones y monitoreo de control de acceso.

c) Las actividades del Administrador de Sistema y el Operador de Sistema se deben registrar.
d) Las facilidades de registro y la información de registro se deben proteger contra la manipulación y el acceso sin autorización.
e) Cualquier modificación, intento de modificación, acceso de lectura, u otro cambio o acceso a cualquier registro, auditoria, o registro de sistema inalámbrico debe ser detectable por el Sistema Inalámbrico. Debe ser posible ver quien ha visto o alterado un registro y cuando.
f) Los registros generados por actividades de monitoreo se deben revisar periódicamente usando un proceso documentado. Se debe mantener un registro de cada revisión.
g) Las fallas del Sistema Inalámbrico se deben registrar, analizar, y tomar la acción apropiada.
h) Los dispositivos de la red con almacenamiento limitado a bordo deben deshabilitar toda comunicación si el registro de auditoría se llena o descargar los registros a un servidor de registro dedicado.

5.4.4 ***Controles Criptográficos.*** Una política en el uso de controles criptográficos para la protección de información se debe desarrollar e implementar.

a) Cualquier información delicada o de identificación personal debe ser encriptada si pasa a través de una red con un nivel de confianza menor.
b) Información que no se necesita esconder pero se va a autenticar debe usar alguna forma de técnica de autenticación de mensaje.
c) La autenticación debe usar un certificado de seguridad de una organización aprobada.
d) El grado de encriptación usado debe ser apropiado para la delicadez de la información.
e) El uso de los algoritmos de encriptación debe ser revisado periódicamente por personal de Gerencia calificado para verificar que los algoritmos de encriptación actuales son seguros.
f) Los cambios a los algoritmos de encriptación para corregir debilidades se deben implementar tan pronto como sea posible. Si tales cambios no están disponibles, se debe reemplazar el algoritmo.
g) Las llaves de encriptación no se deben almacenar sin ellas mismas ser encriptadas a través de un método de encriptación diferente y/o por el uso de una llave de encriptación diferente.

5.4.5 ***Controles de Acceso.*** La asignación de privilegios de acceso debe ser limitada y controlada basada en los requisitos de negocio y el principio de privilegio mínimo.

a) Un procedimiento formal de registración y cancelación de registro debe existir para otorgar y revocar el acceso a todos los servicios y sistemas de información.
b) Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal solamente, y una técnica de autenticación adecuada se debe escoger para comprobar la identidad declarada de un usuario.
c) El uso de cuentas genéricas se debe limitar, y se deben documentar formalmente las razones de uso donde se usen estas cuentas.
d) La provisión de contraseñas se debe controlar a través de un proceso de gestión formal.

e) Las contraseñas deben cumplir con los requisitos de negocio para longitud, complejidad, y duración de vida.
f) El acceso a las aplicaciones y sistemas operativos del Sistema Inalámbrico debe ser controlado por un procedimiento de entrada seguro.
g) Métodos de autenticación apropiados, en adición a las contraseñas, se deben usar para controlar el acceso de usuarios remotos.
h) Se debe registrar cualquier acceso físico a las áreas que albergan los componentes del Sistema Inalámbrico, y cualquier acceso lógico a las aplicaciones o sistema operativo del Sistema Inalámbrico.
i) El uso de identificación automática de equipo para autenticar las conexiones desde localizaciones y equipos específicos se debe documentar formalmente y se debe incluir en la revisión regular de los derechos de acceso por la Gerencia.
j) Los límites en tiempos de conexión se deben usar para proporcionar seguridad adicional para las aplicaciones de alto riesgo.
k) El uso de programas de utilidad que pueden ser capaces de anular los controles de aplicación y de sistema debe ser limitado y estrictamente controlado.
l) Una política formal debe existir, y medidas de seguridad apropiadas deben ser adoptadas para proteger contra los riesgos de usar facilidades de informática y comunicación móvil.
m) El teletrabajo al sistema inalámbrico no se debe permitir excepto bajo las circunstancias donde la seguridad del punto final se puede garantizar.

5.4.6 ***Gestión de Seguridad de la Red.*** Las redes deben estar lógicamente separadas de tal manera que no debe existir trafico de red en un enlace de red que no puede ser atendido por los anfitriones en ese enlace.

a) La falla de cualquier artículo unitario no debe resultar en una negación de servicio.
b) Un Sistema de Detección de Intrusión / Sistema de Prevención de Intrusión debe estar instalado en la red que pueda:
    i. Escuchar las comunicaciones internas y externas;
    ii. Detectar o prevenir los ataques de Distributed Denial of Service (DDOS);
    iii. Detectar o prevenir que shellcode pase a través de la red;
    iv. Detectar o prevenir fraude del Address Resolution Protocol (ARP);
    v. Detectar otros indicadores de Hombre-en-el-Medio e inmediatamente cortar comunicaciones si se detecta;
    vi. Escanear la red inalámbrica para cualquier dispositivo inalámbrico fraudulento o no autorizado conectado a cualquier punto de acceso en la red inalámbrica. Este escaneo se debe realizar por lo menos una vez por trimestre o como definido en los MICS de la parte interesada;
    vii. Escanear la red inalámbrica para cualquier punto de acceso fraudulento. Este escaneo se debe realizar por lo menos una vez por trimestre o como definido en los MICS de la parte interesada;
    viii. Automáticamente deshabilitar cualquier dispositivo inalámbrico fraudulento o no autorizado conectado al sistema;
    ix. Mantener un registro historial de todo acceso inalámbrico para por lo menos los 90 días previos o un periodo definido dentro de los MICS de la parte interesada. Este registro debe contener información completa y detallada de todos los dispositivos inalámbricos involucrados, y debe

poder ser reconciliado con todos los otros dispositivos de red dentro de la propiedad o Lugar de Juego;

c) En los entornos virtuales, las instancias de servidor redundantes no pueden correr bajo el mismo hipervisor.
d) No se deben usar protocolos sin estado (por ejemplo: UDP) para información delicada sin transporte con estados.
e) Todos los cambios a la infraestructura de la red (por ejemplo: configuración del dispositivo de la red) se deben registrar.
f) Escáneres de virus y/o programas de detección deben estar instalados en todos los sistemas de información pertinentes. Estos programas se deben actualizar regularmente para escanear para nuevos tipos de virus.
g) La seguridad de la red se debe evaluar regularmente por un individuo calificado y con experiencia.
h) Los ensayos deben incluir ensayos de los interfaces externos (públicos) y la red interna.
i) Los ensayos de cada dominio de seguridad en la red interna se deben realizar separadamente.

5.4.7 Cortafuegos (Firewalls).

a) Un cortafuegos debe estar localizado en la frontera de cualquier dos dominios de seguridad diferentes.
b) Todas las conexiones a los anfitriones del Sistema Inalámbrico en el centro de datos seguro deben pasar a través de por lo menos un contrafuego de nivel aplicación. Esto incluye las conexiones entre cualquier anfitrión no del Sistema Inalámbrico usado por el operador.
c) El contrafuego debe ser un dispositivo de hardware separado que cuenta con las siguientes características:
    i. Solamente las aplicaciones relacionadas al contrafuego puede residir en el contrafuego; y
    ii. Solamente un número limitado de cuentas puede estar presente en el contrafuego (por ejemplo: solamente los administradores de sistema).
d) El contrafuego debe rechazar todas las conexiones excepto las que han sido específicamente aprobadas.
e) El contrafuego debe rechazar todas las conexiones desde destinos que no pueden residir en la red de donde origino el mensaje (por ejemplo: dirección RFC1918 en el lado publico de un contrafuego de internet.)
f) El contrafuego debe mantener un registro de auditoría de todos los cambios a los parámetros que controlan las conexiones permitidas a través del contrafuego.
g) El contrafuego debe mantener un registro de auditoría de todos los intentos de conexión exitosos y fallidos. Los registros se deben conservar por 90 días y una muestra se debe revisar por tráfico inesperado cada mes. Se recomienda que las direcciones IP de fuente y de destino sean registradas para cada instancia.
h) El contrafuego debe deshabilitar toda comunicación si el registro de auditoría se llena.
i) El límite del número de intentos de conexión fallidos debe ser un parámetro configurable por el operador de la red; y puede ser utilizado para rechazar más solicitudes de conexión si se sobrepasa el límite. Si se sobrepasa el límite, los operadores se deben notificar.

5.4.8 ***Acceso Remoto.*** El acceso remoto es definido como cualquier acceso fuera del sistema o de la red del sistema incluyendo cualquier acceso de otras redes dentro del mismo establecimiento. El acceso remoto solamente se debe permitir si está autorizado por el cuerpo regulatorio y debe tener la opción de ser deshabilitado. Donde se permite, el acceso remoto solo debe aceptar las conexiones remotas permitidas por la aplicación del contrafuego y las configuraciones del Sistema Inalámbrico. La seguridad del acceso remoto será revisada caso por caso, en conjunción con la implementación de la tecnología actual y la aprobación del cuerpo regulatorio local. En adición, debe:

a) No existir funcionalidad de administración de usuario remoto no autorizada (agregar usuarios, cambiar permisos, etc.);
b) No existir acceso no autorizado a cualquier base de datos que no sea para recuperar información usando funciones existentes;
c) No existir acceso no autorizado al sistema operativo; y
d) El Sistema Operativo debe mantener un registro de actividad que se actualiza automáticamente el cual muestra toda la información de acceso remoto.

5.4.9 ***Respaldo.*** Las copias de respaldo de información y software se deben tomar y evaluar regularmente de acurdo con la política de respaldo.

5.5 Controles Físicos y Ambientales

5.5.1 ***Áreas Seguras.*** Los sistemas inalámbricos y los sistemas de comunicación asociados deben estar localizados en las instalaciones que proporcionen protección física contra el daño de fuego, inundación, huracán, terremoto, y otras formas de desastre natural o hecho por el hombre.

a) Perímetros de seguridad (barreras como paredes, portales de entrada controlados por tarjeta, o recepción atendida) se deben usar para proteger las áreas que contienen los componentes de Sistema Inalámbrico.
b) Las áreas seguras se deben proteger con controles de entrada apropiados para asegurar que el acceso es limitado solamente a personal autorizado.
c) Todo acceso se debe registrar en un registro de auditoría seguro.
d) Las áreas seguras deben incluir un sistema de detección de intrusión, y los intentos de acceso no autorizado de deben registrar.

5.5.2 ***Seguridad del Equipo de Juegos.*** Los servidores del Sistema Inalámbrico deben estar localizados un una área que limita el acceso no autorizado.

5.5.3 ***Utilidades de Soporte.***

a) Se les debe proporcionar suficiente electricidad principal a todos los componentes de Sistema Inalámbrico.

b) Todos los componentes de Sistema Inalámbrico responsables por las operaciones lógicas o el almacenamiento de información del sistema deben tener equipo de fuente de electricidad ininterrumpida (UPS) para soportar las operaciones en el evento de un fallido de electricidad.
c) Debe existir protección contra fuego y enfriamiento adecuado para los componentes de Sistema Inalámbrico.
d) Los cables de electricidad y telecomunicaciones que llevan información o servicios de información de soporte deben estar protegidos contra la interceptación o daño.

Glosario

Referencia	Definición
Active Directory (Directorio Activo)	Active Directory es una implementación de los servicios de directorio LDAP de Microsoft para el uso en los entornos de Windows.
AES	Estándares de Encriptación Avanzada
CCMP	Protocolo de Counter Mode CBC MAC
Software de Cliente	El software instalado en un Dispositivo de Cliente Inalámbrico que facilita la comunicación entre el Interfaz de Jugador u Operador y el Sistema Inalámbrico. Ejemplos de Software de Cliente incluyen paquetes de descarga propios, html, flash, etc.
Cuentas predeterminadas	Las cuentas de usuario con niveles de acceso predeterminados usualmente creadas por defecto cuando se instalan los sistemas operativos, bases de datos, y aplicaciones.
Digital Certificate (Certificado Digital)	Un conjunto de datos que se puede usar para verificar la identidad de una entidad por hacer referencia a un tercero confiado (La Autoridad de Certificación). Los certificados digitales frecuentemente se usan para autenticar los mensajes para propósitos no repudios. Uno de las características de un certificado digital es que no se puede modificar sin comprometer su consistencia interna. Los certificados X.509 son un ejemplo de un certificado digital.
Domain Name Service (Servicio de Nombre de Dominio)	El base de datos de Internet distribuido globalmente que (en adición a otros) relaciona los nombres de maquinas a los números IP y viceversa.
EAP	Protocolo de Autenticación Extensible
EAP-TLS	Protocolo de Autenticación Extensible – Seguridad de Capa de Transporte
EAP-TTLS	Protocolo de Autenticación Extensible - Seguridad de Capa de Transporte Tunelizado
Ancho de Banda Efectivo	La cantidad de información que realmente puede ser transferida a través de una red por unidad de tiempo. El ancho de banda efectivo a través de Internet es normalmente menor que el ancho de banda efectivo de cualquier enlace constituyente.
FIPS	Estándar de Proceso de Información Federal
Contrafuego	Una barrera de seguridad de la red. Un contrafuego es un dispositivo que protege la entrada a una red privada y prohíbe la entrada de tráfico no autorizado.
Cuentas de usuario genéricas	Cuentas de usuario que se comparten entre múltiples usuarios (usando la misma contraseña) para obtener acceso a cualquier componente de un sistema de juego, aplicación, base de datos, o sistema operativo.
GMK	Llave Principal de Grupo
HTTP	Protocolo de Transporte Hypertext

IEEE	Instituto de Ingenieros Eléctricos y Electrónicos
LAN	Red de Área Local
LDAP	Protocolo de Acceso de Directorio Liviano
Utilización de Enlace	El porcentaje de tiempo en que un enlace de comunicaciones está transmitiendo información.
MAC	Control de Acceso Mediano
PEAP	Protocolo de Autenticación Extensible Protegido
PMK	Llave Principal Por Parejas
Protocolo	Usado para referir a los interfaces de hardware, disciplina de línea, y formatos de mensaje de las comunicaciones.
PTK	Llave Transitoria Por Parejas
RADIUS	Servicio de Autenticación Remota de Usuario Telefónico
Datos Delicados	Datos que, si se obtienen por un tercero, se pueden usar para afectar el resultado del juego o las cuentas de los jugadores.
Cuentas de servicio	Cuentas en que dependen las funciones de sistema automáticas para poder ser realizadas. Estas cuentas, definidas al nivel de sistema operativo, proporcionan un nivel de acceso necesario para la operación normal de las aplicaciones y/o los procesos por lotes automáticos.
SNMP	Protocolo de Gestión de Red Simple
SSID	Identificador de Set de Servicio, nombre de la Red
TKIP	Protocolo de Integridad de Llave Integral
Control de Versión	El método por el cual un Sistema Inalámbrico evolucionario aprobado es verificado de estar operando en un estado aprobado.
VPN	Red Privada Virtual
WAP	Punto de Acceso Inalámbrico
WCD	Dispositivos de Conectividad Inalámbrica
WEP	Privacidad Equivalente a Por Cable
Wi-Fi	Fidelidad Inalámbrica (WLAN)
Dispositivo de Cliente Inalámbrico	El dispositivo que convierte las comunicaciones del Sistema Inalámbrico a una forma interpretable por un humano, y convierte las decisiones humanas a una forma de comunicación entendible por el Sistema Inalámbrica. Ejemplos de los Dispositivos de Cliente Inalámbrico incluyen los PDA, los celulares, las tabletas, etc.
WLAN	Red de Área Local Inalámbrica
WPA	Acceso Protegido Wi-Fi
WPA2	Acceso Protegido Wi-Fi 2

Ejemplo de la Red Inalámbrica