SERIE DE ESTÁNDARES

GLI-19:

Sistemas de Juegos de Azar Interactivos (Operadores)

Versión: 1.0

Fecha de Publicación: 31 de Mayo de 2011

Esta Página Ha Sido Intencionalmente Dejada en Blanco

SOBRE ESTE ESTÁNDAR

Este Estándar ha sido producido por **TST, Una Compañía Parte de GLI** con el propósito de proporcionar certificaciones independientes bajo este Estándar para proveedores y cumplir con los requisitos aquí establecidos.

Un operador deberá enviar sus equipos junto con una solicitud para que sean certificados de acuerdo a este Estándar. Tras la certificación, TST, Una Compañía Parte de GLI hará entrega de un certificado de cumplimiento evidenciando la certificación en este Estándar.

Índice

CAPÍTULO 1

1.0 Descripción general– Estándares para Sistemas de Juegos de Azar Interactivos

1.1 Introducción

1.1.1. ***Declaración General***. En años recientes, muchas jurisdicciones han optado por solicitar pruebas de estándares sin antes crear sus propios documentos de estándares. Además, con la tecnología cambiando casi mensualmente, las nuevas tecnologías no están siendo incorporadas lo suficientemente rápido en los estándares existentes debido a lo largo del proceso de formulación de normas administrativas. El presente documento, *Estándar GLI 19*, establecerá los Estándares técnicos para los Sistemas de Juegos de Azar Interactivos usados en el entorno de Internet.

1.1.2 ***Historial del Documento***. Líneas abajo hemos listado, y dado crédito, a las agencias cuyos documentos revisamos antes de la redacción de este Estándar. Es política de **TST, Una Compañía Parte de GLI** actualizar este documento tanto como sea posible para reflejar los cambios en la tecnología, en los métodos de pruebas, o en los métodos de trampa.

Este documento será distribuido GRATUITAMENTE para todos los que lo soliciten. Puede obtenerse descargándolo de nuestros sitios web www.gaminglabs.com, www.tstglobal.com o enviándonos un email a: **compliance@gaminglabs.com**

1.2 Reconocimientos de Otros Estándares Revisados

1.2.1 Declaración General. Estos Estándares han sido desarrollados gracias a la revisión y el uso de porciones de documentos de las organizaciones listadas líneas abajo. Nuestro reconocimiento y gracias van para los reguladores que armaron estos documentos:

a) La Oficina ACT de Gestión Financiera;
b) La Comisión de Control de Juegos de Apuestas de Alderney;
c) La Comisión Reguladora de Servicios Financieros de Antigua y Barbuda;
d) La División de Políticas y Cumplimiento de Leyes de los Juegos de Azar de la Columbia Británica;
e) La Administración Autónoma de los Monopolios del Estado de Italia;
f) El Departamento de Juegos de Azar y Apuestas Hípicas de Nueva Gales del Sur;
g) La Autoridad de Juegos de Azar y Apuestas Hípicas del Territorio Norte;
h) La Autoridad de Control de Casinos de Nueva Zelanda;
i) El Departamento de Asuntos Internos de Nueva Zelanda, División de Juegos de Azar, Apuestas Hípicas y Censura;
j) La Oficina de Regulación de Juegos de Azar de Queensland;
k) El Buró Sudafricano de Estándares;
l) La Oficina del Comisionado de Bebidas Alcohólicas y Juegos de Azar del Sur de Australia;
m) El Departamento de Economía y Finanzas de Tasmania, División de Rentas y Juegos de Azar;
n) La Comisión de Juegos de Apuestas del Reino Unido;
o) La Autoridad Victoriana de Casinos y Juegos de Azar;
p) La Oficina de Apuestas Hípicas y Bebidas Alcohólicas del Oeste de Australia.

1.3 Propósitos de los Estándares Técnicos

1.3.1 ***Declaración General***. Los Propósitos de este Estándar Técnico son los siguientes:

a) Eliminar criterios subjetivos en el análisis y certificación de las operaciones de los Sistemas de Juegos de Azar Interactivos (SJAI).

b) Solo hacer pruebas en aquellos criterios que impacten en la credibilidad e integridad de los Sistemas de Juegos de Azar Interactivos desde el punto de vista tanto del recojo de ganancias como del jugador.

c) Crear un estándar que asegure que los juegos puestos a disposición vía Internet sean justos, seguros, y susceptibles de ser auditados y operados correctamente.

d) Distinguir entre las políticas públicas locales y los criterios de laboratorio. En TST, Una Compañía de GLI creemos que cada jurisdicción local es libre de establecer su propia política pública respecto a los juegos de azar.

e) Reconocer que la evaluación de los sistemas de control interno (como aquellos Anti Lavado de Dinero, procesos Financieros y Comerciales) empleados por los operadores del Sistema de Juegos de Azar Interactivos no debe estar incorporada en el estándar sino dejar que el Organismo Regulador de cada jurisdicción local haga dicha evaluación como parte del proceso de entrega de licencias.

f) Reconocer que las pruebas no relacionadas con los juegos (como las Pruebas Eléctricas) no deben ser incorporadas en este estándar sino dejadas a los laboratorios especializados en ese tipo de pruebas. Excepto para los casos específicamente identificados en el estándar, las pruebas no están dirigidas hacia temas de salud o de seguridad. Esos asuntos son responsabilidad del fabricante, del comprador, y del operador del equipo.

g) Construir un estándar que pueda cambiarse o modificarse fácilmente para permitir la incorporación de nuevas tecnologías.

h) Construir un estándar que no especifique ningún método o tecnología particular para ningún elemento o componente de un Sistema de Juegos de Azar Interactivos. Lo que se busca es permitir el uso de una amplia gama de métodos conformes a los estándares, mientras que al mismo tiempo se alienta el desarrollo de nuevos métodos.

1.4 Interpretación de este Documento

1.4.1 ***No hay Limitaciones de Tecnologías***. Este documento no debe ser leído de manera tal que se dé a entender una limitación en el uso de tecnologías futuras. No debe interpretarse que si una tecnología no es mencionada por el documento, entonces no está permitida. Por el contrario, conforme se vayan desarrollando nuevas tecnologías, nosotros revisaremos el estándar, haremos cambios e incorporaremos nuevos estándares mínimos para esas nuevas tecnologías.

1.4.2 *Proveedores y Operadores del Software*. Los componentes de un Sistema de Juegos de Azar Interactivos, aunque puedan estar construidos de forma modular, están diseñados para funcionar perfectamente todos juntos. Asimismo, los componentes de un Sistema de Juegos de Azar Interactivos podrían estar desarrollados para tener características configurables, la configuración final dependerá de las opciones elegidas por el operador final. Desde una perspectiva de realización de pruebas, podría no ser posible probar todas las características configurables de un componente de un Sistema de Juegos de Azar Interactivos enviado por un proveedor de software ante la ausencia de la configuración final elegida por el operador.

Este documento ha sido diseñado para enfocarse en los requisitos específicos de la realización de pruebas para un operador. Debido a la naturaleza integral de los SJAI existen numerosos requisitos en este documento que podrían no aplicar ni para los proveedores ni para los operadores. Es esos casos, cuando se requiere hacer pruebas para una versión de "marca blanca" del componente, se probará y reportará una configuración específica.

Este documento no pretende ser arbitrario al definir cuál de las partes es responsable de cumplir con los requisitos de este documento. Se deja a la libre elección de los depositarios de cada sistema determinar cuál es la mejor manera de cumplir los requisitos especificados en este documento.

1.5 Otros Documentos Que Podrían Ser Pertinentes

1.5.1 *Declaración General*. Este estándar cubre los requisitos actuales para juegos de un solo jugador o multijugador que se juegan a través del uso de diversos dispositivos como

computadoras personales y dispositivos móviles vía Internet. Actualmente, no existen otros documentos que podrían ser pertinentes.

CAPÍTULO 2

2.0 Requisitos para la Plataforma de Juego

2.1 Reservado

2.2 Plataforma de Juego

2.2.1 Declaración General. Si la Plataforma de Juego está compuesta por múltiples sistemas computarizados en varias locaciones, la Plataforma de Juego como un todo y toda la comunicación entre sus componentes deben estar conformes a estos requisitos.

2.2.2 Apagado y Recuperación. La Plataforma de Juego debe tener las siguientes capacidades de apagado y recuperación:

a) La Plataforma de Juego debe ser capaz de recuperarse de reinicios inesperados de sus computadoras centrales o de cualquiera de sus otros componente;
b) La Plataforma de Juego debe ser capaz de realizar un apagado suave ante un simple corte del suministro eléctrico, y solo permite el reinicio automático luego del encendido después que se han realizado los siguientes procedimientos como requisito mínimo:
    i) Rutina (s) de reanudación del programa, incluyendo auto diagnósticos, completada(s) con éxito;
    ii) Todos los archivos críticos de la Plataforma de Juego han sido autentificados utilizando el método aprobado (ej. CRC, MD5, SHA-1, etc.); y
    iii) La comunicación con todos los componentes necesarios para la operación de la Plataforma del Juego ha sido establecida y autentificada de modo similar.
c) La Plataforma de Juego debe ser capaz de identificar y manejar apropiadamente una situación en la que han ocurrido reinicios generales de la configuración de fábrica de otras Plataformas de Juego lo que afectará el resultado del juego, el monto ganado o los medidores;
d) La Plataforma de Juego debe ser capaz de recuperar toda la información crítica desde el momento de la última copia de seguridad hasta el punto en el tiempo en que ocurrió la

falla o reinicio de la Plataforma de Juego (no se especifica un límite de tiempo);

e) El sistema debe tener la suficiente capacidad para asegurar que los derechos y la capacidad de auditoría del jugador estén disponibles en todo momento.

2.2.3 Alojamiento por Parte de Terceros. Cuando uno más componentes de la Plataforma de Juego son alojados por un tercero que se dedica al suministro del servicio, deben cumplirse los siguientes requisitos:

a) La información privada y financiera de todos los jugadores no debe ser accesible al servicio tercerizado, sin embargo; esto no impide el uso de este tipo de servicios para las copias de seguridad y el almacenamiento de datos;

b) Ninguna funcionalidad del juego debe ser accesible al servicio tercerizado,

c) No se utilizará ningún servicio de terceros que requiera que el software cumpla con reglas/regulaciones que sean contradictorias con cualquiera de los artículos de este documento.

2.2.4 Inhabilitación de Juegos de Apuestas. Los siguientes requisitos aplican a la inhabilitación y habilitación de juegos de apuestas en la Plataforma de Juego:

a) La Plataforma de Juego debe ser capaz de deshabilitar o habilitar todo juego de apuestas a voluntad;

b) La Plataforma de Juego debe ser capaz de deshabilitar o habilitar juegos individuales a voluntad;

c) La Plataforma de Juego debe ser capaz de deshabilitar o habilitar sesiones de juego individual a voluntad; y

d) Cuando se deshabilite o habilite cualquier juego de apuestas en la Plataforma de Juego debe hacerse una entrada en el registro de auditoría. La razón de cualquier inhabilitación debe sentarse en un registro de auditoría protegido que no necesariamente tiene que ser parte de la Plataforma de Juego.

e)

2.2.5 Desconexión del Usuario por Tiempo de Inactividad. Si la Plataforma de Juego no es capaz de sondear (o *polling*) el dispositivo del jugador final para confirmar una conexión, debería implementar desconexiones por tiempo de inactividad.

2.2.6 Sondeo de Dispositivos de Jugadores Finales. Si la Plataforma de Juego es capaz de realizar sondeos, debe ser capaz de sondear los dispositivos de los jugadores finales en base a una tabla de tiempo y a voluntad de un operador de la Plataforma de Juego, y:

a) La Plataforma de Juego debe ser capaz de almacenar la hora y fecha del último sondeo realizado;
b) La falla de un dispositivo de jugador final para responder luego de 30 minutos causa que la sesión sea terminada; y
c) El dispositivo del jugador final debe asumir la finalización de la sesión si falla en recibir una respuesta del servidor luego de 30 minutos. El dispositivo del jugador final debe notificar al jugador de la finalización de la sesión. No se permite jugar ningún otro juego hasta que la Plataforma de Juego y el dispositivo del jugador final establezcan una nueva sesión.

2.2.7 Mal Funcionamiento. La Plataforma de Juego debe:

a) No verse afectada por el mal funcionamiento de los dispositivos de los jugadores finales más allá de instituir los procedimientos para juegos incompletos de acuerdo con estos requisitos; e
b) Incluir un mecanismo para anular todas las apuestas y pagos en el evento de un mal funcionamiento de la misma Plataforma de Juego si no es posible lograr una recuperación total.

2.3 Información de Juegos de Apuestas a ser Mantenida en la Plataforma de Juego

2.3.1 Declaración General. El operador debe retener la información de juegos de apuestas por un periodo de siete años a partir del momento actual. La información debe ser almacena fuera de línea. Todos los sellos de tiempo deben provenir de una hora única, si se escoge una hora que no es la Hora Universal Coordinadas (HUC) entonces la diferencia debe ser aparente.

2.3.2 Información de la Cuenta del Jugador. Para cada cuenta de jugador, la información a mantenerse, respaldarse y ponerse a disposición para su inclusión en los reportes de la Plataforma de Juego debe incluir:

a) Detalles de la identidad del jugador (incluyendo un método de verificación);
b) El acuerdo del jugador con los Términos y Condiciones y con la Política de Privacidad del operador;
c) Detalles de la cuenta y balance actual;
d) Niveles de apuesta máximos, y estado de exclusión;
e) Cuentas previas y razón para la desactivación; y
f) La información actual de la sesión.

2.3.3 Información de la Sesión. Para cada sesión de juego (es decir: desde el tiempo de inicio de sesión o *login* del cliente hasta el tiempo de cierre de sesión o *logout*), la información a mantenerse, respaldarse y ponerse a disposición para su inclusión en los reportes de la Plataforma de Juego debe incluir:

a) La ID única del jugador;
b) Tiempo de inicio y final de la sesión;
c) Detalles relevantes del dispositivo del jugador como la dirección IP, versión del navegador y/o versión del cliente;
d) Total de dinero apostado por sesión;
e) Total de dinero ganado por sesión;
f) Fondos añadidos a la cuenta por sesión (con sello de tiempo);
g) Fondos retirados de la cuenta por sesión (con sello de tiempo);
h) Donde se implementen sondeos, hora del último sondeo exitoso por sesión;
i) Razón para la finalización de la sesión;
j) Donde se implementen sondeos, información de juegos por sesión; (es decir, juegos jugados, cantidades apostadas, cantidades ganadas, premios mayores o *jackpots* ganados, etc.);
k) El balance de la cuenta del jugador al inicio de la sesión;
l) Sesiones activas actuales (por ej.: en progreso, completadas, etc.); y
m) Hora y fecha de interrupción.

2.3.4 Información del Jugado del Juego. Para cada juego individual jugado, la información a mantenerse, respaldarse y ponerse a disposición para su inclusión en los reportes de la Plataforma de Juego debe incluir:

a) La ID única del jugador;
b) Tiempo de inicio del juego de acuerdo a la Plataforma de Juego;
c) El balance de la cuenta al inicio del juego;
d) Apuesta por juego;
e) Aportes a los pozos del Premio Mayor (si aplica);
f) Estado del juego (en progreso, completado, etc.);
g) Resultados del juego;
h) Premio mayor ganado (si aplica);
i) Tiempo de finalización del juego de acuerdo a la Plataforma de Juego;
j) Monto ganado;
k) El balance de la cuenta al final del juego;
l) El número de la mesa (si aplica) en la que se juega el juego;
m) La tabla de pagos utilizada; y
n) El identificador y la versión del juego.

2.3.5 Información del Premio Mayor. La información del medidor del premio mayor debe ser transferida desde el Controlador del Premio Mayor hasta la Plataforma de Juego al menos cada 60 segundos. Como mínimo deben mantenerse, respaldarse y ponerse a disposición para su inclusión en los reportes de la Plataforma de Juego las siguientes mediciones del software del premio mayor:

a) Monto total jugado para los premios mayores;
b) Monto total de premios mayores ganados;
c) Total de aportes realizados al premio mayor, (incluye cualquier monto desviado);
d) Total de contribuciones al premio mayor ganadas;
e) Inicio del Premio Mayor u otras semillas que no sean financiadas con el aporte;
f) Monto actual de cada premio mayor; y
g) Valor actual de los aportes desviados hacia el Premio Mayor.

2.3.6 Información de Acontecimientos Significativos. Los siguientes requisitos aplican al registro de la información de acontecimientos significativos en la Plataforma de Juego:

a) La información de acontecimientos significativos a mantenerse, respaldarse y ponerse a disposición para su inclusión en los reportes de la Plataforma de Juego debe incluir:
   i) Grandes ganancias excediendo el valor especificado por la jurisdicción que otorga la licencia;
   ii) Grandes transferencias de fondos (únicas y añadidas a lo largo de un periodo definido de tiempo) excediendo el valor especificado por la jurisdicción que otorga la licencia;
   iii) Cambios hechos por el operador a los parámetros del juego;
   iv) Cambios hechos por el operador a los parámetros del premio mayor;
   v) Nuevos premios mayores creados;
   vi) Veces que se ganó el premio mayor;
   vii) Premios mayores retirados;
   viii) Exclusiones de jugadores (incluyendo razones para la exclusión, solicitudes para el levantamiento de la exclusión y levantamiento actual de la exclusión);
   ix) Eventos que suceden en Plataformas de Juego externas que afectan el resultado del juego y los montos ganados (por ej.: premios mayores ofrecidos externamente);
   x) Pérdidas irrecuperables de datos relativos al cliente; y
   xi) Periodos significativos de indisponibilidad de la Plataforma de Juego.

b) Las Plataformas de Juego externas que afecten el resultado del juego o de los montos ganados deben mantener un registro de eventos significativos si no son transferidas inmediatamente a la Plataforma de Juego;
c) La Plataforma de Juego debe ser capaz de recibir y almacenar todos los eventos significativos de Plataformas de Juego externas que afecten el resultado del juego o de los montos ganados;
d) La Plataforma de Juego debe ser capaz de proveer medios para ver los eventos significativos incluyendo la capacidad de buscar por tipos particulares de eventos; y
e) La Plataforma de Juego debe ser capaz de priorizar eventos en base a su importancia (por

ej.: si es que debe registrar un evento, dar una alerta o deshabilitar el juego).

2.3.7 ***Resultado del Mecanismo de Recuperación***. La Plataforma de Juego debe mantener los siguientes registros para facilitar la recuperación de juegos incompletos:

a) La Plataforma de Juego debe mantener registros de cualquier juego que falle en completarse y la razón por la que el juego no se completó. Esta información debe tratarse como información vital a ser recuperada por la Plataforma de Juego en el caso de una falla.

b) La información suficiente para continuar un juego completado parcialmente debe ser retenida por la Plataforma de Juego. Esta información debe tratarse como información vital a ser recuperada por la Plataforma de Juego en el caso de una falla.

c) Las apuestas asociadas a un juego parcialmente completado que puede continuarse deben ser retenidas en un registro separado hasta que se complete el juego. Las cuentas de los jugadores deben reflejar todo fondo retenido en el registro de un juego incompleto.

d) En caso un juego no pueda continuarse debido a una acción de la Plataforma de Juego, todas las apuestas deben ser regresadas a los jugadores de ese juego.

2.3.8 ***Copia de Seguridad de los Datos***. Debe existir un método de respaldo de todos los datos críticos (que comprenden seguridad financiera e información de acontecimientos) con la frecuencia suficiente para permitir la recuperación en el caso de una interrupción.

CAPÍTULO 3

3.0 Requisitos para el Manejo de la Cuenta del Jugador

3.1 Registro del Jugador

3.1.1 <u>Declaración General</u>. Esta sección discute los principios que aplican a la creación, uso, seguridad y privacidad de los detalles de registro del jugador. La información de registro del jugador debe ser mantenida en una parte segura de la Plataforma de Juego y cumplir con las siguientes reglas:

a) El jugador debe estar registrado con el operador antes de que ocurra cualquier juego de apuestas. Sin embargo, es aceptable que un jugador juegue por diversión sin necesidad de registrarse;
b) Si el registro se realiza en línea, el sistema debe requerir el ingreso de información para verificar la prueba de la identidad, edad, lugar de residencia y aceptación de los Términos y Condiciones establecidos por el regulador de la jurisdicción en la que ocurre el juego;
c) Si el sistema procesa cualquier parte del registro en línea, el sistema debe asegurar que el acceso a la información esté restringido a la persona que suministra dicha información y al personal autorizado del operador;
d) Si el sistema procesa cualquier parte del registro fuera de línea, el sistema no debe permitir que un jugador juegue por dinero, pero podría permitir actividades de "juego por diversión", hasta que el proceso de registro sea autentificado a través de alguna otra forma de comunicación descrita en el sistema de control aprobado por el operador;
e) Durante el proceso de registro, el jugador debe estar de acuerdo con los Términos y Condiciones del servicio y con la Política de Privacidad del operador;
f) Una vez registrado por un operador, cada jugador debe tener un identificador único, para permitir la identificación del jugador y de los detalles de la cuenta por parte del sistema cada vez que un jugador comienza una sesión;
g) Cualquier contraseña inicial debe ser establecida de manera segura por el jugador;
h) Debe aconsejarse al jugador que mantenga sus contraseñas e ID seguras.

i) Debe informársele al jugador sobre los mecanismos existentes para detectar si hay un uso no autorizado de su cuenta, como ver que el Último Registro en el Visualizador de Tiempo, la dirección IP del último registro y cotejar los estados de cuenta de la tarjeta de crédito con los depósitos conocidos;
j) Debe realizarse una revisión completa de la identidad cada vez que un individuo intenta registrarse, haciéndose la autentificación del jugador al comienzo de cada sesión de juego;
k) Los detalles de verificación del jugador deben mantenerse en línea de una manera segura; y
l) Debe mantenerse en línea una lista de todos los registros (actuales o de otro tipo) y cuentas (activas o de otro tipo) del jugador.

3.2 Las Cuentas de los Jugadores

3.2.1 Declaración General. Las siguientes reglas aplican a las cuentas de los jugadores, las mismas que debe mantenerse en una parte segura de la Plataforma de Juego.

a) Solo se registrará a jugadores con edad legal para realizar apuestas en la jurisdicción.
b) Los fondos de un cuenta de jugador solo pueden ser utilizados para apuestas si el jugador está registrado con el operador;
c) La Plataforma de Juego no debe aceptar una apuesta que podría causar que una cuenta quede en saldo negativo;
d) Una persona que es excluida de un juego no debe ser capaz de establecer una nueva cuenta. Sin embargo, los operadores deben ser capaces de regresar el balance a la cuenta de un jugador siempre que no la cuenta no esté sujeta a otros reclamos; y
e) Cuando una cuenta sea terminada, todas las cuentas establecidas como resultado de ella deben ser desactivadas y los balances actuales regresados a los jugadores.

3.2.2 Creación de Cuentas de Jugador. No se debe crear una nueva cuenta si la razón para la desactivación del registro del jugador está asociada con cuentas previas que indican que a esa persona no debe permitírsele crear una nueva cuenta.

3.2.3 Privacidad de la Información del Jugador. Cualquier información obtenida por los operadores respecto al registro o la creación de la cuenta del jugador no debe infringir la Política de Privacidad del operador. Además, deberán cumplirse las siguientes reglas:

a) Cualquier información sobre el estado actual de las cuentas del jugador debe ser mantenida como confidencial para el operador, excepto cuando la liberación de dicha información sea requerida por la ley;

b) Toda información del jugador debe ser borrada de manera segura (es decir no solo suprimida) de discos duros, cintas magnéticas, memorias de estado sólido y otros dispositivos antes que este sea puesto fuera de servicio. Si el borrado no es posible, el dispositivo de almacenamiento debe ser destruido.

3.2.4 Mantenimiento de los Fondos del Jugador. Deben aplicarse los siguientes principios al mantenimiento de los fondos de los jugadores:

a) Las cuentas de los jugadores en la Plataforma de Juego deben estar aseguradas contra accesos no válidos o actualizaciones fuera de los métodos aprobados;
b) Todo depósito, retiro, transferencia o transacciones de ajuste deben ser mantenidas en un registro de auditoría de la Plataforma de Juego;
c) Un depósito en la cuenta del jugador hecho mediante transacción de tarjeta de crédito u otro método que pueda producir un rastro suficiente de auditoría, no debe ser hecho disponible para su apuesta hasta el momento en que los fondos sean recibidos o que el emisor provea un número de autorización al operador indicando que los fondos están autorizados. El número de autorización debe mantenerse en un registro de auditoría de la Plataforma de Juego;
d) La identificación positiva del jugador, incluyendo todo ingreso de su Número de Identificación Personal (PIN en inglés) u otros métodos de seguridad aprobados, debe completarse antes de que pueda realizarse el retiro del dinero retenido en la Plataforma de Juego.
e) Las cuentas inactivas con dinero en la Plataforma de Juego deben ser protegidas contra accesos o retiros ilegales;
f) Toda transacción que involucre dinero debe tratarse como información vital a ser

recuperada por la Plataforma de Juego en caso de falla;

g) Los pagos desde una cuenta deben ser realizados (incluyendo la transferencia de fondos) directamente a una cuenta de una institución financiera a nombre del jugador o hacerse pagable al jugador y remitida a la dirección del jugador. El nombre y la dirección deben ser los mismos que se colocaron en los detalles de registro del jugador.
h) Los estados de cuenta deben ser enviados a la dirección registrada del jugador previa solicitud y a la dirección de e-mail del jugador en forma mensual. Los estados deben incluir la suficiente información para permitir al jugador conciliar dichos estados con sus propios registros a nivel de las sesiones;
i) Cualquier ajuste a las cuentas de los jugadores en la Plataforma de Juego debe estar sujeto a un estricto control de seguridad y rastreo de auditoría;
j) No deberá ser posible transferir créditos que representen un valor monetario entre dos cuentas de usuarios; y
k) Los créditos que son usados en juegos "Jugados por Diversión" y que no tengan ningún valor monetario pueden transferirse en cualquier número entre cuentas de usuarios.

3.3 La Sesión de Juego del Jugador

3.3.1 Declaración General. Una sesión de juego se inicia cuando un jugador se registra en la Plataforma de Juego. Un juego que requiera de un pago monetario solo puede ocurrir durante una sesión de juego. Cuando un operador proporcione acceso a múltiples juegos desde un salón, los jugadores podrán jugar más de un juego durante la sesión.

3.3.2 Identificación del Jugador. La identificación debe cumplir las siguientes reglas:

a) Un jugador debe recibir un identificador electrónico como un certificado digital o una descripción de la cuenta y una contraseña para iniciar una sesión de juego; y
b) La Plataforma de Juego debe permitir que los jugadores cambien sus contraseñas y debería recordarles hacerlo en forma regular.

3.3.3 Fin de la Sesión de Juego.

a) Una sesión de juego finaliza si:
    i) El jugador notifica a la Plataforma de Juego que la sesión ha finalizado (por ej.:

"se desconecta");

ii) Se llega a una desconexión por tiempo de inactividad del usuario;

iii) El servidor (o *host*) de la Plataforma de Juego no obtiene una respuesta después de 30 segundos de parte del dispositivo del jugador final; si aplica; o

iv) El operador finaliza la sesión.

b) Cuando el operador finaliza una sesión, debe hacerse un registro en un archivo de auditoría que incluya la razón de la finalización;

c) La Plataforma de Juego debe intentar enviar un mensaje de finalización de sesión al dispositivo del jugador final cada vez que una sesión sea finalizada por la Plataforma de Juego.

3.4 Programas de Fidelidad del Jugador

3.4.1 ***Declaración General***. Los requisitos de esta sección solo aplican si las promociones de fidelidad del jugador involucran el uso de la fidelidad del jugador para afectar las bases de aplicación de impuestos del operador, por ej. Conversión de los puntos de fidelidad del jugador en horas de juego o su conversión en dinero en efectivo. Si esto es soportado por la Plataforma de Juego, deben aplicarse los siguientes principios:

a) La base de datos de fidelidad del jugador debe mantenerse en una parte segura de la Plataforma de Juego.

b) El uso de los datos de rastreo del jugador no debe infringir la Política de Privacidad del operador.

c) La amortización de puntos de lealtad del jugador debe ser una transacción segura que debite automáticamente puntos del balance por el valor del premio reclamado; y

d) Todas las bases de datos de fidelidad del jugador deben ser registradas como datos críticos por la Plataforma de Juego.

e) Si el programa de Fidelidad del jugador es suministrado por un proveedor externo, la Plataforma de Juego debe ser capaz de comunicarse en forma segura con el servicio.

3.5 Juego Responsable

3.5.1 ***Página de Juego Responsable***. Debe poder accederse fácilmente a una página de juego responsable desde cualquier pantalla donde ocurra un juego. La página de juego responsable debe contener como mínimo:

a) Información sobre riesgos potenciales asociados con los juegos de apuestas, y dónde obtener ayuda para problemas de juego,
b) Una lista de medidas de juego responsable que puedan ser invocadas por el jugador, como tiempos límite de sesión y límites de apuesta, y una opción para permitir al jugador que invoque dichas medidas,
c) Un vínculo a los términos y condiciones acordados por el jugador al entrar y jugar en el sitio,
d) Un vínculo a la política de privacidad del operador,
e) Un vínculo a la página de inicio del sitio web del Organismo Regulador,
f) Toda la información en (a) y (c) debería estar disponible en los idiomas que reflejen a la base de clientes. Deberían hacerse esfuerzos razonables para hacer que la información en (b) esté disponible en los idiomas que reflejen a la base de clientes.
g) Un mecanismo fácil y obvio para avisar al jugador de su derecho a presentar una queja contra el operador, y permitir que el jugador notifique al Organismo Regulador de dicha queja. Esto debe incluir un vínculo a la página de inicio del Organismo Regulador.

3.5.2 ***Servicios de Terceros***. Todos los vínculos a servicios de problemas de juego provistos por terceros deben ser comprobados regularmente por el operador. Cuando el servicio ya no esté disponible o no esté disponible por un periodo significativo de tiempo, el operador debe proporcionar un servicio de soporte alternativo.

3.5.3 ***Reservado***.

3.5.4 ***Auto-Exclusión***. Debe proporcionarse a los jugadores un mecanismo fácil y obvio para auto-excluirse del juego, y este mecanismo debe brindar la siguiente funcionalidad:

a) Como mínimo, este mecanismo de auto-exclusión debe ser accesible desde la página de juego responsable.

b) Debe proporcionarse al jugador la opción de auto-excluirse temporalmente por un periodo específico de tiempo como lo definen los Términos y Condiciones, o permanentemente.
c) En el caso de auto-exclusión temporal, la Plataforma de Juego debe asegurar que:
    i) Inmediatamente después de recibir la orden de auto-exclusión, no se aceptarán nuevas apuestas o depósitos de ese jugador, hasta el momento en que el tiempo temporal de auto-exclusión haya expirado, y
    ii) Durante el periodo temporal de auto-exclusión, el jugador no está prohibido de retirar parte o todo el balance de su cuenta a través de la consola de gestión de la cuenta, siempre que la Plataforma de Juego reconozca que los fondos han sido retirados.
d) En el caso de auto-exclusión temporal, la Plataforma de Juego debe asegurar que:
    i) Inmediatamente después de recibir la orden de auto-exclusión, no se aceptarán nuevas apuestas o depósitos de ese jugador, hasta el momento en que el tiempo temporal de auto-exclusión haya sido revocado,
    ii) El jugador haya cobrado la totalidad de su balance de cuenta, siempre que la Plataforma de Juego reconozca que los fondos han sido retirados, y
    iii) Se proporciona a los jugadores un mecanismo para revocar la orden de auto-exclusión, utilizando un proceso especial a ser identificado por el operador.

3.5.5 Exclusión Involuntaria. La Plataforma de Juego debe proporcionar un mecanismo por el que el personal del operador pueda excluir a un jugador del juego de acuerdo con los Términos y Condiciones del operador acordados por el jugador al momento de su registro. Este mecanismo debe:

a) Incluir un registro de las razones para la exclusión;
b) Asegurar que inmediatamente después de activar la exclusión, no se acepten nuevas apuestas o depósitos de ese jugador, hasta el momento en que la exclusión haya sido revocada;
c) Durante el periodo de exclusión, el jugador no debe ser prohibido de retirar parte o todo el balance de su cuenta, siempre que la Plataforma de Juego reconozca que los fondos hayan sido retirados, y que la razón o razones para la exclusión no prohíba dicho retiro; y

d) Cualquier exclusión de ese tipo solo pueda levantarse por aplicación del jugador

3.5.6 Auto-Limitación. Debe proporcionarse a los jugadores un mecanismo fácil y obvio para auto-limitar su juego, y este mecanismo debe brindar la siguiente funcionalidad:

a) Como mínimo, este mecanismo de auto-limitación debe ser accesible desde la página de juego responsable.
b) Inmediatamente después de recibir la orden de auto-limitación, la plataforma de juego debe asegurar que todos los límites especificados sean correctamente implementados en la Plataforma.
c) Es aceptable que las auto-limitaciones hagan efecto la próxima vez que el jugador inicie su sesión en la plataforma de juego; sin embargo, el jugador debe ser informado con claridad que este es el caso después de establecer el tiempo.
d) Las auto-limitaciones establecidas por un jugador no deben anular cualquier limitación establecida por el operador o las reglas del juego.
e) Una vez establecidas por un jugador, solo debe ser posible reducir la severidad de las auto-limitaciones después de siete días.
f) Las auto-limitaciones no deben verse comprometidas por eventos temporales externos, como años bisiestos y ajustes de horarios.
g) Las auto-limitaciones no deben verse comprometidas por eventos de estado interno, como ordenes de auto-exclusión y revocaciones de auto-exclusión
h) El mecanismo de auto-limitación debería incluir (pero no necesariamente limitarse a) las siguientes opciones:
    i) Límites de apuestas por periodo de tiempo - un promedio máximo de límite de apuestas sobre un periodo específico de tiempo (por ej.: diariamente, semanalmente, etc...),
    ii) Límites de pérdidas por periodo de tiempo - un promedio máximo de limitaciones de pérdidas sobre un periodo específico de tiempo (por ej.: diariamente, semanalmente, etc...),
    iii) Límites de depósitos por periodo de tiempo - un promedio máximo de límites de depósitos sobre un periodo específico de tiempo (por ej.: diariamente, semanalmente, etc...),

3.5.7 Limitación Involuntaria. Es aceptable para el operador establecer límites (como los listados líneas arriba) a los jugadores, y variar dichos límites de tiempo en tiempo. Cualquier límite impuesto por el operador debe ser consistente con los descritos en los Términos y Condiciones firmados por el jugador. Los jugadores deben ser notificados con antelación de cualquier límite impuesto por el operador salvo que el regulador requiera hacerlo de otro modo.

a) Inmediatamente después de recibir la orden de limitación establecida por el operador, la plataforma de juego debe asegurar que todos los límites especificados sean correctamente implementados en la Plataforma.
b) Es aceptable que los límites establecidos por el operador hagan efecto la próxima vez que el jugador inicie su sesión en la plataforma de juego; sin embargo, el jugador debe ser informado con claridad que este es el caso.
c) Los límites establecidos por el operador no deben reducir la severidad de cualquier limitación establecida para el jugador.
d) La limitación del operador podría no extenderse más allá de siete días, excepto cuando lo requieran las reglas y la regulación de la jurisdicción, o los estándares en los que se aprueba el uso de la Plataforma de Juego.
e) Las limitaciones impuestas por el operador no deben verse comprometidas por eventos temporales externos, como años bisiestos y ajustes de horarios.

f) Las limitaciones impuestas por el operador no deben verse comprometidas por eventos de estado interno, como órdenes y revocaciones de auto-exclusión.

3.5.8 Reporte de Actividad Sospechosa del Jugador. Debe haber un método simple y claro para que un jugador reporte cualquier actividad sospechosa de otro jugador, el cual debe ser explicado con precisión en los menús de ayuda y/o en el sitio web. (Por ej. el jugador podría hacer clic derecho en un nombre de cuenta en la ventana del juego y apretar la opción "Reportar Actividad Sospechosa del Usuario" lo que abre una nueva ventana con un formato que el usuario puede llenar con todos los detalles necesarios, incluyendo la hora del incidente, la razón por la que el usuario fue reportado, etc...)

CAPÍTULO 4

4.0 Reservado

CAPÍTULO 5

5.0 Requisitos para el Juego

5.1 Diseño del Juego

5.1.1 ***Reservado***.

5.1.2 ***Reglas del Juego***. Los siguientes requisitos aplican para las reglas del juego mostradas al jugador:

a) Las reglas del juego deben estar disponibles para el jugador directamente en la interface del juego o accesibles desde la interface del juego vía un hipervínculo;
b) Todas las reglas del juego y la información de la tabla de pagos deberían ser accesibles para un jugador antes de que este comprometa su apuesta;
c) La información publicada del juego debe ser suficiente para explicar todas las reglas aplicables y cómo participar en el juego;
d) Las reglas del juego no deberán ser ni injustas ni inducir a error.
e) El juego debe operar e interactuar con el jugador de acuerdo con las reglas mostradas;
f) Las reglas del juego no debe ser cambiadas durante una sesión a menos que se le haya dado una notificación previa al jugador. Las reglas del juego no puede ser cambiada entre el momento en que un jugador hace una apuesta y la decisión resultante por el pago de las ganancias de la apuesta y;
g) Un cambio en las reglas constituye un juego diferente, aunque se permiten variaciones al número máximo de créditos apostados por juego (y/o líneas por juego). Este requisito no excluye implementaciones de juegos con partes o características especiales múltiples siempre que las reglas sean claras para el jugador.

5.1.3 ***Reservado***.

5.1.4 ***Premio Máximo***. El premio máximo pagado por el software de juego deberá ser especificado en las reglas del juego y deberá ser mostrado dentro de las pantallas de ayuda para ese juego en particular.

5.1.5 ***Monto Máximo a Arriesgar***. El monto máximo a arriesgar deberá ser especificado en las reglas del juego y deberá ser mostrado dentro de las pantallas de ayuda para ese juego en particular.

5.2 Ilustraciones del Juego

5.2.1 ***Reservado***

5.2.2 ***Información del Juego***. La siguiente información del juego deberá ser visible o fácilmente accesible al jugador en todo momento ya sea desde un menú de ayuda o un sitio web:

a) El nombre del juego que está siendo jugado;
b) Las instrucciones de cómo jugar, incluyendo una tabla de pagos para todos los premios y características especiales;
c) Las restricciones sobre las jugadas o apuestas como los límites de duración de las jugadas, los valores máximos a ganar, etc.;
d) El balance de créditos actual del jugador;
e) El monto actual de la apuesta. Esto solo ocurre durante el juego base o si el jugador puede hacer crecer la apuesta durante el juego;
f) La denominación de la apuesta y, donde sea aplicable, cualquier otra simbolización implementada en el juego;
g) Todos los posibles resultados ganadores, o estar disponibles como un ítem del menú o en un menú de ayuda:
h) Los montos a ganar para cada posible resultado ganador, o estar disponibles como un ítem del menú o de la pantalla de ayuda;
i) El monto ganado en el último juego completado (hasta que empiece el nuevo juego o se modifiquen las opciones de apuesta);
j) Las opciones elegidas por el jugador (por ej., monto apostado, líneas jugadas) para el último juego completado (hasta que empiece el nuevo juego o se haga una nueva selección);
k) Las opciones iniciales de selección del jugador serán descritas (por ej. la selección de un caballo en una carrera hípica debería identificar el nombre, número y el pago esperado). Una vez que el juego ha comenzado, las opciones de selección del jugador debería

mostrarse en forma clara en la pantalla;

l) El monto ganado para cada apuesta por separado y el monto total de ganancias deben ser mostrados en la pantalla;

m) El %PRJ mínimo teórico y la explicación de cómo calcularlo (por ej. premios totales por ciclo de juego divididos por el número total de diferentes resultados en el ciclo del juego).

***NOTA**: Este requisito no aplica a juegos donde existe la suficiente información disponible para el jugador que le permita determinar fácilmente la ventaja de la casa o el porcentaje de retorno al jugador.*

n) Si es que hay aportes a los premios mayores ("progresivos") y la manera en que el premio mayor opera, por ejemplo si el premio mayor se gana logrando un resultado particular;

o) Toda regla pertinente a la metamorfosis de los juegos, por ejemplo, el número y tipo de fichas que necesitan ser recolectadas para calificar para una característica especial o ronda de bonificación y las reglas pertinentes a dicha ronda de bonificación en caso difieran del juego base; y

p) La siguiente información debe estar fácilmente disponible para el jugador (es decir, mostrada directamente en la "página" del juego o accesible a través de un vínculo en la página):

   i) Información sobre apuestas responsables, incluyendo instrucciones sobre cómo limitar apuestas por juego y/o sesión e invocar arreglos de auto-exclusión; e

   ii) Información sobre los puntos de contacto de servicios de ayuda para problemas con las apuestas.

5.3 Juegos Peer to Peer (P2P)

5.3.1 <u>Declaración General.</u> Las salas de juegos P2P son aquellos entornos en donde a los jugadores se les ofrece la oportunidad de apostar con y contra otros jugadores. En estos entornos, el operador usualmente no se involucra en la apuesta como una de las partes (por ej. juegos bancados), pero usualmente proporciona el servicio de realización de apuestas o el entorno para que lo usen los jugadores, cobrando una comisión, un pago, o un porcentaje por el servicio.

5.3.2 Reglas de los Juegos P2P. Los siguientes requisitos aplican para los juegos P2P:

a) El operador debe describir con claridad los Términos y Condiciones que utiliza para registrar una cuenta.
b) Al cliente no debería permitírsele jugar contra sí mismo cuando el cliente tenga la capacidad de influir en el resultado del juego.
c) Un jugador solo puede ocupar un asiento en cualquier mesa individual.
d) La política de colusión del operador, incluyendo las sanciones posibles debe ser descrita al jugador.
e) El operador debe proporcionar alertas sobre cómo los bots pueden afectar el juego, de modo que los clientes puedan tomar una decisión informada en cuanto a participar o no.
f) Para evitar la colusión entre los jugadores que se sientan a ambos lados de la mesa o de algún otro arreglo colaborativo, la asignación aleatoria de mesas es algo vital tanto en los torneos de sentarse e irse (o *sit-n-go*) como en los de mesas múltiples. Sin embargo, la asignación aleatoria de mesas no es requerida en una mesa del tipo *ring table,* pues allí los jugadores prefieren elegir a sus compañeros de juego;
g) Las reglas deben describir con claridad el procedimiento en caso de desconexión del jugador del servidor de la red durante un juego (por ej. corte de la conexión de internet, colgado de la PC, etc.)
h) El porcentaje de la casa y otras tarifas por servicios de juegos de apuestas ("comisión"), deben ser explicados con claridad y mostrados al jugador.

5.3.3 Jugadores Computarizados. Los siguientes requisitos aplican al uso de jugadores computarizados:

a) El software puede emplear el uso de Inteligencia Artificial (IA) a fin de llenar las mesas multijugador.
b) El uso de software de IA debe ser claramente explicado en los menús de ayuda.
c) El uso de software de IA sólo puede ser realizado a solicitud del jugador y no puede ser usado por el software para llenar automáticamente los sitios vacíos en las mesas.
d) Todos los jugadores de IA deben estar marcados claramente en las mesas de modo que los jugadores estén conscientes de qué jugadores no son humanos.
e) Toda inteligencia artificial utilizada para llenar mesas de juego no debe tener ninguna

ventaja técnica sobre el jugador humano promedio (es decir, ellos no pueden comunicarse con el servidor para ver las cartas que los jugadores tienen a fin de determinar el siguiente curso de acción).

f) Los pasos para reportar un bot sospechoso usado por un jugador debe estar explicado claramente en los menús de ayuda.

5.4 Jugado del Juego

5.4.1 ***Declaración General***. Las siguientes reglas son pertinentes para el jugado del juego:

a) Los vínculos utilizados para proveer información del juego como las reglas y tabla de pagos deben ser revisados diariamente.

b) Solo debe extenderse una invitación para jugar un juego en particular si la Plataforma de Juego determina que el canal encriptado de comunicaciones hacia el dispositivo del jugador final es adecuado para el juego, y si el dispositivo del jugador final tiene las capacidades suficientes para correrlo (p.ej. revisar el número de versión del navegador web y/o el número de la versión del cliente del juego).

   i) Si el software está diseñado de modo que los jugadores puedan invitarse el uno al otro a un juego en particular, o sentarse en una mesa en particular, el software debe prohibir que cualquier jugador envíe una invitación a más jugadores de los que permite el juego, o asientos que se encuentran vacíos en la mesa actual.

   ii) Las invitaciones a los juegos deben requerir que una persona o acepte o descarte dicha invitación. Si el receptor no ha realizado ninguna acción luego de cinco minutos, el software seleccionará automáticamente declinar.

   iii) Una vez que un jugador declina una invitación, el jugador que la envío deberá ser notificado y subsecuentemente permitírsele invitar a otro jugador.

   iv) El software deberá prohibir al jugador escoger el texto de la invitación. El jugador puede escoger una variedad de opciones, que generarán una invitación estandarizada (es decir, "El Jugador1 le ha enviado una invitación para jugar Texas Hold'em en la mesa número 1111, la que tiene una apuesta mínima de 20 créditos y una apuesta máxima ilimitada.", o "El Jugador1 le ha enviado una

invitación para jugar Texas Hold'em en una nueva mesa. Usted será capaz de discutir las opciones de mesa en el salón previo al juego", etc...).

c) Para los juegos multijugador donde el resultado es afectado por el tiempo de respuesta a un evento, la Plataforma de Juego solo deberá ofrecer el juego luego de informar al jugador de cualquier desventaja asociada con el canal de comunicación. Los juegos que sean inherentemente injustos no serán aprobados.
    i) Todos los juegos multijugador deben estar equipados con un medidor de latencia que le permita al jugador determinar fácilmente la fortaleza de la conexión del usuario final al servidor.
    ii) Esto puede visualizarse a través de cualquier método apropiado, como mostrar el tiempo de latencia (ping) en milisegundos, el uso del rojo, amarillo, y verde para la velocidad de conexión, etc...

d) Si se requiere que una cookie sea aceptada para jugar el juego, la invitación para jugar solo puede ser extendida si la Plataforma de Juego determina que el dispositivo del jugador final puede aceptarla.
    i) Ninguna de las cookies utilizadas deberán contener códigos maliciosos.
e) El software cliente no debe funcionar si no tiene los suficientes recursos disponibles. El jugador debe ser informado de las especificaciones mínimas que la Plataforma de Juego requiere para echar a andar el software cliente. Instrucciones visuales deben acompañar cualquier sonido utilizado para proporcionar instrucciones sobre cómo jugar los juegos.
f) Si la Plataforma de Juego extiende una invitación para jugar un juego en particular, debe aceptar todas las apuestas legítimas para ese mismo juego.
g) Debe existir un Menú de Selección del Juego donde el monto total del balance de la sesión del jugador se muestre ya sea en moneda local o en créditos. Si el balance de la sesión de un jugador es diferente de los fondos totales retenidos por un proveedor a nombre del jugador, no debe ser ambiguo para el jugador que ambos son diferentes. Cuando el balance de la sesión de un jugador llega a cero o a menos de una cantidad necesaria para colocar una apuesta o cuando el jugador salga del juego se mostrarán los fondos totales del jugador.
h) La metodología empleada por un jugador para elegir y jugar un juego en particular no

debe ser ambigua.

i) La Plataforma de Juego debe informar con claridad al jugador de todos los juegos disponibles en el momento.

j) El jugador debe en todo momento ser consciente de qué juego ha sido seleccionado o está siendo jugado.

k) El jugador no debe ser forzado a jugar un juego solo por seleccionarlo.

l) No debe ser posible iniciar un nuevo juego antes que todos los medidores relevantes hayan sido actualizados en la Plataforma de Juego así como todas las otras conexiones relevantes y balances de la sesión, o si aplica, se ha actualizado el balance total de los fondos.

m) Un dispositivo de juego solo debería iniciar un juego:
    i) Luego que todos los créditos hayan sido registrados, y
    ii) Luego que el jugador haya elegido el número de créditos a apostar en ese juego, y
    iii) Luego que el jugador presione el botón "jugar" (o similar).

n) Si se incorpora un modo de juego automático, debería ser posible apagar este modo en cualquier momento durante el juego.

5.4.2 Juegos Incompletos. Los siguientes requisitos aplican para los juegos incompletos:

a) Un juego está incompleto cuando el resultado del mismo sigue sin ser resuelto o el resultado no puede ser visto adecuadamente por el jugador. Los juegos incompletos podría ser resultado de:
    i) Pérdida de comunicación entre la Plataforma de Juego y el dispositivo del jugador final;
    ii) Un reinicio de la Plataforma de Juego;
    iii) Un reinicio del dispositivo del jugador final;
    iv) Un juego deshabilitado por la Plataforma de Juego durante el juego; o
    v) Una finalización anormal de la aplicación de apuestas en el dispositivo del jugador final.

b) La Plataforma de Juego debe proporcionar un mecanismo para que un jugador complete un juego incompleto.

c) Luego de que el jugador se reconecte, la Plataforma de Juego debe presentar al jugador el juego incompleto para que lo termine:
   i) Cuando no se requiera de ningún insumo del jugador para completar el juego, el juego debe mostrar el resultado final como lo determina el GNA y las reglas del juego, y la cuenta del jugador debe ser actualizada adecuadamente;
   ii) Para los juegos de un solo jugador, donde se requiere del insumo del jugador para completar el juego, este debe devolver al jugador al estado del juego inmediatamente previo a la interrupción y permitir al jugador que lo complete; y
   iii) Para los juegos multijugador, el juego debe mostrar el resultado final como se determinó de acuerdo a las reglas del operador para juegos multijugador, y las cuentas de los jugadores deben ser actualizadas adecuadamente.
d) Las apuestas asociadas a un juego parcialmente completado que puede continuarse deben ser retenidas por la Plataforma de Juego hasta que se complete el juego. Las cuentas de los jugadores deben reflejar todo fondo retenido por un juego incompleto.
e) Los Términos y Condiciones del operador deben especificar que las apuestas colocadas pero que permanecen como no decididas en juegos incompletos se vaciarán luego de un tiempo especificado, y se anularán.

CAPÍTULO 6

6.0 Requisitos para los Premios Mayores (Progresivos)

6.1 Introducción

6.1.1 ***Declaración General***. Un Premio Mayor o *Jackpot* (Progresivo) es un premio que va creciendo, en función a los créditos que son apostados. Esto incluye a premios que son entregados en base a criterios que no tienen que ver con obtener resultados ganadores en el juego, como en el caso de los 'Premios Mayores Misteriosos.' Sin embargo, esto no incluye premios que sean resultado de características especiales de bonificación parte del tema de un juego, que ofrecen premios que se van incrementando conforme se va jugando y, que tampoco, son configurables.

6.2 Diseño y Operación del Premio Mayor

6.2.1 ***Justicia del Premio Mayor***. A fin de tener un premio mayor que sea justo para los jugadores deben aplicarse los siguientes principios:

a) Todos los jugadores que juegan juegos con premio mayor deben ser conscientes de las acciones que los podrían hacer elegibles para ganar un premio mayor.
b) Cuando los aportes al premio mayor sean parte del cálculo del %PRJ, dichos aportes no pueden ser asimilados en los ingresos. Si se establece un tope para cualquier premio mayor todo aporte adicional una vez que se alcance este tope deberá ser remitido a un Pozo de Desviación. El retorno mínimo para el jugador debe alcanzarse sin tomar en cuenta el número calculado de unidades de apuesta.
c) Las reglas del juego deben incorporar la manera en que se financia y determina el premio mayor.
d) Si existe un monto mínimo de apuesta para que un jugador gane un premio mayor vinculado, entonces el juego base (excluyendo el premio mayor) debe cumplir con el retorno mínimo para el jugador.

e) El monto actual del premio mayor debe ser mostrado en todos los dispositivos de jugador final que participan en el Premio Mayor. Esta visualización debe ser actualizada en todos los dispositivos de jugador final participantes al menos cada 30 segundos.

***NOTA**: Se acepta que, dependiendo del medio, las demoras en la comunicación son variables y más allá del conocimiento o control del operador. Las demoras Servidor-a-cliente variarán de jugador a jugador y de mensaje a mensaje*.

6.2.2 Documentación de Responsabilidad Financiera del Premio Mayor. Las reglas del juego deberán proporcionar lo siguiente:

a) Procedimientos para la disposición de cualquier monto pendiente de pozos en el evento de la finalización de un premio mayor planificado; y
b) Procedimientos para la administración del pozo del premio mayor incluyendo balances positivos y negativos del pozo del premio mayor en el evento de una finalización no planificada del premio mayor.

6.2.3 Controlador del Premio Mayor. El controlador del premio mayor es considerado como parte de la Plataforma de Juego incluso si es uno o más dispositivos separados físicamente.

a) Cuando un "Controlador Maestro" emplee "Controladores Esclavos" para controlar un Premio Mayor se aplicarán los siguientes requisitos:
    i) Todos los Controladores Esclavos deben estar sincronizados en sus tiempos con el Controlador Maestro.
    ii) El Controlador Maestro debe estar sincronizados en sus tiempos con la Plataforma de Juego, y
    iii) Los eventos en los que se gane un premio mayor deben tener un sello de tiempo y el Controlador del Premio Mayor debe asegurar que los aciertos registrados en un tiempo mínimo sean considerados como ganancias simultáneas. El pago del premio por ganancias simultáneas debe hacerse de acuerdo con las Reglas del juego.
b) La ventana de tiempo mínimo (Periodo de Reinicio del Premio Mayor) no debe ser menor que el tiempo que toma:
    i) Registrar que un premio mayor ha sido ganado,
    ii) Anunciar al ganador en las pantallas de todos los dispositivos de jugador final

participantes con una sesión activa, y

iii) Reiniciar los medidores progresivos.

c) Al apoyar un premio mayor que es determinado por los incrementos de las apuestas de los jugadores individuales, el procesamiento de recepción de los incrementos desde todos los dispositivos de jugador final, ya sea que estén adjuntos a los controladores Maestro o Esclavos, debe ser justo.

6.2.4 Premios Mayores Vaciados. Los premios mayores vaciados deben regresarse al pozo del premio mayor tan pronto como sea posible. Los procedimientos respecto a la decisión de vaciar un Premio Mayor deben estar conforme a los requisitos reguladores aplicables.

6.2.5 Notificación de Haber Ganado un Premio Mayor. Los siguientes requisitos deben cumplirse cuando se gana un premio mayor:

a) Un jugador ganador debe ser notificado de haber ganado un premio mayor al final del juego que está jugando;
b) La notificación de que se ganó el premio mayor debe ser proporcionada a todos los dispositivos de jugador final participantes en el premio mayor hasta el momento en que se ganó.
c) El monto del premio mayor debe ser mostrado a todos los dispositivos de jugador final participantes en el premio mayor hasta el momento en que se ganó; y
d) La notificación de haber ganado el premio mayor también debería mostrar el valor en el que se reinicia el premio mayor.

6.2.6 Ganadores Múltiples (Simultáneos) del Premio Mayor. El operador debe abordar la posibilidad de que un premio mayor sea ganado (o parezca ser ganado) por uno o más jugadores en aproximadamente el mismo tiempo. Las reglas del juego deben incluir la resolución de esta posibilidad.

6.2.7 Cambios en los Parámetros del Premio Mayor. Los siguientes requisitos aplican para la configuración de los premios mayores:

a) Una vez que un Premio Mayor ha comenzado, los cambios en sus parámetros no deber tener efecto inmediatamente - en lugar de ello, deberían ser guardados para aplicarlos luego que se gane el Premio Mayor actual. Estos son parámetros 'pendientes'.

b) Un Premio Mayor Misterioso que usa un monto escondido para determinar la ganancia del premio mayor no debe cambiar el monto escondido cuando se cambien los parámetros si el premio está activo (es decir, si se le añade cualquier aporte al pozo).
c) La Plataforma de Juego debe proporcionar un medio para visualizar los parámetros actuales y pendientes del premio mayor.
d) La Plataforma de Juego debe registrar los valores de todos los medidores de premio mayor, así como todos los de los parámetros "Actuales" y "Pendientes" del premio mayor.

6.2.8 Redirección Parcial del Premio Mayor. Esquemas de pozos de desviación, donde una porción de los aportes al premio mayor son redirigidos a otro pozo de modo que cuando se gana el premio mayor, el Pozo de Desviación es añadido a la semilla del próximo premio mayor, son aceptables.

6.2.9 Cierre del Premio Mayor. Hay instancias en las que el premio mayor debería ser cerrado. Los siguientes requisitos deberían aplicar en el evento del cierre de un premio mayor:

a) Debe darse indicaciones claras a los jugadores de que el premio mayor no está funcionando (por ej. mostrando un aviso de "Premio Mayor Cerrado" en los dispositivos de los jugadores finales).
b) No debe ser posible que un premio mayor sea ganado mientras está en estado de cierre.
c) Si el premio mayor funciona conjuntamente con otro juego (por ej. el juego base) y los requisitos de retorno del jugador solo se cumplen cuando los aportes al premio mayor son incluidos, entonces ese otro juego solo podría ofrecerse cuando el premio mayor vuelva a estar disponible.
d) La activación del premio mayor desde su estado de cierre debe regresarlo a sus mismos parámetros anteriores al cierre incluyendo el valor del premio, y el monto escondido para los premios mayores misteriosos.

6.2.10 Recuperación del Premio Mayor. Para lograr la recuperación del valor actual del monto(s) del premio mayor progresivo en el caso de una falla de la Plataforma de Juego o del controlador del premio mayor hay dos posibilidades:

a) El valor actual del monto progresivo deber ser almacenado en al menos dos dispositivos separados físicamente, o

b) El valor actual del monto progresivo debe ser posible de calcularse con precisión a partir de otros medidores de información disponibles, que no estén almacenados en la misma Plataforma de Juego como el monto progresivo.

En cualquier caso, todos los ganadores elegibles del premio mayor deben recibir su pago tan pronto como el valor sea recuperado.

6.2.11 Aportes al Premio Mayor. Las reglas del juego deben especificar con claridad la manera en que se realizan los aportes al premio mayor (en base a la facturación, balance neto de cada operador contribuyendo al pozo de operadores múltiples, etc.).

6.2.12 Premios Mayores de Operadores Múltiples. Los Premios Mayores de Operadores Múltiples serán considerados caso por caso.

6.2.13 Contabilidad del Premio Mayor. Si el cálculo de los ingresos brutos para propósitos de impuestos permiten que los aportes al premio mayor sean totalmente deducibles (en oposición a deducir premios mayores cuando se pagan), la Plataforma de Juego debe proporcionar una adecuada conciliación para asegurar que todos los incrementos del premio mayor deducidos:

a) Hayan sido pagados a los jugadores como premios; o
b) Se muestren como parte del premio; o
c) Son retenidos en reservas contables (que pueden ser demostradas) para ser pagados a los jugadores en el futuro, (es decir, como parte de premios futuros).

CAPÍTULO 7

7.0 Requisitos de Seguridad de los Sistemas de Información (SI)

7.1 Declaración General

Para asegurar que los jugadores no estén expuestos a riesgos de seguridad innecesarios por escoger participar en juegos interactivos deben aplicarse estos requisitos de seguridad a los siguientes componentes críticos de la Plataforma de Juego:

a) Los componentes de la Plataforma de Juego que graban, almacenan, procesan, comparten, transmiten o recuperan información sensible del cliente, por ej. detalles de crédito/tarjeta de crédito, información de autentificación, balances de cuentas de los clientes;
b) Los componentes de la Plataforma de Juego que genere, transmita o procese números aleatorios utilizados para determinar el resultado de los juegos o eventos virtuales;
c) Los componentes de la Plataforma de Juego que almacenan resultados o el estado actual de una apuesta del cliente;
d) Los puntos de entrada y de salida de los sistemas descritos líneas arriba (otros sistemas que son capaces de comunicarse directamente con sistemas críticos); y
e) Redes de comunicación que transmitan información sensible del cliente.

7.2 Política de Seguridad de la Información

7.2.1 ***<u>Declaración General</u>***. Un documento de política de seguridad de la información deberá ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y actores externos relevantes. Los siguientes requisitos deberán aplicar a la política de seguridad de la información:

a) La política de seguridad de la información deberá ser revisada en intervalos planificados y/o conforme ocurran cambios significativos asegurar su continúa adecuación y efectividad.

b) El enfoque del operador a la gestión de la seguridad y su implementación (es decir, objetivos, controles, políticas, procesos y procedimientos para la seguridad de la información) deberá ser revisada independientemente en intervalos planificados, o cuando ocurran cambios significativos a la implementación de la seguridad. Ejemplos de "cambios significativos" podrían incluir una actualización de un sistema operativo, permitiendo el acceso a la Plataforma de Juego a fuentes externas, adición de nuevos componentes de la Plataforma y cambios en la configuración de la red como la adición de nuevas subredes.

7.3 Controles Físicos y Ambientales

7.3.1 Áreas de Seguridad.

a) Las plataformas de juego y los sistemas de comunicaciones asociados deben ser ubicados en instalaciones que proporcionen una protección física contra el daño del fuego, inundación, huracanes, terremotos y otras formas de desastres naturales o provocados por el hombre.
b) Los perímetros de seguridad (barreras como muros, portones automáticos o escritorios de recepción) deben ser usados para proteger áreas que contienen sistemas de procesamiento de información.
c) Las áreas seguras deben ser protegidas por controles apropiadas de entrada para asegurar que el acceso sea restringido solo a personal autorizado.
d) Todo acceso debe ser registrado en un registro de seguridad.
e) Las áreas de seguridad deben incluir un sistema de detección de intrusión, y los intentos de accesos no autorizados deben ser registrados.

7.3.2 Seguridad de los Equipos.

a) Los equipos deberán ser protegidos para reducir el riesgo de amenazas y peligros ambientales, y oportunidades de accesos no autorizados.
b) Los equipos deberán ser protegido de cortes del suministro eléctrico y otras disrupciones causadas por fallas en instalaciones de soporte.
c) El cableado de energía y de telecomunicaciones transportando datos o apoyando servicios de información deberá protegerse de interrupciones o daños.

7.3.3 Manejo de Incidentes.

a) Deberán colocarse políticas, planes y procedimientos para abordar el manejo de cualquier incidente de seguridad.

7.4 Controles Administrativos

7.4.1 Seguridad de los Recursos Humanos.

a) Todos los empleados de la organización y, cuando sea relevante, los contratistas y usuarios terceros deberán recibir una entrenamiento de concientización y actualizaciones regulares en políticas y procedimientos organizacionales relevantes para su función.
b) Los derechos de acceso de todo los empleados, contratistas y usuarios terceros a la información y las instalaciones de procesamiento de la información deberá ser quitados luego de la finalización del empleo, contrato o acuerdo, o ajustado ante un cambio.

7.4.2 Servicios de Terceros.

a) Los acuerdos con terceros involucrando el acceso, procesamiento, comunicación o manejo de la información o de las instalaciones de procesamiento de información del operador, o el agregado de productos o servicios a instalaciones de procesamiento de información deberán cubrir todos los requisitos de seguridad relevantes.
b) Los servicios, reportes y registros proporcionados por el tercero deberán monitorearse y revisarse, y deberán realizarse auditorías al menos una vez al año.
c) Los cambios al suministro del servicio, incluyendo el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de la información existentes deberán ser gestionados, tomando en cuenta los sistemas y procesos del negocio involucrados así como una reevaluación de riesgos.

7.4.3 Política de Copias de Seguridad.

a) Las copias de seguridad de la información y el software deberán ser realizadas y probadas regularmente de acuerdo con la política de copias de seguridad.

7.4.4 Manipulación de Medios.

a) Deben establecerse procedimientos para el manejo de medios removibles.
b) Todos los equipos que contengan medios de almacenamiento deberán ser revisados para

asegurar que ningún dato sensible o software licenciado haya sido removido o sobre escrito seguramente antes de su eliminación.

c) Los medios deben ser desechados de forma segura cuando ya no sean requeridos, utilizando los procedimientos formales.

d) Deberán establecerse procedimientos para la manipulación y almacenamiento de la información para proteger dicha información de aperturas o malos usos no autorizados.

e) La documentación de la Plataforma de Juego deberá protegerse contra accesos no autorizados.

7.4.5 Manejo de Parchado y Actualización.

a) Debe establecerse una política escrita para la implementación de todos los parches y actualizaciones de software.

b) Todos los parches deben ser probados cuando sea posibles en una Plataforma de Juego configurada idénticamente a la Plataforma objetivo. En circunstancias en la que las pruebas del parche no puedan conducirse a tiempo por el nivel de severidad de la alerta, entonces la prueba del parche deberá ser gestionado en riesgos, ya sea aislándolo o quitándolo de la Plataforma de Juego sin probar de una red o aplicando el parche y probándolo luego.

7.4.6 Cambio de los Procedimientos de Control.

a) El programa de cambio de los procedimientos de control debe ser adecuado para asegurar que solo las versiones propiamente aprobadas y probadas de los programas sean implementadas en la producción de la Plataforma de Juego. El cambio de los controles de producción debe incluir:

   i. Una versión apropiada del software o mecanismo de control para todos los componentes de software;
   ii. Detalles de la razón para el cambio;
   iii. Detalles de la persona realizando el cambio; y
   iv. Copias de seguridad completas de las versiones previas del software.

7.4.7 Autentificación.

a) Toda persona (por ej. jugadores, operadores de computadoras, proveedores de servicios de mantenimiento, funcionarios y representantes de la jurisdicción) y sistemas

computarizados (por ej. controladores de premios mayores, sistemas de pasarela financiera, sistemas de certificación de autoridad) que se conecten a la Plataforma de Juego deben ser autentificados a excepción del caso del ítem (b) líneas abajo.

b) Los jugadores que se conecten a la Plataforma de Juego para otros propósito que no sean los juegos de apuestas no necesitan ser autentificados a menos que se acceda a información sensible de la cuenta (es decir, transacciones monetarias, información personal etc...).
c) La Plataforma de Juego debe autentificarse ella misma ante toda persona y sistemas computarizados que establezca una conexión.
d) La autentificación de personas, sistemas computarizados controlados por el operador y Plataforma de Juego de terceros deben basarse en un método de certificación de autentificación reconocido por la Jurisdicción como actualmente seguro.
e) Cuando un jugador haya olvidado su contraseña/PIN, la Plataforma de Juego debe proporcionar un proceso seguro para volver a autentificar al jugador y recobrar y/o volver a establecer la contraseña/PIN.

7.4.8 Desarrollo, Probado, Mantenimiento y Revisión de Software.

a) El software inter-plataforma debe tener un código idéntico para cada versión, con la excepción de las funcionalidad dependiente del sistema operativo.

7.4.9 Código de Seguridad.

a) Software de Código Cerrado. Donde sea apropiado el código debe ser protegido del jugador tanto como sea posible.
b) Software de Código Abierto. Si el software está siendo enviado como un proyecto de código abierto:
    i. Los desarrolladores del software deben obtener una licencia válida de programación de código abierto para que sea clasificado como un envío de código abierto.
    ii. Debe implementarse un procedimiento válido que no viole la licencia de software de código abierto obtenida, a fin de prevenir que individuos publiquen públicamente sus propias modificaciones al código alterando la seguridad e integridad del software y de la Plataforma de Juego.

iii. La Plataforma de Juego debe ser capaz de detectar razonablemente cualquier modificación al código hecha por el usuario final, y prevenir que el software funcione si es que alguna de las modificaciones pueden alterar la integridad del juego y/o Plataforma de Juego.

c) Aspectos Configurables A Través De Cambios en el Código: Si el software cliente permite configuraciones de usuario. (por ej. barajas personalizadas), entonces deben cumplirse los siguientes requisitos:

i. El cliente del juego puede permitir configuraciones de usuario (es decir, tema o *skin* de la interface, barajas personalizadas, etc...). Sin embargo, si el método de personalización se implementa a través de modificaciones en el código, el código solo debe consistir de lenguajes de marcado.

ii. No pueden usarse lenguajes de programación para este propósito, pues son capaces de realizar comandos a nivel de la Plataforma de Juego.

d) Todo paquete de temas públicamente instalables debe ser alojado y monitoreado en el sitio web oficial del juego, y todos los temas cargados deben ser verificados para asegurar que no contienen aprovechadores potenciales o software malicioso.

7.5 Controles Técnicos

*7.5.1 **Reservado***.

*7.5.2 **Requisitos para el Servicio de Nombres de Dominio (DNS)***.

a) Un operador de una Plataforma de Juego debe registrar un nombre reconocible (por ej. compañía.com) en un Servidor de Nombres de Dominio de Internet (DNS). La misma Plataforma de Juego debe estar registrada en el DNS.

b) El servidor primario utilizado para resolver las solicitudes de DNS (es decir, búsquedas hacia adelante y hacia atrás) utilizadas en asociación con la Plataforma de Juego debe ser controlado por el operador y estar físicamente ubicado en un centro de datos seguro;

c) El acceso lógico y físico al servidor primario DNS debe estar restringido a personal autorizado;

d) Debe haber al menos un servidor secundario que sea capaz de resolver las solicitudes de DNS (es decir, búsquedas hacia adelante y hacia atrás). Los servidores secundarios deben

estar ubicados en premisas separadas del servidor primario; y

e) Las transferencias de zonas entre el servidor primario y los servidores secundarios deben ocurrir al menos cada 24 horas.

7.5.3 Auto-Monitoreo.

a) La Plataforma de Juego debe implementar el auto-monitoreo de componentes críticos (por ej. servidores centrales, dispositivos de red, cortafuegos, vínculos a terceros, etc.).

b) Un componente que falla las pruebas de auto-monitoreo debe ser inmediatamente puesto fuera de servicio. El componente no debe ser activado nuevamente hasta que haya evidencia razonable de que el fallo ha sido rectificado.

7.5.4 Protección de Ataques.

a) Deben tomarse todas las precauciones razonables posibles para proteger la Plataforma de Juego contra ataques basados en la repetición de mensajes auténticos o no auténticos (por ejemplo, un Ataque de Denegación de Servicio Distribuido).

b) El software debe ser capaz de detectar y/o prevenir razonablemente un ataque del estilo "Man in the Middle" sin invadir la privacidad del usuario final.

c) Si se sospecha de un ataque "Man in the Middle", todas las comunicaciones entre el cliente sospechoso y el servidor deben ser terminadas mostrando un mensaje al usuario final sobre por qué las comunicaciones fueron finalizadas.

d) Luego de la terminación de las comunicaciones cliente-servidor, deben seguirse los pasos apropiados para determinar si el usuario final estaba realizando un ataque "Man in the Middle". Si se determinó que se intentó un ataque "Man in the Middle", deben tomarse la acciones apropiadas relacionadas con las trampas.

e) Deben tomarse todas las precauciones razonables para asegurar que ningún dato guardado en la Plataforma de Juego o transferido por esta pueda infectarse por un virus de computadora, Troyano, gusano, u otro software malicioso.

f) La prueba de penetración de la Plataforma de Juego debe ser realizada al menos cada seis meses.

7.5.5 Gestión de la Seguridad de la Red.

a) Las redes deben ser gestionadas y controladas adecuadamente, a fin de protegerlas de amenazas, y mantener la seguridad para los sistemas y aplicaciones que la usan,

incluyendo la información en tránsito.

b) Los escaneos de vulnerabilidad interna en los componentes de la red deben ser realizados al menos cada seis meses.

c) Las características de seguridad, niveles de servicio, y requisitos de gestión de todos los servicios de red deberán estar identificados e incluidos en todo acuerdo de servicio de red ya sea que estos sean proporcionados internamente o tercerizados.

7.5.6 Controles de Acceso a la Red.

a) Deberá establecerse, documentarse, y revisarse una política de control del acceso basada en requisitos para negocios y de seguridad para el acceso.

b) Un procedimiento formal de registro o eliminación de usuario debe estar en funcionamiento para otorgar y revocar el acceso a todos los sistemas y servicios de información.

c) La asignación de privilegios de usuario deberá estar restringida y controlada en base a los requisitos del negocio.

d) La gerencia deberá revisar los derechos de acceso de los usuarios en intervalos regulares utilizando un proceso formal.

e) Solo deberá proporcionarse a los usuarios acceso a los servicios a los que han sido específicamente autorizados de usar.

f) Las contraseñas deben ser controladas a través de un proceso de gestión formal.

g) La selección de contraseñas debe seguir buenas prácticas de seguridad.

h) Los equipos no atendidos deberán tener una protección apropiada y cerrar automáticamente la sesión del usuario luego de un intervalo predeterminado.

i) Deberán usarse métodos de autentificación apropiados para controlar el acceso de usuarios remotos.

j) La identificación automática de equipos deberá ser considerada como un medio para autentificar las conexiones de ubicaciones y equipos específicos.

k) El acceso físico y lógico a los puertos de diagnóstico y configuración deberá ser controlado.

l) Los grupos de servicios de información, usuarios, y sistemas de información deberán estar segregados en redes.

m) Para las redes compartidas, especialmente aquellas que se extienden a lo largo de los

límites de la organización, la capacidad de los usuarios para conectarse a la red deberá estar restringida en línea con la política de control del acceso y los requisitos de las aplicaciones del negocio.

n) Deberán implementarse controles de ruteo para las redes que aseguren que las conexiones y los flujos de información de la computadora no viole la política de control del acceso de las aplicaciones del negocio.

7.5.7 Controles de Acceso del Sistema Operativo.

a) El acceso a los sistemas operativos deberá ser controlado por un procedimiento de inicio de sesión seguro.
b) Todos los usuarios deberán tener un identificador único (ID de usuario) solo para su uso personal, y deberá elegirse una técnica adecuada de autentificación para sustentar la identidad reclamada por un usuario.
c) Los sistemas para gestionar las contraseñas deberán ser interactivos y deberán asegurar la calidad de las mismas.
d) El uso de programas utilitarios que podrían ser capaces de controlar los controles del sistema y de las aplicaciones deberá estar restringidos y estrictamente controlados.
e) Las sesiones inactivas deberán cerrarse luego de 30 minutos de inactividad.
f) Deberán usarse restricciones en los tiempos de conexión para proveer seguridad adicional para las aplicaciones de alto riesgo.
g) El acceso a funciones del sistema de información y aplicación para los usuarios y el personal de apoyo deberá ser restringido de acuerdo con la política de control del acceso definida.
h) Los sistemas sensibles deberán tener un entorno computarizado dedicado (aislado).
i) Deberá establecerse una política formal y las medidas apropiadas de seguridad deberán ser adoptadas para proteger contra los riesgos del uso de computadoras e instalaciones de comunicación móviles.
j) Deberá desarrollarse e implementarse una política, planes y procedimientos operativos para las actividades de telecomunicación.

7.5.8 Controles Criptográficos. Deberá desarrollarse e implementarse una política para el uso de controles criptográficos para la protección de la información.

a) Cuando datos sensibles pasen a través de las líneas de comunicación, dichos datos deben ser encriptados. Ejemplos de datos que podrían requerir de encriptación son los PIN o contraseñas, números y detalles de la cuenta (incluyendo números de tarjetas), claves de encriptación, detalles de la identidad del jugador, transferencias de fondos a y desde cuentas de los clientes, cambios en los detalles de la cuenta (por ej.: cambio de dirección, cambio de tarjeta de crédito, cambio de nombre, etc.). y detalles de juego (es decir, juegos jugados, montos apostados, montos ganados, premios mayores ganados, etc.).
b) Los datos que no requieran ser escondidos deber ser autentificados utilizando alguna forma de técnica de autentificación de mensajes;
c) Los datos sensibles deben encriptarse de final a final (es decir los datos nunca deben aparecer en un LAN o WAN sin encriptar). Esto incluye datos sensibles transmitidos entre las Plataformas de Juego computarizadas dentro de las premisas del operador;
d) Los datos sensibles transmitidos entre las Plataformas de Juego de una red cambiada dentro de un único centro de datos seguros no necesitan ser encriptados;
e) Los datos sensibles transmitidos entre las Plataformas de Juego que se ubican dentro de centros de datos seguros separados no necesitan ser encriptados si la vía de comunicación es físicamente segura y no puede ser accedida por personas no autorizadas;
f) Todas las comunicaciones entre las terminales del operador y la Plataforma de Juego deben estar fuertemente autentificadas y encriptadas durante la transmisión fuera de sus respectivos centros de datos seguros; y
g) La autentificación debe estar disponible a través de una Codificación de Enlace Seguro (SSL en inglés) y un certificado de seguridad de una organización aprobada.
h) Los algoritmos de encriptación son demostrablemente seguros contras los ataques criptoanalíticos;
i) Los operadores deben tener procedimientos aprobados para hacer seguimiento a los reportes de debilidades en los algoritmos de encriptación utilizados en cualquier parte de la Plataforma de Juego (incluyendo, pero no limitados a, GNA, cortafuegos, sistemas de autentificación y operación de la Plataforma de Juego). Los cambios en los algoritmos de encriptación para corregir las debilidades deben ser implementados tan pronto como sea posible. Si ninguno de estos cambios están disponibles, el algoritmo debe ser reemplazado.

7.5.9 Gestión de la Clave Criptográfica.

a) El largo mínimo (tamaño) de las claves de encriptación es de 112 bits para algoritmos simétricos y 1024 bits para claves públicas.

b) Debe implementarse un método seguro para cambiar el conjunto de claves actuales de encriptación. No es aceptable usar únicamente la clave actual para establecer la "encriptación" del siguiente conjunto. Un ejemplo de un método aceptable de intercambio de claves es el uso de técnicas de claves de encriptación pública para transferir los nuevos conjuntos de claves.

c) Debe haber un método seguro para almacenar toda clave de encriptación. Las claves de encriptación no deben ser almacenadas sin ser ellas mismas encriptadas utilizando un método diferente de encriptación y/o utilizando una clave diferente de encriptación.

7.5.10 Códigos Maliciosos y Móviles.

a) Deberán implementarse controles de detección, prevención y recuperación; así como procedimientos adecuados de concientización de los usuarios para la protección contra códigos maliciosos.

b) Cuando se autorice el uso de códigos móviles, la configuración deberá asegurar que el código móvil autorizado funcione de acuerdo a una política de seguridad claramente definida, y se deberá prevenir la ejecución de códigos móviles no autorizados.

7.5.11 Monitoreo.

a) Deberán producirse y guardarse registro de auditoría de actividades de los usuarios, excepciones y acontecimientos de seguridad de la información durante un periodo acordado para ayudar a investigaciones futuras y al monitoreo de control del acceso.

b) Cualquier modificación, intento de modificación, lectura de acceso y otros cambios o accesos a cualquier registro o auditoría de la Plataforma de Juego debe ser visible para una Plataforma de Juego a través de un sello de tiempo o de la versión del control. Debe ser posible ver quien ha visto o alterado el registro y cuando.

c) Deberán establecerse procedimientos para el monitoreo del uso de las instalaciones de procesamiento de la información y los resultados de las actividades de monitoreo revisadas quincenalmente o como lo mande la jurisdicción.

d) Las instalaciones y la información de registro deberán protegerse contra alteraciones y accesos no autorizados.
e) Las actividades del Administrador del Sistema y del Operador del Sistema deberán ser registradas.
f) Las fallas deberán ser registradas, analizadas y tomarse los apropiados cursos de acción.
g) Los relojes de todos los sistemas relevantes de procesamiento de la información dentro de un dominio de organización o seguridad deberán estar sincronizados con una fuente acordada y precisa de tiempo.

7.5.12 <u>Gestión de Seguridad de las Comunicaciones</u>. Esta sección se refiere a las comunicaciones entre el servidor de la Plataforma de Juego y el dispositivo del jugador final, pero también aplica a las comunicaciones entre otros componentes y equipos de la Plataforma de Juego.

a) La autentificación de mensajes debe utilizarse para tipos de mensajes críticos, como ganar un premio mayor y las transmisiones de contraseñas/PIN, a fin de verificar la recepción correcta de dicho mensaje por el dispositivo, servidor o equipo relacionado del jugador final. Podría utilizarse un protocolo que no corrija los errores ni vuelva a enviar los paquetes erróneos (por ej. UDP) siempre que no se envíen datos o información crítica del juego de esta manera. Por ejemplo, si se usa un UDP para transferir y visibilizar videos o audios entonces no sería aceptable tener las instrucciones o la tabla de pagos del juego solo en estos formatos.
b) El servidor del juego debe ser capaz de validar toda la información recibida desde el cliente para asegurar que no se haya enviado ningún dato adicional (como un gusano).
c) Si se ha detectado que datos adicionales (como un gusano) se han adjuntado a los datos recibidos, el servidor del juego no debe permitir que el código extraño pase a través de la Plataforma de Juego.
d) Todos los protocolos deben utilizar técnicas de comunicación que tengan detectores adecuados de errores y/o mecanismos de recuperación y que además cumplan las siguientes reglas:
    i. El protocolo de mayor nivel debe emplear técnicas (por ej. reconocimientos de final a final) tales que no se pierdan mensajes - incluso cuando uno finalice o el

otro reinicie;

ii. Estas técnicas no deben causar que ni la Plataforma de Juego ni el dispositivo del jugador final detengan todo proceso mientras esperan por el reconocimiento.

e) El protocolo de mayor nivel debe emplear técnicas (por ej. números de transmisión) tales que los mensajes repetidos sean descartados - incluso cuando uno finalice o el otro reinicie;

f) Estos requisitos no aplican para mensajes inseguros como mensajes de transmisión global;

g) Todas las funciones del protocolo deben estar claramente especificadas en su documentación;

h) Las siguientes reglas aplican para los sellos de tiempo en un protocolo de alto nivel:

i. Debe incluir la provisión del sistema de transmisión (es decir, Plataforma de Juego o dispositivo del jugador final) para insertar un sello de tiempo local en cada mensaje que envía. Este sello de tiempo ayudará en reclamos por el mal funcionamiento de los equipos involucrando problemas de hardware o software; y

ii. Debe incluir la provisión del sistema de transmisión (es decir, Plataforma de Juego o dispositivo del jugador final) para insertar un sello de tiempo en el momento en que se recibió el último mensaje de alto nivel.

i) Los siguientes requisitos aplican para la Interface de Alto Nivel como Protocolos de Menor Nivel:

a) No debe haber restricciones a los caracteres que pueden incluirse en los mensajes enviados o provenientes de los niveles mayores a los niveles menores;

b) Las interfaces entre los protocolos de capa alta y los protocolos de capa baja deben ofrecer mensajes de largo variable incluyendo aquellos que son más largos que el tamaño estándar de amortiguamiento del nivel menor;

c) Debe implementarse un método de flujo de control para prevenir la pérdida de mensajes vitales;

d) La Plataforma de Juego deberá detectar la velocidad máxima de transferencia entre ella y el entorno de los jugadores, y notificar al jugador si la velocidad detectada cae por debajo del requisito mínimo establecido por el Regulador responsable de la Jurisdicción del jugador; y

e) La información deberá ser mostrada al jugador a través de un medidor de latencia que cumpla los requisitos listados en este documento.

7.5.13 <u>Cortafuegos</u>. Los siguientes requisitos aplican para los cortafuegos:

a) Todas las conexiones a la Plataforma de Juego alojada en el centro de datos seguros debe pasar a través de al menos una aplicación aprobada de cortafuegos. Esto incluye las conexiones a y desde cualquier servidor que no sea de la Plataforma de Juego (por ej. Plataformas de Juegos de computadora MIS) utilizado por el operador. El término "conexiones" es utilizado en su sentido más amplio, e incluye transferencias de datos UDP y TCP;

b) La elección del cortafuegos estará afectada por el protocolo de bajo nivel utilizado por la aplicación. (por ej. algunos cortafuegos no tiene la capacidad de tomar decisiones inteligentes sobre las transferencias UDP.) Reducir la efectividad de la aplicación de cortafuegos a un filtro de paquetes no estará permitida simplemente debido a una combinación de mala elección del cortafuegos / protocolo de bajo nivel;

c) Un dispositivo en el mismo dominio de transmisión que el servidor de la Plataforma de Juego no debe tener una instalación que permita establecer una ruta de red alterna que pueda saltearse el cortafuegos. Ejemplos de instalaciones prohibidas son:
   - Una PC operadora equipada con un módem telefónico; y
   - Una PC operadora con una conexión VLAN a la Plataforma de Juego y una conexión al VLAN corporativo.

d) El cortafuegos deber ser un dispositivo de hardware separado con las siguientes características:
   i. Solo las aplicaciones relacionadas con el cortafuegos pueden residir dentro del mismo; y
   ii. Solo un número limitado de cuentas podrán estar presentes en un cortafuegos (por ej. solo para administradores de la Plataforma de Juego).

e) Todos los paquetes de datos enviados al cortafuegos deben ser rechazados si llegan en interfaces a redes que se encuentran fuera del rango. Esto es para restringir el acceso al cortafuegos de estaciones de trabajo autorizadas dentro del rango de línea de base;

f) El cortafuegos debe rechazar todas las conexiones excepto aquellas que han sido específicamente aprobadas por la jurisdicción;

g) El cortafuegos debe mantener un registro de auditoría para todos los cambios a los parámetros que afecten qué conexiones están permitidas a través del cortafuegos;
h) El cortafuegos debe mantener un registro de auditoría para todos los intentos exitosos y fallidos de conexión a través del mismo;
i) El cortafuegos debe deshabilitar todas las comunicaciones si el registro de auditoría se llena;
j) El cortafuegos debe rechazar todo mensaje recibido en una interface si el mensaje pretende ser de un dispositivo adjunto a otra interface;
k) Los operadores deben contar con procedimientos aprobados para el seguimiento de los informes de incidentes de seguridad y para asegurar que los cortafuegos se mantengan actualizados respecto a las recomendaciones publicadas luego de dichos incidentes; y
l) Las redes en el lado seguro del cortafuegos debería utilizar rangos privados RFC1918. Estos rangos deben ser traducidos al rango de la red pública para su transmisión a través de Internet.

7.5.14 <u>Seguridad de la Aplicación Web</u>. Los siguientes requisitos aplican para la seguridad de la aplicación utilizada en el dispositivo del jugador final:

a) La Plataforma de Juego debe ser capaz de detectar la versión del navegador web o software cliente, que está siendo usado por el jugador en el momento en el que el jugador inicia la sesión.
b) Si la versión del navegador web o del software cliente usados por el jugador no tienen la capacidad de correr la aplicación (por ej. el juego requiere del Reproductor Flash 10 pero el navegador solo tiene la versión 8), la Plataforma de Juego no debe permitir que la aplicación sea ejecutada hasta que el software cliente haya sido actualizado, y debe proporcionar un vínculo para descargar cualquier actualización requerida.

Glosario

Descripción del Término o Abreviatura

Sistema de Juegos de Azar Interactivos (SJAI) - Es el hardware, software, firmware, tecnología de comunicaciones y otros equipos que le permiten a un jugador apostar remotamente a través de Internet o de un entorno de red similarmente distribuido, y el equipo correspondiente relacionado con la determinación del resultado del juego, la visualización del juego y los resultados del mismo, así como otra información similar y necesaria para facilitar el jugado del juego. El término no incluye a los equipos computarizados o a las tecnologías de la comunicación utilizadas por el jugador para acceder al sistema de juegos de azar interactivos.

Plataforma de Juego - Es el hardware y software del sistema de juegos de azar interactivos que maneja las características comunes a todos los juegos ofrecidos, y forma la interface primaria del sistema de juego tanto para el jugador como para el operador. La plataforma de juego le proporciona al jugador los medios para registrar una cuenta, iniciar / salir de su cuenta, modificar la información de su cuenta, depositar y retirar fondos hacia / desde sus cuenta, solicitar informes de las actividades de sus cuenta, y cerrar su cuenta. Asimismo, todas las páginas web mostradas al jugador que estén relacionadas con la experiencia de juego ofrecida por el SJAI, pero que no son una pantalla del juego, son consideradas como parte de la plataforma de juego. La plataforma de juego le proporciona al operador los medios para revisar las cuentas de los jugadores, habilitar / deshabilitar juegos, generar diversos informes de juego /de transacciones financieras y de la cuenta, colocar resultados de los juegos en los eventos de apuesta deportiva, habilitar / deshabilitar cuentas de jugadores, y establecer parámetros personalizados.

Ciclos/ Actividades de Segundo Plano - Si el software GNA es ciclado en segundo plano, significa que hay un serie constante de números aleatorios que están siendo generados por el GNA, incluso si esto no es requerido por el juego en este momento. Sin los ciclos /actividades de segundo plano, uno podría predecir el resultado de la siguiente reiteración de la función utilizada para producir números aleatorios si se conocieran los valores y el algoritmo utilizado.

Porcentaje de Retorno para el Jugador (%PRJ) - es el porcentaje esperado de apuestas que un juego específico devolverá al jugador en el largo plazo. El %PRJ puede calcularse a través de un enfoque teórico o de uno simulado. El método utilizado para su cálculo depende del tipo de juego.

Juego con Etapas Múltiples - es un juego que tiene uno o más pasos intermedios que requiere del insumo del jugador para proceder. El Póquer y el Blackjack son dos ejemplos de juegos de etapas múltiples.

Mapeo - Es el proceso por el cual a un número escalado se le asigna un símbolo o valor que es utilizable y aplicable al juego actual (por ej. el número escalado 51 podría ser mapeado como un AS DE ESPADAS).

Escalamiento - El resultado bruto de un GNA normalmente tendrá un rango demasiado excesivo del requerido (por ej.: un GNA de 32-bit tiene más de dos mil millones de resultados posibles, pero (por ejemplo) solo tenemos que determinar cuál de los 52 naipes se sacará). El escalamiento es requerido para dividir este resultado bruto en números más pequeños y utilizables. Estos números 'escalados' pueden ser mapeados a números particulares de naipes, cifras récord, símbolos, etc... Consecuentemente, el resultado bruto de un GNA algunas veces tendrá un rango mucho más pequeño del requerido para el uso que se le pretende dar (por ej.: 0 < resultado bruto < 1). En estos casos, el escalamiento es requerido para expandir el resultado BRUTO en números más grandes y utilizables.

Juego Metamórfico - Un juego metamórfico es aquel en el que las reglas del juego permiten que este tenga una 'memoria' de eventos previos, de modo que estos eventos vayan fortaleciéndose con el tiempo, resultando finalmente en algún cambio en el juego. Por ejemplo, el juego puede ser diseñado para permitir que el jugador junte monedas o fichas especiales a través del juego regular. Una vez que se hayan acumulado suficientes monedas / fichas, el juego entra a una característica especial. Al salir de la característica especial, las monedas / fichas son regresadas a cero, permitiendo que el jugador comience a acumularlas nuevamente.

Generador de Números Aleatorios (GNA)- Es el hardware y / o software del SJAI que determina los resultados aleatorios que son utilizados por todos los juegos alojados / ofrecidos en la plataforma de juego.

Línea de base- Es un método administrativo que permite tomar una instantánea de un sistema en evolución (y en algunos casos definir que porciones del sistema pueden cambiarse sin aprobación).

Dominio de difusión - Es el conjunto de sistemas de computadoras que tienen la capacidad de comunicarse unas con otras utilizando paquetes de difusión a nivel de la red. Un ejemplo de dominio de difusión es una subred IP.

Aportes - Es el método financiero por el cual se financian los pozos del premio mayor.

Componente Crítico - Cualquier subsistema cuya falla o compromiso pueda acarrear la pérdida de derechos de los jugadores, ingresos para el gobierno o el acceso no autorizado a los datos usados para generar los reportes para la jurisdicción.

Certificado Digital - Es un conjunto de datos que pueden ser utilizados para verificar la identidad de una entidad refiriéndose a un tercero de confianza (la Autoridad Certificadora). Los certificados digitales a menudo son utilizados para autentificar mensajes con propósitos de no repudio. Uno de los atributos de un certificado digital es que no puede ser modificado sin comprometer su consistencia interna. Los

certificados X.509 son un ejemplo de un certificado digital.

Sistema de Nombre de Dominio - Es la base de datos de Internet globalmente distribuida que (entre otras cosas) mapea y transforma los nombres de las máquinas en números IP y viceversa.

Ancho de banda efectivo - Es la cantidad de datos que pueden ser transferidos a lo largo de una red por unidad de tiempo. El ancho de banda efectivo a través de Internet es considerablemente menor que el ancho de banda de cualquiera de sus vínculos constituyentes.

Dispositivo de Jugador Final - Es el dispositivo que convierte las comunicaciones desde la Plataforma de Juego a una forma interpretable para los humanos, y convierte las decisiones humanas en un formato de comunicación entendido por la Plataforma de Juego. Ejemplos de Dispositivos de Jugador Final incluyen computadoras personales y teléfonos.

Enlace activo- Es una palabra o un gráfico en una página web que, de ser cliqueado, causa que se visualice una diferente página de información.

ICMP - Protocolo de Mensajes de Control de Internet. Es parte del protocolo de comunicaciones TCP/IP que se usa para medir y controlar dispositivos a nivel de la IP. La solicitud de eco ICMP y la respuesta de eco ICMP son común y colectivamente conocidas como "ping" y "trazo de ruta".

Tasa de Incremento - Es la porción de los aportes al premio mayor que van incrementando el mismo (en comparación con el valor de financiamiento inicial).

Utilización de vínculos - Es el porcentaje de tiempo que un vínculo de comunicaciones compromete para la transmisión de datos.

Premio Mayor Misterioso - Es un tipo de premio mayor en el que se elige un punto desencadenador aleatorio entre el monto inicial del premio, y un monto máximo de ganancia. El acto de ganarlo es activado cuando los aportes al premio mayor llevan al valor de inicio hasta el monto desencadenador.

Pozo - Es un reservorio de acumulación de aportes minoritarios al premio mayor.

Premio Mayor Progresivo - Es un tipo de premio mayor en el que la Plataforma de Juego activa el premio (un premio proveniente de un pozo de aportes de un grupo de máquinas participando en el premio mayor).

Protocolo - Utilizado para referirse a la interface del hardware, la disciplina de la línea y los formatos de mensaje de las comunicaciones.

Datos sensibles - son datos que, de ser obtenidos por un tercero, podrían ser utilizados para afectar el resultado/s del juego o la cuenta del jugador/es.

Revisión de Firmas - Es un mecanismo de seguridad en el que un CMCS verifica SW en dispositivos periféricos o en dispositivos de jugador final.

Producto de apuesta suave - Es un producto de apuestas que cumple con el conjunto de criterios publicados para los productos de apuestas "suaves" o que recibe una aprobación especial bajo el Modelo

Regulador Nacional.

Valor de inicio - Es el valor inicial del premio mayor (no incluye los valores de medidores desbordados).

Premios Mayores Basados en Tiempos - Son un tipo de premio mayor en el que se elige aleatoriamente un momento en el tiempo que lo active entre el inicio del tiempo de funcionamiento del premio mayor hasta su tiempo final de funcionamiento.

Sello de tiempo - Es un registro del valor actual de la fecha y hora de la Plataforma de Juego que se añade al mensaje en el momento en que es creado.

Troyano - Es un programa o módulo que pretende realizar una función particular pero que secretamente realiza una función diferente (que podría o no podría incluir la función pretendida). Los programas troyanos están ampliamente extendidos en todo el Internet.

Control de la Versión - Es el método por el cual una Plataforma de Juego aprobada y en evolución es verificada para funcionar en un estado aprobado.

Apéndice A: Requisitos para el Envío al Proceso de Evaluación

A.1 Introducción

A.1.1 ***<u>Declaración General</u>***. Este capítulo gobernará los tipos de información que son, o que podrían ser requeridos a la parte remitente a fin de realizar pruebas en base al presente Estándar de elementos o componentes del Sistema de Juegos de Azar Interactivos. Cuando la información no se haya enviado o de otro modo, no esté en posesión del laboratorio que realiza las pruebas, se le deberá solicitar a la parte remitente que proporcione información adicional. El no suministrar la información puede resultar en la negación de todo o parte del envío y/o acarrear demoras en la realización de las pruebas.

A.1.2 ***<u>Envío Previo</u>***. Cuando al laboratorio que realiza las pruebas se le haya suministrado previamente esta información en un envío anterior, no se requiere duplicar la documentación, en vista que la información previa está a nombre de la parte remitente, y que dichos documentos son fácilmente localizables en el laboratorio de pruebas. Deberán hacerse todos los esfuerzos posibles para reducir la redundancia en el envío de la información.

A.2 Envío de Prototipo (Envío Completo)

A.2.1 ***<u>Declaración General</u>***. El envío de prototipos (envío completo) es un envío que se hace por primera vez de una pieza particular de hardware o software que no ha sido revisada previamente por el laboratorio que realiza las pruebas. Para Modificaciones de envíos previos, incluyendo cambios requeridos a la certificación de prototipos (envío completo) enviados previamente, ver 'Envíos de Modificaciones (envíos parciales) de un Ítem Certificado Previamente,' Sección A.3.

NOTA: *Debido a la complejidad anormal y/o al costo excesivo de un componente, a veces es necesario realizar pruebas de una Plataforma de Juego in situ en la instalación del fabricante. Los requisitos para la realización de pruebas in situ serán evaluados según sea el caso.*

A.2.2 ***<u>Requisitos para la Carta de Envío</u>.*** Cada envío deberá incluir una carta de solicitud, con un membrete de la compañía, fechada dentro de una (1) semana de la fecha en que el envío es recibido por el laboratorio de pruebas. La carta debería incluir lo siguiente:

a) La(s) jurisdicción(es) para las que usted está solicitando certificación;
b) Los ítems requeridos para su certificación. En el caso de software, la parte remitente deberá incluir los números de ID y los niveles de revisión, si aplican. En caso de ser propietaria del hardware, la parte remitente deberá indicar el fabricante, modelo, y los números de las partes y revisión de los componentes asociados al hardware; y
c) Una persona de contacto que servirá como el punto principal de contacto para las preguntas de ingeniería levantadas durante la evaluación del envío. Esta puede ser o la persona que firma la carta u otro contacto especifico.

A.2.3 ***<u>Requisitos para el Envío de Componentes de Gestión de la Cuenta del Jugador</u>.*** La "Gestión de la Cuenta del Jugador" incluye componentes de la Plataforma de Juego que forman la interface primaria para el jugador. La interface de Gestión de la Cuenta del Jugador le proporciona al jugador los medios para registrar una cuenta, iniciar / salir de su cuenta, modificar la información de su cuenta, depositar y retirar fondos hacia / desde sus cuenta, solicitar informes de las actividades de sus cuenta, y cerrar su cuenta. Asimismo, todas las páginas web mostradas al jugador que estén relacionadas con la experiencia de juego, pero que no son una pantalla actual del juego, son consideradas como parte de los componentes de Gestión de la Cuenta del Jugador.

I. Código Fuente Los siguientes requisitos aplican a cualquier código fuente de componentes de Gestión de la Cuenta del Jugador solicitado por el laboratorio de pruebas para su evaluación:

a) Todo código fuente de un componente de Gestión de la Cuenta del Jugador enviado al laboratorio de pruebas deberá revisarse de una manera segura, controlada y supervisada que sea acordada con el laboratorio de pruebas, el regulador y el vendedor del software;
b) Todo código fuente de un componente de Gestión de la Cuenta del Jugador enviado a un laboratorio de pruebas deberá contener la siguiente información (como mínimo):
    i. Archivo / módulo / nombre(s) de la función; y

ii. Brece descripción del archivo / módulo / propósito(s) de la función; y

c) Todo código fuente de un componente de Gestión de la Cuenta del Jugador enviado al laboratorio de pruebas deberá estar comentado de una manera informativa y útil.

II. Documentación La siguiente documentación debe ser enviada para la evaluación de componentes de Gestión de la Cuenta del Jugador:

a) Descripción detallada y funcional de los componentes de Gestión de la Cuenta del Jugador (incluyendo la página de inicio del sitio web y todas las páginas periféricas del sitio),

b) Descripciones detalladas y funcionales de las siguientes funcionalidades técnicas disponibles en la plataforma de juego:

i. Registro de Cuenta del Jugador,
ii. Entrada a la Cuenta del Jugador (Usuario y Contraseña),
iii. Interface del Jugador a la Cuenta del Jugador,
iv. Características de Juego Responsable,
v. Política de Privacidad, y
vi. Desactivación de la Cuenta del Jugador,

c) Descripción detallada de cómo se protege la verificación de la información del jugador de acceso no autorizado;

d) Descripción detallada de la autentificación del jugador (es decir, cómo se identifican a sí mismos los jugadores registrados a la Plataforma de Juego cada vez que se conectan);

e) Descripción de cómo se protege el registro y la información de la cuenta del jugador (incluyendo información de tarjetas de crédito) de accesos no autorizados;

f) Descripción del registro de premios monetarios no reclamados y cómo esto es mantenido; y

g) Descripción de tratamiento de los ingresos producto de ganancias expiradas o no reclamadas.

III. Entorno de Pruebas – Construcción e Instalación Supervisada Antes de comenzar con las pruebas, el laboratorio supervisará la construcción / compilación del código fuente de la plataforma de juego en un software. En este contexto, "supervisar" significa que un consultor del laboratorio de pruebas debe estar presente, en persona o a través de

un conexión remota, mientras que el código fuente de la plataforma de juego está siendo construido / compilado.

El control de la versión(es) de la plataforma de juego, creado como resultado de la construcción / compilación supervisada, deberá ser instalado en un entorno de pruebas adecuado. El laboratorio de pruebas y el proveedor del software deben asegurar que el software instalado sea la misma versión que el que fue construido / compilado bajo la supervisión del laboratorio de pruebas. Debe prestársele particular atención a cualquier configuración realizada en el entorno de pruebas para acomodar el software que ha sido instalado. El laboratorio de pruebas debe obtener una copia de cualquier archivo de configuración necesario.

El sistema de pruebas resultante debe ser similar al de la Plataforma de Juego, e idéntico respecto a toda funcionalidad crítica relacionada a la plataforma de juego, lo que permitirá la realización de pruebas significativas al software antes de que sea cargado en la Plataforma de Juego en vivo.

Cuando una Plataforma de Juego requiera del uso de papeles definidos de usuarios, o de cuentas con contraseña o números PIN asociados, deberá enviarse una lista por defecto de todos los usuarios y contraseñas o números PIN incluyendo un método para acceder a la base de datos.

A.2.4 ***Requisitos para el Envío de Sistemas de Seguridad de la Información (SI)***. Un SI se refiere a las características ambientales, administrativas y técnicas implementadas para mantener la seguridad e integridad del entorno de juegos. Las siguientes secciones delinean los requisitos de envío para la evaluación de un SI.

I. **Documentación** La siguiente documentación debe enviarse para la evaluación del SI:

a) Una copia de la Política de Seguridad de la Información, incluyendo:

i) Detalles de los procesos físicos de seguridad implementados para proteger el entorno productivo del juego;

ii) Detalles de dónde y cómo cada categoría de información (por ej. crítica, importante, no importante) es almacenada en la Plataforma de Juego, y la evaluación del riesgo y las medidas de protección implementadas para cada categoría de información;

iii) Detalles de los sistemas de protección de contraseñas y algoritmos asociados utilizados por la Plataforma de Juego;
iv) Detalles del método de transacción utilizado;
v) Detalles de cómo se implementa el auto-monitoreo;
vi) Detalles de los métodos de encriptado utilizados para el almacenamiento seguro de información crítica;
vii) Controles del uso previamente no autorizado de consolas o cuentas del operador, y para la prevención de accesos no autorizados a información que podría ayudar a lograr accesos no autorizados de las consolas y cuentas del operador (como nombres de usuarios, direcciones IP o contraseñas);
viii) Detalles del sistema de manejos de incidentes implementado por el operador;
ix) Detalles del plan de recuperación de desastres implementado por el operador;
x) Detalles de reportes de auditoría disponibles desde la Plataforma de Juego; y
xi) Reportes mostrando cuán seguido se revisa la Política de Seguridad de la Información.

b) Una descripción general del diseño de la Plataforma de Juego;
c) Detalles y especificaciones funcionales de todos los componentes de la Plataforma de Juego en el entorno productivo incluyendo, pero no limitándose a:
    i) Hardware de la Plataforma, como:
        - Servidores,
        - Cortafuegos y Sistemas de Detección de Intrusión,
        - Consolas del Operador (locales y remotas),
        - Pasarelas (*Gateways*) y Puntos de Acceso,
        - Controladores Remotos,
        - Servidores de Acceso Remoto,
        - Equipos de Multiplexación,
        - Equipos de Switch,
        - Equipos de Monitoreo,

- Hubs, Switches y Routers, y
- Repetidores,

ii) Sistemas Operativos,

iii) Aplicaciones,

iv) Subsistemas de auditoría, incluyendo cualquier funcionalidad incorporada de los sistemas operativos y aplicaciones utilizada para propósitos de auditoría,

v) Estrategia de Duplicación,

vi) Subsistema de Disco, y

vii) Instalaciones de respaldo.

d) Un diagrama de arquitectura de red, incluyendo lo siguiente:

i) Topología de la red,

ii) Dispositivos utilizados para crear la red,

iii) Direcciones IP internas y externas para todos los dispositivos,

iv) Controles para prevenir modificaciones no autorizadas a las configuraciones de los dispositivos,

v) El diseño de la Red de Área Local (LAN) y de la Red Virtual de Área Local (VLAN), incluyendo todas las subredes y cortafuegos funcionales,

vi) Detalles de las conexiones de la plataforma de juego a internet, y

vii) Detalles de cualquier conexión remotas (por ej. Internet, red de área amplia, dial-up) utilizadas para apoyar las operaciones de la Plataforma de Juego.

e) Una lista de todos los sistemas no productivos (por ej. MIS) y sistemas de terceras partes que conectarán a la Plataforma de Juego. Para cada sistema externo proporciona:

i) El método de conexión (por ej. dial-up, X.25, línea rentada, Internet).

ii) Detalles de la información a ser transferida en cada dirección.

iii) La entidad que inicia la transferencia de la información.

iv) El protocolo usado para realizar la transferencia.

v) Los controles para prevenir el acceso a otra información de la Plataforma de Juego.

vi) Los controles para prevenir el uso no autorizado de las conexiones,

vii) Los controles para prevenir el espiado de las comunicaciones entre sistemas

no productivos y la Plataforma de Juego.

f) Detalles de cualquier sistema de Gestión de la Red asociado con la red de producción interna, incluyendo:
    i) Ubicación física del sistema de Gestión de la Red.
    ii) Clase de personal autorizado para usar el sistema de Gestión de la Red.
    iii) Ubicaciones desde la que las funciones de administración de la red pueden ejecutarse.
    iv) Protocolo de gestión de la red.
    v) Los dispositivos a ser manejados en base a lecturas.
    vi) Los dispositivos a ser manejados en base a lecturas/escrituras.
    vii) Los controles para prevenir el uso no autorizado del acceso a las funciones de gestión de la red.
    viii) Los controles para auditar el uso de las funciones de gestión de la red.
    ix) Los controles para detectar el uso no autorizado de las conexiones a la red,
    x) Los controles para detectar la conexión no autorizada de las conexiones a la red,
    xi) Describa las ubicaciones y los arreglos de seguridad físicos y lógicos asociados con servidores DNS secundarios.

g) Para el encriptado de datos y comunicaciones entre la Plataforma de Juego y el dispositivo de jugador final, se debe entregar la siguiente información:
    i. Detalles del algoritmo utilizado para los mensajes de autentificación:
        - Descripción del algoritmo,
        - Base teórica del algoritmo.
        - Resultados de cualquier análisis o pruebas que demuestren que el algoritmo es adecuado para la aplicación.
        - Reglas de selección de las claves,
        - Reglas para cambiar las claves,
        - Medios para generar y proteger claves.
    ii. Detalles de encriptado a usarse durante el juego, incluyendo:
        - Algoritmo de encriptado,
        - Tamaño de las claves de encriptado,

- Proceso de generación de claves,
- Proceso de almacenamiento de la clave,
- Procedimiento para intercambiar clave al iniciar la sesión,
- Cambios de clave ,
- Proceso de revocación de claves en caso las claves está comprometido y
- Detalles de cualquier información que no esté encriptada con las misma transmisión encriptada.

A.3 Envíos de Modificaciones (Envíos Parciales) de un Ítem Certificado Previamente

A.3.1 ***<u>Declaración General</u>*** Para cualquier actualización de envío (por ej. una revisión a un hardware o software existente que se esté revisando o certificando actualmente o que ha sido revisado pero no certificado), se requerirá de la siguiente información para procesar el envío sumada a los requisitos establecidos en 'Requisitos de la Carta de Envío'. Todas las modificaciones requieren de una nueva prueba, examinación y nueva certificación por parte del laboratorio de pruebas.

NOTA: *Las modificaciones al entorno de soporte que no impacten en la funcionalidad del componente o componentes en evaluación no necesitan ser enviados de nuevo pues estos elementos no son evaluados en nuestro laboratorio en primer lugar, y solo son requeridos para proporcionarle al entorno de soporte el componente a ser evaluado. Sin embargo, cualquier cambio en el entorno que de alguna manera cambie la funcionalidad del componente o componentes en evaluación debe ser nuevamente certificado. Cuando haya alguna duda sobre si la Plataforma de Juego debería ser reenviada o no, estas situaciones se tomarán en consideración dependiendo del caso.*

A.3.2 ***<u>Reenvío del Hardware</u>***. Cada reenvío de hardware deberá:

a) Identificar los ítems individuales que se están enviando (incluyendo número de la parte);
b) Suministrar un juego completo de esquemas, diagramas, hojas informativas, etc. describiendo la modificación junto con las razón para el cambio o cambios; y

c) Proporcionar el hardware nuevo o actualizado, una descripción y el método de conexión a la Plataforma de Juego o los componentes de hardware originales.

A.3.3 ***<u>Reenvío de Componentes de Gestión de la Cuenta del Jugador</u>***. Cada reenvío de componentes de Gestión de la Cuenta del Jugador deberá:

a) Utilizar los mismos requisitos que en los '*Requisitos para el Envío de Componentes de Gestión de la Cuenta del Jugador*' listados líneas arriba excepto cuando la documentación no haya cambiado, en cuyo caso no se requerirá el reenvío de documentos idénticos.
b) Incluir una descripción del cambio o cambios en el software y los módulos afectados;
c) Incluir especificaciones funcionales actualizadas, cuando sea aplicable; y
d) Incluir un paquete actualizado de códigos fuente para la Plataforma de Juego, si aplican.

A.3.4 ***<u>Reenvío del Premio Mayor</u>***. Cada reenvío del premio mayor deberá:

a) Utilizar los mismos requisitos que en los '*Requisitos para el Envío del Premio Mayor*' listados líneas arriba excepto cuando la documentación no haya cambiado, en cuyo caso no se requerirá el reenvío de documentos idénticos;
b) Incluir una descripción del cambio o cambios en el software y los módulos afectados;
c) Incluir especificaciones del premio mayor actualizadas; e
d) Incluir un paquete actualizado de códigos fuente para la Plataforma de Juego.

A.3.5 ***<u>Reenvío del SI</u>***. Cada reenvío de SI deberá:

a) Utilizar los mismos requisitos que en los '*Requisitos para el Envío de Sistemas de Seguridad de Información (SI)*' listados líneas arriba excepto cuando la documentación no haya cambiado, en cuyo caso no se requerirá el reenvío de documentos idénticos;
b) Incluir una descripción detallada del cambio(s) y componente(s) afectados en la Plataforma de Juego, así como la razón o razones para los cambios implementados por el operador; e
c) Incluir diseños y documentos de configuración del SI actualizados cuando se requiera.