SERIE DE ESTÁNDARES TÉCNICOS DE GLI

GLI-33:

ESTÁNDARES PARA SISTEMAS DE APUESTAS DE EVENTOS

VERSIÓN: 1.1

FECHA DE REVISIÓN: 14 DE MAYO DE 2019

Sobre este estándar

Este estándar técnico ha sido producido por **Gaming Laboratories International, LLC (GLI)** con el propósito de proporcionar un análisis técnico independiente y/o certificaciones para los interesados en la industria del juego indicando el estado de cumplimiento para la operación y sistemas de apuestas con los requisitos establecidos en este documento.

La intención de este documento es para ser usado por entidades reguladoras, operadores, y proveedores de la industria como pautas de cumplimiento para tecnologías relacionadas con apuestas de eventos. La intención de este documento no es de representar un conjunto de requisitos preceptivos con los que cada sistema de apuestas de eventos y operador debe cumplir; sin embargo, este establece un estándar técnico relacionado con las tecnologías y procedimientos utilizados para facilitar estas operaciones.

Operadores y fabricantes deben presentar documentación de control interno, credenciales y el acceso asociado a un entorno de ensayos equivalente al de producción con una petición de que sea certificado de acuerdo con este estándar técnico. A partir de la certificación, Gaming Laboratories International, LLC., suministrará un certificado de cumplimiento evidenciando la certificación a este Estándar.

GLI-33 debe ser considerado como un documento en vivo el cual proporciona un nivel de dirección que será adaptado periódicamente para estar de acuerdo con esta industria en desarrollo a lo largo del tiempo según la evolución de las implementaciones de apuestas y operaciones.

Tabla de contenidos

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Capítulo 1: Introducción a Sistemas de Apuestas de Eventos

1.1 Introducción

1.1.1 Declaración general

Gaming Laboratories International, LLC (GLI) ha ensayado dispositivos de juegos desde el año 1989. A través de los años, GLI ha desarrollado una numerosa cantidad de estándares técnicos para jurisdicciones en el mundo entero. Este documento, *GLI-33*, establecerá los estándares técnicos para los Sistemas de Apuestas de Eventos.

1.1.2 Historial del documento

Este documento es una composición de muchos estándares de todo el mundo. Algunos han sido escritos por GLI, otros escritos por reguladores de la industria junto con laboratorios de ensayos y fabricantes, proveedores y operadores de Sistemas de Apuestas de Eventos. GLI ha considerado cada uno de los documentos de estándares, combinando cada una de las regulaciones exclusivas, eliminando algunas regulaciones, y actualizando otras para que reflejen ambos el cambio en tecnología y el propósito de mantener un estándar que cumpla con los objetivos comunes reglamentarios sin impedir innecesariamente la innovación tecnológica. A continuación, GLI incluye una lista dando crédito a las agencias cuyos documentos fueron revisados antes de escribir este estándar. GLI tiene una política de actualizar este documento lo más a menudo posible, para que refleje los cambios de tecnología y/o procedimientos de ensayos. Este documento será distribuido sin costo a todos los que lo soliciten. Este puede ser obtenido descargándolo del sitio de GLI en la internet www.gaminglabs.com o por petición escrita a:

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

1.2 Reconocimiento de otros estándares revisados

1.2.1 Declaración general

Este estándar técnico ha sido desarrollado por medio de evaluaciones y utilizando partes de los documentos de las organizaciones listadas a continuación. GLI reconoce los reguladores y otros participantes de la industria que han ensamblado estos documentos y los agradecemos:

a) Comisión del Juego de Nevada y Junta de Control de Juegos.
b) Política del Juego de Columbia Británica y Rama de Aplicación (GPEB).
c) Asociación Internacional de Comisarios de Carreras (ARCI).
d) Comisión de Licor y Juego de Tasmania.
e) Comisión de Carreras del Territorio del Norte.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

f) Comisión Victoriana para la Regulación del Juego y Licor.
g) Autoridad Danesa del Juego.
h) Dirección General Española para la Regulación del Juego (DGOJ).
i) Oficina de Normas de Sudáfrica (SABS).

1.3 Objetivo de los estándares técnicos

1.3.1 Declaración general

El objetivo de este estándar técnico es el siguiente:

a) Eliminar criterio subjetivo en el análisis y certificación de los Sistemas de Apuestas de Eventos.
b) Ensayar el criterio que impacta la credibilidad e integridad de los Sistemas de Apuestas de Eventos desde la perspectiva de la colección de ingresos y la perspectiva del jugador.
c) Crear un estándar que asegurará que las apuestas de eventos son honradas, seguras, y que puedan ser auditables y operadas correctamente.
d) Para distinguir entre la política pública local y el criterio del laboratorio independiente de pruebas. La responsabilidad de establecer su propia política pública con respecto al juego reside en cada jurisdicción local.
e) Hay que reconocer que la evaluación de sistemas de control interno (así como procesos contra el blanqueo de dinero, procesos financieros y de negocio) utilizados por los operadores de los Sistemas de Apuestas de Eventos no debe ser incorporada dentro de los ensayos de laboratorio de este estándar, sino que será incluida en la auditoría operacional de las jurisdicciones locales.
f) Construir un estándar que pueda ser modificado fácilmente para incluir tecnología nueva.
g) Construir un estándar que no especifique ningún diseño, método, o algoritmo en particular. La intención es de incluir una amplia variedad de métodos a ser utilizados para conformar con los estándares mientras que, al mismo tiempo, dar aliento al desarrollo de nuevos métodos.

1.3.2 Sin limitación de tecnología

Se debe tener precaución que este documento no sea leído de tal manera que limite la utilización de tecnología en el futuro. Este documento no debe ser interpretado de manera que, si la tecnología no está mencionada, entonces no es permitida. Totalmente lo contrario, cuando alguna tecnología nueva es desarrollada, GLI revisará este estándar, realizará cambios e incorporará nuevos estándares mínimos para la tecnología nueva.

1.3.3 Adopción y observancia

Este estándar técnico puede ser adoptado por completo o en parte por cualquier entidad regulatoria que desee implementar una serie completa de requerimientos para los Sistemas de Apuestas de Eventos.

1.4 Otros documentos que pueden aplicar

1.4.1 Otros estándares de GLI

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Este estándar abarca los requisitos para los Sistemas de Apuestas de Eventos. Dependiendo en la tecnología utilizada por un sistema, estándares técnicos adicionales de GLI podrían aplicar.

NOTA: La serie completa de Estándares de GLI está disponible sin ningún costo en www.gaminglabs.com.

1.4.2 Estándares de controles internos mínimos del operador (MICS)

La implementación de un Sistema de Apuestas de Eventos es una tarea compleja, y debido a esto requerirá el desarrollo de procesos internos y procedimientos para asegurar que el sistema es configurado y operado con el nivel de control y seguridad necesario. En este respecto, está previsto que el operador establecerá una serie de Especificaciones de Controles Internos Mínimos (MICS) para definir los procesos internos para la creación, administración, y el procesamiento de transacciones de apuestas además de los requerimientos para el control interno de cualquier software y hardware del sistema o componentes, y sus cuentas asociadas.

1.5 Interpretación de este documento

1.5.1 Declaración general

Este estándar técnico aplica a los sistemas que soportan apuestas sobre deportes, competiciones, partidos, y otro tipo de eventos aprobados por la entidad regulatoria. Los requisitos en este estándar técnico aplican a las apuestas de eventos de forma general y no limita o autoriza los eventos específicos, mercados o tipos de apuestas. La intención es de proveer un marco que abarque aquellos reconocidos y permitidos por la ley en la actualidad. Este documento no tiene la intención de definir cuales partes son responsables para cumplir con los requisitos de este estándar técnico. Es la responsabilidad de las partes interesadas de cada operador de determinar la mejor manera de cumplir con los requisitos establecidos en este documento.

1.5.2 Proveedores de software y operadores

Los componentes de un Sistema de Apuestas de Eventos, aunque pueden ser construidos de forma modular, están diseñados para funcionar conjuntamente sin problemas. Adicionalmente, los componentes del Sistema de Apuestas de Eventos pueden ser desarrollados para incluir funciones configurables, cuya configuración final dependerá en las opciones seleccionadas por el operador. Desde la perspectiva de los ensayos, podría no ser posible hacer pruebas de todas las funciones configurables de un Sistema de Apuestas de Eventos presentado por un proveedor de software a falta de la configuración final seleccionada por el operador; sin embargo, la configuración que será utilizada en producción debe ser comunicada al laboratorio independiente de pruebas para soportar la creación de un entorno funcionalmente equivalente para los ensayos. Debido al carácter integrado de un Sistema de Apuestas de Eventos, este documento incluye un número de requisitos que pueden aplicar a ambos operadores y proveedores. En estos casos, cuando los ensayos son solicitados para una versión de "marca blanca" del sistema, una configuración específica será utilizada para los ensayos y reportes.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

1.6 Ensayos y auditoría

1.6.1 Ensayos de laboratorio

El laboratorio independiente de pruebas hará las pruebas de integridad y certificación de los componentes del Sistema de Apuestas de Eventos conforme con los capítulos de este estándar técnico en un entorno de ensayos controlado, según sea aplicable. Si cualquiera de estos requisitos requiere un procedimiento operacional adicional para cumplir con la intención del requisito, esto debe ser documentado en el reporte de evaluación y usado para complementar el alcance de la auditoría operacional.

1.6.2 Auditoría operacional

La integridad y exactitud de la operación de un Sistema de Apuestas de Eventos depende en gran medida del procedimiento operacional, configuración, y la infraestructura de la red en el entorno de producción. Por lo tanto, la auditoría operacional es una adición esencial a los ensayos y certificación de un Sistema de Apuestas de Eventos. La auditoría operacional definida en los siguientes anexos de este estándar técnico debe ser realizada con una frecuencia especificada por la entidad regulatoria:

a) Anexo A: Auditoría operacional de procedimientos y práctica de juego. Esto incluye, pero no está limitado a revisar MICS, procedimientos y prácticas de las operaciones de juego, incluyendo, pero no limitado al establecimiento de las reglas para el juego, suspender eventos, procesar varias transacciones de apuestas y financieras, crear mercados, pagar apuestas, cerrar mercados, cancelar eventos, anular o cancelar apuestas, gestión de la cuenta del jugador, métodos fundamentales pertinentes para la limitación de riesgos, y cualquier otro objetivo establecido por la entidad regulatoria.
b) Anexo B: Auditoría operacional de controles técnicos de seguridad. Esto incluye, pero no está limitado a una evaluación del sistema de seguridad de información (ISS), revisión de procesos operacionales que son críticos para el cumplimiento, pruebas de penetración enfocadas en la infraestructura externa e interna, además de las aplicaciones que transfieren, almacenan y/o procesan los datos del jugador y/o información confidencial, y cualquier otro objetivo establecido por la entidad regulatoria.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Capítulo 2: Requisitos del Sistema

2.1 Introducción

2.1.1 Declaración general

Si el Sistema de Apuestas de Eventos consiste de múltiples sistemas de computadoras en varios locales, el sistema completo y toda la comunicación entre sus componentes deben conformar con los requisitos técnicos aplicables en este documento.

2.2 Requisitos del reloj del sistema

2.2.1 Reloj del sistema

El Sistema de Apuestas de Eventos debe mantener un reloj interno que refleja la fecha y hora actual, el cual será utilizado para proveer lo siguiente:

a) Sellado de tiempo para todas las transacciones y eventos;
b) Sellado de tiempo para los eventos significativos; y
c) Reloj de referencia para los reportes.

2.2.2 Sincronización de tiempo

El Sistema de Apuestas de Eventos debe estar equipado con un mecanismo para asegurar que la fecha y hora están sincronizadas entre todos los componentes del sistema.

2.3 Requisitos del programa de control

2.3.1 Declaración general

En adición a los requisitos contenidos en esta sección, los procedimientos de auditoría indicados en la sección “Procedimientos de Verificación” de este documento también deben ser cumplidos.

2.3.2 Verificación automática del programa de control

El Sistema de Apuestas de Eventos debe tener la capacidad para verificar después de la instalación que todos los componentes del programa de control crítico contenidos en el sistema son copias auténticas de los componentes aprobados del sistema, al menos una vez cada 24 horas, y por solicitud usando un método aprobado por la entidad regulatoria. El mecanismo de autenticación del programa de control crítico deberá:

a) Emplear un algoritmo de hash que produzca un resumen de mensaje de 128 bits, como mínimo;
b) Incluir todos los componentes del programa de control crítico que puedan afectar las operaciones de juego, incluyendo, pero no limitado a: ejecutables, librerías, configuración del sistema o

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

apuestas, archivos del sistema operativo, componentes que controlan los reportes requeridos del sistema, y los elementos de la base de datos que afectan las operaciones del sistema; y
c) Prover una indicación del fallo de autenticación cuando se determina que cualquier componente del programa de control crítico es inválido.

2.3.3 Verificación independiente del programa de control

Se debe establecer un método para que cada componente del programa de control crítico del Sistema de Apuestas de Eventos pueda ser verificado a través de un procedimiento de verificación independiente de terceros. El proceso de verificación de terceros debe operar independientemente de cualquier proceso o software de seguridad del sistema. El laboratorio de pruebas independiente debe aprobar el método de verificación de integridad antes de la aprobación del sistema.

2.3.4 Apagado y recuperación

El Sistema de Apuestas de Eventos debe tener una función de apagado precisa, y solo permitir un reinicio automático después de realizar los siguientes procedimientos durante el encendido, como mínimo:

a) Rutina(s) de reanudación del programa, incluyendo autocomprobación, han completado con éxito;
b) Todos los componentes del programa de control crítico del sistema han sido autenticados utilizando un método aprobado por la entidad regulatoria; y
c) La comunicación con todos los componentes necesarios para la operación del sistema ha sido establecida y del mismo modo autenticada.

2.4 Gestión de Juego

2.4.1 Gestión de juego

El Sistema de Apuestas de Eventos debe tener la capacidad para suspender lo siguiente por solicitud:

a) Toda actividad de juego;
b) Evento individual;
c) Mercado individual;
d) Dispositivo de juego individual (si es aplicable); y
e) Acceso de jugador individual (si es aplicable).

2.5 Gestión de la cuenta del jugador

2.5.1 Declaración general

Los requisitos de esta sección aplican a la cuenta del jugador si está soportado por el Sistema de Apuestas de Eventos. En adición a los requisitos contenidos en esta sección, también debe conformar con la sección “Controles de la Cuenta del Jugador”.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

NOTA: El registro y verificación de la cuenta del jugador son requeridos por el Sistema de Apuestas de Eventos para que el jugador participe en apuestas remotas.

2.5.2 Registro y verificación

Debe existir un método para recolectar la información del jugador antes del registro de una cuenta de juego. Si el registro y verificación de la cuenta de juego son soportados por el Sistema de Apuestas de Eventos directamente por el sistema o junto con el software del proveedor de servicio de terceros, deben conformar con los siguientes requisitos:

a) Solamente jugadores de edad legal para participación en el juego en la jurisdicción pueden registrarse para una cuenta del jugador. Cualquier persona que presenta una fecha de nacimiento que indica que es menor de edad será rechazada para el registro de una cuenta del jugador.
b) La verificación de identidad debe ser realizada antes de que un jugador es permitido colocar una apuesta. Proveedores de servicio de terceros pueden ser utilizados para la verificación de identidad, según sea permitido por la entidad regulatoria.
    i. La verificación de identidad debe autenticar el nombre legal, dirección física, y edad del individuo como mínimo, según es requerido por la entidad regulatoria.
    ii. La verificación de identificación también debe confirmar que el jugador no está en ninguna lista de exclusión retenida por el operador o la entidad regulatoria, o prohibido establecer o mantener una cuenta por cualquier otro motivo.
    iii. Los detalles de la verificación de identidad deben ser mantenidos de manera segura.
c) La cuenta del jugador solo puede ser activada una vez que la verificación de edad e identidad es completada con éxito, y se determina que el jugador no está en ninguna lista de exclusión, y el jugador ha reconocido todas las políticas de privacidad necesarias y términos y condiciones, y el registro de la cuenta del jugador está completo.
d) Un jugador solo debe ser permitido tener una cuenta de juego activa en todo momento, a menos que sea autorizado específicamente por la entidad regulatoria.
e) El sistema debe tener la capacidad para actualizar la contraseña, la información del registro y la cuenta utilizada para transacciones financieras para cada jugador. Un proceso de autenticación de múltiples factores será utilizado para este propósito.

2.5.3 Accesso del jugador

Un jugador accede su cuenta de juego a través del uso de un nombre de usuario (o similar) y una contraseña o una forma alternativa segura para que el jugador realice la autenticación para acceder al Sistema de Apuestas de Eventos. Los métodos de autenticación están sujetos a la discreción de la entidad regulatoria según sea necesario. El requisito no prohibe la opción para más de un método de autenticación disponible para que un jugador acceda su cuenta.

a) Si el sistema no reconoce el nombre del usuario y/o contraseña cuando es ingresado, un mensaje explicativo debe ser mostrado al jugador indicando que ingrese la información de nuevo.
b) Cuando un jugador ha perdido su nombre de usuario y/o contraseña, un proceso de autenticación de múltiples factores será utilizado para la recuperación del nombre de usuario/ restablecimiento de la contraseña.
c) La información del saldo actual de la cuenta y las opciones de transacciones deben estar

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

disponibles al jugador una vez autenticado.

d) El Sistema de Apuestas de Eventos debe soportar un mecanismo que permita que una cuenta sea bloqueada en caso de que actividad sospechosa es detectada (ej., demasiados intentos fallidos para el acceso). Un proceso de autenticación de múltiples factores debe ser utilizado para desbloquear la cuenta.

2.5.4 Inactividad del jugador

Para cuentas de juego con acceso remoto para apuestas o gestión de la cuenta, después de 30 minutos de inactividad en ese dispositivo, o un período de tiempo determinado por la entidad regulatoria, el jugador debe ser requerido a autenticarse de nuevo para acceder su cuenta de juego.

a) Ninguna transacción de juego o financiera es permitida en el dispositivo hasta que el jugador ha sido autenticado de nuevo.
b) El jugador podría ser ofrecido una manera más simple para autenticarse de nuevo en ese dispositivo, así como la autenticación a nivel del sistema operativo (ej., biometría) o un Número de Identificación Personal (PIN). Cada forma de reautenticación será evaluada caso por caso por el laboratorio independiente de pruebas.
    i. Esta funcionalidad puede ser desactivada basado en la preferencia del jugador y/o entidad regulatoria.
    ii. Una vez cada 30 días, o un período especificado por la entidad regulatoria, el jugador será requerido a proveer autenticación completa en el dispositivo.

2.5.5 Limitaciones y exclusiones

El Sistema de Apuestas de Eventos debe tener la capacidad para implementar correctamente cualquier limitación y/o exclusión establecida por el jugador y/u operador, según es requerido por la entidad regulatoria:

a) Si el sistema tiene la capacidad para gestionar las limitaciones y/o exclusiones directamente, los requisitos aplicables en las secciones de “Limitaciones” y “Exclusiones” de este documento deberán ser evaluados;
b) Las limitaciones autoimpuestas establecidas por el jugador no invalidarán las limitaciones más restrictivas impuestas por el operador. Las limitaciones más restrictivas deberán tener prioridad; y
c) Las limitaciones no deberán ser comprometidas por el estado de eventos internos, así como órdenes de exclusión autoimpuesta y revocaciones.

2.5.6 Mantenimiento de fondos del jugador

Cuando las transacciones financieras pueden ser realizadas automáticamente por el Sistema de Apuestas de Eventos, los siguientes requisitos serán aplicables:

a) El sistema debe proveer la confirmación/ rechazo de cada transacción financiera iniciada.
b) El depósito en una cuenta de juego debe ser realizado por medio de una transacción de tarjeta de crédito u otros métodos que produzcan un registro de auditoría adecuado.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

c) Los fondos no deben estar disponibles para el juego hasta que estos han sido recibidos del usuario o el usuario provee un número de autorización indicando que los fondos han sido autorizados. El número de autorización debe ser mantenido en un registro de auditoría.
d) Los pagos desde una cuenta deben ser enviados (incluyendo una transferencia de fondos) directamente a una cuenta en una institución financiera en el nombre del jugador o deben ser procesados en nombre del jugador y enviados a la dirección del jugador utilizando un servicio de distribución seguro o por otro método que no esté prohibido por la entidad regulatoria. El nombre y la dirección deben ser los mismos detallados en el registro del jugador.
e) Si un jugador inicia una transacción en la cuenta de juego la cual excedería los límites establecidos por el operador y/o entidad regulatoria, esta transacción solo puede ser procesada provisto que el jugador es notificado claramente de que ha retirado o depositado menos de lo requerido.
f) No debe ser posible transferir fondos entre dos cuentas de juego.

2.5.7 Registro de transacción o resumen de cuenta

El Sistema de Apuestas de Eventos debe tener la capacidad para proveer al jugador un registro de transacciones o historial del resumen de cuenta por solicitud. La información provista debe incluir suficientes datos para permitir la reconciliación del registro o resumen por el jugador contra sus propios registros financieros. Esta información debe incluir como mínimo un detalle de los siguientes tipos de transacciones:

a) Transacciones financieras (con sellado de tiempo y código de identificación de la transacción único):
   i. Depósitos en la cuenta de juego;
   ii. Retiros de la cuenta de juego;
   iii. Créditos promocionales o de bonificación agregados a/retirados de la cuenta de juego (aparte de créditos ganados en el juego);
   iv. Ajustes manuales o modificaciones en la cuenta de juego (ej. para un reembolso);
b) Transacciones de apuestas:
   i. Número de identificación único de la apuesta;
   ii. La fecha y hora en que la apuesta fue colocada;
   iii. La fecha y hora en que cada evento comenzó y finalizó o cuando ocurrirá en caso de eventos en el futuro (si es conocido);
   iv. La fecha y hora en que los resultados fueron confirmados (en blanco hasta que sean confirmados);
   v. Todas las opciones del jugador incluidas en la apuesta, incluyendo la línea del mercado y cuota, selección de apuesta, y cualquier condición(es) especial aplicable a la apuesta;
   vi. Los resultados de la apuesta (en blanco hasta que sean confirmados);
   vii. Cantidad total apostada, incluyendo créditos promocionales/de bonificación (si es aplicable);
   viii. Cantidad total ganada, incluyendo créditos promocionales/ de bonificación (si es aplicable);
   ix. Comisión o tasas recaudadas (si es aplicable); y
   x. La fecha y hora en que la apuesta ganadora fue pagada al jugador;

2.5.8 Programas de fidelidad del jugador

Programas de fidelidad del jugador son todos los programas que ofrecen incentivos para los

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

jugadores basado en el volumen de juego o ingresos recibidos de un jugador. Si los programas de fidelidad del jugador son soportados por el sistema de apuestas de eventos, las siguientes normas deben aplicar:

a) Todos los premios deben estar disponibles por igual para todos los jugadores que alcanzan el nivel de calificación definido para puntos de fidelidad del jugador;
b) La redención de puntos de fidelidad del jugador obtenidos debe ser una transacción segura que automáticamente agrega el valor del premio redimido al balance de puntos; y
c) Todas las transacciones de puntos de fidelidad del jugador deben ser registradas por el sistema.

2.6 Funcionalidad de instrumentos financieros para el juego

2.6.1 Declaración general

Los sistemas de apuestas de eventos que soportan la emisión y/o redención de instrumentos financieros de juego (boletos y cupones) deben cumplir con los requisitos aplicables establecidos en la sección "Boletos/Vales de la Máquina" de *GLI-11 Estándares para Dispositivos de Juego* y los "Requisitos del Sistema de Validación" de *GLI-13 Estándares para Sistemas de Monitoreo y Control En Línea (MCS) y Sistemas de Validación* y otros requisitos jurisdiccionales aplicables observados por la entidad regulatoria.

2.7 Requisitos de localización para apuestas remotas

2.7.1 Declaración general

Donde sea requerido por la entidad regulatoria, los requisitos en esta sección aplicarán cuando el sistema de apuestas de eventos soporta apuestas remotas.

NOTA: El operador o proveedor de servicio de terceros manteniendo estos componentes, servicios y/o aplicaciones deberá cumplir con los procedimientos de auditoría indicados en la sección "Proveedor de Servicio de Localización" de este documento.

2.7.2 Prevención de fraude de localización

El sistema de apuestas de eventos debe incorporar un mecanismo para detectar el uso de software de PC remoto, rootkits, virtualización, y/o cualquier otro programa identificado con capacidad para evadir detección de la localización. Este debe observar las mejores prácticas en medidas de seguridad para:

a) Detectar y bloquear el fraude de los datos de localización (ej. aplicaciones de localización falsa, máquinas virtuales, programas de PC remotos, etc.) antes de completar cada apuesta;
b) Examinar la dirección IP de cada conexión de dispositivos de apuestas remotas en la red para asegurar que no está siendo usada una red virtual privada (VPN) o servicio de proxy;
c) Detectar y bloquear dispositivos que indican manipulación a nivel del sistema (ej. rooting (conversión), jailbreaking (liberación), etc.);

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

d) Defender contra ataques de "intermediarios" o técnicas de hacking o piratería informática similares y prevenir la manipulación del código;
e) Utilizar mecanismos de detección y bloqueo verificables a un nivel de aplicación; y
f) Monitorear y evitar las apuestas colocadas por una sola cuenta de juego desde localizaciones geográficas inconsistentes (ej. identificación de localizaciones desde que se colocaron apuestas pero a las que sería imposible viajar en el tiempo informado).

2.7.3 Detección de localización para apuestas remotas en una WLAN

Cuando las apuestas remotas se producen a través de una red inalámbrica de area local (WLAN), el sistema de apuestas de eventos debe implementar uno de los siguientes métodos para rastrear la localización de todos los jugadores conectados en la WLAN:

a) Un servicio o aplicación de detección de localización por el que se debe verificar la ubicación de todos los jugadores antes de completar las apuestas. Este servicio o aplicación debe cumplir con los requisitos especificados en la siguiente sección para “Detección de localización para apuestas remotas sobre la Internet”; o
b) Un componente de detección de localización que detecta en tiempo real cuando los jugadores están fuera del area permitida y no permite colocar más apuestas. Esto se puede realizar utilizando hardware específico de informática, así como antenas direccionales, sensores de Bluetooth u otros métodos que deben ser evaluados caso por caso por el laboratorio independiente de pruebas.

2.7.4 Detección de localización para apuestas remotas sobre la Internet

Cuando las apuestas remotas se producen a través de la Internet, el sistema de apuestas de eventos debe implementar un servicio o aplicación de detección de localización para detectar correctamente y monitorear la ubicación de un jugador tratando de colocar una apuesta; y para monitorear y bloquear todos los intentos de colocar una apuesta sin autorización.

a) La ubicación de cada jugador debe ser verificada adecuadamente antes de completar la primera apuesta, después de conectar con un dispositivo de juego remoto. Cuando transcurre un período de 30 minutos desde la última verificación de localización, o según lo especificado por la entidad regulatoria, se debe realizar una subsiguiente verificación de localización antes de completar las apuestas:
    i. Si la verificación de localización indica que el jugador está fuera del perímetro autorizado o no se puede localizar el jugador, la apuesta debe ser rechazada y el jugador notificado en este caso.
    ii. Cada vez que se detecte una localización errónea, esta debe ser registrada en un registro con sello de tiempo, incluyendo la identificación del jugador y la localización detectada.
b) Un método de geolocalización debe ser utilizado para proveer la ubicación física del jugador y un radio de confianza asociado. El radio de confianza debe estar localizado por completo en el perímetro autorizado.
c) El método de geolocalización debe utilizar fuentes de datos de localización precisos (Wi-Fi, GSM, GPS, etc.) para confirmar la ubicación del jugador. Cuando la única fuente de datos de localización disponible para un dispositivo de apuestas remotas es una dirección IP, los datos de localización

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

de un dispositivo móvil registrado a la cuenta de juego pueden ser usados como una fuente de datos de localización secundaria con las siguientes condiciones:
   i. Se debe comprobar que el dispositivo de juego remoto (donde la apuesta se coloca) y el dispositivo móvil están cerca el uno del otro.
   ii. Si es permitido por la entidad regulatoria, los datos de localización del portador de datos de un dispositivo móvil pueden ser utilizados si ninguna otra fuente de datos de localización está disponible aparte de la dirección IP.

d) El método de geolocalización debe tener la capacidad para controlar si el radio de precisión de la fuente de datos de localización puede coincidir con o exceder la zona de separación o el perímetro autorizado; y
e) Para tener en cuenta y mitigar las discrepancias entre los recursos del mapa y variaciones en los datos geoespaciales, se deben utilizar polígonos de convergencia basados en mapas auditados aprobados por la entidad regulatoria, además de superponer los datos de localización en estos polígonos de convergencia.

2.8 Información que debe ser mantenida

2.8.1 Retención de datos y sellado de tiempo

El sistema de apuestas de eventos debe tener la capacidad para mantener y respaldar toda la información registrada como es indicado en esta sección:

a) El reloj del sistema debe ser utilizado para todo el sellado de tiempo.
b) El sistema debe proveer un mecanismo para exportar los datos para el propósito de análisis de datos y auditoría/verificación (ej., CSV, XLS).

2.8.2 Información del registro de apuesta

Para cada apuesta individual colocada por el jugador, la información que debe ser mantenida y respaldada por el sistema de apuestas de eventos incluirá:

a) La fecha y hora en que la apuesta fue colocada;
b) Cualquier opción del jugador incluida en la apuesta:
   i. Línea de mercado y cuota (ej. apuesta simple, apuestas de margen, apuestas de más/menos, ganador/colocado/show);
   ii. Selección de la apuesta (ej. nombre del atleta o del equipo y número);
   iii. Cualquier condición(es) especial que aplica a la apuesta;
c) Los resultados de la apuesta (en blanco hasta confirmados);
d) Cantidad total apostada, incluyendo créditos de bonificación/promocionales (si es aplicable);
e) Cantidad total ganada, incluyendo créditos de bonificación/promocionales (si es aplicable);
f) Comisión o tasas recaudadas (si es aplicable);
g) La fecha y hora en que la apuesta ganadora fue pagada al jugador;
h) Número de identificación único de la apuesta;
i) Identificación del usuario o identificación única del dispositivo de juego que emitió el cupón de apuesta (si es aplicable);
j) Información pertinente de la localización (si es aplicable);

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

k) Identificadores de evento y mercado;
l) Estado de la apuesta actual (activa, cancelada, no redimida, pendiente, anulada, inválida, redención en progreso, redimida, etc.);
m) Identificación única del jugador, para apuestas realizadas usando una cuenta de juego;
n) Período de redención (si es aplicable); y
o) Campo de texto abierto para que el asistente ingrese la descripción del jugador o archivo de imagen (si es aplicable).

2.8.3 Información del mercado

Para cada mercado individual disponible para las apuestas, la información que debe ser mantenida y respaldada por el sistema de apuestas de eventos incluye:

a) La fecha y hora en que el período de apuestas comenzó y finalizó;
b) La fecha y hora en que el evento inició y finalizó o es previsto que esto ocurra para eventos en el futuro (si se conoce);
c) La fecha y hora en que los resultados fueron confirmados (en blanco hasta confirmados);
d) Cantidad total de apuestas recolectadas, incluyendo todos los créditos de bonificación/ promocionales (si es aplicable);
e) Las líneas de cuotas que estaban disponibles a lo largo de la duración de un mercado (con sello de tiempo) y el resultado confirmado (ganancia/pérdida/empate);
f) Cantidad total de ganancias pagadas a los jugadores, incluyendo todos los créditos de bonificación/ promocionales (si es aplicable);
g) Cantidad total de apuestas anuladas o canceladas, incluyendo todos los créditos de bonificación/ promocionales (si es aplicable);
h) Comisión o tasas recaudadas (si es aplicable);
i) Estado del evento (en progreso, completado, confirmado, etc.); y
j) Identificadores de evento y mercado.

2.8.4 Información del torneo/evento

Para sistemas de apuestas de eventos que soportan torneos/eventos, la información que debe ser mantenida y respaldada por el sistema de apuestas de eventos incluirá para cada torneo/ evento:

a) Nombre del evento/ torneo;
b) La fecha y hora en que el evento/ torneo occurrió o tendrá lugar (si se conoce);
c) Identificación única del jugador y nombre de cada jugador registrado, precio de entrada pagado, y la fecha de pago;
d) Identificación única del jugador y nombre de cada jugador que ha ganado, cantidad pagada, y la fecha de pago;
e) Cantidad total de tarifas de entrada recaudada, incluyendo todos los créditos de bonificación/ promocionales (si es aplicable);
f) Cantidad total de ganancias pagadas a los jugadores, incluyendo todos los créditos de bonificación/ promocionales (si es aplicable);
g) Comisión o tasas recaudadas (si es aplicable);
h) Estado del evento/ torneo (en progreso, completado, etc.).

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

2.8.5 Información de la cuenta de juego

Para sistemas de apuestas de eventos que soportan la gestión de la cuenta de juego, la información para ser mantenida y respaldada por el sistema de apuestas de eventos debe incluir lo siguiente para cada cuenta de juego:

a) Identificación única del jugador y nombre del jugador;
b) Información del jugador (incluyendo el método de verificación);
c) La fecha de acuerdo del jugador con los términos y condiciones y política de privacidad del operador;
d) Detalles de la cuenta y saldo actual;
e) Campo de texto abierto para que el asistente ingrese la descripción del jugador o archivo de imagen (si es aplicable);
f) Cuentas previas, si es applicable, y el motivo para la desactivación;
g) La fecha y método por el cual la cuenta fue registrada (ej. remoto o local);
h) La fecha y hora de la última sesión;
i) Información de exclusiones/limitaciones según es requerido por la entidad regulatoria:
    i. La fecha y hora de la solicitud (si es aplicable);
    ii. Descripción y motivo de la exclusión/limitación;
    iii. Tipo de exclusión/restricción (ej. exclusión impuesta por el operador, limitación autoimpuesta);
    iv. La fecha de inicio de la exclusión/limitación;
    v. La fecha de finalización de la exclusión/limitación (si es aplicable);
j) Información de la transacción financiera:
    i. Tipo de transacción (ej. depósito, retiro, ajuste);
    ii. La fecha y hora de la transacción;
    iii. Identificación única de la transacción;
    iv. Cantidad de la transacción;
    v. Saldo total de la cuenta antes/ después de la transacción;
    vi. Cantidad total de tarifas pagadas por la transacción (si es aplicable);
    vii. Identificación del usuario o identificación única del dispositivo de juego que procesó la transacción (si es aplicable);
    viii. Estado de la transacción (pendiente, completa, etc.);
    ix. Método de depósito/ retiro (ej. Dinero en efectivo, tarjeta de débito o crédito, cheque personal, cheque de caja, transferencia bancaria, giro postal);
    x. Número de autorización del depósito; y
    xi. Información pertinente de la localización.

2.8.6 Información de bonificación/ promoción

Para sistemas de apuestas de eventos que soportan promociones y/ o bonificaciones que son redimibles en efectivo, créditos para apostar, o mercancía, la información que debe ser mantenida y respaldada por el sistema de apuestas de eventos debe incluir para cada promoción/bonificación:

a) La fecha y hora de inicio y finalización del período de promoción/bonificación o cuando finalizará

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

(si se conoce);
b) Balance actual de promoción/ bonificación;
c) Cantidad total de promociones/ bonificaciones otorgadas;
d) Cantidad total de promociones/ bonificaciones redimidas
e) Cantidad total de promociones/ bonificaciones expiradas;
f) Cantidad total de ajustes de promociones/ bonificaciones; y
g) Identificación única de la promoción/ bonificación.

2.8.7 Información del dispositivo de juego

Para cada dispositivo de juego de autoservicio o dispositivo terminal de eventas (POS), la información para ser mantenida y respaldada por el sistema de apuestas de eventos debe incluir, si es aplicable:

a) Identificación única del dispositivo de juego;
b) Registro de compras de apuestas;
c) Registro de redención de apuestas ganadoras, si es soportado;
d) Registro de anulación y cancelación de apuestas; y
e) Identificación del usuario e información de la sesión, para dispositivos de juego POS;

2.8.8 Información de evento significativo

La información de eventos significativos que debe ser mantenida y respaldada por el sistema de apuestas de eventos incluirá:

a) Intentos de registro fallidos;
b) Error del programa o discrepancia en la autenticación;
c) Períodos significativos de indisponibilidad de cualquier componente crítico del sistema;
d) Ganancias mayores (únicas y agregadas en un período de tiempo definido) en exceso de un valor especificado por la entidad regulatoria, incluyendo la información del registro de la apuesta;
e) Apuestas mayores (únicas y agregadas en un período de tiempo definido) en exceso de un valor especificado por la entidad regulatoria, incluyendo la información del registro de la apuesta;
f) Anulaciones, invalidaciones, y correcciones del sistema;
g) Cambios en los archivos de datos en vivo ocurriendo fuera de la ejecución normal del programa y sistema operativo;
h) Cambios que son hechos en la librería de descarga de datos, incluyendo la adición, cambio o eliminación de software, cuando es soportado;
i) Cambios en el sistema operativo, base de datos, la red, y políticas de la aplicación y parámetros;
j) Cambios en la fecha/hora del servidor maestro del tiempo;
k) Cambios en el criterio establecido previamente para un evento o mercado (no incluye cambios en la línea de cuotas para mercados activos);
l) Cambios de los resultados de un evento o mercado;
m) Cambios de los parámetros de promoción y/o bonificación;
n) Gestión de la cuenta de juego:
    i. Ajustes del saldo de la cuenta de juego;
    ii. Cambios hechos en la información del jugador e información confidencial registrada de una

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

cuenta de juego;
iii. Desactivación de una cuenta de juego;
iv. Transacciones financieras mayores (únicas y agregadas en un período de tiempo definido) en exceso de un valor especificado por la entidad regulatoria, incluyendo la información de la transacción;

o) Pérdida sin recuperación de información confidencial;
p) Cualquier otra actividad que requiera la intervención del usuario y que ocurra fuera del alcance normal de la operación del sistema; y
q) Otros eventos significativos o inusuales según es considerado aplicable por la entidad regulatoria.

2.8.9 Información de acceso del usuario

Para cada cuenta de usuario, la información para ser mantenida y respaldada por el Sistema de Apuestas de Eventos incluirá:

a) Nombre del empleado y título o posición;
b) Identificación del usuario;
c) Lista completa y descripción de las funciones que cada cuenta de usuario o grupo puede ejecutar;
d) La fecha y hora en que la cuenta fue abierta;
e) La fecha y hora del último registro;
f) La fecha y hora del último cambio de contraseña;
g) La fecha y hora en que la cuenta fue activada/ desactivada; y
h) Miembros del grupo o cuenta de usuario (si es aplicable).

2.9 Requisitos para los reportes

2.9.1 Requisitos para reportes en general

El sistema de apuestas de eventos debe tener la capacidad para generar la información requerida para compilar los reportes, según es requerido por la entidad regulatoria. En adición al cumplimiento con los requisitos en la sección anterior para "Retención de datos y sellado de tiempo", los siguientes requisitos deben aplicar para los reportes requeridos:

a) El sistema debe tener la capacidad para proveer la información de los reportes a petición y para los intervalos requeridos por la entidad regulatoria incluyendo, pero no limitado a, diario, mes hasta la fecha (MTD), año hasta la fecha (YTD), y hasta la fecha (LTD).
b) Cada reporte requerido debe contener:
   i. El operador, el período seleccionado y la fecha/hora en que el reporte fue generado; y
   ii. Una indicación de "No hay actividad" o un mensaje similar si no aparecen datos para el período especificado.

NOTA: En adición a los reportes descritos en esta sección, la entidad regulatoria también puede requerir otros reportes utilizando la información almacenada bajo la sección "Información para ser mantenida" de este documento.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

2.9.2 Reporte de ingresos del operador

El sistema de apuestas de eventos debe tener la capacidad para proveer la siguiente información requerida para compilar uno o más reportes de los ingresos del operador para cada evento por completo y para cada mercado individual en este evento, los cuales pueden ser usados para la información de impuestos del operador:

a) La fecha y hora en que cada evento comenzó y finalizó;
b) Cantidad total de apuestas recaudada;
c) Cantidad total de las ganancias pagadas a los jugadores;
d) Cantidad total de las apuestas anuladas o canceladas;
e) Comisión y tasas recaudadas; (si es aplicable);
f) Identificadores del evento y mercado; y
g) Estado del evento (en progreso, completo, confirmado, etc.).

2.9.3 Reporte de responsabilidad del operador

El sistema de apuestas de eventos debe tener la capacidad para proveer la siguiente información requerida para compilar uno o más reportes de responsabilidad del operador:

a) Cantidad total retenida por el operador para las cuentas de juego (si es aplicable);
b) Cantidad total de apuestas colocadas sobre eventos en el futuro; y
c) Cantidad total de ganancias acumuladas de apuestas ganadoras, pero no pagadas por el operador.

2.9.4 Reporte de eventos futuros

El sistema de apuestas de eventos debe tener la capacidad para proveer la siguiente información requerida para compilar uno o más reportes de eventos en el futuro del día de juego:

a) Apuestas colocadas antes del día de juego para eventos en el futuro (total y por apuesta);
b) Apuestas colocadas en el día de juego para eventos en el futuro (total y por apuesta);
c) Apuestas colocadas antes del día de juego para eventos ocurriendo en ese mismo día (total y por apuesta);
d) Apuestas colocadas en el día de juego para eventos ocurriendo en ese mismo día (total y por apuesta);
e) Apuestas anuladas o canceladas en el día de juego (total y por apuesta); y
f) Identificadores del evento y mercado.

2.9.5 Reporte de eventos significativos y alteraciones

El sistema de apuestas de eventos debe tener la capacidad para proveer la siguiente información requerida para compilar uno o más reportes de cada evento significativo o alteración, según sea aplicable:

a) La fecha y hora de cada evento significativo o alteración;
b) Identificación del evento/componente (si es aplicable);

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

c) Identificación del usuario(s) que realizó y/o autorizó el evento significativo o alteración;
d) Motivo/descripción del evento significativo o alteración, incluyendo los datos o parámetro alterado;
e) Valor de los datos o parámetro antes de la alteración; y
f) Valor de los datos o parámetro después de la alteración.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Capítulo 3: Requisitos de Dispositivos de Juego

3.1 Introducción

3.1.1 Declaración general

Una apuesta puede ser colocada usando uno de los siguientes tipos de dispositivos de juego según es permitido por la entidad regulatoria. Cualquier otro tipo de dispositivo de juego será revisado caso por caso, según es permitido por la entidad regulatoria.

a) Dispositivo de Juego - Terminal de venta (POS): Un terminal del asistente que como mínimo será usado por un asistente para la ejecución o formalización de apuestas colocadas en nombre del jugador.
b) Dispositivo de juego de autoservicio: Un kiosco que como mínimo será usado para la ejecución o formalización de apuestas colocadas directamente por el jugador y, si es soportado, puede ser usado para la redención de registros de apuestas ganadoras.
c) Dispositivo de juego remoto: Un dispositivo del jugador operado en una red inalámbrica en el local o sobre la internet que como mínimo será usado para la ejecución o formalización de apuestas colocadas directamente por el jugador. Tipos de dispositivo de juego remoto incluyen una computadora (PC), teléfono móvil, tableta, etc.

3.2 Software de juego

3.2.1 Declaración general

El software de juego es usado para participar en las transacciones de juego y financieras en el sistema de apuestas de eventos, el cual basado en su diseño, es descargado o instalado en el dispositivo de juego, ejecutado desde el sistema de apuestas de eventos que es accedido por el dispositivo de juego, o una combinación de ambos.

3.2.2 Identificación del software

El software de juego debe contener suficiente información para identificar el software y su versión.

3.2.3 Validación del software

Para software de juego instalado localmente en el dispositivo de juego, debe ser posible autenticar que todos los componentes críticos contenidos en el software son válidos cada vez que el software es cargado para el uso, y si es soportado por el sistema, por solicitud según es requerido por la entidad regulatoria. Los componentes críticos pueden incluir, pero no están limitados a, las reglas de juego, elementos que controlan la comunicación entre el dispositivo de juego y el sistema de apuestas de eventos, u otros componentes que son requeridos para asegurar la operación correcta del software. En caso de autenticación fallida (ej. incompatibilidad del programa o fallo de autenticación), el software debe prevenir las operaciones de juego y mostrar un mensaje de error adecuado.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

NOTA: Los mecanismos de verificación del programa serán evaluados caso por caso y aprobados por la entidad regulatoria y el laboratorio independiente de pruebas basado en las prácticas de seguridad estándares de la industria.

3.2.4 Requisitos del interfaz del usuario

El interfaz del usuario es definido como una aplicación de interfaz o programa a través del cual el usuario puede ver y/o interactuar con el software de juego. El interfaz del usuario debe cumplir con los requisitos siguientes:

a) Las funciones de todos los botones, puntos de clic o táctiles deben ser indicados claramente en el area del botón, o punto para hacer clic/táctil o en el menú de ayuda. La funcionalidad a través de cualquier botón o punto para hacer clic/táctil en el interfaz del usuario no debe estar disponible si está indocumentada.
b) Todo cambio de tamaño o superposición del interfaz del usuario debe ser mapeado con precisión para reflejar los cambios del despliegue visual y puntos de hacer clic/táctiles.
c) Las instrucciones del interfaz del usuario, además de la información sobre las funciones y servicios provistos por el software, deben ser comunicadas claramente al usuario y no deben ser engañosas o incorrectas.
d) El despliegue visual de las instrucciones e información debe ser adaptado al interfaz del usuario. Por ejemplo, cuando un dispositivo de juego implementa la tecnología con una pantalla más pequeña, está permitido presentar una versión abreviada de las reglas de juego accesible directamente desde la pantalla de juego y hacer disponible la versión completa de las reglas de juego a través de otro método, así como una pantalla secundaria, menú de ayuda, u otro interfaz que es identificado fácilmente en la pantalla de juego.

3.2.5 Entradas simultáneas

El software de juego no debe ser afectado de manera adversa por la activación simultánea o secuencial de varias entradas y resultados que podrían, intencionalmente o no, causar el mal funcionamiento o resultados inválidos.

3.2.6 Impresoras del cupón de apuesta

Si el dispositivo de juego utiliza una impresora para emitir un cupón de apuesta impreso para el jugador, el cupón de apuesta impreso debe incluir la información indicada en la sección “Registro de la apuesta” de este documento. Puede ser admisible que parte de esta información esté incluida en el cupón mismo.

3.2.7 Comunicaciones

El software de juego debe ser diseñado o programado de forma que solo pueda comunicarse de manera segura con componentes autorizados. Si se pierde la comunicación entre el Sistema de Apuestas de Eventos y el dispositivo de juego, el software debe impedir operaciones de juego

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

adicionales y mostrar un mensaje de error apropiado. Es admisible que el software detecte este error cuando el dispositivo intente comunicarse con el sistema.

3.3 Dispositivos de juego de autoservicio

3.3.1 Declaración general

El jugador coloca una apuesta en un dispositivo de juego de autoservicio usando los fondos de su cuenta de juego o utilizando dispositivos periféricos según es autorizado por la entidad regulatoria. En adición a los requisitos para "Software de juego", los requisitos aplicables establecidos en *GLI-20 Estándares para Kioskos* y otros requisitos jurisdiccionales aplicables observados por la entidad regulatoria deben conformar para todos los componentes propietarios del dispositivo de juego de autoservicio.

3.4 Dispositivos de juego – Terminal de venta (POS)

3.4.1 Declaración general

El jugador coloca una apuesta en un dispositivo de juego – terminal de venta (POS) usando los fondos de su cuenta de juego o haciendo el pago para la apuesta(s) directamente al asistente. En adición a los requisitos para "Software de juego", los requisitos establecidos en esta sección deben conformar para los dispositivos de juego (POS).

3.4.2 Pantallas táctiles

Las pantallas táctiles, si son usadas por el software de juego, deben ser precisas y según lo requerido por el diseño, deberán soportar un método de calibración para mantener la precisión; alternativamente, el hardware del despliegue visual podría soportar la calibración automática.

3.4.3 Cupón de apuesta impreso

Si el dispositivo de juego (POS) conecta a una impresora para producir un cupón de apuesta impreso y/o instrumentos de juego (boletos y cupones), la impresora y/o software de juego debe tener la capacidad para detectar e indicar las siguientes condiciones de error, si es aplicable. Es admisible que la condición de error sea detectada cuando se intenta imprimir:

a) Batería baja (cuando el suministro de energía es externo al dispositivo de juego (POS));
b) Quedó sin papel/papel bajo; e
c) Impresora desconectada.

3.4.4 Dispositivos de juego – Terminal de venta (POS) inalámbrico

Para dispositivos de juego (POS) inalámbricos, los requisitos aplicables para la "Interacción del cliente-servidor" de la siguiente sección también deben conformar. Adicionalmente, la comunicación

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

solo puede ser establecida entre los dispositivos de juego (POS) inalámbricos y el sistema de apuestas de eventos a través de puntos de acceso autorizados en el local.

3.5 Dispositivos de juego remoto

3.5.1 Declaración general

El jugador solo puede colocar una apuesta en un dispositivo de juego remoto usando los fondos de su cuenta de juego (ej. están prohibidas las transacciones de apuestas anónimas). Dependiendo en la implementación(es) autorizada por la entidad regulatoria, los dispositivos de juego remoto pueden ser utilizados en una red de area local inalámbrica (WLAN) o en la internet. En adición a los requisitos para "Software de juego", los requisitos establecidos en esta sección deben conformar para los dispositivos de juego remoto.

3.5.2 Interacción del cliente-servidor

El jugador puede obtener/descargar una aplicación o paquete de software conteniendo el software de juego o acceder el software vía un navegador para participar en las transacciones de juego y financieras en el sistema de apuestas de eventos.

a) Los jugadores no deben ser habilitados para usar el software para transferir datos unos a otros, aparte de las funciones de chat (ej. mensajes de texto, voz, video, etc.) y archivos aprobados (ej. imágenes del perfil del usuario, fotos, etc.);
b) El software no debe alterar automáticamente las reglas del cortafuegos (firewall) especificadas por el dispositivo para puertos abiertos que son bloqueados por un cortafuegos de hardware o software;
c) El software no debe tener acceso a ningún puerto (ya sea automáticamente o indicando al usuario para el acceso manual) que no sea necesario para la comunicación entre el dispositivo de juego remoto y el servidor;
d) Si el software incluye funcionalidad adicional sin relación al juego, esta funcionalidad adicional no debe afectar la integridad del software de ninguna forma;
e) El software no debe tener la capacidad para invalidar el ajuste del volumen del dispositivo de juego remoto; y
f) El software no debe ser usado para almacenar información confidencial. Se recomienda que los métodos de auto completar, almacenamiento de contraseñas, u otros métodos que completarían el campo de la contraseña sean desactivados por defecto para el software.

3.5.3 Verificación de compatibilidad

Durante cualquier instalación o inicialización y antes de comenzar las operaciones de juego, el software de juego usado en conjunto con el sistema de apuestas de eventos debe detectar cualquier incompatibilidad o limitación de recursos del dispositivo de juego remoto que impediría la operación correcta del software (ej. versión de software, incumplimiento de las especificaciones mínimas, tipo de navegador, versión de navegador, versión de plug-in, etc.). Si se detectan incompatibilidades o limitaciones de recursos, el software debe impedir las operaciones de juego y mostrar un mensaje de error adecuado.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

3.5.4 Contenido del software

El software de juego no debe contener código malicioso o funcionalidad que es considerada maliciosa por la entidad regulatoria. Esto incluye, pero no está limitado a, la extracción/transferencia de archivos sin autorización, modificaciones desautorizadas del dispositivo, acceso sin autorización a cualquier información personal almacenada localmente (ej. contactos, calendario, etc.) y malware (programa maligno).

3.5.5 Cookies

Cuando cookies son usadas, los jugadores deben ser informados del uso de cookies después de la instalación del software de juego o durante el registro del jugador. Cuando cookies son requeridas para el juego, las apuestas no pueden ser colocadas si no son aceptadas por el dispositivo de juego remoto. Todas las cookies usadas no deben contener código malicioso.

3.5.6 Acceso de información

El software de juego debe tener la capacidad para mostrar, ya sea directamente en el interfaz del usuario o en una página accesible al jugador, los ítems especificados en las siguientes secciones de este documento. Para dispositivos de juego remoto que solo permiten apuestas en el local, es aceptable la divulgación al jugador del método para obtener la información requerida en esta sección:

a) “Reglas de juego y contenido”;
b) “Información para la protección del jugador”;
c) “Términos y condiciones”;
d) “Política de privacidad”;
e) “Visualización del juego e información”;
f) “Visualización de los resultados”.

NOTA: Es admisible que a veces el sistema estará sujeto a ciertos retrasos de sincronización para la actualización de esta información cuando se muestra por software, y es posible que la información solo pueda ser actualizada durante la siguiente interacción del jugador con el software que causa la actualización de la información en la pantalla.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Capítulo 4: Requisitos de Apuestas de Eventos

4.1 Introducción

4.1.1 Declaración general

Este capítulo establece los requisitos técnicos para las operaciones de juego, incluyendo, pero no limitado a las reglas para colocar apuestas y los resultados para los mercados de un evento.

4.2 Visualización del juego e información

4.2.1 Anuncio de las reglas del juego

El operador debe publicar las reglas completas de juego para los tipos de mercados y eventos ofrecidos actualmente. Cuando el software de juego incluye estas reglas de juego en directo, el software será evaluado conforme con los requisitos en la sección “Reglas de juego” de este documento.

4.2.2 Información dinámica del juego

La siguiente información debe estar disponible sin necesidad de colocar una apuesta. En un local, esta información puede ser mostrada en un dispositivo de juego y/o indicador externo.

a) Información sobre los eventos y mercados disponibles para las apuestas;
b) Probabilidades/pagos y precios actuales para los mercados disponibles;
c) Para tipos de mercados en los que las apuestas individuales son recolectadas en fondos:
   i. Información actualizada de probabilidades/pagos para fondos de mercado simple. Para fondos de mercado complejo, es aceptable que existan limitaciones razonables en la exactitud de la actualización de la estimación de fondos mostrada al jugador;
   ii. Valores actualizados de la inversión total para todos los fondos de los mercados; y
   iii. Los dividendos de cualquier mercado determinado.

NOTA: Esta información debe ser mostrada con la mayor exactitud posible considerando las dificultades de retrasos y latencia de la comunicación.

4.2.3 Recursos/funciones del jugador

Donde sea permitido por la entidad regulatoria, se pueden proveer recursos/funciones al jugador, así como el que ofrece consejo, indicios, o sugerencias a un jugador, o un flujo de datos que puede ser usado para facilitar la selección de apuesta externamente, si conforman con los requisitos siguientes:

a) El jugador debe ser informado de cada recurso/función que está disponible, la ventaja que ofrece (si es aplicable), y las opciones que existen para seleccionar.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

b) El método para obtener cada recurso/función debe ser divulgado al jugador. Todos los recursos/funciones que son ofrecidos al jugador para su compra deben mostrar claramente el costo.
c) La disponibilidad y funcionalidad de los recursos/funciones del jugador debe ser consistente para todos los jugadores.
d) Para apuestas entre pares (peer-to-peer), el jugador debe ser provisto con suficiente información para tomar decisiones informadas, antes de la participación, en cuanto a si debería participar con el jugador(es) que podría tener estos recursos/funciones.

4.3 Colocación de apuestas

4.3.1 Declaración general

Las apuestas son colocadas en relación a una cuenta de juego o fondos provistos a un asistente o en un dispositivo de juego. Dependiendo del tipo de dispositivo de juego, las apuestas pueden ser colocadas directamente por el jugador o en nombre del jugador por un asistente.

NOTA: Apuestas colocadas usando un dispositivo de juego remoto solamente pueden ser colocadas en relación con una cuenta de juego.

4.3.2 Colocación de una apuesta

Las reglas siguientes solo aplican a la colocación de una apuesta pagada directamente por el jugador en el dispositivo de juego:

a) El método de colocar una apuesta debe ser fácil, con todas las selecciones identificadas (incluyendo el orden, si es aplicable). Cuando la apuesta consiste de múltiples eventos (ej. parlays), este agrupamiento debe ser identificado.
b) Los jugadores deben ser habilitados para seleccionar el mercado deseado para colocar una apuesta.
c) Las apuestas no deben ser colocadas automáticamente en nombre del jugador sin el consentimiento/autorización del jugador.
d) Los jugadores deben tener la oportunidad para revisar y confirmar sus selecciones antes de completar la apuesta. Esto no excluye hacer apuestas de “un solo clic” si es permitido por la entidad regulatoria y es optado por el jugador.
e) Se deben identificar situaciones en las que el jugador ha colocado una apuesta para que las probabilidades/pagos o precios han cambiado, y a menos que el jugador haya optado aceptar automáticamente los cambios según es permitido por la entidad regulatoria, proveer una notificación para confirmar la apuesta considerando los nuevos valores.
f) Se debe proveer una indicación clara al jugador de que una apuesta ha sido aceptada o rechazada (por completo o en parte). Cada apuesta debe ser reconocida e indicada claramente por separado de forma que no haya duda cuales apuestas han sido aceptadas.
g) Para apuestas realizadas usando una cuenta de juego:
    i. El saldo de la cuenta debe ser fácilmente accesible.
    ii. No se debe aceptar una apuesta que resulte en un balance negativo para el jugador.
    iii. El balance de la cuenta debe ser debitado cuando la apuesta es aceptada por el sistema.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

4.3.3 Aceptación automática de cambios en las apuestas

Donde esté permitido por la entidad regulatoria, el sistema de apuestas de eventos puede soportar una función que permite a un jugador auto-aceptar cambios en probabilidades/pagos o el costo de la apuesta mientras está colocando una apuesta, provisto que cumpla con los siguientes requisitos:

a) Todas las opciones de auto-aceptar disponibles (ej. auto-aceptar todas las apuestas con un precio más alto, auto-aceptar todas las apuestas con un precio más bajo, etc.) deben ser explicadas al jugador;
b) El jugador debe optar manualmente para el uso de esta funcionalidad (ej. no debe ser configurada por defecto); y
c) El jugador debe tener la habilidad para no optar en cualquier momento.

4.3.4 Cupón de apuesta

Después de completar una transacción de juego, el jugador debe tener acceso a un registro de la apuesta, el cual incluye la siguiente información:

a) La fecha y hora en que la apuesta fue colocada;
b) La fecha y hora en que se espera que el evento ocurra (si se conoce);
c) Cualquier selección del jugador incluida en la apuesta:
    i. Línea de mercado y cuota (ej., apuesta simple, apuestas de margen, apuestas de más/menos, ganador/colocado/show, etc.);
    ii. Selección de apuesta (ej., atleta o nombre del equipo y número);
    iii. Cualquier condición(es) especial que aplica a la apuesta;
d) Cantidad total apostada, incluyendo créditos de bonificación/promocionales (si es aplicable);
e) Número de identificación único y/o código de barra de la apuesta;
f) Identificación del usuario o identificación única del dispositivo de juego que expidió el cupón de apuesta (si es aplicable);
g) Nombre del local/Identificador del sitio (para un cupón de apuesta impreso, es admisible que la información esté incluida en el cupón mismo); y
h) Período de redención (para un cupón de apuesta impreso, es admisible que esta información esté incluida en el cupón mismo);

NOTA: Algunos de los datos mencionados anteriormente también pueden ser parte del número de identificación único y/o código de barra. Múltiples códigos de barra son permitidos y pueden representar más datos que solo el número de identificación único

4.3.5 Cierre del período de juego

No debe ser posible colocar apuestas una vez que el período de juego haya cerrado.

4.3.6 Modalidad de juego gratis

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Donde esté permitido por la entidad regulatoria, el sistema de apuestas de eventos puede soportar la modalidad de juego gratis, la cual permite a un jugador participar en las apuestas sin pagar. La modalidad de juego gratis no debería confundir al jugador sobre las probabilidades/pagos disponibles en la versión pagada.

4.4 Resultados y pagos

4.4.1 Visualización de los resultados

El registro de los resultados debe incluir acceso a toda la información que pueda afectar los resultados de todo tipo de apuestas ofrecidas para ese evento.

a) Debe ser posible para un jugador obtener los resultados de sus apuestas en cualquier mercado determinado una vez que los resultados han sido confirmados.
b) Cualquier cambio en los resultados (ej. a causa de estadísticas/correcciones de línea) debe estar disponible.

4.4.2 Pago de las ganancias

Una vez que los resultados del evento son registrados y confirmados, el jugador recibe el pago por su apuesta ganadora. Esto no excluye la opción del jugador para recibir un pago ajustado antes de la conclusión del evento cuando sea ofrecido y es permitido por la entidad regulartoria.

4.4.3 Redención del cupón de apuesta ganador

Los siguientes requisitos aplican a la redención de una apuesta ganadora en un dispositivo de juego, según es permitido por la entidad regulatoria. Esta sección no aplica a las apuestas ganadoras asociadas a una cuenta de juego que automáticamente acredita el saldo de la cuenta.

a) El sistema de apuestas de eventos debe procesar la redención del cupón de apuesta ganador según el protocolo de comunicación segura implementado.
b) El jugador no recibe ninguna ganancia antes de la confirmación de validez del cupón de apuesta ganador.
c) El sistema de apuestas de eventos debe tener la capacidad para detectar y mostrar una notificación en el caso de cupones de apuestas ganadores que son inválidos o no se deben redimir por las condiciones siguientes:
    i. Cupón de apuesta que no está archivado;
    ii. Cupón de apuesta no es ganador;
    iii. Cupón de apuesta ganador ya se ha pagado; o
    iv. La cantidad del cupón de apuesta ganador no coincide con la cantidad registrada (este requisito puede conformar mostrando la cantidad de la apuesta ganadora para la confirmación durante el proceso de redención).
d) El sistema de apuestas de eventos debe actualizar el correspondiente estado del cupón de apuesta en la base de datos durante cada fase del proceso de redención. En otras palabras, cada vez que el estado del cupón de apuesta cambia, el sistema actualiza la base de datos.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

4.5 Apuestas de evento virtual

4.5.1 Declaración general

Las apuestas de evento virtual permiten colocar apuestas en simulaciones de eventos deportivos, competiciones, y carreras cuyos resultados están basados solamente en el producto de un generador de números aleatorios (RNG) según es permitido por la entidad regulatoria. Los siguientes requisitos solo aplican en caso de que la apuesta de evento virtual es realizada por completo por el sistema de apuestas de eventos donde una apuesta es colocada en un dispositivo de juego o por la interacción con un asistente y después el evento virtual es mostrado vía un indicador común o público (ej. pantalla externa, página web, etc.). Para eventos virtuales realizados por un dispositivo de juego (ej. el jugador hace una apuesta y el evento es desarrollado en su máquina o una pantalla compartida en una máquina de múltiples jugadores), por favor consulte *GLI-11 Estándares para dispositivos de juego* u otros requisitos jurisdiccionales para el cumplimiento en la entidad regulatoria.

4.5.2 Aleatoridad y eventos virtuales

Un RNG criptográfico debe ser utilizado para determinar los resultados del evento virtual y debe conformar con los requisitos jurisdiccionales aplicables establecidos para RNGs. A falta de estándares jurisdiccionales específicos, el capítulo "Generador de números aleatorios (RNG)" de *GLI-11 Estándares para Dispositivos de Juego* debe ser usado si es aplicable. Adicionalmente, la evaluación de los resultados de un evento virtual utilizando un RNG debe cumplir con las reglas siguientes:

a) Cuando más de un RNG es usado para determinar los diferentes resultados de eventos virtuales, cada RNG debe ser evaluado por separado; y
b) Cuando cada instancia de un RNG es idéntica, pero consiste de una implementación diferente en el evento virtual, cada implementación debe ser evaluada por separado.

4.5.3 Proceso de selección del evento virtual

La determinación de eventos al azar que resultan en un premio monetario no debe ser influenciada, afectada, o controlada por cualquier otra cosa aparte de los valores seleccionados por un RNG aprobado, conforme con los siguientes requisitos:

a) No debe ser posible determinar los resultados de un evento virtual antes del comienzo;
b) Cuando se hacen solicitudes al RNG, el evento virtual no debe limitar los resultados disponibles para seleccionar, excepto según lo previsto por el diseño;
c) El evento virtual no debe modificar o rechazar los resultados seleccionados por el RNG a causa de comportamiento adaptivo. En adición, los resultados deben ser usados según es definido por las reglas del evento virtual;
d) Después del comienzo del evento virtual, no se deben tomar acciones o decisiones que afecten el funcionamiento de cualquiera de los elementos de probabilidad en el evento virtual, aparte de las decisiones del jugador;
e) Los eventos al azar deben ser independientes excepto según lo provisto por las reglas del evento virtual, y no deben corresponder con ningún otro evento en el mismo evento virtual, o eventos en previos eventos virtuales;

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

f) Cualquier equipo asociado utilizado en conjunto con un sistema de apuestas de eventos no debe influenciar o modificar el funcionamiento del RNG del sistema y/o el proceso de selección al azar, excepto cuando está autorizado o es previsto por el diseño;
g) Los resultados del evento virtual no deben ser afectados por el ancho de banda efectivo, utilización del enlace, tasa de error de bit u otras características del canal de comunicación entre el sistema de apuestas de eventos y el dispositivo de juego; y
h) El software de juego no debe contener la lógica utilizada para generar el resultado de cualquier evento virtual. Todas las funciones críticas incluyendo la generación de cualquier evento virtual deben ser generadas por el sistema de apuestas de eventos y deben ser independientes del dispositivo de juego.

4.5.4 Visualización del evento virtual

Las pantallas para un evento virtual deben conformar con los requisitos para la visualización aplicables de este estándar. En adición, los siguientes requisitos aplican para la visualización:

a) Los datos de estadística que se hacen disponibles al jugador con respecto al evento virtual no deben malinterpretar las habilidades de ningún participante virtual. Esto no impide que el uso de un elemento de aleatoriedad afecte los resultados de un participante virtual durante el evento virtual.
b) Para eventos virtuales programados, se debe mostrar al jugador una cuenta regresiva del tiempo restante para colocar una apuesta. No debe ser posible colocar apuestas en el evento una vez que este tiempo ha transcurrido; sin embargo, este requisito no prohibe la implementación de las apuestas durante el juego.
c) Cada participante virtual debe tener una apariencia única, cuando corresponde a una apuesta. Por ejemplo, si la apuesta es por un equipo ganando a otro, no hay necesidad de que los participantes virtuales por sí mismos tengan una apariencia única, sin embargo, los equipos en que participan deben ser claramente distintos el uno del otro.
d) El resultado de un evento virtual debe ser evidente, inequívoco, y debe ser mostrado durante un período de tiempo adecuado para dar al jugador la oportunidad de verificar el resultado del evento virtual.

4.5.5 Simulación de objetos físicos

Cuando un evento virtual incorpora una representación gráfica o simulación de un objeto físico que es usada para determinar el resultado del evento virtual, el funcionamiento exhibido por la simulación debe ser consistente con el objeto del mundo real, a menos que las reglas del evento virtual indiquen lo contrario. Este requisito no aplica a las representaciones gráficas o simulaciones que son utilizadas solo para propósitos de entretenimiento. Lo siguiente debe aplicar a la simulación:

a) La probabilidad de cualquier evento ocurriendo en la simulación que afecta el resultado del evento virtual debe ser análoga a las propiedades del objeto físico;
b) Cuando el evento virtual simula múltiples objetos físicos que normalmente serían independientes uno del otro basado en las reglas del evento virtual, cada simulación debe ser independiente de cualquier otra simulación; y

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

c) Cuando el evento virtual simula objetos físicos sin la memoria de eventos previos, el funcionamiento de los objetos simulados debe ser independiente de su funcionamiento anterior, para no ser adaptable o previsible, a menos que se indique lo contrario al jugador.

4.5.6 Motor de física

Los eventos virtuales pueden utilizar un "motor de física", lo cual es software especializado que aproxima o simula un entorno físico, incluyendo efectos tales como movimiento, gravedad, velocidad, aceleración, inercia, trayectoria, etc. Un motor de física debe ser diseñado para mantener constante el funcionamiento del juego y el entorno del evento virtual a menos que se indique lo contrario al jugador en las reglas del evento virtual. Un motor de física puede utilizar las propiedades de aleatoridad de un RNG para afectar los resultados del evento virtual.

NOTA: Las implementaciones de un motor de física en un evento virtual serán evaluadas caso por caso por el laboratorio independiente de pruebas.

4.6 Sistemas de juego externo

4.6.1 Declaración general

Esta sección contiene requisitos para las circunstancias en las que el sistema de apuestas de eventos se comunica con un sistema de juego externo en cualquiera de las siguientes configuraciones:

a) El sistema de apuestas de eventos actúa como el "sistema de juego anfitrión" que recibe, para sus propios mercados, las apuestas de uno o más "sistemas de juego cliente" externos; o
b) El sistema de apuestas de eventos actúa como un "sistema de juego cliente" enviando las apuestas a un "sistema de juego anfitrión", para los mercados de ese sistema.

NOTA: Los requisitos de esta sección aplican a la interoperabilidad del sistema de apuestas de eventos con el dispositivo de juego externo, y no son una evaluación completa del sistema de juego externo por sí mismo. El sistema de juego externo puede ser sometido independientemente a una evaluación por el laboratorio independiente de pruebas según la discreción de la entidad regulatoria.

4.6.2 Información

Los requisitos siguientes aplican a la información siendo enviada entre el sistema de juego anfitrión y el sistema de juego cliente:

a) Si el sistema de juego anfitrión proporciona apuestas pari-mutuel para el sistema de juego cliente, el sistema de apuestas de eventos debe tener la capacidad para:
   i. Cuando actúa como el sistema de juego cliente, recibir los dividendos actuales para fondos activos enviados del sistema de juego anfitrión.
   ii. Cuando actúa como el sistema de juego anfitrión, enviar los dividendos actuales para fondos activos a todos los sistemas de juego cliente conectados.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

b) Si el sistema de juego anfitrión proporciona apuestas de probabilidades fijas para el sistema de juego cliente y en el que las probabilidades/pagos y precios pueden ser cambiados dinámicamente, el sistema de apuestas de eventos debe tener la capacidad para:
   i. Cuando actúa como el sistema de juego cliente, recibir las probabilidades/pagos y precios actuales enviados del sistema de juego anfitrión cada vez que cualquier probabilidad/pago y precio ha cambiado.
   ii. Cuando actúa como el sistema de juego anfitrión, enviar las probabilidades/pagos y precios actuales a todos los sistemas de juego clientes conectados cada vez que cualquier probabilidad/pago y precio ha cambiado.
c) Un cambio de información del estado del evento debe ser enviado desde el sistema de juego anfitrión al sistema de juego cliente cada vez que ocurra cualquier cambio, incluyendo:
   i. Selecciones retiradas/ restablecidas;
   ii. Hora de comienzo del evento ha cambiado;
   iii. Mercados individuales abiertos/cerrados;
   iv. Resultados ingresados/modificados;
   v. Resultados confirmados; y
   vi. Evento cancelado.

4.6.3 Apuestas

Los siguientes requisitos aplican a las apuestas siendo colocadas entre el sistema de juego anfitrión y el sistema de juego cliente:

a) Las apuestas colocadas en el sistema de juego cliente deben recibir claramente el reconocimiento de aceptación, aceptación parcial (incluyendo detalles), o rechazo enviados desde el sistema de juego anfitrión.
b) Si el costo de la apuesta es determinado por el sistema de juego anfitrión, se debe establecer una secuencia de confirmación positiva para habilitar al jugador para aceptar el costo de la apuesta, y el sistema de juego cliente para determinar que hay suficientes fondos en el saldo de la cuenta para cubrir el costo de la apuesta antes de hacer la oferta al sistema de juego anfitrión.
c) Cuando las apuestas pueden ser colocadas al por mayor, los siguientes requisitos son aplicables:
   i. Si el flujo de las apuestas es interrumpido por cualquier razón, debe haber un método disponible para determinar cuando en la transmisión ocurrió la interrupción.
   ii. Ninguna apuesta debe ser transmitida si esta es mayor que el saldo de la cuenta. Si hay un intento de este tipo de apuesta se debe parar la transmisión completa.
d) El saldo de la cuenta debe ser debitado por una cantidad igual a la oferta y costo del sistema de juego anfitrión. Los fondos deben permanecer como una transacción pendiente con los detalles de la oferta registrados en el sistema de juego anfitrión. Cuando el reconocimiento del sistema de juego anfitrión es recibido, se deben hacer los ajustes apropiados a la cuenta “pendiente” y el saldo de la cuenta en el sistema de juego cliente.
e) Solicitudes de cancelación del sistema de juego cliente deben recibir claramente un reconocimiento de aceptación o rechazo por el sistema de juego anfitrión. El jugador no debe ser acreditado por el sistema de juego cliente hasta que la confirmación final es recibida del sistema de juego anfitrión incluyendo la cantidad de la apuesta anulada o cancelada.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

4.6.4 Resultados

Cuando los resultados son ingresados y confirmados en el sistema de juego anfitrión, cada apuesta ganadora debe ser transferida al sistema de juego cliente con la cantidad de la ganancia. La confirmación del recibo de las apuestas ganadoras debe ser reconocida por el sistema de juego cliente.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Anexo A: Auditoría operacional para procedimientos y prácticas de juego

A.1 Introducción

A.1.1 Declaración general

Este anexo establece los procedimientos y prácticas para las operaciones de juego que serán revisados en una auditoría operacional como parte de la evaluación del sistema de apuestas de eventos, incluyendo, pero no limitado a: establecer reglas de juego , suspender eventos, procesar varias transacciones de apuestas y financieras, crear mercados, abonar apuestas, cerrar mercados, cancelar eventos, anular o cancelar apuestas, gestión de la cuenta del jugador, prácticas fundamentales pertinentes a la limitación de riesgos, y cualquier otro objetivo establecido por la entidad regulatoria.

NOTA: Es entendido que los procedimientos y prácticas que no están especificamente incluidos en este estándar también serán aplicables y requeridos para una auditoría operacional según es determinado por el operador y/o entidad regulatoria en sus normas, reglamentos, y estándares de controles internos mínimos (MICS por sus siglas en inglés).

A.2 Procedimientos de controles internos

A.2.1 Procedimientos de controles internos

El operador debe establecer, mantener, implementar y cumplir con los procedimientos de controles internos para las operaciones de juego, incluyendo realizar apuestas y transacciones financieras.

A.2.2 Gestión de datos

Los controles internos del operador deben incluir procesos para mantener la información registrada especificada en la sección titulada “Información para ser mantenida” por un período de cinco años o según es especificado por la entidad regulatoria.

A.2.3 Gestión de riesgo

Los controles internos del operador deben incluir los detalles del marco de gestión de riesgos, incluyendo, pero no limitado a:

a) Procedimientos manuales y automatizados de la gestión de riesgos;
b) Gestión de empleados, incluyendo controles de acceso y segregación de sus funciones;
c) Información con respecto a la identificación y reporte del fraude y actividades sospechosas;
d) Controles que aseguran el cumplimiernto regulatorio;

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

e) Descripción de estándares de cumplimiento contra el blanqueo de dinero (AML por sus siglas en inglés) incluyendo procedimientos para detectar la estructuración para eludir requerimientos de los reportes;
f) Descripción de todas las aplicaciones de software que comprenden el sistema de apuestas de eventos.
g) Descripción de todos los tipos de apuestas disponibles para las ofertas del operador;
h) Descripción del método para impedir la colocación de apuestas antes/después;
i) Descripción de todos los proveedores de servicios de terceros; y
j) Cualquier otra información requerida por la entidad regulatoria.

A.2.4 Jugadores restringidos

Los controles internos del operador deben describir el método para prevenir que los jugadores apuesten sobre eventos en los que podrían tener información privilegiada, incluyendo, pero no limitado a los siguientes ejemplos, según es requerido por la entidad regulatoria:

a) Jugadores identificados como empleados, subcontratistas, directores, propietarios, y oficiales del operador, así como aquellos en la misma residencia, no deben colocar apuestas sobre ningún evento, excepto en fondos privados en los que su asociación con el operador es divulgada con claridad.
b) Jugadores identificados como atletas a nivel universitario o profesional, empleados y propietarios del equipo, entrenadores, gerentes, asistentes, fisioterapeutas, oficiales y empleados de la liga, árbitros, jueces, agentes deportivos, y empleados de un sindicato de jugadores o árbitros, así como aquellos en la misma residencia, no deben colocar apuestas sobre ningún evento del deporte en que participan, o en que el atleta que representan participa.

A.3 Controles de la cuenta de juego

A.3.1 Registro y verificación

Cuando el registro de la cuenta de juego es realizado manualmente por el operador, se deben establecer procedimientos para cumplir con los requisitos para el “Registro y verificación” como es indicado en este documento.

A.3.2 Cuentas fraudulentas

El operador debe tener una política pública documentada para el procesamiento de cuentas de juego descubiertas siendo utilizadas de manera fraudulenta, incluyendo, pero no limitado a:

a) El mantenimiento de información sobre la actividad de la cuenta, de forma que si actividad fraudulenta es detectada el operador tiene la información necesaria para tomar medidas adecuadas;
b) La suspensión de cualquier cuenta descubierta a ser utilizada para actividad fraudulenta, así como un jugador proveyendo acceso a personas menores de edad; y
c) El procesamiento de depósitos, apuestas, y ganancias asociadas con una cuenta fraudulenta.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

A.3.3 Términos y condiciones

Un conjunto de términos y condiciones debe estar disponible para el jugador. Durante el proceso de registro y cuando cualesquieras términos y condiciones son actualizados significativamente (ej. más a fondo de cambios gramaticales u otros cambios menores), el jugador debe aceptar los términos y condiciones. Los términos y condiciones deben:

a) Declarar que solamente personas legalmente permitidas por su respectiva jurisdicción pueden participar en el juego;
b) Recomendar al jugador mantener sus credenciales de autenticación (ej. contraseña y nombre de usuario) seguros;
c) Divulgar todos los procesos con respecto a credenciales de autenticación perdidas, cambios de contraseña forzados, seguridad de la contraseña y otros ítems relacionados;
d) Especificar las condiciones bajo las cuales una cuenta es declarada inactiva y explicar que medidas serán adoptadas sobre la cuenta una vez hecha esta declaración; y
e) Definir claramente lo que ocurre con las apuestas del jugador pendientes colocadas antes de cualquier exclusión autoimpuesta o impuesta por el operador, incluyendo la devolución de todas las apuestas, o el proceso de todas las apuestas, según sea aplicable.

A.3.4 Política de privacidad

Una política de privacidad debe estar disponible para el jugador. Durante el proceso de registro y cuando la política de privacidad es actualizada significativamente (ej. más a fondo de cambios gramaticales u otros cambios menores), el jugador debe aceptar la política de privacidad. La política de privacidad debe incluir:

a) La información del jugador requerida para ser recolectada;
b) El propósito para la recopilación de información;
c) El período en que la información es almacenada;
d) Las condiciones bajo las cuales la información puede ser divulgada; y
e) Una declaración de que existen medidas para prevenir la divulgación desautorizada o innecesaria de la información.

A.3.5 Seguridad de datos del jugador

Cualquier información obtenida con respecto a la cuenta del jugador, incluyendo los datos del jugador, debe conformar con la política de privacidad y las normas y estándares de privacidad locales observadas por la entidad regulatoria. Adicionalmente:

a) Cualquier información del jugador que no esté sujeta a divulgación conforme con la política de privacidad debe ser mantenida confidencial, excepto cuando la divulgación de la información es requerida por la ley.
b) Deben establecerse procedimientos para la seguridad y divulgación de los datos del jugador, fondos en una cuenta del jugador y otra información confidencial según es requerido por la entidad regulatoria, incluyendo, pero no limitado a:

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

i. La designación e identificación de uno o más empleados con responsabilidad principal para el diseño, implementación y evaluación continua de estos procedimientos y prácticas;
ii. Los procedimientos utilizados para determinar el carácter y alcance de toda la información recolectada, la localización en que toda la información está almacenada, y los dispositivos de memoria en los que dicha información puede ser guardada para el propósito de almacenamiento o transferencia;
iii. Las medidas a ser utilizadas para proteger la información contra el acceso sin autorización; y
iv. Los procedimientos utilizados en caso de que el operador determine que ha ocurrido una violación de la seguridad de los datos, incluyendo la notificación requerida a la entidad regulatoria.

A.3.6 Transacciones financieras

Deben establecerse procedimientos para asegurar que todas las transacciones financieras son realizadas conforme con la reglamentación del comercio local y requisitos establecidos por la entidad regulatoria:

a) Cuando las transacciones financieras no pueden ser realizadas automáticamente por el sistema de apuestas de eventos, deben establecerse procedimientos para cumplir con los requisitos para el "Mantenimiento de fondos del jugador" según es indicado en este documento.
b) La identificación positiva o autenticación del jugador debe ser completada antes de que el jugador pueda retirar los fondos.
c) Una solicitud del jugador para retirar los fondos (ej. fondos depositados y autorizados o apuestas ganadas) debe ser completada por el operador en un período de tiempo razonable, a menos que exista un reclamo/disputa del jugador sin resolver o investigación pendiente. Esta investigación debe ser documentada por el operador y debe estar disponible para la revisión por la entidad regulatoria.
d) El operador debe establecer procedimientos de autorización o seguridad para asegurar que solo se pueden realizar ajustes en la cuenta del jugador con autorización, y estos cambios se puedan auditar.

A.3.7 Limitaciones

Los jugadores deben ser provistos con un método para imponer limitaciones en los parámetros de juego incluyendo, pero no limitado a depósitos y apuestas según es requerido por la entidad regulatoria. En adición, un método debe ser establecido para que el operador pueda imponer cualquier limitación en los parámetros de juego según es requerido por la entidad regulatoria.

a) Una vez establecidas por el jugador e implementadas por el operador; solo debe ser posible reducir la severidad de limitaciones autoimpuestas con una notificación de 24 horas, o según es requerido por la entidad regulatoria.
b) Los jugadores deben ser notificados previamente de todos los límites impuestos por el operador y su fecha efectiva. Una vez actualizados, los límites impuestos por el operador deben conformar con lo divulgado al jugador; y
c) Después de recibir una orden de limitación autoimpuesta o impuesta por el operador, el operador debe asegurar que todos los límites especificados son correctamente implementados

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

inmediatamente o en un momento (ej. sesión siguiente, al día siguiente) claramente indicado al jugador.

A.3.8 Exclusiones

Los jugadores deben ser provistos con un método para la autoexclusión de juego por un período especificado o indefinitivamente, según es requerido por la entidad regulatoria. En adición, se debe establecer un método para que el jugador sea excluido del juego por el operador, según es requerido por la entidad regulatoria.

a) Los jugadores deben recibir una notificación conteniendo el estado de la exclusión e instrucciones generales de resolución, si es posible;
b) Immediatamente después de recibir la orden de exclusión, no se debe aceptar ninguna apuesta o depósito de ese jugador, hasta que la exclusión ha sido eliminada;
c) Mientras el jugador está excluido este no debe ser impedido retirar parte o el total del balance de su cuenta, provisto que el operador reconoce que los fondos están autorizados, y que el motivo(s) para la exclusión no prohibiría un retiro; y
d) Ningún contenido de publicidad o marketing debe ser dirigido específicamente a jugadores que han sido excluidos del juego.

A.3.9 Cuentas inactivas

Una cuenta del jugador es considerada como inactiva según las condiciones especificadas en los términos y condiciones. Se deben establecer procedimientos para:

a) Proteger las cuentas de jugador inactivas que contienen fondos contra el acceso sin autorización, cambios o eliminación; y
b) Procesar los fondos no reclamados de cuentas de jugador inactivas, incluyendo la devolución de los fondos restantes al jugador si es posible.

A.4 Procedimiento de operación en general

A.4.1 Reservas del operador

El operador debe establecer procesos para mantener y proteger reservas en efectivo adecuadas, según es determinado por la entidad regulatoria, incluyendo la segregación de cuentas de fondos mantenidos para cuentas de jugador y fondos operacionales tales como los utilizados para cubrir apuestas ganadoras no reclamadas, apuestas potencialmente ganadoras en el día de juego, etc.

A.4.2 Protección de fondos del jugador

El operador debe establecer procesos para asegurar que los fondos en una cuenta del operador son mantenidos en depósito para el jugador en una cuenta segregada con fines especiales que es mantenida y controlada por una entidad corporativa legítima que no sea el operador y cuya junta directiva incluye uno o más directores corporativos que son independientes del operador y de cualquier corporación relacionada o controlada por el operador. En adición, el operador debe

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

establecer procedimientos que son utilizados razonablemente para:

a) Asegurar que los fondos generados por el juego son contabilizados y garantizados;
b) Explicar que los fondos en la cuenta segregada no pertenecen al operador y no están disponibles para los acreedores, aparte del jugador que tiene los fondos retenidos; y
c) Impedir la mezcla de fondos en la cuenta segregada con otros fondos incluyendo, sin limitación, los fondos del operador.

A.4.3 Impuestos

El operador debe establecer un proceso para identificar todas las ganancias que están sujetas a impuestos (ganancias únicas o ganancias acumuladas en un período definido, según es requerido) y proveer la información necesaria conforme con los requisitos para los impuestos de cada entidad regulatoria.

NOTA: Cantidades de las ganancias que exceden cualquier límite jurisdiccional especificado requieren completar la documentación correspondiente antes de pagar el jugador que ha ganado.

A.4.4 Proceso para reclamos/disputas

El operador debe establecer un método para que el jugador pueda hacer un reclamo/disputa, y habilitar al jugador para notificar la entidad regulatoria si este reclamo/disputa no ha sido o no puede ser atendido por el operador, o bajo otras circunstancias según es especificado por la ley de la entidad regulatoria.

a) Los jugadores deben ser habilitados para hacer un registro del reclamo/disputa a base de 24/7.
b) Los registros de toda la correspondencia relacionada con un reclamo/disputa deben ser mantenidos durante un período de cinco años o según lo especificado por la entidad regulatoria.
c) Se debe establecer un proceso documentado entre el operador y la entidad regulatoria para el proceso del informe y resolución del reclamo/disputa.

A.4.5 Información para la protección del jugador

La información para la protección del jugador debe estar disponible al jugador. La información para la protección del jugador debe incluir como mínimo:

a) Información sobre los riesgos potenciales asociados con el juego excesivo, y donde se puede obtener ayuda para un problema con el juego;
b) Una declaración de que ninguna persona menor de edad es permitida a participar en el juego;
c) Una lista de opciones disponibles para la protección del jugador que pueden ser utilizadas por el jugador, así como la exclusión autoimpuesta, e información sobre como utilizar estas opciones;
d) Para cuentas del jugador, mecanismos en su lugar que pueden ser utilizados para detectar el uso no autorizado de su cuenta, así como la revisión del estado de una tarjeta de crédito contra los depósitos reconocidos;
e) Información de contacto u otros medios para reportar un reclamo/disputa; e
f) Información de contacto para la entidad regulatoria y/o un enlace con su sitio de web.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

A.5 Reglas de juego y contenido

A.5.1 Reglas de juego

Reglas de juego se refiere a cualquier información escrita, gráfica, y auditiva provista al público con respecto a las operaciones de apuestas de eventos. El operador debe adoptar, y adherirse a las reglas completas de juego que deben ser aprobadas por la entidad regulatoria:

a) Las reglas de juego deben ser completas, inequívocas, y no engañosas o injustas para el jugador.
b) Las reglas de juego que deben ser presentadas auditivamente (por sonido o voz) también deben ser mostradas de forma escrita.
c) Las reglas de juego deben ser mostradas en un color que contrasta con el color de fondo para asegurar que toda la información es claramente visible/legible.
d) El operador debe mantener un registro de cualquier cambio en las reglas de juego relacionado con la colocación de apuestas.
e) Cuando las reglas de juego son alteradas para los eventos o mercados siendo ofrecidos, todo cambio en las reglas debe incluir un sellado de fecha y hora mostrando la regla aplicable en cada período. Si múltiples reglas aplican en un evento o mercado, el operador debe aplicar las reglas vigentes cuando la apuesta fue aceptada.

A.5.2 Contenido de las reglas de juego

La siguiente información debe ser disponible al jugador. Para apuestas colocadas en un local, es admisible que esta información sea mostrada por el dispositivo de juego o por indicadores externos, formularios, o catálogos disponibles:

a) Los métodos de aplicar fondos para una apuesta o cuenta del jugador, incluyendo una explicación clara y concisa de todas las tarifas (si es aplicable);
b) Según es permitido por la entidad regulatoria, cualquier premio que es ofrecido en forma de mercancía, anualidades, pagos de suma fija, o plan de pagos en lugar de pagos en efectivo para cada mercado que está ofreciendo ese premio;
c) Los procedimientos que abordan cualquier mal funcionamiento irrecuperable de hardware/software incluyendo si este proceso resulta en la anulación o cancelación de cualquier apuesta; y
d) Los procedimientos para solucionar las interrupciones causadas por una discontinuidad en la transmisión de datos del servidor de la red durante un evento.
e) Reglas de participación, incluyendo toda eligibilidad de juego y criterio para la puntuación, eventos disponibles y mercados, tipos de apuestas aceptados, línea de cuota, todos los premios anunciados, y el efecto de cambios de programación;
f) Información de pagos, incluyendo las combinaciones ganadoras posibles, calificación, y resultados, junto con sus pagos correspondientes, para cualquier opción de apuesta disponible;
g) Cualquier función restrictiva de juego, así como la cantidad de la apuesta o el valor máximo de la ganancia;
h) Una descripción de los jugadores restringidos, incluyendo cualquieras limitaciones aplicables en sus apuestas (ej. los atletas no deben apostar en su deporte);

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

i) Los procedimientos para manejar el anuncio incorrecto de eventos, mercados, probabilidades/pagos, precios, apuestas, o resultados;
j) Una política de cancelatión de apuesta que incluye las apuestas por múltiples eventos (ej. parlays) e indicar cualquier prohibición de anular o cancelar apuestas (ej. después de un período de tiempo fijo);
k) Si las probabilidades/pagos son fijos en el momento de la apuesta, o si las probabilidades/pagos pueden cambiar dinámicamente antes del comienzo del evento y el método de anunciar cambios en las probabilidades/pagos;
l) Para tipos de apuestas en las que las probabilidades/pagos son fijos en el momento en que la apuesta es colocada, cualquier situación en que las probabilidades/pagos pueden ser ajustados tales como resultados ganadores atípicos (ej. empate técnico), partes canceladas de apuestas con múltiples eventos (ej. parlays), y prorrateo;
m) Para tipos de apuestas en las que las apuestas individuales son recolectadas en fondos, las reglas para el cálculo de dividendos incluyendo la formula predominante para la adjudicación de fondos y las estipulaciones del evento siendo apostado por la entidad regulatoria;
n) Para las apuestas durante el juego, debido a velocidades de transmisión variantes o latencia de transmisión:
    i. Actualización de la información mostrada podría resultar en desventaja de un jugador con otros que podrían tener información más actual; y
    ii. Puede haber retrasos incorporados en el tiempo registrado de una apuesta durante el juego para prevenir las apuestas antes-después y cancelaciones.
o) Una declaración de que el operador reserva el derecho para:
    i. Rechazar cualquier apuesta o parte de una apuesta o rechazar o limitar selecciones antes de la aceptación de una apuesta por la razón indicada al jugador en estas reglas;
    ii. Aceptar una apuesta con términos diferentes a los publicados;
    iii. Cerrar períodos de juego a su discreción;
p) Si los premios deben ser pagados por combinaciones incluyendo otros participantes que el finalista en primer lugar (ej. en una competición Olímpica), el orden de los participantes que es asociado con estos premios (ej. resultado 8-4-7);
q) Las reglas para cualquier opción de apuesta exótica (ej. perfecta, trifecta, quinella, etc.) y los pagos previstos;
r) Lo que debe ocurrir cuando un evento o mercado es cancelado o retirado, incluyendo el manejo de selecciones de apuestas con múltiples eventos (ej. parlays) cuando una o más de las partes son canceladas o retiradas;
s) Como se determina una apuesta ganadora y el manejo de un premio en caso de que un empate sea posible;
t) El pago de las apuestas ganadoras, incluyendo el período de redención y el método para el cálculo. Cuando el cálculo de los pagos pueda incluir el redondeo, la información sobre el manejo de estas circunstancias debe explicar claramente:
    i. Redondeo hacia arriba, redondeo hacia abajo (truncado), redondeo auténtico; y
    ii. Redondeo a cual nivel (ej. 5 centavos).

A.5.3 Promociones y/o bonificaciones

Los jugadores podrán tener acceso a la información de las reglas de juego correspondiente a todas las promociones y/o bonificaciones disponibles, incluyendo la forma de notificar al jugador cuando

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

este ha recibido un premio promocional o ganancia de bonificación y los términos de su retiro. Esta información debe ser clara e inequívoca, especialmente cuando las promociones o bonificaciones están limitadas a ciertos eventos, mercados, o cuando aplican otras condiciones específicas.

A.5.4 Competiciones/Torneos

Una competición/torneo, la cual permite a un jugador comprar o ser ofrecido la oportunidad de participar en competición de juego contra otros jugadores, puede ser admisible provisto que cumpla con las reglas siguientes:

a) Las reglas deben ser disponibles a un jugador para revisarlas antes de su registro en la competición/ torneo. Las reglas deben incluir como mínimo:
   i. Todas las condiciones que los jugadores registrados deben cumplir para poder inscribirse y avanzar en la competición/torneo;
   ii. Información específica correspondiente a una competición/torneo único incluyendo los premios o recompensas disponibles y la distribución de fondos basado en resultados específicos; y
   iii. El nombre de la organización (o personas) que realizaron la competición/torneo en nombre de, o en conjunto con el operador (si es aplicable).
b) Se deben establecer procedimientos para registrar los resultados de cada competición/torneo y disponerlos al público para que los jugadores registrados puedan revisarlos durante un período de tiempo razonable. Después de ser anunciados públicamente, los resultados de cada competición/torneo deben ser disponibles por solicitud. Los resultados incluyen lo siguiente:
   i. Nombre de la competición/torneo;
   ii. Fecha(s)/hora(s) de la competición/torneo;
   iii. Número total de entradas;
   iv. Cantidad de las tarifas de entradas;
   v. Fondo de premios total; y
   vi. Cantidad pagada por cada categoría ganadora.

NOTA: Para competiciones/torneos gratis (ej. jugadores registrados no pagan una tarifa de entrada), la información requerida mencionada anteriormente debe ser registrada excepto por el número de entradas, precio de entrada y fondo total de premios.

A.6 Procedimientos y Controles del Juego

A.6.1 Probabilidades/Pagos y Precios

Se deben establecer procedimientos para configurar y actualizar las probabilidades/pagos y precios incluyendo proveer al público las probabilidades/pagos y precios actuales, cambiar probabilidades/pagos y precios según sea necesario para manejar excepciones, y registrar correctamente y periódicamente las probabilidades/pagos y precios

A.6.2 Estadísticas/Datos de Línea

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

El operador debe asegurar que todos los datos de estadísticas/línea que son disponibles al jugador con respecto a un evento utilizan una fuente permitida por la entidad regulatoria y se mantiene con exactitud y adecuadamente actualizada. Según es requerido por la entidad regulatoria, el operador debe implementar controles para:

a) Revisar la exactitud y actualidad de todos los servicios de línea/estadística; y
b) Cuando ocurre un incidente o error que resulta en la pérdida de comunicación con los servicios de línea/estadística, se debe ingresar el incidente o error junto con la fecha y hora de la ocurrencia, su duración, carácter, y una descripción de su impacto en el funcionamiento del sistema. Esta información debe ser mantenida por un período de 90 días, o según es especificado por la entidad regulatoria.

A.6.3 Suspender mercados o eventos

Se deben establecer procedimientos para suspender mercados o eventos (ej. dejar de aceptar apuestas para el mercado o mercados asociados con este evento). Cuando el juego es suspendido para un evento activo, se debe hacer una entrada en un registro de auditoría que incluye la fecha y hora de la suspensión y el motivo.

A.6.4 Cancelaciones de Apuestas

Las transacciones de apuestas no pueden ser modificadas excepto para ser anuladas o canceladas según es provisto en la política de privacidad publicada por el operador. Se puede ofrecer un plazo adicional de cancelación para permitir a los jugadores solicitar la cancelación de las apuestas colocadas. Los siguientes requisitos aplican a la cancelación de las apuestas:

a) Las cancelaciones iniciadas por el jugador pueden ser autorizadas conforme con la política de cancelación.
b) Las cancelaciones iniciadas por el operador deben proveer al jugador un motivo para su cancelación (ej. apuesta antes-después).
c) Un operador no debe anular o cancelar ninguna apuesta sin previa autorización de la entidad regulatoria.

A.6.5 Período de Juego

Debe existir documentación para indicar como se controla el período de juego. Esto incluye todos los casos cuando el período de juego es abierto inicialmente, cuando se cierra, o cualquier momento en este período cuando una apuesta no se puede colocar (ej. probabilidades/pagos y precios están siendo actualizados).

A.6.6 Resultados

Antes de anunciar los resultados públicamente y declarar los ganadores, se debe establecer una política para la confirmación de los resultados basado en fuentes aprobadas y calificadas, a menos que esto sea automatizado por transmisión externa. Si se utiliza la transmisión externa, se deben establecer procedimientos para casos en que el acceso a la transmisión externa no es disponible.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

También se debe establecer un procedimiento para manejar cambios en los resultados (ej. debido a correcciones de línea/estadísticas).

A.6.7 Pago de apuestas ganadoras

En caso de un fallo en la capacidad del sistema de apuestas de eventos para pagar las apuestas ganadoras, el operador debe establecer controles detallando el método para pagar estas apuestas.

A.6.8 Eventos virtuales

Un operador que ofrece apuestas de eventos virtuales debe mantener toda la información necesaria para reproducir adecuadamente los eventos virtuales, incluyendo los resultados de eventos virtuales y/o acciones de los participantes virtuales, realizados durante los últimos 90 días o según es requerido por la entidad regulatoria. Esta información puede ser registrada por el sistema de apuestas de eventos o equipo asociado, utilizando una combinación de texto, registros, video, grápficos, capturas instantáneas, u otros métodos (ej. mecanismo "registrador de vuelo"). Alternativamente, se pueden incluir procedimientos para el grabado de la visualización pública del evento virtual por el sistema de vigilancia.

A.7 Especificaciones del Local de Juego

A.7.1 Auditoría de verificación del local

El local de juego será requerido cumplir con los aspectos aplicables de la política apropiada y/o documentos del procedimiento según es determinado por el operador en consulta con la entidad regulatoria. Para mantener la integridad de las operaciones de juego, los locales pueden ser sujetos a una auditoría de verificación adicional según es requerido por la entidad regulatoria. Las siguientes especificaciones aplican para los locales:

A.7.2 Equipo de juego

El local debe proveer una localización segura para la colocación, operación, y uso del equipo de juego, incluyendo dispositivos de juego, despliegues visuales, y equipo de comunicación. Se debe establecer la política de seguridad y procedimientos y revisarlos periódicamente para asegurar que los riesgos son identificados, mitigados y asegurados en planes de emergencia. En adición:

a) El equipo de juego debe ser instalado conforme con un plan específico y se deben mantener registros de todo el equipo de juego instalado.
b) El equipo de juego debe ser ubicado o protegido para reducir los riesgos de:
   i. Amenazas y peligros ambientales;
   ii. Oportunidades para acceso sin autorización;
   iii. Fallos de energía; y
   iv. Otras interrupciones causadas por fallos en utilidades de soporte.
c) Acceso al equipo de juego por un empleado debe ser controlado por un procedimiento de registro seguro u otro proceso seguro aprobado por la entidad regulatoria para asegurar al acceso por

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

empleados autorizados solamente. No debe ser posible modificar los ajustes de configuración del equipo de juego sin un proceso seguro y autorizado.

d) Una sesión del usuario, cuando es soportado por el equipo de juego, es iniciada por el empleado accediendo su cuenta de usuario usando su nombre de usuario y contraseña seguros o una manera alternativa para el empleado para proveer la información de identificación según es permitido por la entidad regulatoria.
   i. Todas las opciones disponibles presentadas al empleado deben estar relacionadas a su cuenta de juego.
   ii. Si el equipo de juego no recibe entradas del empleado en 5 minutos, o un período especificado por la entidad regulatoria, la sesión del usuario debe entrar en tiempo de espera o bloquearse, requiriendo al empleado restablecer su acceso para continuar.
e) Para asegurar su disponibilidad continua e integridad, el equipo de juego debe ser mantenido, inspeccionado y atendido a intervalos regulares para asegurar que no tenga defectos o mecanismos que pudieran interferir con su operación.
f) Antes de su retiro o re-utilización, el equipo de juego conteniendo los medios de almacenamiento deben ser comprobados para asegurar que cualquier software con licencia, información de la cuenta del jugador, y otra información confidencial ha sido removida o sobrescrita de forma segura (ej. no solamente borrada).

A.7.3 Operaciones de juego

Se deben establecer los siguientes procedimientos para las operaciones de juego en el local:

a) Procedimientos para habilitar una respuesta adecuada para cualquier problema de seguridad en el local.
b) Procedimientos para prevenir a cualquier persona manipular o interferir con la operación del juego o equipo de juego;
c) Procedimientos para describir las operaciones y el mantenimiento de dispositivos de juego POS y dispositivos de juego de auto servicio, incluyendo el procesamiento de condiciones de error y realizando las reconciliaciones;
d) Procedimientos para asegurar que los requisitos de accesibilidad observados por la entidad regulatoria conforman para la instalación de los dispositivos de juego de auto servicio.
e) Procedimientos para las transacciones de apuestas utilizando un dispositivo de juego POS, incluyendo:
   i. Aceptar las apuestas de los jugadores solamente durante el período para las apuestas;
   ii. Notificar a los jugadores si su intento de apuesta es rechazado;
   iii. Requerir el registro de la información del jugador o el registro de la cuenta del jugador si su apuesta excede un valor especificado por la entidad regulatoria;
   iv. Proveer notificación de cualquier cambio de probabilidades/pagos o precios que ocurra mientras se está procesando una apuesta;
   v. Proveer al jugador con acceso a un registro de apuesta una vez que la apuesta es autorizada;
f) Procedimientos para el procesamiento de eventos cancelados y selecciones eliminadas para apuestas con múltiples eventos (ej. parlays), incluyendo reembolsar los jugadores que no fueron reembolsados automáticamente por el sistema (ej. apuestas colocadas de forma anónima); y
g) Procedimientos para la redención de apuestas ganadoras, incluyendo:

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

i. Escanear el código de barra de un cupón de apuesta (a través de un lector de código de barra o equivalente); o
ii. Ingresar manualmente el número de identificación de la apuesta y realizar la verificación con el sistema.

A.7.4 Seguridad y grabación

El local será requerido a instalar, mantener, y operar un sistema de seguridad que tenga la capacidad para monitorear y grabar continuamente vistas sin obstrucción de todas las transacciones de apuestas y financieras además de los despliegues visuales dinámicos de la información del juego. Se deben establecer procedimientos para asegurar que la grabación:

a) Cubre las areas de juego definidas con detalle suficiente para identificar cualquier discrepancia;
b) Es captada de forma que impida interferencia o el borrado;
c) Puede ser revisada por el operador y/o entidad regulatoria en caso de un reclamo/disputa del jugador; y
d) Es mantenida por al menos 90 días o según es requerido por la entidad regulatoria.

A.8 Procedimientos para el monitoreo

A.8.1 Monitoreo para colusión y fraude

El operador debe tomar medidas para reducir el riesgo de colusión o fraude, incluyendo establecer procedimientos para:

a) Identificar y/o rechazar apuestas sospechosas, las cuales podrían indicar trampas, manipulación, interferencia con el desarrollo normal de un evento, o violaciones de la integridad de cualquier evento en el que se colocaron apuestas;
b) Detectar razonablemente patrones irregulares o series de apuestas para prevenir colusión de jugadores o el uso deautorizado de sofware de jugador artificial; y
c) Monitorear y detectar eventos y/o irregularidades del volumen de operación o cambios en las probabilidades/pagos y precios que podrían indicar actividades sospechosas, además de todos los cambios de probabilidades/pagos y precios y/o suspensiones a lo largo de un evento.

A.8.2 Monitoreo contra el lavado de dinero (AML por sus siglas en inglés)

El operador debe establecer procedimientos y políticas AML, según es requerido por la entidad regulatoria, para asegurar que:

a) Los empleados son capacitados en AML, y este entrenamiento es mantenido actualizado;
b) Las cuentas del jugador son monitoreadas para ser abiertas y cerradas en un período muy breve y para depósitos y retiros sin transacciones de juego asociado; y
c) Transacciones agregadas en un período definido podrían requerir una comprobación más a fondo y deberían ser reportables a la organización relevante si exceden el límite prescrito por la entidad regulatoria.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

A.8.3 Monitoreo de proveedor del servicio de localización

Cuando es requerido por la entidad regulatoria, operadores que ofrecen el juego remoto, o proveedores de servicio de localización de terceros autorizados por la entidad regulatoria, deberán:

a) Establecer procedimientos para mantener una transmisión de datos en tiempo real de todas las comprobaciones de localización y una lista actualizada de riesgos potenciales de fraude de localización (ej. aplicaciones de localización falsa, máquinas virtuales, programas de PC remota, etc.);
b) Ofrecer un sistema de alerta para identificar el acceso indebido o sin autorización;
c) Permitir la auditoría periódica para evaluar y determinar su capacidad continua para detectar y mitigar los riesgos de fraude de localización emergentes;
d) Asegurar que el servicio de detección de localización o aplicación usada para la detección de localización:
    i. Utiliza bases de datos de código cerrado (IP, proxy, VPN, etc.) que son actualizadas frecuentemente y ensayadas periódicamente para su exactitud y confiabilidad; y
    ii. Es actualizado frecuentemente para mantener una recopilación avanzada de datos, la compatibilidad de los dispositivos, y la capacidad de prevención de fraude contra los riesgos de fraude de localización.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Anexo B: Auditoría Operacional de los Controles Técnicos de Seguridad

B.1 Introducción

B.1.1 Declaración General

Este anexo establece los controles técnicos de seguridad que serán revisados en una auditoría operacional como parte de la evaluación del sistema de apuestas de eventos, incluyendo, pero no limitado a, una evaluación del sistema de seguridad de información (ISS), revisión de los procesos operacionales que son críticos para el cumplimiento, pruebas de penetración enfocadas en la infraestructura externa e interna, además de las aplicaciones que transfieren, almacenan y/o procesan los datos del jugador y/o información confidencial, y cualquieras otros objetivos establecidos por la entidad regulatoria. Los controles de seguridad definidos en este anexo aplican a los siguientes componentes críticos del sistema.

a) Componentes que registran, almacenan, procesan, comparten, transmiten u obtienen información confidencial (ej. Números de validación, PINs, datos del jugador);
b) Componentes que generan, transmiten, o procesan los números aleatorios usados para determinar el resultado de los eventos virtuales (si es aplicable);
c) Componentes que almacenan los resultados o el estado actual de una apuesta del jugador;
d) Puntos de entrada y salida de los componentes mencionados anteriormente (otros sistemas con la capacidad para comunicarse directamente con los sistemas críticos principales); y
e) Redes de comunicación que transmiten información confidencial.

NOTA: También es reconocido que los controles técnicos de seguridad adicionales que no están incluidos específicamente en este estándar serán aplicables y requeridos para una auditoría operacional según es determinado por el operador y/o entidad regulatoria en sus normas, reglamentos, y estándares de controles internos mínimos (MICS).

B.2 Operación y seguridad del sistema

B.2.1 Procedimientos del sistema

El operador debe ser responsable de documentar y utilizar los procedimientos aplicables del sistema de apuestas de eventos. Estos procedimientos deben incluir lo siguiente como mínimo, según es requerido por la entidad regulatoria:

a) Procedimientos para monitorear los componentes críticos y la transmisión de datos del sistema completo, incluyendo la comunicación, paquetes de datos, redes, además de los componentes y la transmisión de datos de cualquier servicio de terceros utilizado, con el objetivo de asegurar la integridad, confiabilidad y disponibilidad;
b) Procedimientos y estándares de seguridad para el mantenimiento de todos los aspectos de seguridad del sistema para garantizar la comunicación segura y confiable, incluyendo la protección contra hacking o manipulación;

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

c) Procedimientos para definir, monitorear, documentar, y el reporte, investigación, respuesta, y resolución de incidentes de seguridad, incluyendo detectar el incumplimiento y posible o actual hacking o la manipulación del sistema;
d) Procedimiento para monitorear y ajustar la utilización de los recursos y mantener un registro del funcionamiento del sistema, incluyendo una función para compilar los informes del rendimiento;
e) Procedimientos para investigar, documentar y resolver el mal funcionamiento, incluyendo lo siguiente:
   i. Determinación de la causa del mal funcionamiento;
   ii. Revisión de los registros aplicables, reportes, archivos y registros de seguridad;
   iii. Restauración o reemplazo del componente crítico;
   iv. Verificación de la integridad del componente crítico antes de restablecer su operación;
   v. Completar un reporte del incidente para la entidad regulatoria documentando la fecha, hora y razón del mal funcionamiento con la fecha y hora de recuperación del sistema; y
   vi. Anular o cancelar las apuestas y pagos si una recuperación completa no es posible.

B.2.2 Ubicación física de los servidores

El servidor(es) del sistema de apuestas de eventos debe ser ubicado en una o más localización(es) seguras, y pueden ser ubicados en un solo local, o localizados remotamente fuera del local según es permitido por la entidad regulatoria. Adicionalmente, la localización(es) segura debe:

a) Tener suficiente protección contra la alteración, manipulación o acceso sin autorización;
b) Ser equipada con un sistema de seguridad que debe conformar con los procedimientos establecidos por la entidad regulatoria;
c) Estar protegida por perímetros de seguridad y controles de acceso adecuados para asegurar que el acceso está restringido a personal autorizado solamente y cualquier intento de acceso físico es registrado en un archivo seguro; y
d) Estar equipada con controles para proveer protección física contra daños a causa de incendio, inundación, huracán, terremoto y otras formas de desastre natural o artificial.

B.2.3 Control de acceso de lógica

El sistema de apuestas de eventos debe ser asegurado lógicamente contra el acceso sin autorización por credenciales de autenticación permitidas por la entidad regulatoria, tales como contraseñas, autenticación de múltiples factores, certificados digitales, biometría, y otros métodos de acceso (ej. cinta magnética, tarjetas de proximidad, tarjetas de chip integrado).

a) Cada usuario individual debe tener sus propias credenciales de autenticación, cuya provisión debe ser controlada por un proceso formal.
b) El registro de las credenciales de autenticación debe ser mantenido manualmente o por sistemas que registran automáticamente los cambios en la autenticación y fuerzan los cambios de las credenciales de autenticación.
c) El almacenamiento de las credenciales de autenticación debe ser seguro. Si las credenciales de autenticación son codificadas por hardware en un componente del sistema, estas deben ser encriptadas.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

d) Una solución alternativa para la autenticación fallida (ej. contraseña perdida) también debe ser segura, al igual que el método primario.
e) Credenciales de autenticación perdidas o comprometidas y las credenciales de autenticación de usuarios terminados deben ser desactivadas, aseguradas o eliminadas tan pronto como sea posible.
f) El sistema debe tener múltiples niveles de acceso de seguridad para controlar y restringir los diferentes tipos de acceso al servidor, incluyendo la visualización, cambio o eliminación de archivos críticos y directorios. Se deben establecer procedimientos para asignar, revisar, modificar, y eliminar los derechos de acceso y privilegios de cada usuario, incluyendo:
    i. La capacidad de la administración de cuentas de usuario para proporcionar una separación de funciones adecuada;
    ii. Limitación de usuarios que tienen los permisos requeridos para ajustar los parámetros críticos del sistema;
    iii. La aplicación de parámetros de credenciales de autenticación adecuados, así como longitud mínima y período de expiración; y
g) Se deben establecer procedimientos para identificar y marcar cuentas sospechosas que podrían incluir credenciales robadas.
h) Cualquier intento de acceso de lógica en las aplicaciones del sistema o sistemas operativos debe ser registrado en un archivo seguro.
i) El uso de utilidades que pueden invalidar los controles de la aplicación o sistema operativo debe ser restringido y controlado estrictamente.

NOTA: Cuando se utilizan contraseñas como credenciales de autenticación, se recomienda que estas sean cambiadas al menos una vez cada 90 días, tengan 8 caracteres de longitud e incluyan una combinación de dos de los criterios siguientes, como mínimo: letras mayúsculas, letras minúsculas, caracteres numéricos y/o especiales.

B.2.4 Autorización del usuario.

El sistema de apuestas de eventos debe implementar los siguientes requisitos de autorización del usuario:

a) Se debe utilizar un mecanismo seguro y controlado para verificar que el componente del sistema está siendo operado por solicitud de un usuario autorizado de forma regular según es requerido por la entidad regulatoria.
b) El uso de identificación automatizada del equipo para autenticar las conexiones desde localizaciones específicas y el equipo deben ser documentados y deben ser incluidos en la revisión de derechos de acceso y privilegios.
c) Cualquier dato de autorización comunicado por el sistema para el propósito de identificación debe ser obtenido en el momento de solicitud del sistema y no debe ser almacenado en el componente del sistema.
d) El sistema debe tener la capacidad para notificar el administrador del sistema y bloquear el usuario o hacer una entrada en el registro de auditoría, tras un número determinado de intentos de autorización sin éxito.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

B.2.5 Programación del servidor

El sistema de apuestas de eventos debe ser suficientemente seguro para prevenir la habilidad de programación iniciada por el usuario en el servidor que pueda resultar en modificaciones de la base de datos. Sin embargo, es aceptable que los administradores de la red o sistema realicen el mantenimiento autorizado de la infraestructura de la red o la resolución de problemas de la aplicación con derechos de acceso adecuados. El servidor también debe ser protegido contra la ejecución deasautorizada de código móvil.

B.2.6 Procedimientos de verificación

Se deben establecer procedimientos para verificar por solicitud que los componentes críticos del programa de control del sistema de apuestas de eventos en el entorno de producción son idénticos a los aprobados por la entidad regulatoria.

a) Las firmas digitales de los componentes críticos del programa de control deben ser obtenidas en el entorno de producción utilizando un proceso aprobado por la entidad regulatoria.
b) El proceso debe incluir una o más fases analíticas para comparar las firmas actuales de los componentes críticos del programa de control en el entorno de producción con las firmas de verificación de las versiones actualmente aprobadas de los componentes críticos del programa de control.
c) El resultado de este proceso debe ser almacenado en un formato inalterable, con detalles del resultado de la verificación de cada autenticación del programa de control crítico y:
    i. Ser registrado en un archivo del sistema o reporte que debe ser retenido por un período de 90 días o según es especificado por la entidad regulatoria;
    ii. Ser accesible por la entidad regulatoria en un formato que permitirá el análisis de los registros de verificación por la entidad regulatoria; y
    iii. Formar parte de los registros del sistema que serán recuperados en caso de un desastre o fallo del equipo o software.
d) Un fallo de comunicación de cualquier componente del sistema requerirá una notificación del fallo de autenticación siendo comunicada al operador y entidad regulatoria, según es requerido.
e) Se debe establecer un proceso para responder a fallos de autenticación, incluyendo determinar la causa del fallo y realizar las correcciones correspondientes o re-instalaciones requeridas de manera oportuna.

B.2.7 Sistema de retención de documentos electrónicos

Los reportes requeridos por este estándar y la entidad regulatoria pueden ser almacenados en un sistema de retención de documentos electrónicos, provisto que el sistema:

a) Está configurado correctamente para mantener la versión original junto con todas las versiones subsiguientes reflejando todos los cambios del reporte;
b) Mantiene una firma de verificación única para cada versión del reporte, incluyendo el original;
c) Puede retener y reportar un registro completo de cambios de todos los reportes incluyendo quien (identificación del usuario) realizó los cambios y cuando (fecha y hora);

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

d) Provee un método de indización para localizar e identificar el reporte fácilmente, incluyendo lo siguiente como mínimo (lo cual puede ser ingresado por el usuario):
   i. Fecha y hora en que el reporte fue generado;
   ii. Aplicación o sistema generando el reporte;
   iii. Título y descripción del reporte;
   iv. Identificación de usuario de la persona generando el reporte; y
   v. Cualquier otra información que pueda ayudar para la identificación del reporte y su propósito;
e) Está configurado para limitar el acceso para modificar o agregar reportes al sistema mediante la seguridad de lógica de cuentas de usuario específico;
f) Está configurado para proveer un registro de auditoría completo de toda la actividad de las cuentas de usuarios administrativos;
g) Está asegurado adecuadamente mediante el uso de medidas de seguridad de lógica (cuentas de usuario con acceso apropiado, niveles adecuados del registro de eventos, y documentación de control de la versión, etc.);
h) Está asegurado físicamente con todos los otros componentes críticos del sistema de apuestas de eventos; y
i) Está equipado para prevenir la interrupción de la disponibilidad del reporte y pérdida de datos mediante las mejores prácticas de redundancia de hardware y software, y procesos de respaldo.

B.2.8 Gestión del Equipo

Todo el equipo que aloja, procesa o comunica información confidencial, incluyendo el equipo que constituye el entorno operativo del sistema de apuestas de eventos y/o sus componentes, debe ser contabilizado y tener un propietario designado.

a) Se debe hacer y mantener un inventario de todo el equipo que contiene ítems controlados.
b) Se debe establecer un procedimiento para agregar equipo nuevo y remover equipo de servicio.
c) Se debe incluir una política sobre el uso aceptable del equipo asociado con el sistema y su ambiente operativo.
d) Cada equipo debe tener un "propietario" designado responsable para:
   i. Asegurar que la información y el equipo son clasificados adecuadamente en términos de su criticidad, sensibilidad, y valor; y
   ii. Definir y revisar periódicamente la restricción del acceso y clasificación.
e) Se debe establecer un procedimiento para asegurar que la contabilidad registrada del equipo es comparada con el equipo actual a los intervalos requeridos por la entidad regulatoria y se toman medidas adecuadas con respecto a las discrepancias.
f) Se puede implementar la protección contra copias para prevenir la duplicación desautorizada o modificación de software, provisto que:
   i. El método de protección contra copias es documentado por completo y provisto al laboratorio de pruebas independiente, para verificar que la protección funciona según lo provisto; o
   ii. El programa o componente responsable de aplicar la protección contra copias puede ser verificado individualmente por la metodología aprobada por la entidad regulatoria.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

B.3 Respaldo y Recuperación

B.3.1 Seguridad de datos

El sistema de apuestas de eventos debe proveer un método lógico para asegurar los datos del jugador y datos del juego, incluyendo la contabilidad, reportes, eventos significativos, u otra información confidencial, contra alteración, manipulación, o acceso sin autorización.

a) Se deben implementar métodos para el procesamiento correcto de datos, incluyendo la validación de entradas y el rechazo de datos corrompidos.
b) El número de estaciones de trabajo donde las aplicaciones críticas o bases de datos asociadas pueden ser accedidos será limitado.
c) Encriptación o protección de contraseña o seguridad equivalente debe ser utilizado para los archivos y directorios conteniendo los datos. Si la encriptación no es usada, el operador debe restringir la vista del contenido de dichos archivos y directorios para los usuarios, y como mínimo proporcionará la segregación de las funciones del sistema y responsabilidades además de monitorear y registrar el acceso en dichos archivos y directorios por cualquier persona.
d) La operación normal de todo el equipo que contiene la información no debe incluir ninguna opción o mecanismo que pueda compremeter los datos.
e) Ningún equipo debe tener un mecanismo en el que un error resultaría en el borrado automático de los datos.
f) Ningún equipo que mantiene los datos en su memoria debe permitir la retirada de la información, a menos que esta ha sido transferida a la base de datos u otro componente(s) seguro del sistema.
g) Los datos deben ser almacenados en areas del servidor que son encriptados y asegurados contra el acceso sin autorización, ambos externo e interno.
h) La bases de datos de producción conteniendo los datos debe formar parte de una red separada del servidor de cualquier interfaz del usuario.
i) Los datos deben ser mantenidos en todo momento independientemente de si el servidor tiene el suministro eléctrico.
j) Los datos deben ser almacenados de una forma para prevenir la pérdida de datos cuando se reemplazan las partes o módulos durante el mantenimiento normal.

B.3.2 Alteración de los datos

La alteración de los datos de contabilidad, reportes o eventos significativos no debe der permitida sin controles de acceso supervisado. En caso de cualquier cambio en los datos, la siguiente información debe ser documentada o registrada:

a) Número de identificación único para la alteración;
b) Elemento de datos alterado;
c) Valor del elemento de datos antes de la alteración;
d) Valor del elemento de datos después de la alteración;
e) Fecha y hora de la alteración; y
f) Personal que realizó la alteración (identificación del usuario).

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

B.3.3 Frequencia del respaldo

La implementación del plan de respaldo debe ocurrir al menos diariamente o según es especificado por la entidad regulatoria, sin embargo todos los métodos serán revisados caso por caso.

B.3.4 Respaldo de los medios de almacenamiento

Registros de auditoría, bases de datos del sistema, y cualquieras otros datos del jugador y datos de juego pertinentes deberán ser almacenados usando métodos de protección razonables. El sistema de apuestas de eventos debe ser diseñado para proteger la integridad de estos datos en el evento de un fallo. Copias redundantes de estos datos deben ser mantenidos en el sistema con soporte abierto para respaldos y restauración, de forma que ningún fallo de una sola parte del sistema pueda causar la pérdida o corrupción de datos.

a) El respaldo debe estar contenido en medios físicos no volátiles, o una implementación equivalente de la arquitectura, de forma que si los medios de almacenamiento primario fallan, las funciones del sistema y el proceso de auditoría de estas funciones puede continuar sin pérdida de los datos críticos.
b) Donde la entidad regulatoria permite el uso de plataformas de nube, si el respaldo está almacenado en una plataforma de nube, otra copia puede ser almacenada en una plataforma de nube diferente.
c) Si se utilizan unidades de disco duro como medios de respaldo, la integridad de los datos debe ser asegurada en el evento de un fallo del disco. Métodos aceptables incluyen, pero no están limitados a, múltiples discos duros en una configuración RAID aceptable, o duplicación de datos en dos o más discos duros.
d) Cuando el proceso de respaldo finaliza, los medios de respaldo son transferidos inmediatamente a una localización separada físicamente de la localización alojando los servidores y datos siendo respaldados (para almacenamiento temporario y permanente).
    i. La localización de almacenamiento es segura para prevenir el acceso sin autorización y provee protección adecuada para prevenir la pérdida permanente de los datos.
    ii. Los archivos de datos de respaldo y componentes de recuperación de datos deben ser gestionados con al menos el mismo nivel de seguridad y controles de acceso que el sistema.

NOTA: La distancia entre las dos localizaciones debe ser determinada basado en las amenazas y peligros ambientales potenciales, fallos del suministro eléctrico, y otras interrupciones pero también debería considerar las dificultades potenciales en la réplica de los datos, además de la capacidad para acceder el sitio de recuperación en un plazo razonable (Objetivo del tiempo de recuperación).

B.3.5 Fallo del sistema

El sistema de apuestas de eventos debe tener suficiente redundancia y modularidad de forma que si un solo componente o parte de un componente falla, las funciones del sistema y el proceso de auditoría de estas funciones puede continuar sin pérdida de los datos críticos. Cuando dos o más componentes están vinculados:

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

a) El proceso de todas las operaciones de juego entre los componentes no debe ser afectado negativamente por el reinicio o recuperación de ningún componente (ej. las transacciones no deben ser perdidas o duplicadas a causa de la recuperación de un componente o el otro); y
b) Después del reinicio o recuperación, los componentes deben sincronizar inmediatamente el estado de todas las transacciones, datos, y configuraciones el uno con el otro.

B.3.6 Contabilidad de reinicio maestro

El operador debe tener la habilidad para identificar y procesar correctamente situaciones en las que ha ocurrido un reinicio maestro de cualquier componente que afecta las operaciones de juego.

B.3.7 Requisitos para la recuperación

En caso de un fallo catastrófico en el que el sistema de apuestas de eventos no puede ser reiniciado de ninguna otra manera, debe ser posible restaurar el sistema desde el último punto de respaldo y recuperarlo por completo. El contenido de este respaldo debe incluir la siguiente información crítica incluyendo, pero no limitado a:

a) La información registrada especificada bajo la sección titulada “Información para ser Mantenida”;
b) Información específica del sitio o local, así como la configuración, cuentas de seguridad, etc.;
c) Claves actuales de encriptación del sistema; y
d) Cualquier otro parámetro del sistema, modificaciones, re-configuración (incluyendo sitios o locales participantes), adiciones, combinaciones, eliminaciones, ajustes y cambios de parámetro.

B.3.8 Soporte de sistema de alimentación ininterrumpida (UPS por sus siglas en inglés)

Todos los componentes del sistema deben ser provistos con alimentación primaria adecuada. Cuando el servidor es una aplicación independiente, este debe tener un sistema de alimentación ininterrumpida (UPS) conectado y debe tener suficiente capacidad para permitir un apagado correcto que retiene todos los datos del jugador y datos del juego durante una pérdida de energía. Es aceptable que el sistema sea un componente de una red que es soportada por un UPS para toda la red provisto que el servidor está incluido como un dispositivo protegido por el UPS. Se debe utilizar un sistema de protección de sobretensión si este no está incorporado en el UPS.

B.3.9 Plan de continuidad de operaciones y recuperación en caso de desastre

Se debe establecer un plan de continuidad de operaciones y recuperación en caso de desastre para reanudar las operaciones de juego si el entorno de producción del sistema de apuestas de eventos queda inoperable. El plan de continuidad de operaciones y recuperación en caso de desastre debe:

a) Incluir un método de almacenar los datos del jugador y del juego para minimizar las pérdidas. Si la reproducción asíncrona es utilizada, se debe describir el método para recuperar los datos o la pérdida potencial de datos debe ser documentada;
b) Definir las circunstancias por las cuales el plan será invocado;
c) Incluir el establecimiento de un sitio de recuperación físicamente separado del sitio de producción;

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

d) Contener guías de recuperación detallando las fases técnicas requeridas para restablecer la funcionalidad del juego en el sitio de recuperación; y
e) Incluir el proceso requerido para reanudar las operaciones administrativas de las actividades del juego después de la activación del sistema recuperado en varios escenarios adecuados para el contexto operacional del sistema.

B.4 Comunicaciones

B.4.1 Declaración General

En esta sección se discutirán los varios métodos de comunicación por cable e inalámbrica, incluyendo la comunicaciones realizadas sobre la internet o una red pública o de terceros, según es permitido por la entidad regulatoria.

B.4.2 Conectividad

Solamente los dispositivos autorizados deben ser permitidos establecer la comunicación entre cualquieras componentes del sistema. El sistema de apuestas de eventos debe proveer un método para:

a) Registrar y dar de baja los componentes del sistema;
b) Activar y desactivar componentes específicos del sistema;
c) Asegurar que solamente los componentes del sistema registrados y activados, incluyendo los dispositivos de juego, participan en las operaciones de juego; y
d) Asegurar que la condición pre-determinada para los componentes es de no registrado y desactivado.

B.4.3 Protocolo de comunicación

Cada componente del sistema de apuestas de eventos debe funcionar según es indicado por un protocolo de comunicación seguro documentado.

a) Todos los protocolos deben utilizar tecnología de comunicación que contiene mecanismos para la detección de errores y recuperación adecuada, la cual está diseñada para prevenir la intrusión, interferencia, intercepción y manipulación. Todas las implementaciones alternativas serán revisadas caso por caso y aprobadas por la entidad regulatoria.
b) Todas las comunicaciones de datos críticos para el juego o la gestión de la cuenta del jugador deben ser encriptadas y autenticadas.
c) La comunicación en la red segura solo debe ser posible entre componentes del sistema aprobados que han sido registrados y autenticados como válidos en la red. No se debe permitir la comunicación desautorizada entre componentes y/o puntos de acceso.

B.4.4 Comunicación sobre la Internet/ redes públicas

La comunicación entre todos los componentes del sistema, incluyendo dispositivos de juego, que es realizada sobre la internet/redes públicas, debe ser asegurada por un método aprobado por la

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

entidad regulatoria. Los datos del jugador, información confidencial, apuestas, resultados, información financiera, e información de las transacciones el jugador siempre deben ser encriptados sobre la internet/ red pública y protegida contra la transmisión incompleta, desvios erróneos, modificación de mensajes sin autorización, divulgación, duplicación o reproducción.

B.4.5 Comunicaciones de la red inalámbrica de area local (WLAN)

Las comunicaciones de la red inlámbrica de area local (WLAN), según es permitido por la entidad regulatoria, deben conformar con los requisitos jurisdiccionales aplicables específicos para los dispositivos inalámbricos y seguridad de la red. A falta de estándares jurisdiccionales específicos, los "Requisitos de dispositivos inalámbricos" y "Requisitos de seguridad de redes inalámbricas" en *GLI-26 Estándares de sistemas inalámbricos"* deberán ser usados según es aplicable.

NOTA: Es imperativo para los operadores revisar y actualizar las políticas de los controles internos y procedimientos para asegurar que la red es segura y las amenazas y vulnerabilidades son abordadas adecuadamente. Se recomienda la inspección periódica y verificación de integridad de la WLAN.

B.4.6 Gestión de seguridad de la red

Las redes deben ser separadas lógicamente de manera que no haya tráfico en un enlace de la red que no pueda ser mantenido por el anfitrión del enlace. Los siguientes requisitos aplican:

a) Todas las funciones de la gestión de la red deben autenticar todos los usuarios en la red y encriptar todas las comunicaciones de la gestión de la red.
b) El fallo de un solo ítem no debe resultar en la denegación de servicio.
c) Un sistema de detección de intrusión/sistema de prevención de intrusión (IDS/IPS) debe ser instalado en la red y recibir comunicaciones internas y externas, además de detectar o evitar:
    i. Ataques de denegación de servicio distribuido (DDOS);
    ii. Shellcode atravesando la red;
    iii. Spoofing del protocolo de resolución de direcciones (ARP); y
    iv. Otros indicadores de ataque de "Intermediarios" y cortar la comunicación inmediatamente si es detectado.
d) En adición a los requisitos en (c), un IDS/IPS instalado en la WLAN debe tener la capacidad para:
    i. Escanear la red para puntos de acceso clandestinos o desautorizados o dispositivos conectados en cualquier punto de acceso de la red por lo menos trimestralmente o según es definido por la entidad regulatoria;
    ii. Desactivar automáticamente cualquier dispositivo desautorizado o clandestino conectado al sistema; y
    iii. Mantener un registro del historial de todos los accesos inalámbricos por al menos los 90 días anteriores o según es especificado por la entidad regulatoria. Este registro debe contener información completa sobre todos los dispositivos inalámbricos en el sitio o local.
e) El equipo de comunicación de la red (NCE) debe cumplir con los requisitos siguientes:
    i. El NCE debe ser construido de forma que es resistente a daños físicos del hardware o corrupción del firmware/software contenido por el uso normal.
    ii. El NCE debe estar físicamente asegurado contra el acceso sin autorización.
    iii. Las comunicaciones del sistema vía el NCE deben ser lógicamente seguras contra el acceso sin

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

autorización.
iv. El NCE con almacenamiento limitado debe, si el registro de auditoría está lleno, desactivar toda la comunicación o descargar los registros en un servidor de registros dedicado.

f) Todos los núcleos de la red, servicios y puertos de conexión deben ser seguros para prevenir el acceso de la red sin autorización. Los servicios no usados y puertos no indispensables deben ser físicamente bloqueados o desactivados por software si es posible.
g) En entornos virtualizados, los servidores redundantes no deben ejecutar bajo el mismo hipervisor.
h) Protocolos sin estado, tales como el protocolo de datagramas de usuario (UDP), no deben ser usados para información confidencial sin transporte con estado. Por favor tome nota que aunque el protocolo de transporte de hipertexto (HTTP) es técnicamente sin estado, cuando es ejecutado en el protocolo de control de transmisión (TCP) el cual es con estado, esto es permitido.
i) Todos los cambios en la infraestructura de la red (ej. configuración del equipo de comunicación de la red) deben ser registrados.
j) Detectores de virus y/o programas de detección deben ser instalados en todos los sistemas. Estos programas deben ser actualizados regularmente para escanear para nuevas variedades de virus.

B.5 Proveedores de servicios de terceros

B.5.1 Comunicación de terceros

Cuando se implementa la comunicación con proveedores de terceros, así como programas de fidelidad del jugador, servicios financieros (bancos, procesadores de pagos, etc.), proveedores del servicio de localización, proveedores del servicio de la nube, servicio de estadísticas/línea, y servicios de verificación de identidad, los siguientes requisitos aplican:

a) El sistema de apuestas de eventos debe tener la capacidad para la comunicación segura con proveedores de servicio de terceros usando encriptación y autenticación fuerte.
b) Todos los eventos de registro involucrando servicios de terceros debe ser registrado en en archivo de auditoría.
c) La comunicación con proveedores de servicio de terceros no debe interferir o deteriorar las funciones normales del sistema de apuestas de eventos.
   i. Los datos de proveedores de servicio de terceros no deben afectar la comunicación del jugador.
   ii. Las conexiones con los proveedores de servicio de terceros no deben usar la misma infraestructura de la red que las conexiones del jugador.
   iii. El juego debe ser desactivado en todas las conexiones de la red excepto la red del jugador;
   iv. El sistema no debe enviar paquetes de datos de proveedores de servicio de terceros directamente a la red del jugador y viceversa
   v. El sistema no debe actuar como un enrutador de IP entre las redes y proveedores de servicio de terceros.
d) Todas las transacciones financieras deben ser reconciliadas con instituciones financieras y procesadores de pagos diariamente o según es especificado por la entidad regulatoria.

B.5.2 Servicios de terceros

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Las funciones de seguridad y responsabilidades de proveedores de servicio de terceros deben ser definidos y documentados según es requerido por la entidad regulatoria. El operador debe establecer políticas y procedimientos para gestionarlas y monitorear su cumplimiento con los requisitos de seguridad aplicables:

a) Los acuerdos con proveedores de servicio de terceros que incluyen el acceso, procesamiento, comunicación o gestión del sistema y/o sus componentes, o agregan productos o servicios en el sistema y/o sus componentes deben cubrir todos los requisitos de seguridad aplicables.
b) Los servicios, reportes y registros provistos por los proveedores de servicio de terceros deben ser monitoreados y revisados anualmente o según es requerido por la entidad regulatoria.
c) Cambios en la provisión de proveedores de servicio de terceros, incluyendo mantener y mejorar la política de seguridad existente, procedimientos y controles, deben ser gestionados considerando la criticalidad de los sistemas y procesos incluidos y la re-evaluación de riesgos.
d) Los derechos de acceso de los proveedores de servicio de terceros en el sistema y/o sus componentes deben ser removidos después de la terminación del contrato o acuerdo o ajustados después de un cambio.

B.6 Controles técnicos

B.6.1 Requisitos del servicio de nombre de dominio (DNS)

Los siguientes requisitos aplican a los servidores usados para resolver las consultas del servicio de nombre de dominio (DNS) usadas en asociación con el sistema de apuestas de eventos.

a) El operador debe utilizar un servidor DNS primario seguro y un servidor DNS secundario seguro que están separados lógicamente y físicamente el uno del otro.
b) El servidor DNS primario debe estar físicamente ubicado en un centro de datos seguro o un anfitrión virtualizado en un hipervisor asegurado adecuadamente o equivalente.
c) El acceso físico y de lógica en el servidor(es) DNS debe ser restringido al personal autorizado.
d) No se deben permitir las transferencias de zona hacia anfitriones arbitrarios.
e) Un método para prevenir el envenenamiento de caché, así como extensiones de seguridad DNS (DNSSEC), es requerido.
f) Se debe establecer la autenticación de múltiples factores.
g) Se debe establecer el bloqueo de registro, de manera que cualquier solicitud para cambiar el servidor(es) deberá ser verificada manualmente.

B.6.2 Controles criptográficos

Una política sobre el uso de controles criptográficos para la protección de información debe ser desarrollada e implementada.

a) Todos los datos del jugador y/o información confidencial deben ser encriptados si atraviesan una red con un nivel de confianza menor.
b) Datos que no requieren ser ocultados pero que serán autenticados deberán usar algún tipo de tecnología de autenticación de mensajes.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

c) La autenticación debe utilizar un certificado de seguridad de una organización aprobada.
d) El nivel de encriptación usado debe ser adecuado para la sensibilidad de los datos.
e) El uso de algoritmos de encriptación debe ser revisado periódicamente para verificar que los algoritmos de encriptación actuales son seguros.
f) Se deben implementar cambios en los algoritmos de encriptación para corregir deficiencias cuanto antes posible. Si estos cambios no están disponibles, el algoritmo debe ser reemplazado.
g) Las claves de encriptación deben ser mantenidas en un medio de almacenamiento seguro y redundante después de que las mismas hayan sido encriptadas por un método de encriptación diferente y/o usando una clave de encriptación diferente.

B.6.3 Gestión de la clave de encriptación

La gestión de las claves de encriptación debe utilizar procesos específicos establecidos por el operador y/o entidad regulatoria. Estos procesos específicos deben cubrir lo siguiente:

a) Obtener o generar claves de encriptación y almacenarlas;
b) Gestión de expiración de las claves de encriptación, si es aplicable;
c) Revocar claves de encriptación;
d) Cambio seguro del conjunto de claves de encriptación; y
e) Recuperar datos encriptados con una clave de encriptación revocada o expirada durante un período específico después que la clave de encriptación queda invalidada.

B.7 Acceso remoto y firewalls

B.7.1 Seguridad de acceso remoto

Acceso remoto es definido como cualquier acceso desde fuera del sistema o red del sistema incluyendo el acceso desde otras redes en el mismo sitio o local. El acceso remoto solo será permitido si es autorizado por la entidad regulatoria y deberá:

a) Ser realizado vía un método seguro;
b) Tener la opción para ser desactivado;
c) Aceptar solamente las conexiones remotas permitidas por la aplicación de firewall (cortafuegos) y la configuración del sistema;
d) Ser limitado a únicamente las funciones de la aplicación necesarias para que los usuarios desempeñen sus funciones de trabajo:
    i. Ninguna funcionalidad remota de administración del usuario sin autorización (agregando usuarios, cambio de permisos, etc.) es permitida; y
    ii. Esta prohibido el acceso sin autorización al sistema operativo o a cualquier base de datos aparte de para obtener información utilizando las funciones existentes.

NOTA: La seguridad del acceso remoto será revisada caso por caso, en conjunto con la implementación de la tecnología actual y aprobación de la entidad regulatoria.

B.7.2 Procedimientos de acceso remoto y cuentas del cliente

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Se debe establecer un procedimiento para el acceso remoto estrictamente controlado. Es reconocido que según es requerido el proveedor puede acceder el sistema y sus componentes asociados remotamente para el soporte del producto y del usuario o actualización/mejoras, según es permitido por la entidad regulatoria y el operador. Este acceso remoto debe utilizar cuentas del cliente específicas que son:

a) Monitoreadas continuamente por el operador;
b) Desactivadas cuando no están en uso; y
c) Restringidas por controles lógicos de seguridad para acceder solamente la aplicación(es) y/o base(s) de datos para el soporte del producto y usuario o proveer actualizaciones/mejoras.

B.7.3 Registro de actividad del acceso remoto

La aplicación del acceso remoto debe mantener un registro de actividad que se actualiza automáticamente presentando toda la información de acceso remoto, incluyendo:

a) Identificación del usuario(s) que realizó y/o autorizó el acceso remoto;
b) Direcciones IP remotas, números de puerto, protocolos, y donde sea posible, direcciones MAC;
c) Fecha y hora en que se realizó la conexión y la duración de la conexión; y
d) Actividad durante la sesión, incluyendo las areas específicas accedidas y los cambios realizados.

B.7.4 Firewalls

Todas las comunicaciones, incluyendo el acceso remoto, deben pasar por al menos un firewall (cortafuegos) aprobado al nivel de la aplicación. Esto incluye las conexiones hacia y desde cualquier anfitrión no del sistema usado por el operador.

a) El firewall debe estar localizado en el límite entre dos dominios de seguridad disimilares.
b) Un dispositivo en el mismo dominio de transmisión que el anfitrión del sistema no debe tener una utilidad que permita establecer una ruta alternativa para la red que eluda el firewall.
c) Cualquier ruta alternativa de la red que existe para el propósito de redundancia también debe pasar a través de por lo menos un firewall a nivel de aplicación.
d) Solamente aplicaciones relacionadas al firewall pueden residir en el firewall.
e) Solamente un número limitado de cuentas de usuario pueden estar presentes en el firewall (ej. administradores de la red o sistema solamente).
f) El firewall debe rechazar todas las conexiones excepto aquellas que han sido aprobadas específicamente.
g) El firewall debe rechazar todas las conexiones desde localizaciones que no deben residir en la red en la que el sistema originó (ej. direcciones RFC1918 en el lado público de un firewall de la internet).
h) El firewall solo debe permitir el acceso remoto sobre el protocolo de encriptación más reciente.

B.7.5 Registros de auditoría de firewall

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

La aplicación firewall debe mantener un registro de auditoría y debe desactivar todas las comunicaciones y generar un error si el registro de auditoría está lleno. El registro de auditoría debe contener:

a) Todos los cambios en la configuración del firewall;
b) Todos los intentos de conexión con éxito y sin éxito a través del firewall; y
c) Las direcciones IP de origen y destino, números de puertos, protocolos, y si es posible, direcciones MAC.

NOTA: Un parámetro configurable 'intentos de conexión sin éxito' puede ser utilizado para denegar más solicitudes de conexión cuando se excede el límite pre-determinado. El administrador del sistema también debe ser notificado.

B.7.6 Revisión de las reglas del firewall

Si es requerido por la entidad regulatoria, las reglas del firewall deben ser revisadas periódicamente para verificar las condiciones operativas del firewall y la efectividad de su configuración de seguridad y conjunto de reglas y esto debe ser realizado en todos los firewalls del perímetro y los firewalls internos.

B.8 Gestión de cambio

B.8.1 Declaración general

La política de gestión de cambio es seleccionada por la entidad regulatoria para procesar la actualización del sistema de apuestas de eventos y sus componentes basado en la propensidad para frecuentes mejoras en el sistema y la tolerancia de riesgos seleccionada. Para sistemas que requieren actualizaciones con frecuencia, un programa de gestión de cambios basado en riesgo puede ser utilizado para mejorar la eficiencia de la actualización. Los programas de gestión de cambio basados en riesgo típicamente incluyen una categorización de los cambios propuestos basado en el impacto regulatorio y definen los procedimientos de certificación asociados para cada categoría. El laboratorio independiente de pruebas evaluará el sistema y las modificaciones futuras conforme con la política de gestión de cambio seleccionada por la entidad regulatoria.

B.8.2 Procedimiento de control de cambios del programa

El procedimiento de control de cambios del programa debe ser adecuado para asegurar que solo versiones de programas autorizadas son implementadas en el entorno de producción. Estos controles de cambios deben incluir:

a) Un control de versión de software adecuado o mecanismo para todos los componentes de software y código fuente;
b) Mantener registros de todas las instalaciones nuevas y/o modificaciones en el sistema, incluyendo:
   i. La fecha de la instalación o modificación;
   ii. Detalles del motivo o carácter de la instalación o cambio, ej. software nuevo, reparación del

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

servidor, modificaciones significantes de la configuración;
iii. Una descripción del procedimiento requerido para poner en servicio el componente nuevo o modificado (conversión o entrada de datos, procedimiento para la instalación, etc.);
iv. La identidad del usuario(s) realizando la instalación o modificación;

c) Una estrategia para revertir a la última implementación (rollback o plan de reducción) si la instalación no tiene éxito, incluyendo el respaldo completo de versiones previas de software y un ensayo del plan de reducción antes de la implementación del entorno de reducción;
d) Una política que incluye procedimientos para cambios de emergencia;
e) Procedimientos para los ensayos y migración de cambios;
f) Segregación de funciones entre los desarrolladores, equipo de control de calidad, equipo de la migración y los usuarios; y
g) Procedimientos para asegurar que la documentación técnica y del usuario es actualizada como resultado del cambio.

B.8.3 Ciclo de vida de desarrollo de software

La adquisición y desarrollo de software nuevo debe utilizar procesos específicos establecidos por el operador y/o entidad regulatoria.

a) El entorno de producción debe estar separado lógicamente y físicamente de los entornos de desarrollo y ensayos. Cuando las plataformas de la nube son usadas, no puede existir una conexión directa entre el entorno de producción y ningún otro entorno.
b) El personal de desarrollo debe ser excluido del acceso para promover cambios del código en el entorno de producción.
c) Se debe establecer un método documentado para verificar que el software de ensayos no es desplegado en el entorno de producción.
d) Para prevenir la pérdida de información confidencial, se debe establecer un método documentado para asegurar que los datos primarios de producción no son usados en los ensayos.
e) Toda la documentación relacionada con el desarrolo de la aplicación y software debe estar disponible y ser mantenida por la duración de su ciclo de vida.

B.8.4 Parches de actualización

Todos los parches deben ser ensayados cuando sea posible en un entorno de desarrollo y ensayos configurado idénticamente al entorno de producción objetivo. Bajo circunstancias en las que el parche no puede ser ensayado por completo a tiempo para cumplir con el plazo para el nivel de severidad de la alerta y si es autorizado por la entidad regulatoria, los ensayos del parche deben ser gestionados para el riesgo, ya sea por aislamiento o removiendo el componente no ensayado de la red o aplicando el parche y ensayándolo después.

B.9 Pruebas de seguridad periódicas

B.9.1 Pruebas técnicas de seguridad

Se deben realizar pruebas técnicas de seguridad periódicamente en el entorno de producción según es requerido por la entidad regulatoria para garantizar que no existen vulnerabilidades poniendo en

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

riesgo la seguridad y operación de los sistemas de apuestas de eventos. Estos ensayos deben consistir de un método de evaluación de seguridad mediante una simulación de ataque por terceros utilizando una metodología reconocida, y el análisis de vulnerabilidades consistirá en la identificación y cuantificación pasiva de los riesgos potenciales del sistema. Intentos de acceso sin autorización deben ser realizados hasta en el nivel de acceso más alto posible y deben ser completados con y sin las credenciales de autenticación disponibles (ensayos de tipo caja blanca/caja negra). Estos permiten hacer las evaluaciones de los sistemas operativos y configuraciones de hardware, incluyendo pero no limitado a:

a) Escaneo de puertos UDP/TCP;
b) Identificación de pila y predicción de secuencia TCP para identificar sistemas operativos y servicios;
c) Apropiación de anuncio de servicio público;
d) Escaneo de la Web usando escáners de vulnerabilidad HTTP y HTTPS; y
e) Escaneo de enrutadores usando el protocolo de encaminamiento BGP (Border Gateway Protocol), protocolo de multidifusión de encaminamiento BGMP (Border Gateway Multicast Protocol) y protocolo simple de administración de red SNMP (Simple Network Management Protocol).

B.9.2 Evaluación de vulnerabilidad

El propósito de la evaluación de vulnerabilidad es para identificar vulnerabilidades, de las cuales se podrían aprovechar más tarde durante las pruebas de penetración haciendo consultas básicas con relación a los servicios ejecutando en los sistemas en cuestión. La evaluación debe incluir al menos las siguientes actividades:

a) Evaluación de vulnerabilidad externa – El objetivo son los dispositivos de la red y servidores que son accesibles por terceros (ya sea una persona o una empresa), por medio de una dirección IP pública (expuesta públicamente), relacionada al sistema desde el cual es posible acceder información confidencial.
b) Evaluación de vulnerabilidad interna – El objetivo son los servidores comunicados hacia el interior (en el DMZ, o en el LAN si no existe un DMZ) relacionados al sistema desde el cual es posible acceder la información confidencial. Los ensayos de cada dominio de seguridad en la red interna deben ser realizados por separado.

B.9.3 Pruebas de penetración

El propósito de las pruebas de penetración es para aprovecharse de cualquier vulnerabilidad descubierta durante la evaluación de vulnerabilidad en cualquier aplicación expuesta públicamente o sistema anfitrión de aplicaciones que procesan, transmiten y/o almacenan información confidencial. Las pruebas de penetración incluyen las siguientes actividades como mínimo:

a) Pruebas de penetración de niveles de la red – Esta prueba imita las acciones de un atacante actual aprovechándose de las deficiencias en la seguridad de la red y examina los sistemas para cualquier deficiencia que podría ser usada por un atacante externo para perturbar la confidencialidad, disponibilidad y/o integridad de la red.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

b) Pruebas de penetración de niveles de la aplicación – Esta prueba usa utilidades para identificar deficiencias en las aplicaciones con escaneos autenticados y no autenticados, análisis de los resultados para remover positivos falsos, y pruebas manuales para confirmar los resultados de las utilidades y para identificar el impacto de las deficiencias.

B.9.4 Auditoría del sistema de gestión de seguridad de información (ISMS)

La auditoría del sistema de gestión de seguridad de información (ISMS) debe ser realizada, incluyendo todas las localizaciones donde información confidencial es accedida, procesada, transmitida y/o almacenada. El ISMS será revisado conforme con criterios comunes de seguridad de información en relación a la confidencialidad, integridad y disponibilidad, así como los recursos siguientes o equivalente:

a) ISO/IEC 27001 Sistemas de gestión de seguridad de información (ISMS);
b) Estándares de seguridad de datos en la industria de tarjetas de pago (PCI-DSS); y
c) Estándares de control de la asociación de lotería del mundo (WLA-SCS).

B.9.5 Auditoría del servicio de la nube

Un operador utilizando un proveedor de servicio de la nube (CSP), según es permitido por la entidad regulatoria, para almacenar, transmitir o procesar información confidencial debe ser sometido a una auditoría específica según es requerido por la entidad regulatoria. El CSP será revisado conforme con criterios comunes de seguridad de información relacionados con la provisión y uso de los servicios de la nube, así como ISO/IEC 27017 y ISO/IEC 27018, o equivalente.

a) Si la información confidencial es almacenada, procesada o transmitida en un entorno de la nube, los requisitos pertinentes aplicarán en este entorno, y típicamente consistirán en la validación de la infraestructura CSP y el uso de este entorno por el operador.
b) La designación de responsabilidades entre el CSP y el operador para gestionar los controles de seguridad no excluyen al operador para garantizar que la información confidencial es adecuadamente segura conforme con los requisitos aplicables.
c) El CSP y el operador deben estar de acuerdo con la política y procedimientos transparentes para todos los requisitos de seguridad, y las responsabilidades para la operación, gestión y reportes deben ser claramente definidas y entendidas para cada requisito aplicable.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Glosario de términos clave

Acceso remoto – Cualquier acceso desde fuera del sistema o red del sistema incluyendo el acceso desde otras redes en el mismo sitio o local.

Acceso sin autorización – Una persona que obtiene acceso físico o acceso de lógica sin permiso en una red, sistema, aplicación, datos, u otro recurso.

Administrador del sistema – El individuo(s) responsable para mantener la operación estable del sistema de apuestas de eventos (incluyendo la infraestructura de software y hardware y el software de la aplicación).

Afiliciación de Grupo – Un método de organizar las cuentas de usuarios en una sola unidad (por posición de trabajo) por lo que el acceso a las funciones del sistema puede ser modificado al nivel de la unidad y los cambios se efectúan para todas las cuentas de usuarios asignadas a la unidad.

Algoritmo – Un conjunto finito de instrucciones inequívocas realizadas en una secuencia definida para alcanzar un objetivo, especialmente una regla matemática o procedimiento utilizado en el cálculo de un resultado deseado. Los algoritmos son la base de la mayoría de los programas de computadora.

Algoritmo hash – Una función que convierte una secuencia de datos resultando en una secuencia alfanumérica de longitud fija.

Amenaza – Cualquier circunstancia o evento con el potencial para afectar negativamente las operaciones de la red (incluyendo la misión, funciones, imagen, o reputación), activos, o individuos a través de un sistema vía el acceso desautorizado, destrucción, divulgación, modificación de información, y/o denegación de servicio. En adición, el potencial de una fuente de amenazas para explotar con éxito una vulnerabilidad del sistema.

Apuesta – Cualquier compromiso de créditos o dinero por el jugador sobre los resultados de eventos.

Apuesta Antes/Después – Una apuesta que fue colocada después que el resultado del juego ha sido aceptado o después que el participante seleccionado ha obtenido una ventaja material (ej. una puntuación).

Apuesta en juego – Una apuesta que es colocada mientras un evento está en progreso o actualmente ocurriendo.

Apuestas de Eventos – Las apuestas sobre deportes, competiciones, partidos, y otro tipo de eventos aprobados por la entidad regulatoria en los que el jugador coloca apuestas en mercados dentro del evento.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Apuestas de eventos virtuales – Una forma de juego que permite colocar apuestas sobre deportes, competiciones, y partidos cuyos resultados son determinados únicamente por un generador de números aleatorios (RNG).

Apuestas de probabilidades fijas – Tipo de apuestas en las que el pago se fija al mismo tiempo que la apuesta es colocada. Si las predicciones son correctas, las probabilidades primero son multiplicadas entre sí y después por la cantidad de la apuesta.

Apuestas Pari-Mutuel – Tipos de apuestas en los que las apuestas individuales son recolectadas en un fondo. Las ganancias son calculadas compartiendo el fondo entre todas las apuestas ganadoras.

Apuestas remotas – Apuestas realizadas utilizando dispositivos de juego remoto en una red inalámbrica en el local o a través de la internet, dependiendo en la implementación(es) autorizadas por la entidad regulatoria.

ARP, *Protocolo de resolución de direcciones* – El protocolo usado para traducir direcciones IP a direcciones MAC para soportar la comunicación en una red de area local conectada por cable o inalámbrica.

Ataque de "intermediarios" – Un ataque en el que el atacante secretamente envía y posiblemente altera la comunicación entre dos partes que consideran que se están comunicando directamente una con otra.

Autenticación – Verificación de la identidad de un usuario, proceso, paquete de software, o dispositivo, a menudo como un requerimiento para permitir el acceso a los recursos del sistema.

Autenticación de múltiples factores – Un tipo de autenticación que utliza dos o más de lo siguiente para verificar la identidad del usuario: Información conocida solamente por el usuario (ej. una contraseña, patrón o respuesta a una pregunta de seguridad); Un ítem en posesión del usuario (ej. una ficha electrónica, ficha física o tarjeta de identificación); Los datos biométricos del usuario (ej. huellas digitales, reconocimiento facial o de voz).

Autenticación del mensaje – Una medida de seguridad usada para establecer la autenticidad de un mensaje por medio de un autenticador en la transmisión derivado de ciertos elementos predeterminados del mensaje mismo.

Biometría – Una forma de identificación biológica, así como huellas digitales o patrones de la retina.

Bluetooth – Un protocolo de comunicación inalámbrica de corto alcance y baja potencia utilizado para la interconexión de teléfonos celulares, computadoras, y otros dispositivos electrónicos, incluyendo dispositivos de juego. Las conexiones de Bluetooth típicamente operan sobre distancias de 10 metros o menos y son basadas en ondas de radio para transmitir los datos a través del aire.

Boleto – Un instrumento de juego que puede ser redimido en efectivo o usado subsecuentemente para redimir por créditos.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Certificado de seguridad – Información, a menudo guardada en un archivo de texto, que es utilizada por el protocolo TSL (seguridad de capa de transporte) para establecer una conexión segura. Un certificado de seguridad contiene información acerca de a quien pertenece, quien lo emitió, fechas válidas, un número de serie único u otra identificación única que puede ser usada para verificar el contenido del certificado. Para que una conexión TSL pueda ser creada, los dos lados deben tener un Certificado de Seguridad válido, también conocido como un ID digital.

Clave – Un valor usado para controlar las operaciones criptográficas, tales como el cifrado, descifrado, generación de la firma o verificación de la firma.

Clave de encriptación – Una clave criptográfica que ha sido cifrada para ocultar el valor del texto simple subyacente.

Código de barra – Una representación óptica de los datos que es legible por máquina. Un ejemplo de código de barra es hallado en los cupones de apuesta impresos.

Código móvil – Código ejecutable que se traslada de computadora a computadora, incluyendo ambos código legítimo y código malicioso, así como un virus informático.

Comisión – Una cantidad retenida y no distribuida por el operador de la cantidad total apostada en un evento.

Componente crítico – Cualquier sub-sistema en el que un fallo o compromiso puede resultar en la pérdida de derechos del jugador, ingresos del gobierno o acceso sin autorización a los datos usados para generar reportes para la entidad regulatoria.

Contraseña – Una línea de caracteres (letras, números, y otros símbolos) usados para autenticar la identidad o para verificar la autorización del acceso.

Control de versión – El método por el cual se verifica que un sistema de apuestas de eventos aprobado en desarrollo está funcionando en estado aprobado.

Control del acceso – El proceso de conceder o denegar solicitudes específicas para obtener y utilizar la información confidencial y servicios asociados específicos del sistema; y para entrar físicamente en facilidades específicas que alojan la infraestructura crítica de la red o sistema.

Copia de seguridad – Una copia de los archivos y programas obtenida para facilitar la recuperación si es necesario.

Cuenta del jugador (también conocida como “Cuenta de juego”) **–** Una cuenta mantenida para un jugador en la que se registra la información relacionada con transacciones de juego y financieras en nombre del jugador incluyendo, pero no limitado a, depósitos, retiros, apuestas, ganancias, y ajustes del balance. El término no incluye una cuenta utilizada únicamente por el operador para rastrear puntos promocionales o créditos, o beneficios similares otorgados por el operador a un jugador, los cuales pueden ser redimidos por mercancía y/o servicios.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Cuota – Un valor que establece el pago potencial de una apuesta (ej. línea de cuota + 175) o las condiciones para que una apuesta sea ganadora o perdedora (ej. Margen de puntos + 2.5).

Cupón – Un instrumento de juego que es usado principalmente para propósitos promocionales y que puede ser redimido por créditos restringidos o no restringidos.

Datos del jugador – Información confidencial con respecto a un jugador y que puede incluir ítems tales como el nombre y apellidos, fecha de nacimiento, lugar de nacimiento, número de seguridad social, dirección, número de teléfono, historial médico o laboral, u otra información personal según es definido por la entida regulatoria.

DDOS, *Denegación de servicio distribuido* – Un tipo de ataque en el que múltiples sistemas comprometidos, usualmente infectados con un programa de software destructivo, son usados con el objetivo de un solo sistema. Las víctimas de un ataque DDOS consisten en ambos el sistema objetivo final y todos los sistemas utilizados maliciosamente y controlados por el hacker en el ataque distibuido.

Dirección IP, *Dirección del protocolo de Internet* – Un número para una única computadora que es usado para determinar a donde se deben enviar los mensajes transmitidos en la Internet. La dirección IP es análoga al número de un domicilio para el correo postal regular.

Dispositivo de juego remoto – Un dispositivo propietario del jugador operado en una red inalámbrica en el local o a través de la internet que como mínimo será utilizado para la ejecución o formalización de las apuestas colocadas por un jugador directamente. Ejemplos de un dispositivo de juego remoto incluyen una computadora (PC), teléfono móvil, tableta, etc.

Dispositivo de juego – Un dispositivo electrónico que convierte la comunicación del sistema de apuestas de eventos de forma que pueda ser interpretada por una persona y convierte las decisiones de una persona en un formato de comunicación entendido por el sistema de apuestas de eventos.

Dispositivo de juego de autoservicio – Un kiosco que como mínimo será utilizado para la ejecución o formalización de las apuestas colocadas por un jugador directamente y, si es soportado, puede ser usado para la redención de cupones de apuestas ganadoras.

Dispositivo de juego POS, *Dispositivo de juego- terminal de venta* – Una estación del asistente que por lo mínimo será usada por un asistente para la ejecución o formalización de apuestas colocadas en nombre del jugador.

Dividendo – La cantidad correspondiente al ganador de una apuesta pari-mutuel.

DNS, *Servicio de nombre de dominio* – La base de datos de la internet distribuida globalmente, la cual (entre otras cosas) mapea los nombres de la máquina a números de IP y vice-versa.

Dominio – Un grupo de computadoras y dispositivos en la red que son administrados como una unidad con reglas comunes y procedimientos.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

DRP, *Plan de recuperación de desastres* – Un plan para procesar aplicaciones críticas y prevenir la pérdida de datos en el evento de un fallo grave de hardware o software o destrucción de las facilidades.

Encriptación – La conversión de datos en una forma, llamada texto cifrado, que no puede ser entendida fácilmente por personas sin autorización.

Envenenamiento de caché – Un ataque en el que el atacante ingresa datos corruptos en la base de datos del caché del servicio de nombre del dominio (DNS).

Escáner de virus – Software usada para prevenir, detectar y remover viruses informáticos, incluyendo malware, gusanos y caballos de Troya.

Evento – Ocurrencia relacionada con deportes, competiciones, partidos, y otro tipo de actividades aprobadas por la entidad regulatoria sobre la que se pueden colocar apuestas.

Firewall (Cortafuegos) – Un componente de un sistema de computadoras o de la red que está diseñado para bloquear el acceso desautorizado o tráfico, al mismo tiempo permitiendo la comunicación hacia el exterior.

Geolocalización – Identificación de la localización geográfica en el mundo real de un dispositivo de juego remoto conectado en la internet.

Gestión de Claves – Actividades que consisten en el procesamiento de claves criptográficas y otros parámetros de seguridad relacionados (ej. contraseñas) durante el ciclo de vida entero de las claves, incluyendo su generación, almacenamiento, establecimiento, entrada y salida, y función de 'zeroize'.

HTTP, *Protocolo de transferencia de hipertexto* – El protocolo base utilizado para definir como los mensajes son formateados y transmitidos, y que acciones los servidores y navegadores deben adoptar en respuesta a varios comandos.

IDS/IPS, *Sistema de detección de intrusión/Sistema de prevención de intrusión* – Un sistema que inspecciona toda la actividad entrante y saliente de la red e identifica patrones sospechosos que pueden indicar un ataque de la red o sistema por alguien intentando acceder o comprometer el sistema. La detección de intrusión es usada para la seguridad de computadoras y se refiere al proceso de monitorear las actividades de la computadora y la red y analizar estos eventos para buscar indicaciones de intrusión en el sistema.

Impresora – Un periférico del dispositivo de juego que imprime los cupones de apuestas y/o instrumentos de juego.

Información confidencial – Información así como los datos del jugador, datos del juego, números de validación, PINs, contraseñas, semillas y claves seguras, y otros datos que deben ser procesados de forma segura.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Instrumento de juego – Una representación de valor impresa o virtual, aparte de una ficha o vale incluyendo cupones y boletos. Un instrumento de juego virtual es una clave electrónica intercambiada entre un dispositivo móvil del jugador y el dispositivo de juego que es usado para la inserción y redención de crédito.

Integridad de los datos – Propiedad de que los datos son exactos y consistentes y no han sido alterados de forma desautorizada durante el procesamiento, y en tránsito.

Interfaz del usuario – Una aplicación de interfaz o programa a través del cual el usuario ve y/o interactúa con el software de juego para comunicar sus acciones al sistema de apuestas de eventos.

Internet – Un sistema de redes interconectadas que conecta computadoras en todo el mundo vía TCP/IP.

Jailbreaking (liberación) – Modificación de un teléfono inteligente u otro dispositivo electrónico para remover las restricciones impuestas por el fabricante u operador y permitir la instalación de software desautorizado.

Lector de código de barra – Un dispositivo que tiene la capacidad para leer o interpretar un código de barra. Esto puede aplicar a algunos teléfonos inteligentes u otros dispositivos electrónicos que pueden ejecutar una aplicación para leer el código de barra.

MAC, *Código de autenticación de mensaje* – Una suma de control criptográfica sobre los datos que utiliza una clave simétrica para detectar modificaciones, ambas accidentales e intencionales, de los datos.

Malware – Un programa que es insertado en un sistema, a menudo secretamente, con la intención de comprometer la confidencialidad, integridad, o disponibilidad de los datos de la víctima, aplicaciones, o sistemas operativos, o de otra forma molestar o perturbar la víctima.

Mercado – Un tipo de apuesta (ej. simple, margen de puntos, más de/menos de) en el que se crean oportunidades para apostar sobre uno o más eventos.

Modalidad de juego gratis – Una modalidad que permite al jugador participar en el juego sin colocar una apuesta financiera, principalmente para el propósito de aprender o entender la mecánica del juego.

Motor de física – Software especializado que aproxima las leyes de física, incluyendo los efectos del movimiento, gravedad, velocidad, aceleración, masa, etc. para los elementos u objetos de un evento virtual. El motor de física es utilizado para introducir los elementos/objetos de un evento virtual en el contexto del mundo físico cuando se reproducen gráficos informáticos o simulaciones de video.

NCE, *Equipo de comunicación de la red* – Uno o más dispositivos que controlan la comunicación de datos en un sistema incluyendo, pero no limitado a, cables, conmutadores, concentradores, enrutadores, puntos de acceso inalámbrico, y teléfonos.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Operador – Una persona o entidad que opera un sistema de apuestas de eventos, utilizando la capacidad técnica del sistema de apuestas de eventos además de sus propios procedimientos internos.

Pantalla táctil – Un dispositivo con pantalla de video que también actúa como un dispositivo para entradas del usuario usando las localizaciones de puntos táctiles de conexión eléctrica en la pantalla.

Parlay – Una apuesta sencilla que vincula dos o más apuestas individuales y es dependiente en todas esas apuestas ganando juntas.

Participante – El atleta, equipo, u otra entidad que compite en un evento.

Participante virtual – El atleta u otra entidad que compite en un evento virtual.

Perfecta (también conocida como "Exacta") – Una apuesta en la que el jugador selecciona los finalistas en primera y segunda posición en el orden correcto.

PIN, *Número de identificación personal* – Un código numérico asociado con un individuo y que permite el acceso seguro en un dominio, cuenta, red, sistema, etc.

Plan de contingencia – Política de gestión y procedimientos diseñados para mantener o restaurar las operaciones de juego, posiblemente en una localización alternativa, en caso de emergencias, fallos del sistema, o desastre.

Política de seguridad – Un documento que define la estructura de gestión de seguridad y designa claramente las responsabilidades de seguridad, y establece la base necesaria para medir de forma fiable el progreso y cumplimiento.

Programa de control crítico – Un programa de software que controla el funcionamiento con relación a cualquier estándar técnico aplicable y/o requisito regulatorio.

Programa de fidelidad del jugador – Un programa que provee incentivos para los jugadores basado en el volumen de juego o ingresos recibidos de un jugador.

Protocolo – Un conjunto de reglas y convenios que especifica el intercambio de información entre dispositivos, a través de una red u otros medios.

Protocolo de comunicación seguro – Un protocolo de comunicación que proporciona la confidencialidad adecuada, autenticación y protección de integridad del contenido.

Protocolo sin estado – Un plan de comunicación que considera cada solicitud como una transacción independiente que no está relacionada con ninguna solicitud previa, de forma que la comunicación consiste de pares independientes de solicitudes y respuestas.

Proxy – Un proxy es una aplicación que "interrumpe" la conexión entre el cliente y el servidor. El proxy acepta ciertos tipos de tráfico entrando o saliendo de una red y lo procesa y envía. Esto

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

efectivamente cierra la ruta directa entre la red interna y externa, lo que hace más dificil que un atacante obtenga la dirección interna y otros detalles de la red interna.

Puerto – Un punto de entrada o salida de un módulo que proporciona el acceso al módulo para señales físicas, representadas por el flujo de información lógica (puertos separados físicamente no comparten el mismo pin o cable).

Quinella – Una apuesta en la que las dos primeras posiciones en una competición deben predecirse, pero no necesariamente en el orden de los finalistas.

Registro de apuesta – Un cupón impreso o mensaje electrónico confirmando la aceptación de una o más apuestas.

Registro de auditoría – Un registro mostrando quien ha accedido un sistema y que operaciones ha realizado el usuario durante un período especificado.

Reglas de juego – Cualquier información escrita, gráfica, y auditiva provista al público con respecto a las operaciones de las apuestas sobre eventos.

Riesgo – La probabilidad del éxito de una amenaza durante un ataque contra una red o sistema.

RNG cryptográfico – Un generador de números aleatorios (RNG) que es resistente a los ataques o compromisos por un atacante inteligente con recurso de computadoras modernas que tiene conocimiento del código fuente del RNG y/o su algoritmo. RNGs criptográfios no pueden ser factiblemente 'descifrados' para prever valores futuros.

RNG, *Generador de números aleatorios* – Un dispositivo físico o computacional, algoritmo, o sistema diseñado para producir números de forma indistinguible de una selección aleatoria.

Rooting – Obtener acceso a la raiz del código del sistema operativo para modificar el código de software en el teléfono móvil u otro dispositivo de apuestas remotas o instalar software que el fabricante no permitiría que fuera instalada.

Seguridad de información – Protección de la información y sistemas de información contra el acceso sin autorización, uso, divulgación, disrupción, modificación, o destrucción para proporcionar la integridad, confidencialidad, y disponibilidad.

Sello de tiempo – Un registro del valor actual de la fecha y hora del sistema de apuestas de eventos que es agregado al mensaje en el momento en que el mensaje es creado.

Servidor – Una instancia de software ejecutando que tiene la capacidad para aceptar solicitudes de los clientes, y la computadora que ejecuta este software. Los servidores operan en una arquitectura de Cliente-Servidor, en la que los "servidores" son programas de computadora ejecutando para atender las solicitudes de otros programas ("clientes"). En este caso el "servidor" sería el sistema de apuestas de eventos y los "clientes" serían los dispositivos de juego.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Shellcode – Una parte pequeña del código usada como una carga para la explotación de seguridad. Shellcode abusa las vulnerabilidades y resulta en un atacante con la habilidad para reducir la garantía de información del sistema.

Sistema de apuestas de eventos – El hardware, software, firmware, tecnología de comunicación, otro equipo, además de los procedimientos del operador implementados para permitir al jugador participar en el juego, y si es soportado, el equipo correspondiente relacionado a la visualización de los resultados de las apuestas, y otra información similar necesaria para facilitar la participación del jugador. El sistema provee al jugador con los medios para colocar y gestionar apuestas. El sistema provee al operador con los medios para revisar la cuenta del jugador, si es soportado, suspender eventos, generar varias transacciones de juego/financieras y reportes de cuentas, ingresar los resultados para los eventos, y ajustar todos los parámetros configurables.

Sistema de juego externo – Hardware y software del sistema separado de lo que constituye el sistema de apuestas de eventos, el cual puede controlar las funciones comunes a las ofertas de apuestas, configuración de las apuestas, reportes, etc. El jugador inicialmente se comunica directamente con el sistema de apuestas de eventos, el cual puede ser integrado con uno o más sistemas de juego externo.

Software de juego – El software usado para participar en transacciones de apuestas y financieras con el sistema de apuestas de eventos el cual, basado en el diseño, es descargado o instalado en el dispositivo de juego, ejecutado en el sistema de apuestas de eventos el cual es accedido por el dispositivo de juego, o una combinación de los dos. Ejemplos de software de juego incluyen paquetes propietarios de descarga de software, html, flash, etc.

TCP/IP, *Protocolo de control de transmisión/Protocolo de internet* – La serie de protocolos de comunicación usada para conectar anfitriones en la Internet.

Trifecta – Una apuesta en la que un jugador gana al seleccionar los tres primeros finalistas de una competición en el orden correcto.

Virus – Un programa que se autoreproduce, típicamente con mala intención, que ejecuta y se propaga modificando otros programas o archivos.

VPN, *Red privada virtual* – Una red lógica que es establecida sobre una red física existente y que típicamente no incluye cada nodo presente en la red física.

Vulnerabilidad – Software, hardware, u otra deficiencia en una red o sistema que puede proporcionar un "portal" para introducir una amenaza.

Wi-Fi – La tecnología estándar de la red de area local inalámbrica (WLAN) para conectar computadoras y dispositivos electrónicos unos con otros y/o la internet.

Propiedad Literaria © 2019 Gaming Laboratories International, LLC Todos los Derechos Reservados.