SÉRIE DE NORMAS

GLI-33

NORMAS PARA SISTEMAS DE APOSTAS DE EVENTO

VERSÃO 1.1

DATA DE REVISÃO: 14 DE MAIO DE 2019

Sobre esta norma

Esta norma técnica foi produzida pela **Gaming Laboratories International, LLC (GLI)** com o objetivo de fornecer análises técnicas independentes e/ou certificações para as partes interessadas da indústria de jogos indicando o estado de conformidade para as operações e sistemas de apostas com os requisitos estabelecidos neste documento.

Este documento destina-se a ser usado por órgãos reguladores, operadores e fornecedores do setor como uma diretriz de conformidade para tecnologias e procedimentos relativos a apostas em eventos. Esta norma não pretende representar um conjunto de requisitos prescritivos que todos os sistemas de apostas de eventos e operadores devem cumprir; no entanto, estabelece um padrão em relação às tecnologias e procedimentos utilizados para facilitar essas operações.

Operadores e fornecedores devem apresentar documentação de controle interno, credenciais e acesso associado a um ambiente de teste equivalente ao de produção, com uma solicitação para que seja certificado de acordo com esta norma técnica. A partir da certificação, a GLI fornecerá um certificado de conformidade que comprove a certificação desta norma.

O GLI-33 deve ser visto como um documento vivo que fornece um nível de orientação que será adaptado periodicamente para se alinhar com esse setor em desenvolvimento ao longo do tempo a medida que as implementações e operações de apostas evoluem.

Índice

Capítulo 1: Introdução ao Sistemas de Apostas de Eventos

1.1 Introdução

1.1.1 Declaração Geral

A **Gaming Laboratories International, LLC (GLI)** testa equipamentos de jogos desde 1989. Ao longo dos anos, a GLI desenvolveu várias normas técnicas utilizados por jurisdições em todo o mundo. Este documento, GLI-33, estabelece as normas técnicas para os Sistemas de Apostas de Eventos.

1.1.2 Histórico do Documento

Este documento é uma compilação baseada em muitas normas de todo o mundo. Alguns foram escritos por GLI; outros foram escritos por reguladores da indústria com a contribuição de laboratórios de testes independentes e operadores, desenvolvedores e fornecedores de Sistemas de Apostas de Eventos. A GLI considerou cada um dos documentos normativos, combinando cada uma das regulações exclusivas, eliminando algumas regras e atualizando outras, para refletir tanto a mudança na tecnologia quanto o propósito de manter uma norma que alcance objetivos regulatórios comuns sem impedir desnecessariamente a inovação tecnológica. A GLI lista abaixo, e dá crédito as agências cujos documentos foram revisados antes de escrever esta norma. É política da GLI atualizar este documento com a frequência necessária para refletir as mudanças na tecnologia e/ou nos procedimentos de teste. Este documento será distribuído gratuitamente e poderá ser obtido por download no site da GLI em www.gaminglabs.com ou entrando em contato com a GLI:

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

1.2 Reconhecimento de Outras Normas Revisadas

1.2.1 Declaração Geral

Essa norma técnica foi desenvolvida revisando e usando partes de documentos das seguintes organizações, listadas a seguir. A GLI reconhece e agradece aos reguladores e outros participantes do setor que montaram esses documentos:

a) Nevada Gaming Commission and Gaming Control Board.
b) British Columbia Gaming Policy and Enforcement Branch (GPEB).
c) Association of Racing Commissioners International (ARCI).
d) Tasmanian Liquor and Gaming Commission.
e) Northern Territory Racing Commission.
f) Victorian Commission for Gambling and Liquor Regulation.

g) Danish Gambling Authority.
h) Spanish Directorate General for the Regulation of Gambling (DGOJ).
i) South African Bureau of Standards (SABS).

1.3 Objetivo das Normas Técnicas

1.3.1 Declaração Geral

O objetivo desta norma técnica é o seguinte:

a) Eliminar critérios subjetivos na análise e certificação de Sistemas de Apostas de Eventos.
b) Testar os critérios que afetam a credibilidade e a integridade dos sistemas de apostas de eventos desde perspectiva da entrada de valores e da perspectiva do jogador.
c) Criar um padrão que garanta que as apostas em eventos sejam justas, seguras e capazes de serem auditadas e operadas corretamente.
d) Distinguir entre política pública local e os critérios do Laboratório de Testes Independente. Cabe a cada jurisdição local definir sua própria política pública em relação às apostas.
e) Reconhecer que a avaliação de sistemas de controle interno (como os processos de Prevenção a Lavagem de Dinheiro, Financeiros e de Negócios) empregados pelos operadores do Sistema de Apostas de Eventos não deverá ser incorporada aos testes de laboratório desta norma, mas, em vez disso, ser incluído na auditoria operacional realizada para jurisdições locais.
f) Elaborar uma norma que poderá ser facilmente ajustada para permitir novas tecnologias.
g) Construir uma norma que não especifique nenhum design, método ou algoritmo específico. A intenção é permitir que uma ampla gama de métodos seja usada para se adequar as normas e, ao mesmo tempo, encorajar novos métodos a serem desenvolvidos.

1.3.2 Sem Limitação de Tecnologia

Deve-se ter cautela para que este documento não seja lido de maneira a limitar o uso de tecnologia futura. Este documento não deve ser interpretado de maneira que, se a tecnologia não for mencionada, ela não será permitida. GLI revisará esta norma e fará mudanças para incorporar padrões mínimos para qualquer tecnologia nova.

1.3.3 Adesão e Cumprimento

Esta norma técnica poderá ser adotada no todo ou em parte por qualquer órgão regulador que deseje implementar um conjunto abrangente de requisitos para Sistemas de Jogos Interativos.

1.4 Outros Documentos que Podem ser Aplicados

1.4.1 Outras Normas GLI

Esta norma técnica cobre os requisitos para os Sistemas de Apostas de Eventos. Dependendo da tecnologia utilizada por um sistema, normas técnicas adicionais da GLI também poderão ser aplicados.

OBSERVAÇÃO: Todas as normas GLI estão disponíveis gratuitamente no site www.gaminglabs.com.

1.4.2 Padrões Mínimos de Controle Interno do Operador (MICS)

A implementação de um Sistema de Apostas de Eventos é uma tarefa complexa e, como tal, exigirá o desenvolvimento de processos e procedimentos internos para garantir que o sistema seja configurado e operado com o nível necessário de segurança e controle. Para esse fim, espera-se que o operador estabeleça um conjunto de Especificações Mínimas de Controle Interno (MICS) para definir os processos internos para a criação, administração e processamento de transações de apostas, além dos requisitos para controle interno de qualquer software e hardware do sistema ou componentes, e suas contas associadas.

1.5 Interpretação Deste Documento

1.5.1 Declaração Geral

Esta norma técnica aplica-se a sistemas que suportam apostas em esportes, competições, partidas e outros tipos de evento aprovados pelo órgão regulador. Os requisitos desta norma técnica aplicam-se a apostas em eventos de uma forma geral e não limitam ou autorizam eventos específicos, mercados ou tipos de apostas. A intenção é fornecer uma estrutura para cobrir aquelas atualmente conhecidas e permitidas por lei. Este documento não pretende definir quais partes são responsáveis por cumprir os requisitos desta norma técnica. É da responsabilidade das partes interessadas de cada operador determinar a melhor forma de atender aos requisitos estabelecidos neste documento.

1.5.2 Fornecedores de Softwares e Operadores

Os componentes de um Sistema de Apostas de Eventos, embora possam ser construídos de forma modular, são projetados para funcionar perfeitamente em conjunto. Além disso, o Sistemas de Apostas de Eventos pode ser desenvolvidos para ter funcionalidades configuráveis, cuja configuração final dependerá das opções escolhidas pelo operador. Do ponto de vista de teste, poderá não ser possível testar todas as funcionalidades configuráveis de um Sistema de Apostas de eventos enviados por um fornecedor de software se for omitida alguma funcionalidade escolhida pelo operador; no entanto, a configuração que será utilizada no ambiente de produção deverá ser comunicada ao laboratório de teste independente para facilitar a criação de um ambiente de teste funcionalmente equivalente ao de produção. Devido à natureza integrada de um Sistema de Apostas de Eventos, existem vários requisitos neste documento que poderão se aplicar a operadores e fornecedores. Nos casos, onde o teste é solicitado para uma versão “white-label” do sistema, uma configuração específica será testada e relatada.

1.6 Testes e Auditorias

1.6.1 Testes de Laboratório

O laboratório de teste independente testará e certificará os componentes do Sistema de Apostas de Eventos de acordo com os capítulos desta norma técnica em um ambiente de teste controlado, conforme aplicável. Quaisquer requisitos que necessitem de procedimentos operacionais adicionais

para atender aos requisitos definidos nesta norma, deverão ser documentados no relatório de avaliação e usado para complementar o escopo da auditoria operacional.

1.6.2 Auditoria Operacional

A integridade e a precisão da operação de um Sistema de Apostas de Eventos é altamente dependente dos procedimentos operacionais, configurações e da infraestrutura de rede do ambiente de produção. Por este motivo, uma auditoria operacional é um complemento essencial para o teste e certificação de um Sistema de Apostas de Eventos. A auditoria operacional, está descrita nos seguintes anexos desta norma técnica e deverá ser realizada com uma frequência que será especificada pelo órgão regulador:

a) Anexo A: Auditoria Operacional de Procedimentos e Práticas de Aposta. Auditoria operacional de procedimentos e práticas de Aposta. Isto inclui, mas não se limita a, revisão do MICS, procedimentos e práticas para operações de aposta, incluindo, mas não se limitadando a estabelecer regras para a aposta, suspender eventos, processar várias transações financeiras e de apostas, criar mercados, pagar apostas, fechar mercados, cancelamentos de eventos, anulação ou cancelamento de apostas, gerenciamento de contas de jogadores, práticas fundamentais relevantes para a limitação de riscos e quaisquer outros objetivos estabelecidos pelo órgão regulador.
b) Anexo B: Auditoria Operacional de Controles Técnicos de Segurança. Anexo B: Auditoria operacional de controles técnicos de segurança. Isso inclui, mas não está limitado a, avaliação do sistema de segurança da informação (ISS), revisão dos processos operacionais críticos para a conformidade, testes de penetração focados na infraestrutura externa e interna, bem como na transferência, armazenamento e/ou processamento de dados do jogador e/ou informações confidenciais pelos aplicativos, e quaisquer outros objetivos estabelecidos pelo órgão regulador.

Capítulo 2: Requisitos do Sistema

2.1 Introdução

2.1.1 Declaração Geral

Se o Sistema de Apostas de Eventos for composto de vários sistemas de computador em vários sites, o sistema como um todo e toda a comunicação entre seus componentes deverá estar em conformidade com estes requisitos.

2.2 Requisitos do Relógio do Sistema

2.2.1 Relógio do Sistema

O Sistema de Apostas de Eventos deve manter um relógio interno que garanta a data e hora atuais que serão utilizados para fornecer as seguintes informações:

a) Registro de data e hora de todas as transações e eventos;
b) Registro de data e hora de eventos relevantes; e; e
c) Referência de hora para relatórios.

2.2.2 Sincronização de Tempo

O Sistema de Apostas de Eventos deverá ser equipado com um mecanismo para garantir que a data e hora entre todos os componentes que compõem o sistema estejam sincronizadas.

2.3 Requisitos do Programa de Controle

2.3.1 Declaração Geral

Além dos requisitos contidos nesta seção, os procedimentos de auditoria indicados na seção "Procedimentos de Verificação" deste documento também devem ser cumpridos.

2.3.2 Auto Verificação do Programa de Controle

O Sistema de Aposta de Evento deverá ser capaz de verificar, após a instalação, se todos os componentes críticos do programa de controle contidos no sistema são cópias autênticas dos componentes aprovados do sistema, pelo menos uma vez a cada 24 horas e quando solicitado usando um método aprovado pelo órgão regulador. O mecanismo de autenticação do programa de controle crítico deve:

a) Empregar um algoritmo de *hash* que produza um *digest* da mensagem de pelo menos 128 bits;
b) Incluir todos os componentes críticos do programa de controle que poderão afetar as operações de jogos, incluindo, mas não limitado a, executáveis, bibliotecas, jogos ou configurações de

sistema, arquivos de sistema operacional, componentes que controlam sistema de geração de relatórios e elementos de banco de dados que afetam a operação do sistema; e
c) Fornecer uma indicação da falha de autenticação se algum componente crítico do programa de controle crítico for considerado inválido.

2.3.3 Verificação Independente do Programa de Controle

Cada componente crítico do programa de controle do Sistema de Aposta de Evento deverá ter um método para ser verificado por meio de um procedimento independente de verificação de terceiros. O processo de verificação de terceiros deverá operar independentemente de qualquer processo ou software de segurança dentro do sistema. O laboratório de testes independente, antes da aprovação do sistema, deverá aprovar o método de verificação de integridade.

2.3.4 Desligamento e Recuperação

O Sistema de Aposta de Evento deve ser capaz de executar um desligamento normal e somente permitir o reinício automático após a execução dos procedimentos a seguir, ao ligar, como mínimo:

a) Rotina(s) de retomada do programa, incluindo autotestes, concluída(s) com sucesso
b) Todos os componentes críticos do programa de controle do sistema foram autenticados usando um método aprovado pelo órgão regulador; e
c) A comunicação com todos os componentes necessários para a operação do sistema foi estabelecida e autenticada de forma semelhante.

2.4 Gestão de Aposta

2.4.1 Gestão de Aposta

O Sistema de Aposta de Evento deverá ter a capacidade de suspender o seguinte, sob demanda:

a) Todas as atividades de Aposta;
b) Eventos individuais;
c) Mercados individuais;
d) Dispositivos de apostas individuais (se aplicável); e
e) Logins de jogadores individuais (se aplicável).

2.5 Gestão da Conta do Jogador

2.5.1 Declaração Geral

Os requisitos desta seção se aplicam a contas de jogadores quando suportadas pelo Sistema de Apostas de Eventos. Além dos requisitos contidos nesta seção, a seção "Controles de conta de jogador" deste documento também deve ser cumprida.

OBSERVAÇÃO: O registro e a verificação da conta do jogador são exigidos pelo Sistema de Apostas de Evento para que um jogador participe de apostas remotas.

2.5.2 Registro e Verificação

Deverá ser disponibilizada um meio para coletar informações do jogador antes do registro de uma conta de jogador. Quando o registro e a verificação da conta do jogador forem disponibilizados pelo Sistema de Apostas de Eventos, seja diretamente pelo sistema ou em conjunto com o software de um prestador de serviços terceirizado, os seguintes requisitos deverão ser atendidos:

a) Apenas jogadores com a idade legal para jogar, conforme estipulado pela jurisdição, poderão se registrar para uma conta de jogador. Qualquer pessoa que informar uma data de nascimento que indique que é menor de idade deverá ser negado ao se registrar para uma conta de jogador.
b) Efetuar a verificação de identidade antes que um jogador seja autorizado a fazer uma aposta. Prestadores de serviços terceirizados para verificação de identidade poderão ser usados, conforme permitido pelo órgão regulador.
    i. A verificação da identidade deverá autenticar o nome, o endereço físico e a idade do indivíduo, no mínimo, conforme exigido pelo órgão regulador.
    ii. A verificação da identidade também deverá verificar se o jogador não está em nenhuma lista de exclusão mantida pelo operador ou pelo órgão regulador ou proibido de estabelecer ou manter uma conta por qualquer outro motivo.
    iii. Detalhes da verificação de identidade deverão ser mantidos de maneira segura.
c) A conta do jogador só poderá ser ativada depois que a verificação de idade e identidade forem concluídas com sucesso; que estiver comprovado que o jogador não está em nenhuma lista de exclusão ou mesmo proibido de estabelecer ou manter uma conta por qualquer outro motivo, o jogador aceita as políticas de privacidade e os termos e condições necessários, e o registro da conta do jogador estiver completo.
d) Um jogador só poderá ter uma conta de jogador ativa por vez, a menos que seja especificamente autorizado pelo órgão regulador.
e) O sistema deve ter a funcionalidade de atualização de senhas, informações de registro e a conta usada para transações financeiras de cada jogador. Um processo de autenticação multifatorial deverá ser empregado para estes fins.

2.5.3 Acesso do Jogador

Um jogador acessa sua conta de jogador usando um nome de usuário (ou similar) e uma senha ou um meio alternativo seguro para o jogador realizar autenticação para acessar o Sistema de Apostas de Eventos. Os métodos de autenticação estão sujeitos ao critério do órgão regulador, conforme necessário. O requisito não proíbe a opção de disponibilizar mais de um método de autenticação para um jogador acessar sua conta.

a) Se o sistema não reconhecer o nome de usuário e/ou senha quando inserido, uma mensagem explicativa deverá ser exibida ao jogador, solicitando que insira novamente as informações.
b) Quando um jogador esquecer seu nome de usuário e/ou senha, um processo de autenticação multifatorial deverá ser utilizado para a recuperação do nome de usuário/redefinição da senha.
c) As informações do saldo atual da conta e as opções de transação devem estar disponíveis para o jogador uma vez autenticado.
d) O sistema deverá possibilitar que uma conta seja bloqueada no caso de ser detectada atividade

suspeita (por exemplo, muitas tentativas malsucedidas de login). Um processo de autenticação multifatorial deverá ser utilizado para desbloquear a conta.

2.5.4 Inatividade do Jogador

Para contas de jogadores acessadas remotamente para apostas ou gerenciamento de conta, após 30 minutos de inatividade naquele dispositivo, ou um período determinado pelo órgão regulador, o jogador deverá ser autenticado novamente para acessar sua conta de jogador.

a) Nenhuma aposta ou transação financeira terá acesso permitido no dispositivo até que o jogador seja autenticado novamente.
b) Um meio mais simples poderá ser oferecido ao jogador para a reautenticação no dispositivo, como autenticação em nível de sistema operacional (por exemplo, biometria) ou um Número de Identificação Pessoal (PIN). Outros meios de reautenticação deverão ser avaliados, caso a caso, pelo laboratório de teste independente.
    i. Esta funcionalidade poderá ser desativada baseada nas preferências do jogador e/ ou do órgão regulador.
    ii. Uma vez a cada trinta dias, ou em um período determinado pelo órgão regulador, o jogador será solicitado a se autenticar, informando todos os dados novamente, no dispositivo.

2.5.5 Limitações e Exclusões

O Sistema de Apostas de Evento deverá ser capaz de acatar corretamente quaisquer limitações e/ou exclusões estabelecidas pelo jogador e/ou operador, conforme exigido pelo órgão regulador:

a) Quando o sistema possui a funcionalidade de gerenciar diretamente as limitações e/ou exclusões, os requisitos aplicáveis nas seções "Limitações e Exclusões", deste documento, deverão ser avaliados;
b) As limitações configuradas pelo jogador não deverão anular as limitações impostas pelo operador, se estas são mais restritivas. As limitações mais restritivas deverão ser as prioritárias; e
c) As limitações não deverão ser comprometidas por eventos de status internos, como pedidos de exclusão feitos pelo jogador e revogações.

2.5.6 Manutenção de Fundos do Jogador

Quando as transações financeiras são processadas automaticamente pelo Sistema de Apostas de Eventos, os seguintes requisitos deverão ser atendidos:

a) O sistema deve confirmar/negar todas as transações financeiras iniciadas.
b) Depósitos na conta de um jogador poderão ser feitos por meio de uma transação com cartão de crédito ou outros métodos que ofereçam uma trilha de auditoria robusta;
c) Os fundos estarão disponíveis para apostas somente após receber do emissor ou o emissor fornecer um número de autorização, indicando que os fundos estão autorizados. O número de autorização deverá ser mantido em um log de auditoria.
d) Os pagamentos de uma conta de jogador (incluindo transferência de fundos) deverão ser

efetuados diretamente para uma conta em nome do jogador em uma instituição financeira ou encaminhar para o endereço do jogador o pagamento usando um serviço de entrega seguro ou por outro método que não seja proibido pelo órgão regulador. O nome e endereço deverão ser os mesmos que informados nos detalhes de registro do jogador.

e) Se um jogador iniciar uma transação na conta de jogador e essa transação exceder os limites estabelecidos pelo operador e/ou órgão regulador, esta transação somente poderá ser processada desde que o jogador seja claramente notificado de que será permitida uma transação de um valor menor que o solicitado.
f) Não será permitido transferir fundos entre duas contas de jogador.

2.5.7 Histórico de Transações ou Extrato de Conta

O Sistema de Aposta de Evento deverá fornecer um registro de transações ou um extrato de conta ao jogador quando solicitado. As informações enviadas deverão ser suficientes para permitir ao jogador reconciliar o registro ou o extrato contra seus próprios registros financeiros. As informações a serem fornecidas deverão incluir, no mínimo, detalhes sobre os seguintes tipos de transações:

a) Transações financeiras (com registro de data/hora e com um ID de transação exclusivo):
   i. Depósitos efetuados na conta do jogador;
   ii. Saques efetuados na conta do jogador;
   iii. Créditos promocionais ou bônus adicionados/sacados da conta do jogador (exceto os créditos ganhos nas apostas);
   iv. Ajustes ou modificações manuais efetuados na conta do jogador (por exemplo, devido a reembolsos);
b) Transações de aposta:
   i. Número de identificação exclusivo da aposta;
   ii. A data e hora em que a aposta foi feita;
   iii. A data e a hora em que o evento começou e terminou ou é esperado que ocorra, para eventos futuros (se conhecidos);
   iv. A data e a hora em que os resultados foram confirmados (em branco até a confirmação);
   v. Todas as escolhas do jogador envolvidas na aposta, incluindo a linha do mercado, seleção de aposta e qualquer condição especial aplicada à aposta;
   vi. Os resultados da aposta (em branco até a confirmação);
   vii. Montante total apostado, incluindo quaisquer créditos promocionais/bônus (se aplicável);
   viii. Montante total ganho, incluindo quaisquer créditos promocionais/bônus (se aplicável);
   ix. Comissão ou taxas recolhidas (se aplicável); e
   x. A data e hora em que a aposta ganhadora foi paga ao jogador.

2.5.8 Programas de Fidelidade do Jogador

Programas de fidelidade de jogadores são quaisquer programas que oferecem incentivos para os jogadores, normalmente baseados no volume da aposta ou valores recebidos de um jogador. Se os programas de fidelidade do jogador forem oferecidos pelo Sistema de Apostas de Eventos, os seguintes princípios deverão ser aplicados:

a) Os prêmios deverão estar igualmente disponíveis para todos os jogadores que atingirem o

mesmo nível definido de qualificação, com base nos pontos de fidelidade;
b) O resgate dos pontos de fidelidade ganhos deverá ser uma transação segura que debita automaticamente o saldo dos pontos pelo valor do prêmio resgatado; e
c) Todas as transações referentes a pontos de fidelidade do jogador deverão ser registradas pelo sistema.

2.6 Funcionalidade de Instrumentos Financeiros para a Aposta

2.6.1 Declaração Geral

Os Sistemas de Aposta de Evento que suportem a emissão e/ou resgate de instrumentos de financeiros de aposta (vouchers e cupons) devem cumprir os requisitos aplicáveis estabelecidos na secção "Vouchers/Vales de Máquinas" da GLI-11 Normas para Dispositivos de Apostas e nos "Requisitos do Sistema de Validação" da GLI-13 Normas para Sistemas de Monitoramento e Controle On-Line (MCS) e Sistemas de Validação e outros requisitos jurisdicionais aplicáveis observados pelo órgão regulador.

2.7 Requisitos de Localização para Apostas Remotas

2.7.1 Declaração Geral

Quando exigido pelo órgão regulador, os requisitos desta seção devem ser aplicados quando o Sistema de Apostas de Eventos oferecer suporte a apostas remotas.

OBSERVAÇÃO: O operador ou provedor de serviços terceirizado que mantiver esses componentes, serviços e/ou aplicativos deve estar em conformidade com estes procedimentos de auditoria indicados na seção "Fornecedor de serviços de localização" deste documento.

2.7.2 Prevenção de Fraude de Localização

O Sistema de Apostas de Eventos deverá possuir um mecanismo para detectar o uso de software de desktop remoto, *rootkits*, virtualização e/ou quaisquer outros programas identificados como tendo a capacidade de contornar a detecção da localização. Para tal, deverá seguir as melhores práticas de medidas de segurança para:

a) Detectar e bloquear a fraude de dados de localização antes de concluir cada aposta (por exemplo, aplicativos de localização falsos, máquinas virtuais, programas de área de trabalho remota, etc.);
b) Verificar o endereço IP de cada conexão de dispositivo de apostas remoto a uma rede, para garantir que uma rede privada virtual (VPN) ou serviço proxy não esteja em uso;
c) Detectar e bloquear dispositivos que indicam violação ao nível do sistema (por exemplo, *root*, *jailbreaking*, etc.);
d) Impedir ataques do tipo "man-in-the-middle" ou técnicas de hacking semelhantes e evitar a manipulação de código;
e) Utilizar mecanismos de detecção e bloqueio verificáveis para um nível de aplicativo; e

f) Monitorar e evitar apostas feitas por uma única conta de jogador a partir de locais geograficamente inconsistentes (por exemplo, foram identificados locais de posicionamento de apostas que seriam impossíveis de viajar no período relatado).

2.7.3 Detecção de Localização para Apostas Remotas em uma WLAN

Quando as apostas remotas ocorrerem através de uma Rede de Área Local sem Fio (WLAN), o Sistema de Apostas de Eventos deverá incorporar um dos seguintes métodos que podem rastrear as localizações de todos os jogadores conectados à WLAN:

a) Um serviço ou aplicativo de detecção de localização em que cada jogador deverá passar por uma verificação de localização antes de iniciar cada aposta. Este serviço ou aplicativo deverá atender aos requisitos especificados na próxima seção "Detecção de localização para apostas remotas pela Internet"; ou
b) Um componente de detecção de localização que detecta em tempo real quando algum jogador não está mais na área permitida e impeça que outras apostas sejam feitas. Isto poderá ser feito utilizando hardware de TI específico, como antenas direcionais, sensores Bluetooth ou outros métodos a serem avaliados caso a caso pelo laboratório de testes independente.

2.7.4 Detecção de Localização para Apostas Remotas pela Internet

Quando apostas remotas ocorrerem pela Internet, o Sistema de apostas de eventos deve incorporar um serviço ou aplicativo de detecção de localização para detectar e monitorar corretamente a localização de um jogador que tentar fazer uma aposta; e monitorar e bloquear todas as tentativas não autorizadas de fazer uma aposta.

a) Cada jogador deve passar por uma verificação de localização antes de completar a primeira aposta após o login em um dispositivo de apostas remoto específico. As verificações de localização subsequentes nesse dispositivo devem ocorrer antes de concluir as apostas após um período de 30 minutos desde a verificação da localização anterior, ou conforme especificado pelo órgão regulador:
    i. Se a verificação de localização indicar que o jogador está fora dos limites permitidos ou não conseguir localizar o jogador, a aposta será rejeitada e o jogador será notificado sobre isso.
    ii. Um registro deverá ser gravado com a data/hora informada, sempre que uma violação de localização for detectada, incluindo o ID único do jogador e a localização encontrada.
b) Um método de geolocalização deverá ser utilizado para fornecer a localização física de um jogador e um raio de confiança associado. O raio de confiança deverá estar localizado inteiramente dentro do limite permitido.
c) Fontes de dados de localização precisa (Wi-Fi, GSM, GPS, etc.) deverão ser utilizadas pelo método de geolocalização para confirmar a localização do jogador. Se a única fonte de dados de localização disponível de um dispositivo de apostas remoto for um endereço IP, os dados de localização de um dispositivo móvel registrado na conta do jogador poderá ser usado como uma fonte de dados de localização alternativa nas seguintes condições:
    i. O dispositivo de apostas remoto (onde a aposta está sendo feita) e o dispositivo móvel deverão estar próximos um do outro.

ii. Se permitido pelo órgão regulador, os dados de localização, com base na operadora de um dispositivo móvel, poderão ser usados se nenhuma outra fonte de dados de localização além de de endereços IP, estiver disponível.

d) O método de geolocalização deverá possuir a capacidade de controlar se o raio de precisão da fonte de dados de localização está permitida sobrepor ou exceder as zonas de segurança definidas ou o limite permitido; e
e) Para mitigar e contabilizar as discrepâncias entre as fontes de mapeamento e variações nos dados geoespaciais, polígonos de limite com base em mapas auditados e aprovados pelo órgão regulador, bem como dados de localização de sobreposição, polígonos de limite deverão ser utilizados.

2.8 Informação a Serem Mantidas

2.8.1 Retenção de Dados e Informações de Data/Hora

O Sistema de Apostas de Eventos deverá ser capaz de manter e fazer backup de todos os dados conforme exposto nesta seção:

a) O relógio do sistema deverá ser utilizado para obter todas as informações de data/hora.
b) O sistema deverá fornecer um mecanismo para exportar os dados para fins de análise e auditoria/verificação (por exemplo, CSV, XLS).

2.8.2 Informações do Registro de Apostas

Para cada aposta individual feita pelo jogador, as informações a serem mantidas e contidas em backups pelo Sistema de Apostas de Eventos deverão incluir:

a) A data e hora em que a aposta foi feita;
b) Qualquer escolha de jogador envolvida na aposta:
   i. Linha de mercado e quotas (por exemplo, apostas simples, apostas de margens, valores a mais/menos, *win*/*place*/*show*, etc.);
   ii. Seleção de aposta (por exemplo, nome e número do atleta ou da equipe);
   iii. Qualquer condição especial aplicada à aposta;
c) Os resultados da aposta (em branco até a confirmação);
d) Valor total apostado, incluindo quaisquer créditos promocionais/bônus (se aplicável);
e) Valor total ganho, incluindo quaisquer créditos promocionais/bônus (se aplicável);
f) Comissão ou taxas recolhidas (se aplicável);
g) A data e hora em que a aposta ganhadora foi paga ao jogador.
h) Número de identificação exclusivo da aposta;
i) Identificação do usuário ou identificação exclusiva do dispositivo de apostas que emitiu o cupom de aposta (se aplicável);
j) Informações relevantes de localização (se aplicável);
k) Identificadores de evento e mercado;
l) Status da aposta atual (ativa, cancelada, não resgatada, pendente, anulada, inválida, resgate em andamento, resgatada, etc.);
m) Identificação de usuário exclusiva para apostas realizadas usando uma conta de jogador:

n) Período de resgate (se aplicável); e
o) Campo de texto aberto para que o atendente informe a descrição do jogador ou arquivo de imagem (se aplicável);

2.8.3 Informações de Mercado

Para cada mercado individual disponível para apostas, as informações a serem mantidas e contidas em backups pelo Sistema de Apostas de Eventos deverão incluir:

a) A data e hora em que o período de apostas começou e terminou;
b) A data e a hora em que o evento começou e terminou ou é esperado que ocorra, para eventos futuros (se conhecidos);
c) A data e a hora em que os resultados foram confirmados (em branco até a confirmação);
d) Quantia total de apostas coletadas, incluindo quaisquer créditos promocionais/bônus (se aplicável);
e) As linhas de quotas que estavam disponíveis durante a duração de um mercado (com registro de tempo) e o resultado confirmado (ganho/perda/empate);
f) Quantia total de ganhos pagos a jogadores, incluindo quaisquer créditos promocionais/bônus (se aplicável);
g) Quantia total de apostas anuladas ou canceladas, incluindo quaisquer créditos promocionais/bônus (se aplicável);
h) Comissão ou taxas recolhidas (se aplicável);
i) Status do evento (em andamento, finalizado, confirmado, etc.); e
j) Identificadores de evento e mercado;

2.8.4 Informações de Competição/Torneio

Para os Sistemas de Apostas de Eventos que suportam competição/torneio, as informações a serem mantidas e contidas em backups pelo Sistema de Apostas de Eventos devem incluir para cada competição/torneio:

a) Nome da competição/torneio;
b) Data/hora em que a competição/torneio ocorreu ou irá ocorrer (se conhecido);
c) Identificação exclusiva do jogador e nome de cada jogador registrado, valor de entrada pago e a data de pagamento;
d) Identificação de jogador exclusiva de cada jogador vencedor, quantia de taxa de entrada paga e a data paga;
e) Valor total cobrado de taxas de inscrição, incluindo quaisquer créditos promocionais/bônus (se aplicável) ;
f) Valor total de ganhos pagos aos jogadores, incluindo quaisquer créditos promocionais/bônus (se aplicável) ;
g) Comissão ou taxas recolhidas (se aplicável); e
h) Status do competição/torneio (em andamento, concluído, etc.).

2.8.5 Informações da Conta do Jogador

Para os Sistemas de Apostas de Eventos que suportam gerenciamento de conta de jogador, as informações a serem mantidas e contidas em backups pelo Sistema de Apostas de Eventos devem incluir o seguinte:

a) ID único do jogador e nome do jogador ;
b) Dados do jogador (incluindo método de verificação);
c) Data em que o jogador aceitou os termos e condições do operador e a política de privacidade ;
d) Detalhes da conta e saldo atual;
e) Campo de texto aberto para que o atendente informe a descrição do jogador ou arquivo de imagem (se aplicável);
f) Contas anteriores, se houver, e motivo para desativação; ;
g) A data e a forma em que a conta foi registrada (por exemplo, remoto ou no local);
h) A data e hora do último login;
i) Informações sobre exclusões/limitações, conforme exigido pelo órgão regulador:
    i. A data e hora em que foi solicitado (se aplicável);
    ii. Descrição e motivo da exclusão/limitação;
    iii. Tipo de exclusão/restrição (por exemplo, exclusão imposta pelo operador, restrição imposta pelo jogador);
    iv. Data de início da Exclusão/limitação (se aplicável);
    v. Data de fim da Exclusão/limitação (se aplicável);
j) Informações sobre transações financeiras
    i. Tipo de transação (por exemplo, depósito, saque, ajuste);
    ii. Data/hora da transação;
    iii. ID único da transação;
    iv. Valor da transação;
    v. Saldo total antes/depois da transação;
    vi. Valor total de taxas pagas pela transação (se aplicável);
    vii. Identificação do usuário ou identificação exclusiva do dispositivo que processou a transação (se aplicável);
    viii. Status da transação (pendente, confirmada etc.);
    ix. Forma de depósito/saque (por exemplo, dinheiro, cartão de débito ou crédito, cheque pessoal, cheque administrativo, transferência bancária, ordem de pagamento);
    x. Número de autorização de depósito; e
    xi. Informações relevantes de localização.

2.8.6 Informações sobre Promoções/Bônus

Para os Sistemas de Apostas de Eventos que suportam promoções e/ou bônus que são resgatados em dinheiro, créditos para apostar ou mercadorias, as informações a serem mantidase backupeadas pelo Sistema de Apostas de Eventos devem incluir para cada promoção/bônus:

a) A data e hora em que o período promocional/de bônus começou e terminou ou terminará (se conhecido);
b) Saldo atual para promoção/bônus;
c) Valor total de promoções/bônus emitidos;
d) Valor total de promoções/bônus resgatados;

e) Valor total de promoções/bônus expirados;
f) Valor total de ajustes de promoções/bônus; e
g) Identificação exclusiva da promoção/bônus.

2.8.7 Informações sobre o Dispositivo de Aposta

Para cada dispositivo de aposta de autoatendimento ou dispositivo de apostas POS, as informações a serem mantidas e contidas em backups pelo Sistema de Apostas de Eventos deverão incluir, se aplicável:

a) Identificação exclusiva do dispositivo de apostas.
b) Registro de compras de apostas;
c) Registro de resgate de apostas ganhadoras, se suportado;
d) Registro de anulação e cancelamento de apostas; e
e) Identificação do usuário e informações da sessão, para dispositivos de aposta POS;

2.8.8 Informações de Eventos Relevantes

As informações de Eventos Relevantes a serem mantidas e backupeadas pelo Sistema de Apostas de Eventos devem incluir:

a) Tentativas de login malsucedidas;
b) Erros de programa ou incompatibilidade de autenticação;
c) Períodos significantes de indisponibilidade de qualquer componente crítico do sistema;
d) Valores ganhos que excedem um valor determinado pelo órgão regulador (individual e em conjunto, ao longo de um período de tempo pré-definido), incluindo informações de registro de apostas;
e) Valores apostados que excedem um valor determinado pelo órgão regulador (individual e em conjunto, ao longo de um período de tempo pré-definido), incluindo informações de registro de apostas;
f) Sistemas vencidos (caducados), alterações e correções;
g) Alterações em arquivos de dados ativos que foram efetuados fora da execução normal do programa e do sistema operacional;
h) Alterações feitas na biblioteca de dados de download, incluindo inclusão, alteração ou exclusão de software, quando suportado;
i) Alterações no sistema operacional, banco de dados, rede e políticas da aplicação e parâmetros;
j) Mudanças na data/hora do servidor mestre que controla o relógio do sistema;
k) Alterações nos critérios previamente estabelecidos para um evento ou mercado (não incluindo alterações de linhas de quotas para mercados ativos);
l) Mudanças nos resultados de um evento ou mercado;
m) Mudanças nos parâmetros de promoção e/ou bônus;
n) Gerenciamento da Conta do Jogador:
    i. Ajustes no saldo da conta do jogador;
    ii. Alterações feitas nos dados do jogador e informações confidenciais registradas em uma conta de jogador;
    iii. Desativação da conta do jogador;

iv. Transações financeiras de valores que excedem um valor determinado pelo órgão regulador (únicas e em conjunto ao longo de um período de tempo), incluindo informações da transação;

o) Perda irrecuperável de informações confidenciais;
p) Qualquer outra atividade que requeira intervenção do usuário e que tenha ocorrido fora do escopo normal da operação do sistema; e
q) Outros eventos relevantes ou incomuns que forem considerados aplicáveis pelo órgão regulador.

2.8.9 Informações de Acesso do Usuário

Para cada conta de usuário, as informações a serem mantidas e backupeadas pelo Sistema de Apostas de Eventos deverão incluir:

a) Nome do funcionário e cargo ou posição;
b) Identificação do usuário;
c) Lista completa e descrição das funções que cada grupo ou conta de usuário poderá executar;
d) Data/hora em que a conta foi criada;;
e) Data/hora do último login;
f) Data/hora da última alteração de senha;
g) Data/hora em que a conta foi desabilitada/desativada; e
h) Grupo ao qual a conta do usuário está vinculada (se aplicável);

2.9 Requisitos de Relatório

2.9.1 Requisitos Gerais de Relatórios

O Sistema de Apostas de Eventos deverá ser capaz de fornecer as informações necessárias para gerar relatórios conforme exigido pelo órgão regulador. Além de atender os requisitos da seção acima "Retenção de dados e Informação de Data/Hora", os seguintes requisitos deverão ser observados na geração dos relatórios necessários:

a) O sistema deverá ser capaz de fornecer as informações necessárias para geração de relatório sempre que for solicitado e por intervalos exigidos pelo órgão regulatório, incluindo, mas não limitado a, diariamente, começo do mês até data atual (MTD), começo do mês até data atual (MTD), começo do ano até data atual (YTD), do início da operação até hoje (LTD).
b) Cada relatório solicitado deve conter:
   i. O operador, a periodicidade selecionado e a data/hora em que o relatório foi gerado; e
   ii. Se para a periodicidade selecionada não tem nehuma informação, apresentar a mensagem “Sem Informação” ou alguma outra semelhante;.

OBSERVAÇÃO: Além dos relatórios descritos nesta seção, o órgão regulador também poderá exigir outros relatórios utilizando as informações citadas na seção "Informações a Serem Mantidas" deste documento.

2.9.2 Relatórios de Receita do Operador

O Sistema de Apostas de Eventos deve ser capaz de fornecer as seguintes informações necessárias

para compilar um ou mais relatórios sobre a receita do operador para cada evento como um todo e para cada mercado individual dentro daquele evento que possa ser usado para informações de tributação do operador:

a) A data e hora em que o evento começou e terminou;
b) Quantia total de apostas coletadas;
c) Quantia total de ganhos pagos a jogadores;
d) Quantia total de apostas vazias ou canceladas;
e) Comissão e taxas recolhidas (se aplicável);
f) Identificadores de evento e mercado; e
g) Status do evento (em andamento, completo, confirmado, etc.).

2.9.3 Relatórios de Responsabilidade do Operador

O Sistema de Apostas de Eventos deverá ser capaz de fornecer as informações necessárias para gerar um ou mais relatórios de responsabilidade do operador:

a) Valor total retido pelo operador para as contas do jogador (se aplicável);
b) Quantia total de apostas feitas em eventos futuros; e
c) Quantia total de ganhos acumulados de apostas ganhadoras, mas não pagos pelo operador.

2.9.4 Relatórios de Eventos Futuros

O Sistema de Apostas de Eventos deve ser capaz de fornecer as seguintes informações necessárias para compilar um ou mais relatórios de eventos futuros do dia da aposta:

a) Apostas feitas antes do dia de jogo para eventos futuros (total e por aposta);
b) Apostas feitas no dia de jogo para eventos futuros (total e por aposta);
c) Apostas feitas antes do dia de jogo para eventos ocorrendo neste mesmo dia (total e por aposta);
d) Apostas feitas no dia do jogo para eventos ocorrendo neste mesmo dia (total e por aposta);
e) Apostas anuladas ou canceladas no dia de jogo (total e por aposta); e
f) Identificadores de evento e mercado;

2.9.5 Relatórios de Eventos Relevantes e Alterações

O Sistema de Apostas de Eventos deverá ser capaz de fornecer as informações necessárias para gerar um ou mais relatórios para cada evento relevante ou alteração , se aplicável:

a) a) Data/hora do evento relevante e/ou alteração;
b) Identificação do evento/componente (se aplicável);
c) Identificação do(s) usuário(s) que realizou e/ou autorizou o evento relevante ou a alteração;
d) Motivo/descrição do evento relevante ou alteração, incluindo o dado ou parâmetro alterado;
e) Valor do dado ou parâmetro antes da alteração; e
f) Valor do dado ou parâmetro após a alteração.

Capítulo 3: Requisitos do Dispositivo de Aposta

3.1 Introdução

3.1.1 Declaração Geral

Uma aposta pode ser feita usando um dos seguintes tipos de dispositivos de aposta, conforme permitido pelo órgão regulador. Quaisquer outros tipos de dispositivos de aposta serão analisados caso a caso, conforme permitido pelo órgão regulador.

a) Dispositivo de Aposta - Ponto de Venda (POS): Um terminal de atendimento que, no mínimo, será usado por um atendente para a execução ou formalização de apostas feitas em nome de um jogador.
b) Dispositivo de Aposta de Autoatendimento: Um quiosque que, no mínimo, será usado para a execução ou formalização de apostas feitas diretamente pelo jogador e, se suportado, poderá ser usado para resgate de registros de apostas vencedoras.
c) Dispositivo de Aposta Remoto: Um dispositivo de propriedade de jogador operado em uma rede sem fio no local ou pela Internet que, no mínimo, será usado para a execução ou formalização de apostas feitas diretamente por um jogador. Exemplos de um dispositivo de aposta remoto incluem um computador pessoal, telefone celular, tablet etc.

3.2 Software de Aposta

3.2.1 Declaração Geral

O Software de aposta será utilizado para permitir que o jogador efetue apostas e transações financeiras no Sistema de Apostas de Eventos que, baseado no design em que foi desenvolvido, poderá ser baixado ou instalado no Dispositivo de Aposta, executado a partir do sistema de Apostas de Eventos, que será acessado pelo Dispositivo de Aposta ou uma combinação dos dois.

3.2.2 Identificação do Software

O Software de Aposta deverá conter informações suficientes para identificar o software e sua versão.

3.2.3 Validação do Software

Para o software de aposta instalado localmente no dispositivo de aposta, deve ser possível autenticar que todos os componentes críticos contidos no software são válidos cada vez que o software é carregado para uso e, quando suportado pelo sistema, por solicitação, conforme exigido pelo órgão regulador. São considerados Componentes de Software Críticos, mas não estão limitados a: regras de aposta, elementos que controlam as comunicações entre o Dispositivo de Aposta e o Sistema de Apostas de Eventos, ou outros componentes de software que são necessários para garantir a operação adequada do software. No caso de erro no processo de autenticação (ou seja, incompatibilidade de programa ou falha de autenticação), o software deverá impedir as operações

de jogo e exibir uma mensagem de erro apropriada.

OBSERVAÇÃO: Os mecanismos de verificação do programa serão avaliados caso a caso e aprovados pelo órgão regulador e pelo laboratório de testes independente, com base nas práticas de normas de segurança da indústria.

3.2.4 Requisitos da Interface do Usuário

A interface do usuário será definida como um aplicativo ou programa de interface pelo qual o usuário visualiza e/ou interage com o Software de jogo. A interface do usuário deve cumprir com os seguintes requisitos:

a) As funções de todos os botões, touch ou pontos de clique devem ser claramente indicadas dentro da área da botoneira, ou touch/ponto de clique ou dentro do menu de ajuda. Não deve haver nenhuma funcionalidade disponível através de botoneiras ou pontos de clique/Touch na interface do usuário que não estejam documentados.
b) Qualquer redimensionamento ou sobreposição da interface do usuário deve ser mapeado com precisão para refletir as alterações de exibição visual e os pontos de clique/touch.
c) As instruções da interface do usuário, bem como as informações sobre as funções e serviços fornecidos pelo software, devem ser claramente comunicadas ao usuário e não devem ser enganosas ou imprecisas.
d) A exibição das instruções e informações deverão ser adaptadas à interface do usuário. Por exemplo, quando um Dispositivo de Aposta utilizar tecnologias com uma tela menor, será permitido apresentar uma versão resumida das informações do jogo, que estarão acessível diretamente na tela do jogo, e disponibilizar a versão completa das informações das regras de aposta através de outro método, como uma tela secundária, tela de ajuda ou outra interface que seja facilmente identificada na tela de aposta.

3.2.5 Entradas Simultâneas

O Software de Aposta não deve ser adversamente afetado pela ativação simultânea ou sequencial de várias entradas e saídas que podem, intencionalmente ou não, causar o mau funcionamento ou resultados inválidos.

3.2.6 Impressoras de Cupom de Apostas

Se o Dispositivo de Aposta usar uma impressora para emitir um cupom de apostas impressos para o jogador, o cupom de apostas impresso deverá incluir as informações conforme indicado na seção “Registro de apostas” deste documento. Pode ser admissível que algumas dessas informações estejam contidas no próprio cupom.

3.2.7 Comunicações

O Software de Aposta deverá ser projetado ou programado de forma que possa se comunicar apenas com componentes autorizados através de meios de comunicação seguro. Se a comunicação entre o Sistema de Apostas de Eventos e o Dispositivo de Aposta for perdida, o software deverá impedir que

outras operações de apostas sejam efetuadas e exibir uma mensagem de erro apropriada. Será permitido que o software detecte este erro quando o dispositivo tentar se comunicar com o sistema.

3.3 Dispositivos de Aposta de Autoatendimento

3.3.1 Declaração Geral

Um jogador faz uma aposta em um dispositivo de aposta de autoatendimento usando fundos de sua conta de jogador ou usando dispositivos periféricos conforme autorizado pelo órgão regulador Além dos requisitos para "Software de apostas", os requisitos aplicáveis estabelecidos no GLI-20 Normas para Quiosques e outros requisitos jurisdicionais aplicáveis observados pelo órgão regulador devem ser cumprido para todos os componentes proprietários do Dispositivo de aposta de autoatendimento.

3.4 Dispositivos de Aposta – Terminal de Venda (POS)

3.4.1 Declaração geral

Um jogador aposta no dispositivo de aposta – terminal de venda (POS) usando fundos da sua conta de jogador ou fornecendo o pagamento da(s) aposta(s) diretamente ao atendente. Além dos requisitos para "Software de Aposta", os requisitos estabelecidos nesta seção devem ser atendidos para os dispositivos de aposta (POS).

3.4.2 Telas Touchscreen

As telas touchscreen, se estiverem em uso pelo Software de Aposta, devem ser precisas e, se exigido pelo seu design, devem suportar um método de calibração para manter essa precisão; alternativamente, o hardware de exibição visual pode suportar calibração automática.

3.4.3 Cupom de Aposta impresso

Se o Dispositivo de Aposta (POS) se conectar a uma impressora para produzir cupom de aposta impressos e/ou instrumentos de apostas (vouchers e cupons), a impressora e/ou o Software de Aposta deverá ser capazes de detectar e indicar as seguintes condições de erro, quando suportadas. É permitido que a condição de erro seja detectada na tentativa de impressão:

a) Bateria fraca (quando a alimentação de energia é externa ao dispositivo de Aposta (POS));
b) Sem papel/pouco papel; e
c) Impressora desconectada.

3.4.4 Dispositivos de Aposta – Terminal de Venda (POS) sem Fio

Para dispositivos de aposta (POS) sem fio, os requisitos aplicáveis para "Interações cliente-servidor" da próxima seção também devem ser atendidos. Além disso, a comunicação só deve ocorrer entre o Dispositivo de aposta (POS) sem fio e o Sistema de Apostas de Eventos via pontos de acesso autorizados no local.

3.5 Dispositivos de Aposta Remoto

3.5.1 Declaração Geral

Um jogador só pode fazer uma aposta em um Dispositivo de aposta remoto usando fundos de sua conta de jogador (isto é, transações de apostas anônimas são proibidas). Dependendo da(s) implementação(ões) autorizada(s) pelo órgão regulador, os dispositivos de aposta remoto podem ser usados em uma rede local sem fio (WLAN) ou pela Internet. Além dos requisitos para "Software de Aposta", os requisitos estabelecidos nesta seção devem ser atendidos para os dispositivos de aposta remoto.

3.5.2 Interações Cliente-Servidor

O jogador pode obter/baixar um aplicativo ou pacote de software contendo o Software de aposta ou acessar o software utilizando um navegador para participar de apostas e transações financeiras no Sistema de Apostas de Eventos.

a) Os jogadores não poderão usar o software para transferir dados entre si, além das funções de bate-papo (por exemplo, texto, voz, vídeo, etc.) e arquivos autorizados (por exemplo, imagens de perfil de usuário, fotos, etc.);
b) O software não deve alterar automaticamente quaisquer regras de firewall especificadas pelo dispositivo para portas abertas que são bloqueadas por um firewall de hardware ou software;
c) O software não deverá acessar nenhuma porta (seja automaticamente ou solicitando que o usuário acesse manualmente) que não são seja necessária para a comunicação entre o Dispositivo de aposta remoto e o servidor;
d) Se o software incluir funcionalidades adicionais não relacionadas a aposta, essas funcionalidades adicionais não deverão alterar a integridade do software de nenhuma maneira;
e) O software não deverá ter a capacidade de substituir as configurações de volume definidas pelo do Dispositivo de Aposta remoto; e
f) O software não deverá ser usado para armazenar informações confidenciais. É recomendado que o preenchimento automático, o cache de senhas ou outros métodos que preencherão os campos de senhas sejam desabilitados por default para o software.

3.5.3 Verificação de Compatibilidade

Durante qualquer instalação ou inicialização e antes de iniciar as operações de apostas, o Software de Aposta usado em conjunto com o Sistema de Apostas de Eventos deverá detectar quaisquer incompatibilidades ou limitações de recursos com o Dispositivo de Aposta remoto que impedirá a operação adequada do software (por exemplo, versão do software, especificações mínimas não atendidas, tipo de navegador, versão do navegador, versão do plug-in, etc.). Se forem detectadas incompatibilidades ou limitações de recursos, o software deverá impedir as operações de jogo e deverá exibir uma mensagem de erro apropriada.

3.5.4 Conteúdo do Software

O Software de apostas não deverá conter nenhum código malicioso ou funcionalidade considerada de natureza maliciosa, pelo órgão regulador. Isso inclui, mas não está limitado a: extração/transferência de arquivos não autorizados, modificações de dispositivos não autorizadas, acesso não autorizado a qualquer informação pessoal armazenada localmente (por exemplo, contatos, calendário, etc.) e malware.

3.5.5 Cookies

Quando cookies são utilizados, os jogadores deverão ser informados sobre o uso do cookie na instalação do Software de Aposta ou durante o registro do jogador. Quando os cookies são necessários para a aposta, as apostas não podem ocorrer se eles não forem aceitos pelo Dispositivo de aposta remoto. Todos os cookies utilizados não poderão conter código malicioso.

3.5.6 Acesso à Informação

O Software de Aposta deverá ser capaz de exibir, diretamente na interface do usuário ou em uma página acessível ao jogador, os itens especificados nas seguintes seções deste documento. Para os Dispositivos de Aposta remoto que permitem apenas apostas dentro de um local, é aceitável divulgar ao jogador os meios de obter as informações exigidas por esta seção:

a) “Regras e conteúdo de Aposta”;
b) “Informações de proteção do jogador”;
c) “Termos e condições”;
d) “Política de privacidade”;
e) “Telas de Aposta e informações”; e
f) “Exibição de resultados”.

OBSERVAÇÃO: É aceito que o sistema estará inevitavelmente sujeito a um certo grau de atraso de sincronização para atualizações desta informação, conforme exibido por software, e é possível que as informações só sejam atualizadas na próxima interação do jogador com o software que faz com que as informações na tela sejam atualizadas.

Capítulo 4: Requisitos de Apostas em Eventos

4.1 Introdução

4.1.1 Declaração Geral

Este capítulo estabelece requisitos técnicos para operações de aposta, incluindo, mas não se limitando a, regras para realização de apostas e resultados para mercados de um evento.

4.2 Visualização da Aposta e Informação

4.2.1 Anúncio das Regras da Aposta

O operador deverá publicar as regras completas da aposta para os tipos de mercado e eventos oferecidos atualmente. Quando o Software de Aposta inclui estas regras de apostas diretamente, o software será avaliado em relação aos requisitos dentro da seção "Regras de Aposta" deste documento.

4.2.2 Informações Dinâmicas da Aposta

As seguintes informações devem ser disponibilizadas sem a necessidade de fazer uma aposta. Dentro de um local, essas informações podem ser exibidas em um Dispositivo de Aposta e/ou em um indicador externo.

a) Informações sobre eventos e mercados disponíveis para apostas;
b) Probabilidades/pagamentos e preços atuais para os mercados disponíveis;
c) Para tipos de mercados onde as apostas individuais são coletadas em fundos:
    i. Informações atualizadas de probabilidades/pagamentos para fundos de mercado simples. Para fundos de mercado complexos, é aceito que possa haver limitações razoáveis para a precisão de atualização das estimativas do fundo, exibidas ao jogador;
    ii. Valores atualizados de investimentos totais para todos os fundos do mercado; e
    iii. Os dividendos de qualquer mercado determinado.

OBSERVAÇÃO: Esta informação deve ser exibida com a maior precisão possível considerando as restrições de atrasos e latências de comunicação.

4.2.3 Recursos/Funções do Jogador

Quando permitido pelo órgão regulador, poderão ser oferecidos recursos/funções aos jogadores, como quem oferece conselhos, dicas ou sugestões a um jogador, ou um fluxo de dados que possa ser usado para facilitar a seleção de apostas externamente, se estiverem em conformidade com os seguintes requisitos:

a) O jogador deve estar ciente de cada recurso/função que está disponível, a vantagem que oferece (se houver) e as opções que existem para a seleção.

b) O método para obter cada recurso/função deve ser divulgado ao jogador. Quaisquer recursos/funções que são oferecidos ao jogador para compra devem divulgar claramente o custo.
c) A disponibilidade e funcionalidade dos recursos/funções do jogador devem ser consistentes para todos os jogadores.
d) Para apostas entre pares (*peer-to-peer)*, o jogador deve receber informações suficientes para tomar uma decisão informada, antes da participação, sobre a participação ou não com jogadores que possuam tais recursos.

4.3 Fazendo uma Aposta

4.3.1 Declaração Geral

As apostas são feitas em conjunto com uma conta de jogador ou por fundos fornecidos a um Dispositivo de Aposta ou a um atendente. Dependendo do tipo de Dispositivo de Aposta, as apostas podem ser feitas diretamente pelo jogador ou por um atendente em nome de um jogador.

OBSERVAÇÃO: As apostas feitas usando um Dispositivo de Aposta remoto só pode ser feitas atreladas a uma conta de jogador.

4.3.2 Efetuando uma Aposta

As seguintes regras aplicam-se somente à realização de uma aposta paga diretamente por um jogador no Dispositivo de Aposta:

a) O método de realização de uma aposta deve ser simples, com todas as seleções identificadas (incluindo sua ordem, se relevante). Quando a aposta envolve vários eventos (por exemplo, *parlays*), esses agrupamentos devem ser identificados.
b) Os jogadores devem ter a capacidade de selecionar o mercado no qual desejam apostar.
c) As apostas não devem ser feitas automaticamente em nome do jogador sem o consentimento/autorização do jogador.
d) Os jogadores devem ter a oportunidade de revisar e confirmar suas seleções antes que a aposta seja enviada. Isso não impede o uso de apostas “de um clique” quando permitido pelo órgão regulador e aceito pelo jogador.
e) Deverão ser identificadas situações em que o jogador fez uma aposta para a qual as probabilidades/pagamentos ou preços associados mudaram e, a menos que o jogador tenha optado por aceitar automaticamente as alterações conforme permitido pelo órgão regulador, fornecer uma notificação para confirmar a aposta considerando os novos valores.
f) Deverá ser fornecida ao jogador informação clara de que uma aposta foi aceita ou rejeitada (total ou parcialmente). Cada aposta deve ser reconhecida e claramente indicada separadamente para que não haja dúvidas sobre quais apostas foram aceitas.
g) Para apostas realizadas usando uma conta de jogador:
    i. O saldo da conta deve ser facilmente acessível.
    ii. Não deve ser aceita uma aposta que possa fazer com que o jogador tenha um saldo negativo.
    iii. O saldo da conta deve ser debitado quando a aposta é aceita pelo sistema.

4.3.3 Aceitação Automática de Mudanças na Aposta

Quando permitido pelo órgão regulador, um Sistema de Apostas de Evento pode suportar um recurso que permite que um jogador, ao fazer uma aposta, aceite automaticamente as alterações em probabilidades/pagamentos ou preço da aposta, desde que esteja em conformidade com os seguintes requisitos:

a) Todas as opções de aceitação automática disponíveis (por exemplo, aceitação automática de todas as apostas com preço mais alto, aceitação automática de todas as apostas com preço mais baixo, etc.) devem ser explicadas ao jogador;
b) O jogador deve optar manualmente por usar esta funcionalidade (ou seja, não deve ser definida por default); e
c) O jogador deve poder desistir da aceitação automática a qualquer momento.

4.3.4 Cupom de Apostas

Após a conclusão de uma transação de aposta, o jogador terá acesso a um registro de apostas que contém as seguintes informações:

a) A data e hora em que a aposta foi feita;
b) A data e a hora em que se espera que o evento ocorra (se conhecido);
c) Qualquer escolha de jogador envolvida na aposta:
    i. Linha de mercado e quota (aposta simples, apostas de margem, valores a mais/menos, *win*/*place*/*show*, etc.);
    ii. Aposta na seleção (por exemplo, nome e número do atleta ou da equipe);
    iii. Qualquer condição especial aplicada à aposta;
d) Quantia total apostado, incluindo quaisquer créditos promocionais/bônus (se aplicável);
e) Número de identificação único e/ou código de barras da aposta;
f) Identificação do usuário ou identificação exclusiva do dispositivo de aposta que emitiu o registro de aposta (se aplicável);
g) Nome do local/identificador do site (para cupom de aposta impressa, é permitido que esta informação esteja contida no próprio cupom); e
h) Período de resgate (para cupom de aposta impresso, é permitido que essas informações estejam contidas no próprio cupom).

OBSERVAÇÃO: Algumas das informações listadas acima também podem fazer parte do número de identificação exclusivo e/ou código de barras. Vários códigos de barras são permitidos e podem representar mais do que apenas o número de identificação exclusivo.

4.3.5 Encerramento do Período de Aposta

Não será possível fazer apostas após o encerramento do período de aposta.

4.3.6 Modo de Jogo Gratuito

Quando permitido pelo órgão regulador, o Sistema de Apostas de Evento pode suportar o modo de jogo gratuito, que permite que um jogador participe das apostas sem pagar. O modo de jogo grátis não deve confundir o jogador sobre as probabilidades/pagamentos disponíveis na versão paga.

4.4 Resultados e Pagamento

4.4.1 Visualização dos Resultados

O registro de resultados deve incluir acesso a todas as informações que possam afetar os resultados de todos os tipos de apostas oferecidas para aquele evento.

a) Deve ser possível para um jogador obter os resultados de suas apostas em qualquer mercado assim que os resultados forem confirmados.
b) Qualquer alteração de resultados (por exemplo, devido a estatísticas/correções de linha) deve ser disponibilizada.

4.4.2 Pagamento de Ganhos

Uma vez que os resultados do evento são registrados e confirmados, o jogador receberá o pagamento de suas apostas vencedoras. Isso não exclui a opção do jogador de receber um pagamento ajustado antes da conclusão do evento, quando oferecido e permitido pelo órgão regulador.

4.4.3 Resgate do Cupom de Apostas Ganhadoras

Os seguintes requisitos se aplicam ao resgate de uma aposta ganhadora em um dispositivo de aposta, conforme permitido pelo órgão regulador. Esta seção não se aplica a apostas ganhadoras vinculadas a uma conta de jogador que atualiza automaticamente o saldo da conta.

a) O Sistema de Apostas de Eventos processará o resgate do cupom de apostas ganhadoras de acordo com o protocolo de comunicação segura implementado.
b) Nenhum prêmio é emitido ao jogador antes da confirmação da validade do cupom de apostas ganhadoras.
c) O Sistema de Apostas de Evento deve ter a capacidade de identificar e fornecer uma notificação no caso de cupons de apostas ganhadoras que estão inválidos ou não serão resgatados nas seguintes condições:
    i. O cupom da aposta não se encontra em nenhum arquivo;
    ii. O cupom da aposta não é um vencedor;
    iii. O cupom da aposta ganhadora já foi pago; ou
    iv. A quantia do cupom da aposta ganhadora difere da quantia no arquivo (este quesito pode ser confirmado mostrando a quantia da aposta ganhadora para a confirmação durante o processo de resgate).
d) O Sistema de Apostas de Evento atualizará o status do cupom de apostas no banco de dados durante cada fase do processo de resgate. Em outras palavras, sempre que o status do registro de apostas for alterado, o sistema deverá atualizar o banco de dados.

4.5 Apostas em Eventos Virtuais

4.5.1 Declaração Geral

As apostas em eventos virtuais permitem efetuar apostas em simulações de eventos esportivos, competições e corridas cujos resultados são baseados exclusivamente na informação gerada por um Gerador de Números Aleatórios (RNG) aprovado, se permitido pelo órgão regulador. Os requisitos a seguir são aplicáveis apenas aos casos em que as apostas em eventos virtuais são totalmente conduzidas pelo Sistema de Apostas de Eventos, onde uma aposta é colocada em um dispositivo de aposta ou por interação com um atendente e, em seguida, o evento virtual é exibido em uma tela pública ou comum (por exemplo, tela externa, site, etc.). Para eventos virtuais realizados por um dispositivo de apostas (por exemplo, o jogador faz uma aposta e o evento é exibido em sua máquina ou em uma tela compartilhada em uma máquina multijogador), consulte o GLI-11Normas para Dispositivos de Aposta ou outros requisitos jurisdicionais para estar em conformidade no órgão regulador.

4.5.2 Aleatoriedade e Eventos Virtuais

Um RNG criptográfico deve ser utilizado para determinar os resultados de eventos virtuais e deve obedecer aos requisitos jurisdicionais aplicáveis e estabelecidos para os RNGs. Na ausência de normas jurisdicionais específicas, o capítulo "Gerador de Números Aleatórios (RNG)" da GLI-11 Normas para Dispositivos de Apostas deve ser usado conforme aplicável. Além disso, a avaliação dos resultados de eventos virtuais usando um RNG obedecerá às seguintes regras:

a) Quando mais de um RNG for utilizado para determinar diferentes resultados do evento virtual, cada RNG deverá ser avaliado separadamente; e
b) Se cada instância de um RNG for idêntica, mas envolver uma implementação diferente dentro do evento virtual, cada implementação deve ser avaliada separadamente.

4.5.3 Processo de Seleção de Evento Virtual

A determinação de eventos de oportunidades que resultarem em um prêmio monetário não deverá ser influenciada, afetada ou controlada por qualquer coisa que não seja os valores selecionados por um RNG aprovado, de acordo com os seguintes requisitos:

a) Não deve ser possível determinar o resultado do evento virtual antes de seu início;
b) Ao fazer chamadas para o RNG o evento virtual não deverá limitar os resultados disponíveis para seleção, exceto se estiver previsto no projeto do jogo;
c) O evento virtual não deverá modificar ou descartar os resultados selecionados pelo RNG para se adaptar a um comportamento. Além disso, os resultados deverão ser utilizados de acordo com as regras do jogo;
d) Após o início de um evento virtual, nenhuma outra ação ou decisão poderá ser tomada para alterar o comportamento de qualquer elemento do acaso no evento virtual, além das decisões do jogador;

e) Exceto, se previsto nas regras do evento virtual, os eventos de probabilidade deverão ser independentes e não deverão se correlacionar com quaisquer outros eventos dentro do mesmo evento virtual, ou eventos em eventos virtuais anteriores;
f) Qualquer equipamento associado que será utilizado em conjunto com um Sistema de Apostas de Eventos não deverá influenciar ou modificar os comportamentos do RNG do jogo e/ou o processo de seleção aleatória, exceto se autorizado ou pretendido pelo projeto;
g) Os resultados de eventos virtuais não devem ser afetados pela capacidade de banda larga, pela utilização de links, pela taxa de erro de bit ou por outras características do canal de comunicação entre o Sistema de apostas de eventos e o dispositivo de aposta; e
h) O software de aposta não deve conter nenhuma lógica utilizada para gerar o resultado de qualquer evento virtual. Todas as funções críticas, incluindo a geração de qualquer evento virtual, devem ser geradas pelo Sistema de Apostas de Eventos e ser independentes do dispositivo de aposta.

4.5.4 Visualização de Evento Virtual

As telas de um evento virtual devem estar conforme os requisitos para visualização definidos por esta norma. Além disso, os seguintes requisitos se aplicam para a visualização:

a) Os dados estatísticos que são disponibilizados para o jogador a respeito do evento virtual não devem deturpar as capacidades de nenhum participante virtual. Isso não impede o uso de um elemento de probabilidade ou aleatoriedade de afetar os resultados do participante virtual durante o evento virtual.
b) Para eventos virtuais agendados, uma contagem regressiva do tempo restante para fazer uma aposta nesse evento deverá ser exibida ao jogador. Não deverá ser possível fazer apostas no evento uma vez que este tempo tenha passado; no entanto, este requisito não proíbe a implementação de apostas durante o jogo.
c) Cada participante virtual deve ter uma aparência única, quando aplicável à aposta. Por exemplo, se a aposta for em uma equipe para vencer outra, os participantes virtuais não precisam ter uma aparência única, no entanto, as equipes em que estão devem ser visualmente distintas uma da outra.
d) O resultado de um evento virtual deve ser claro, sem ambiguidade e exibido por um período suficiente para dar ao jogador uma oportunidade razoável de verificar o resultado do evento virtual.

4.5.5 Simulação de Objetos Físicos

Quando um evento virtual incorporar uma representação gráfica ou simulação de um objeto físico utilizado para determinar o resultado de um jogo, os comportamentos retratados pela simulação deverão ser consistentes e de acordo com objeto do mundo real, a menos que indicado de outra forma na artwork do jogo. Este requisito não se aplicará a representações gráficas ou simulações utilizadas apenas para fins de entretenimento. Os seguintes requisitos deverão ser aplicados quando se tratar de uma simulação:

a) A probabilidade de qualquer evento ocorrer durante a simulação que afete o resultado do evento virtual deverá ser análoga as propriedades do objeto físico;

b) Quando o evento virtual simular vários objetos físicos, que normalmente seriam independentes uns dos outros, com base nas regras do evento virtual, cada simulação deverá ser independente de quaisquer outras simulações; e
c) Quando o evento virtual simula objetos físicos que não têm memória de eventos anteriores, o comportamento dos objetos simulados deverá ser independente de seu comportamento anterior, de modo a ser não adaptativo e imprevisível, a menos que seja informado de outra forma ao jogador.

4.5.6 Mecanismo Físico

Os eventos virtuais podem utilizar um "mecanismo físico" que é um software especializado que aproxima ou simula um ambiente físico, incluindo comportamentos como movimento, gravidade, velocidade, aceleração, inércia, trajetória, etc. O mecanismo físico deverá ser projetado para manter comportamentos de jogo e ambiente do evento virtual consistentes, a menos que se indique o contrário ao jogador. Um mecanismo físico poderá utilizar as propriedades aleatórias de um RNG para impactar o resultado do evento virtual.

OBSERVAÇÃO: As implementações de um mecanismos físico em um evento virtual serão avaliadas caso a caso por um laboratório de testes independente.

4.6 Sistemas de Apostas Externo

4.6.1 Declaração Geral

Esta seção contém requisitos para as circunstâncias em que o Sistema de Apostas de Eventos se comunica com um sistema de aposta externo em qualquer uma das seguintes configurações:

a) O Sistema de Apostas de Eventos está agindo como o "sistema de aposta anfitrião" recebendo, para seus próprios mercados, apostas de um ou mais "sistemas de aposta cliente" externo; ou
b) O Sistema de Apostas de Eventos está agindo como um "sistema de aposta cliente", passando as apostas para um "sistema de aposta anfitrião", para os mercados desse sistema.

OBSERVAÇÃO: Os requisitos desta secção aplicam-se à interoperabilidade do Sistema de Apostas de Eventos com o sistema de aposta externo e não são uma avaliação completa do próprio sistema de aposta externo. O sistema de aposta externo pode ser independentemente submetido a avaliação pelo laboratório de testes independente por critério do órgão regulador.

4.6.2 Informações

Os requisitos a seguir se aplicam às informações que estão sendo transmitidas entre o sistema de aposta anfitrião e o sistema de aposta cliente:

a) Se o sistema de aposta anfitrião fornecer apostas parimutuel para o sistema de aposta cliente , o Sistema de Apostas de Eventos deverá ser capaz de:
   i. Ao atuar como o sistema de aposta cliente, receba os dividendos atuais para fundos ativos enviados do sistema de aposta anfitrião.

ii. Ao atuar como o sistema de aposta anfitrião, passe os dividendos atuais para os fundos ativos para todos os sistemas de apostas cliente conectados.

b) Se o sistema de aposta anfitrião fornecer apostas de probabilidades fixas para o sistema de aposta cliente onde as probabilidades/pagamentos e preços podem ser alterados dinamicamente, o Sistema de Apostas de Eventos deve ser capaz de:
   i. Ao atuar como o sistema de aposta cliente, receba as probabilidades/pagamentos e os preços autais enviados do sistema de aposta anfitrião sempre que quaisquer probabilidades/pagamentos e preços forem alterados
   ii. Ao atuar como o sistema de aposta anfitrião, passe as probabilidades/pagamentos e os preços atuais para todos os sistemas de apostas clientes conectados sempre que quaisquer probabilidades/pagamentos e preços forem alterados.
c) A mudança das informações de status do evento deve ser passada do sistema de aposta anfitrião para o sistema de o sistema de aposta cliente sempre que ocorrer qualquer alteração, incluindo:
   i. Escolhas recusadas/reintegradas;
   ii. Hora de início do evento alterada;
   iii. Mercados individuais fechados/abertos;
   iv. Resultados inseridos/modificados;
   v. Resultados confirmados; e
   vi. Evento cancelado.

4.6.3 Apostas

Os requisitos a seguir se aplicam as apostas que estão sendo efetuadas entre o sistema de apostas anfitrião e o sistema de apostas cliente:

a) As apostas feitas no sistema de aposta cliente devem receber uma confirmação clara de aceitação, aceitação parcial (incluindo detalhes) ou rejeição enviado pelo sistema de apostas anfitrião.
b) Se o custo da aposta for determinado pelo sistema de apostas anfitrião, deverá existir uma sequência positiva de confirmação para permitir que o jogador aceite o custo da aposta e o sistema de aposta cliente para determinar se existem fundos suficientes no saldo da conta para cobrir o custo da aposta antes de fazer a oferta ao sistema de aposta anfitrião.
c) Quando apostas podem ser feitas aos poucos, os seguintes requisitos se aplicam:
   i. Se o fluxo de apostas for interrompido por qualquer motivo, deverá haver um meio disponível para determinar em que ponto do fluxo a interrupção ocorreu.
   ii. Nenhuma aposta pode ser transmitida se esta for maior que o saldo da conta. Se houver a tentativa de efetivar uma aposta nestas condições, todo o fluxo deve ser interrompido.
d) O saldo da conta será debitado em um montante igual a oferta e o custo do sistema de aposta anfitrião. Os fundos devem permanecer como uma transação pendente com detalhes da oferta para o sistema de aposta do anfitrião. Ao receber a confirmação do sistema de aposta anfitrião, os ajustes apropriados devem ser feitos à conta "pendente" e ao saldo da conta no sistema de aposta cliente.
e) Os pedidos de cancelamento do sistema de aposta cliente devem receber uma confirmação clara de aceitação ou rejeição pelo sistema de aposta anfitrião. O jogador não deve ser creditado pelo sistema de aposta cliente até que a confirmação final seja recebida do sistema de aposta anfitrião, incluindo o valor da aposta anulada ou cancelada.

4.6.4 Resultados

Quando os resultados são inseridos e confirmados no sistema de aposta anfitrião, cada aposta ganhadora será transferida para o sistema de aposta cliente com o valor ganho. A confirmação do recebimento das apostas ganhadoras deve ser reconhecida pelo sistema de aposta cliente.

Anexo A: Auditoria Operacional de Procedimentos e Práticas de Jogos

A.1 Introdução

A.1.1 Declaração Geral

Este anexo estabelecerá os procedimentos e práticas para operações de aposta que serão revisadas em uma auditoria operacional como parte da avaliação do Sistema de Apostas de Eventos, incluindo, mas não se limitando a: estabelecer regras de aposta, suspensão de eventos, processamento de várias transações financeiras e de apostas, criação de mercados., pagamentos de apostas, fechamento de mercados, cancelamentos de eventos, anulação ou cancelamento de apostas, gerenciamento de contas de jogadores, práticas fundamentais relevantes para a limitação de riscos e quaisquer outros objetivos estabelecidos pelo órgão regulador.

OBSERVAÇÃO: Também será reconhecido que procedimentos e práticas adicionais que não estão especificamente incluídos nesta norma serão relevantes e necessários para uma auditoria operacional conforme determinado pelo operador e/ou pelo órgão regulador dentro de suas regras, regulamentos e Padrões Mínimos de Controle Interno (MICS).

A.2 Procedimentos de Controles Internos

A.2.1 Procedimentos de Controles Internos

O operador deverá estabelecer, manter, implementar e cumprir os procedimentos de controle interno para operações de apostas, incluindo a realização de aposta e transações financeiras.

A.2.2 Gerenciamento de Informação

Os controles internos do operador deverão incluir os processos para manter as informações especificadas na seção intitulada "Informações a Serem Mantidas" armazenadas por um período de cinco anos ou conforme especificado pelo órgão regulador.

A.2.3 Gerenciamento de Riscos

Os controles internos do operador deverão conter detalhes sobre o contexto de sua estratégia de gestão de riscos, incluindo, mas não se limitando a:

a) Procedimentos automatizados e manuais de gerenciamento de riscos;
b) Gestão de funcionários, incluindo controles de acesso e segregação de funções;
c) Informações sobre a identificação e denúncias de fraude e condutas suspeitas;
d) Controles que irão garantir a conformidade regulatória;
e) Descrição das normas de conformidade contra a Lavagem de Dinheiro (AML), incluindo procedimentos para detectar qualquer tentativa de mascarar dados dos relatórios;

f) Descrição de todas os aplicativos de softwares que compõem o Sistema de Apostas de Eventos;
g) Descrição de todos os tipos de apostas disponíveis a serem oferecidas pelo operador;
h) Descrição do método para impedir que sejam feitas apostas antes/depois;
i) Descrição de todos os prestadores de serviços terceirizados; e
j) Qualquer outra informação requerida pelo órgão regulador.

A.2.4 Jogadores Restritos

Os controles internos do operador deverão descrever os métodos para impedir que os jogadores apostem em eventos dos quais possam ter informações privilegiadas, incluindo, entre outros, os exemplos a seguir, conforme exigido pelo órgão regulador:

a) Jogadores identificados como empregados, subcontratados, diretores, proprietários e oficiais de um operador, bem como aqueles que residem no mesmo domicílio, não devem fazer apostas em nenhum evento, exceto em fundos privados onde sua associação com o operador é claramente divulgada.
b) Jogadores identificados como atletas profissionais ou universitários, funcionários da equipe e proprietários, treinadores, gerentes, assistentes, fisioterapeutas, oficiais e funcionários da liga, árbitros, juízes, agentes esportivos e funcionários de um sindicato de jogadores, bem como aqueles que residem no mesmo domicílio, não devem fazer apostas em nenhum evento do esporte em que participem, ou no qual o atleta que eles representam participe.

A.3 Controles da Conta do Jogador

A.3.1 Registro e Verificação

Quando o registro da conta do jogador for feito manualmente pelo operador, deverão ser estabelecidos procedimentos para cumprir com os requisitos do capítulo “Registro e Verificação” conforme indicado neste documento.

A.3.2 Contas Fraudulentas

O operador deverá disponibilizar uma política pública documentada para o tratamento das contas de jogadores descobertas como sendo usadas de forma fraudulenta, incluindo, mas não se limitando a:

a) A manutenção de informações sobre a atividade de qualquer conta, de modo que, se for detectada atividade fraudulenta, o operador tenha as informações necessárias para tomar as medidas cabíveis;
b) A suspensão de qualquer conta envolvida em atividades fraudulentas, como por exemplo, quando um jogador permitir através de sua conta o acesso a menores; e
c) O tratamento de depósitos, apostas e ganhos associados a uma conta fraudulenta.

A.3.3 Termos e Condições

Um conjunto de termos e condições deverão estar disponíveis para o jogador. Durante o processo de registro e quando quaisquer termos e condições forem significantemente atualizados (ou seja,

quando for modificações mais importantes que alterações gramaticais ou outras de menor importância), o jogador deverá dar seu de acordo com os termos e condições. Estes documentos deverão:

a) Declarar que apenas indivíduos legalmente permitidos por sua respectiva jurisdição poderão participar de apostas;
b) Orientar o jogador a manter suas credenciais de autenticação (por exemplo, usuário e senha) seguras;
c) Divulgar todos os processos a serem cumpridos nos casos de perda de credenciais de autenticação, alterações obrigatórias de senha, segurança das senhas e outros itens relacionados;
d) Especificar as condições sob as quais uma conta deverá ser considerada inativa e explicar quais ações deverão ser realizadas na conta depois que for considerada inativa; e
e) Definir claramente o que acontece com as apostas pendentes do jogador feitas antes de qualquer exclusão autoimposta ou imposta pelo operador, incluindo o reembolso de todas as apostas ou o processamento de todas as apostas, conforme apropriado.

A.3.4 Política de Privacidade

A Política de Privacidade deverá estar disponível para o jogador. Durante o processo de registro e quando a política de privacidade for significantemente atualizados (ou seja, quando for modificações mais importantes que alterações gramaticais ou outras de menor importância), o jogador deverá dar seu de acordo a política de privacidade. Este documento deverá conter:

a) Os dados do jogador que precisam ser coletados;
b) O objetivo da coleta de informações;
c) O período em que as informações são armazenadas;
d) As condições sob as quais as informações podem ser divulgadas; e
e) Afirmação de que medidas estarão em vigor para evitar a divulgação não autorizada ou desnecessária das informações.

A.3.5 Segurança de Dados do Jogador

Qualquer informação obtida em relação à conta do jogador, incluindo dados do jogador, deve ser feita em conformidade com a política de privacidade e as normas e padrões de privacidade locais observados pelo órgão regulador. Além disso:

a) Quaisquer dados de jogadores que não estejam sujeitos à divulgação de acordo com a política de privacidade devem ser mantidos confidenciais, exceto quando a divulgação dessas informações for exigida por lei.
b) Deverão existir procedimentos para a segurança e compartilhamento de dados de jogadores, valores de uma conta de jogador e outras informações confidenciais conforme exigido pelo órgão regulador, incluindo, mas não se limitando a:
    i. A designação e identificação de um ou mais funcionários com responsabilidade primária pelo projeto, implementação e avaliação contínua de tais procedimentos e práticas;
    ii. Os procedimentos a serem utilizados para determinar a natureza e o escopo de todas as informações coletadas, os locais em que essas informações serão armazenadas e os

dispositivos de armazenamento nos quais essas informações poderão ser guardadas para fins de armazenamento ou transferência;
iii. As medidas a serem utilizadas para proteger as informações de acesso não autorizado; e
iv. Os procedimentos a serem utilizados no caso de o operador determinar que ocorreu uma violação da segurança dos dados, incluindo a notificação necessária ao órgão regulador.

A.3.6 Transações Financeiras

Os procedimentos deverão estar em vigor para garantir que todas as transações financeiras sejam conduzidas de acordo com os regulamentos e requisitos comerciais locais exigidos pelo órgão regulador:

a) Quando as transações financeiras não puderem ser realizadas automaticamente pelo Sistema de Apostas de Eventos, os procedimentos deverão estar em vigor para cumprir com os requisitos de "Manutenção de fundos de jogadores", conforme indicado neste documento.
b) A identificação ou autenticação positiva do jogador deverá ser concluída antes que o saque de qualquer valor possa ser feita pelo jogador.
c) O pedido de um jogador para saques de valores (ou seja, valores depositados e liberados e apostas ganhas) deverá ser concluído pelo operador dentro de um período de tempo razoável, a menos que haja uma reclamação/disputa ou investigação pendente. Tal investigação deverá ser documentada pelo operador e disponibilizada para revisão pelo órgão regulador.
d) O operador deverá ter procedimentos de segurança ou autorização em vigor para garantir que apenas ajustes autorizados possam ser feitos nas contas dos jogadores, e essas alterações deverão ser auditáveis.

A.3.7 Limitações

Os jogadores deverão receber orientação de como proceder para impor limitações aos parâmetros de aposta,incluindo, mas não se limitando a, depósitos e apostas, conforme exigido pelo órgão regulador. Além disso, deverá haver uma forma para que o operador possa também impor quaisquer limitações aos parâmetros de aposta, conforme exigido pelo órgão regulador.

a) Uma vez estabelecido por um jogador e implementado pelo operador, só será possível reduzir uma limitação definida pelo jogador mediante aviso de vinte e quatro horas, ou conforme exigido pelo órgão regulador;
b) Os jogadores deverão ser notificados com antecedência sobre quaisquer limites impostos pelo operador e suas datas de vigência. Uma vez atualizados, os limites impostos pelo operador deverão ser consistentes com o que for divulgado ao jogador; e
c) Ao receber qualquer pedido de limitação feita pelo jogador ou pelo operador, o operador deverá garantir que todos os limites especificados sejam corretamente implementados imediatamente ou no momento indicado para o jogador (por exemplo, próximo login, dia seguinte).

A.3.8 Exclusões

Os jogadores deverão receber orientações de como fazer para se excluírem do jogo por um período especificado ou indefinidamente, conforme exigido pelo órgão regulador. Além disso, deverá haver

uma forma do operador excluir um jogador do jogo, conforme exigido pelo órgão regulador.

a) Os jogadores deverão receber uma notificação contendo o status de exclusão e instruções gerais para a resolução, sempre que possível;
b) Imediatamente após o recebimento da ordem de exclusão, nenhuma nova aposta ou depósito deverão ser aceitos daquele jogador, até que a exclusão seja removida;
c) Durante o período que estiver excluído, o jogador não deverá ser impedido de sacar qualquer ou todo o saldo da sua conta, desde que o operador reconheça que os valores foram compensados e que o(s) motivo(s) da exclusão não proíbem o saque; e
d) Nenhum material de propaganda ou marketing deverá ter como alvo específico os jogadores que foram excluídos do jogo.

A.3.9 Contas Inativas

Uma conta de jogador será considerada inativa de acordo com as condições especificadas nos termos e condições. Os procedimentos deverão estar em vigor para:

a) Proteger contas de jogadores inativos que contêm saldos, de acesso não autorizado, alterações ou remoção; e
b) Operar com os valores não reclamados de contas de jogadores inativas, incluindo devolver quaisquer valores restantes para o jogador sempre que possível.

A.4 Procedimentos Gerais de Operação

A.4.1 Reservas do Operador

O Operador deverá ter processos em vigor para manter e proteger as reservas de caixa adequadamente, conforme determinado pelo órgão regulador, incluindo contas segregadas de valores mantidos para contas de jogadores e quaisquer fundos operacionais como aqueles usados para cobrir apostas ganhadoras não reclamadas, apostas possivelmente vencedoras no dia de, etc.

A.4.2 Proteção dos Saldos do Jogador

O operador deverá ter processos em vigor para garantir que os valores em uma conta de operador sejam mantidos em segurança para o jogador em uma conta segregada para fins especiais que será mantida e controlada por uma entidade corporativa adequadamente constituída que não seja o operador e cujo conselho administrativo inclua um ou mais diretores corporativos que são independentes do operador e de qualquer corporação relacionada ou controlada pelo operador. Além disso, o operador deve estabelecer procedimentos que sejam razoavelmente utilizados para:

a) Garantir que os fundos gerados pela aposta sejam garantidos e contabilizados;
b) Deixar claro que os fundos de contas segregadas não pertencem ao operador e não estão disponíveis para outros credores além do jogador para o qual os valores estão sendo mantidos; e
c) Impedir a mistura de valores de contas segregadas com outros valores, incluindo sem limitação, fundos do operador.

A.4.3 Tributação

O operador deverá ter um processo implementado para identificar todos os ganhos que estão sujeitos a tributação (ganhos únicos ou ganhos agregados ao longo de um período definido, conforme necessário) e fornecer as informações necessárias de acordo com os requisitos de tributação de cada entidade reguladora.

OBSERVAÇÃO: Valores ganhos que excederem qualquer limite especificado pela jurisdição exigirão que a documentação apropriada seja preenchida antes que o jogador seja pago.

A.4.4 Processo de Reclamação/Disputa

O operador deverá fornecer uma forma para que o jogador possa fazer uma reclamação/disputa e permitir que o jogador notifique o órgão regulador se tal reclamação/disputa não for ou não puder ser tratada pelo operador, ou em outras circunstâncias, conforme especificado pela lei do órgão regulador.

a) Os jogadores deverão ser capazes de registrar reclamações/disputas 24 horas por dia, 7 dias por semana.
b) Deverá ser estabelecido um processo documentado entre o operador e o órgão regulador para o procedimento de informar e o de resolver uma reclamação/disputas.
c) Deverá ser estabelecido um processo documentado entre o operador e o órgão regulador para o registro da informação e resolução de reclamações/disputas.

A.4.5 Informação para a Proteção do Jogador

As informações para a proteção do jogador deverão estar disponíveis para o jogador. As informações para a proteção do jogador deverão conter no mínimo:

a) Informações sobre os riscos potenciais associados ao jogo excessivo e onde obter ajuda para um problema de jogo;
b) Uma declaração de que nenhum menor de idade está autorizado a participar de qualquer jogo;
c) Uma lista das medidas de proteção ao jogador disponíveis que poderão ser solicitadas pelo jogador, como a exclusão pelo próprio jogador, e informações sobre como solicitar estas medidas;
d) Para contas de jogadores, mecanismos em vigor que possam ser usados para detectar o uso não autorizado de suas contas, como checar o extrato de cartão de crédito contra depósitos conhecidos;
e) Informações de contato ou outros meios para relatar uma reclamação/disputa; e
f) Informações de contato do órgão regulador e/ou link para seu site.

A.5 Regras de Aposta e Conteúdo

A.5.1 Regras de Aposta

As regras de aposta referem-se a qualquer informação escrita, gráfica e auditiva fornecida ao público em relação as operações de apostas de eventos. O operador deve adotar e aderir a regras de apostas dabrangentes, que deverão ser aprovadas pela entidade reguladora:

a) As regras de apostas deverão ser completas, inequívocas e não enganosas ou injustas para o jogador.
b) As regras de aposta apresentadas auditivamente (por som ou voz) também deverão ser apresentadas por escrito.
c) As regras de aposta deverão ser apresentadas em uma cor que contraste com a cor de fundo da tela para garantir que todas as informações sejam claramente visíveis/legíveis.
d) O operador deverá manter um registro de quaisquer mudanças nas regras de aposta relacionadas a fazer apostas.
e) Quando as regras de apostas forem alteradas para eventos ou mercados oferecidos, todas as alterações de regras deverão ter a data e hora de vigência, mostrando a regra aplicável em cada período. Se várias regras estiverem vigentes para um jogo, o operador deverá aplicar as regras que estava vigente no momento em que a aposta foi aceita.

A.5.2 Conteúdo das Regras de Aposta

As seguintes informações devem ser disponibilizadas ao jogador. Para apostas feitas em um local, é aceitável que essas informações sejam exibidas diretamente pelo Dispositivo de apostas ou por meio de sinalização externa, formulários ou folhetos disponíveis:

a) Os métodos de financiamento de uma aposta ou conta de jogador, incluindo uma explicação clara e concisa de todas as taxas (se aplicável);
b) Se permitido pelo órgão regulador, quaisquer prêmios oferecidos na forma de mercadorias, anuidades, pagamentos de valor fixo ou planos de pagamento em vez de pagamentos em dinheiro, para cada jogo que poderá oferecer tal forma de pagamento de prêmio;
c) Os procedimentos pelos quais quaisquer avarias irrecuperáveis de hardware/software serão tratadas, incluindo se este processo resultar na anulação ou cancelamento de quaisquer apostas;
d) Os procedimentos para lidar com interrupções causadas pela descontinuidade da transmissão de dados do servidor de rede durante um evento;
e) Regras de participação, incluindo toda elegibilidade de aposta e critério para a pontuação, eventos disponíveis e mercados, tipos de apostas aceitas, linhas de quotas, todos os prêmios anunciados e o efeito das mudanças de programação;
f) Informações de pagamento, incluindo as combinações ganhadoras possíveis, qualificação e resultados, juntamente com seus pagamentos correspondentes, para qualquer opção de aposta disponível;
g) Quaisquer funções restritivos de apostas, como valores de apostas ou valores máximos de ganhos;
h) Uma descrição sobre jogadores restritos, incluindo quaisquer limitações aplicáveis em apostas para eles (por exemplo, os atletas não devem apostar em seu esporte);
i) Os procedimentos para lidar com anúncio incorreto de eventos, mercados, probabilidades/pagamentos, preços, apostas ou resultados;
j) Uma política de cancelamento de aposta que inclui apostas com múltiplos eventos (por exemplo, *parlays*) e indicar quaisquer proibições de anular ou cancelar apostas (por exemplo, após um

período fixo);

k) Se os pagamentos/probabilidades são fixos no momento da aposta, ou se as probabilidades/pagamentos podem mudar dinamicamente antes do início do evento e o método de anunciar alterações nas probabilidades/pagamentos;
l) Para tipos de apostas em que os pagamentos/probabilidades são fixados quando a aposta é feita, quaisquer situações em que as probabilidades/pagamentos possam ser ajustadas, como resultados vencedores atípicos (por exemplo, *empates*), *partes canceladas* de apostas com múltiplos eventos (por exemplo, *parlays*) e rateio;
m) Para os tipos de apostas em que as apostas individuais são reunidas em fundos, as regras para cálculo de dividendos incluem a fórmula predominante para alocações de fundos e as estipulações do evento que está sendo apostado conforme aprovado pelo órgão regulador;
n) Para apostas durante o jogo, devido a diferentes velocidades de transmissão ou latências de transmissão:
    i. Atualizações das informações exibidas podem colocar um jogador em desvantagem em relação a outros que possam ter informações mais atualizadas; e
    ii. Pode haver atrasos incorporados no tempo registrado de uma aposta durante o jogo para prevenir apostas antes/depois e cancelamentos.
o) Uma declaração de que o operador se reserva o direito de:
    i. Recusar qualquer aposta ou parte de uma aposta ou rejeitar ou limitar seleções antes da aceitação de uma aposta por razões indicadas ao jogador nestas regras;
    ii. Aceitar uma aposta em termos diferente dos que foram publicados; e
    iii. Encerrar os períodos de apostas a seu critério;
p) Se os prêmios devem ser pagos por combinações envolvendo participantes que não sejam apenas o primeiro colocado (por exemplo, em uma competição olímpica), a ordem dos participantes que podem estar envolvidos com esses prêmios (por exemplo, resultado 8-4-7);
q) As regras para quaisquer opções de apostas exóticas (por exemplo, *perfecta*, *trifeta*, *quiniela*, etc.) e os pagamentos esperados;
r) O que deve ocorrer quando um evento ou mercado é cancelado ou retirado, incluindo o tratamento de apostas de seleção com múltiplos eventos (por exemplo, *parlays*) em que uma ou mais partes são cancelados ou retirados;
s) Como uma aposta ganhadora é determinada e o tratamento de um prêmio em caso em que um empate é possível;
t) O pagamento de apostas ganhadoras, incluindo o período de resgate e o método de cálculo. Quando o cálculo dos pagamentos puder envolver arredondamentos, as informações sobre como essas circunstâncias são tratadas devem explicar claramente:
    i. Arredondamento para mais, para menos (truncamento), arredondamento autêntico; e
    ii. Arredondamento a qual nível (por exemplo, 5 centavos).

A.5.3 Promoções e/ou Bonificações

Os jogadores devem poder acessar as informações contidas nas regras de apostas referentes a quaisquer promoções e/ou bonificações disponíveis, incluindo a forma como o jogador é notificado quando recebeu um prêmio promocional ou ganhou um bônus e os termos da sua retirada. Essas informações devem ser claras e não ambíguas, especialmente quando promoções ou bonificações são limitados a certos eventos, mercados ou quando outras condições específicas se aplicam.

A.5.4 Competições/Torneios

Uma competição/torneio, que permite que um jogador comprar ou ter a oportunidade de participar de competição de apostas contra outros jogadores, poderá ser permitido desde que as seguintes regras sejam cumpridas:

a) As regras deverão ser disponibilizadas para que o jogador possa revisá-la antes de seu registro na competição/torneio. As regras deverão incluir, no mínimo:
   i. Todas as condições que os jogadores registrados deverão atender para se qualificar para entrar e avançar na competição/torneio;
   ii. Informações específicas relativas qualquer competição/torneio único, incluindo os prêmios ou recompensas disponíveis e a distribuição de valores com base em resultados específicos; e
   iii. O nome da organização (ou das pessoas) que conduzirá a competição/torneio em nome ou em conjunto com o operador (se aplicável).
b) Procedimentos deverão ser estabelecidos para registrar os resultados de cada competição/torneio e disponibilizar publicamente para os jogadores registrados revisarem por um período de tempo razoável. Após serem divulgados publicamente, os resultados de cada competição/torneio deverão ser disponibilizados mediante solicitação. Os resultados incluem o seguinte:
   i. Nome da competição/torneio;
   ii. Data/hora da competição/torneio;
   iii. Número total de entradas;
   iv. Valor total de taxas de inscrição;
   v. Valor total do prêmio acumulado; e
   vi. Valor pago para cada categoria ganhadora.

OBSERVAÇÃO: Para competições/torneios gratuitos (ou seja, o jogador registrado não paga uma taxa de inscrição), as mesmas informações exigidas acima deverão ser registradas, exceto o número total de entradas, valor total de taxas de inscrição e o valor total do prêmio acumulado.

A.6 Procedimentos e Controles de Aposta

A.6.1 Probabilidades/Pagamentos e Preços

Deverão ser estabelecidos procedimentos para configurar e atualizar as probabilidades/pagamentos e preços, incluindo informar publicamente as probabilidade/pagamentos e preços atuais, alterar probabilidades/pagamentos e preços conforme necessário para tratar exceções e registrar adequadamente e periodicamente as probabilidades/pagamentos e preços.

A.6.2 Estatísticas/Linha de Ensaio

O operador deve assegurar que quaisquer dados estatísticos/de ensaio que forem disponibilizados ao jogador a respeito de um evento usem uma fonte permitida pelo órgão regulador e sejam mantidos razoavelmente precisos e atualizados. Conforme exigido pelo órgão regulador, o operador deve implementar controles para:

a) Revisar a precisão e a oportunidade de quaisquer serviços de estatística/ensaio; e
b) Quando ocorrer um incidente ou erro que resulte na perda de comunicação com serviços de estatísticas/ensaio, o incidente ou erro deverá ser registrado juntamente com a data e hora da ocorrência, sua duração, natureza e uma descrição de seu impacto no desempenho sistema. Esta informação deve ser mantida por um período de 90 dias, ou conforme especificado pelo órgão regulador.

A.6.3 Suspensão de Mercados ou Eventos

Deverão ser estabelecidos procedimentos para suspender mercados ou eventos (por exemplo, deixar de aceitar apostas para esse mercado ou mercados associados a esse evento). Quando as apostas são suspensas para um evento ativo, deverá ser criada uma informação em um registro de auditoria que inclua a data e hora da suspensão e seu motivo.

A.6.4 Cancelamento de Apostas

As transações de apostas não podem ser modificadas, exceto para serem anuladas ou canceladas, conforme previsto na política de cancelamento publicada pela operadora. Um período de carência de cancelamento pode ser oferecido para permitir que os jogadores solicitem o cancelamento de apostas feitas. Os seguintes requisitos se aplicam ao cancelamento de apostas:

a) Cancelamentos iniciados por jogadores podem ser autorizados de acordo com a política de cancelamento.
b) Cancelamentos iniciados pelo operador devem fornecer uma razão de cancelamento para o jogador (por exemplo, uma aposta antecipada).
c) Um operador não deve anular ou cancelar nenhuma aposta sem a aprovação prévia do órgão regulador.

A.6.5 Períodos de Aposta

Deverá existir uma documentação para definir como o período de apostas é controlado. Isso inclui todos os casos quando o período de apostas é inicialmente aberto, quando é encerrado ou qualquer outro momento neste período em que uma aposta não possa ser feita (por exemplo, probabilidades/pagamentos e preços estão sendo atualizados).

A.6.6 Resultados

Antes de anunciar os resultados publicamente e declarar os ganhadores, deve haver uma política para confirmação de resultados com base em fontes qualificadas e aprovadas, a menos que seja automatizada por uma fonte externa. Se uma fonte externa estiver em uso, devem existir procedimentos em vigor para casos em que o acesso a fonte externa não esteja disponível. Deve haver também um procedimento para tratar mudanças nos resultados (por exemplo, devido a correções de estatísticas/linha).

A.6.7 Pagamento de Apostas Ganhadoras

No caso de uma falha na capacidade do Sistema de Apostas de Eventos de pagar as apostas ganhadoras, o operador deve estabelecer controles detalhando o método de pagamento dessas apostas.

A.6.8 Eventos Virtuais

Um operador que oferece apostas de eventos virtuais deve manter todas as informações necessárias para reconstruir adequadamente os eventos virtuais, incluindo o resultado de eventos virtuais e / ou ações de participantes virtuais, realizados nos últimos 90 dias ou conforme exigido pelo órgão regulador. Essas informações podem ser registradas pelo Sistema de Apostas de Eventos ou equipamentos associados, usando uma combinação de texto, registros, vídeo, gráficos, capturas de tela ou outros meios (por exemplo, mecanismo "registro de voo"). Alternativamente, procedimentos podem ser incluídos para que a exibição pública do evento virtual seja registrada pelo sistema de vigilância .

A.7 Especificações de Local de Apostas

A.7.1 Auditoria de Verificação do Local

O local de apostas será obrigado a cumprir com os aspectos aplicáveis da política adequada e/ou documentos de procedimento, conforme determinado pelo operador em consulta com o órgão regulador. Para manter a integridade das operações de apostas, os locais podem estar sujeitos a uma auditoria de verificação adicional, conforme exigido pelo órgão regulador. As seguintes especificações se aplicam a locais:

A.7.2 Equipamento de Aposta

O local deverá fornecer um lugar seguro para a colocação, operação e uso de equipamentos de apostas, incluindo Dispositivos de apostas, telões e equipamentos de comunicação. Políticas e procedimentos de segurança devem ser implementados e revisados periodicamente para assegurar que os riscos sejam identificados, mitigados e garantidos por planos de contingência. Além disso:

a) O equipamento de apostas deve ser instalado de acordo com um plano definido e deverão ser mantidos os registos de todos os equipamentos de apostas instalados.
b) O equipamento de apostas deve estar colocado ou protegido a fim reduzir os riscos de:
   i. Ameaças e perigos ambientais;
   ii. Oportunidades para acesso não autorizado;
   iii. Falhas de energia; e
   iv. Outras interrupções causadas por falhas em suporte a utilitários.
c) O acesso de um funcionário ao equipamento de apostas deve ser controlado por um procedimento de acesso seguro ou outro processo seguro aprovado pelo órgão regulador para garantir que somente funcionários autorizados tenham acesso permitido. Não deverá ser possível modificar os ajustes de configuração do equipamento de apostas sem um processo seguro autorizado.

d) Uma sessão de usuário, quando suportada pelo equipamento de apostas, é iniciada pelo funcionário que faz login em sua conta de usuário usando seu nome de usuário e senha seguros ou um meio alternativo para o funcionário fornecer suas credenciais de acesso conforme permitido pelo órgão regulador.
   i. Todas as opções disponíveis apresentadas ao funcionário deverão estar vinculadas à sua conta de usuário.
   ii. Se o equipamento de apostas não receber nenhuma entrada do funcionário em 5 minutos, ou um período especificado pelo órgão regulador, a sessão do usuário será interrompida ou travada, exigindo que o funcionário restabeleça seu login para continuar.
e) Para garantir sua disponibilidade e integridade contínuas, os equipamentos de apostas deverão ser mantidos, inspecionados e reparados em intervalos regulares para garantir que estejam livres de defeitos ou mecanismos que possam interferir em sua operação.
f) Antes do descarte ou reutilização, o equipamento de apostas contendo mídia de armazenamento deverá ser verificado para garantir que qualquer software licenciado, informações de conta do jogador e outras informações confidenciais foram removidas ou sobrescritas com segurança (ou seja, não apenas excluídas).

A.7.3 Operações de Aposta

Os procedimentos a seguir deverão ser aplicados para as operações de apostas dentro do local:

a) Os procedimentos deverão estar em vigor para permitir uma resposta adequada a qualquer problema de segurança dentro do local.
b) Os procedimentos deverão estar em vigor para impedir que qualquer pessoa adultere ou interfira na operação de qualquer aposta ou equipamento de apostas;
c) Procedimentos para descrever as operações e a manutenção de dispositivos de apostas POS e dispositivos de apostas de autoatendimento, incluindo o tratamento de condições de erro e a realização de reconciliações;
d) Procedimentos para garantir que os requisitos de acessibilidade observados pelo órgão regulador sejam atendidos para a instalação de dispositivos de apostas de autoatendimento.
e) Procedimentos para transações de apostas usando um dispositivo de apostas POS, incluindo:
   i. Aceitar apostas de jogadores somente durante o período de aposta;
   ii. Notificar os jogadores se a sua tentativa de aposta for rejeitada;
   iii. Exigir o registro de dados do jogador ou registro de conta do jogador se a aposta dele exceder um valor especificado pelo órgão regulador;
   iv. Fornecer notificação de quaisquer alterações de probabilidades/pagamentos ou de preço que ocorram estiver processando uma aposta;
   v. Fornecer a um jogador o acesso a um registro de aposta uma vez que a aposta seja autorizada;
f) Procedimentos para lidar com eventos cancelados e escolhas recusadas para apostas com vários eventos (por exemplo, *parlays*), incluindo o fornecimento de reembolsos a jogadores que não foram reembolsados automaticamente pelo sistema (por exemplo, apostas feitas anonimamente); e
g) Procedimentos para resgate de apostas ganhadoras, incluindo:
   i. Digitalizar o código de barras de um cupom de apostas (por meio de um leitor de código de barras ou equivalente); ou

ii. Inserir manualmente o número de identificação da aposta e realizar uma verificação com o sistema.

A.7.4 Vigilância e Gravação

O local será solicitado a instalar, manter e operar um sistema de vigilância que tenha a capacidade de monitorar e registrar visualizações contínuas e desobstruídas de todas as transações financeiras e de apostas, bem como quaisquer exibições dinâmicas de informações sobre apostas. Devem existir procedimentos em vigor para garantir que a gravação:

a) Abrange as áreas de apostas definidas com detalhes suficientes para identificar quaisquer discrepâncias;
b) Capture de forma a impedir a interferência ou exclusão;
c) Possa ser analisada pelo operador e/ou órgão regulador em caso de reclamação/disputa de um jogador; e
d) Seja mantida por no mínimo noventa dias ou conforme exigido pelo órgão regulador.

A.8 Procedimentos de Monitoramento

A.8.1 Monitoramento de Conluio e Fraude

O operador deverá tomar medidas destinadas a reduzir o risco de conluio ou fraude, incluindo procedimentos para:

a) Identificar e/ou recusar-se a aceitar apostas suspeitas que possam indicar fraude, manipulação, interferência no desenvolvimento normal de um evento ou violações da integridade de qualquer evento em que as apostas foram feitas;
b) Detectar padrões irregulares ou séries de apostas para evitar conluio do jogador ou o uso não autorizado de software de jogador artificial; e
c) Monitorar e detectar eventos e/ou irregularidades no volume de operações ou mudanças nas probabilidades/pagamentos e preços que possam sinalizar atividades suspeitas, bem como todas as alterações de probabilidades/pagamentos e preços e/ou suspensões durante um evento.

A.8.2 Monitoramento contra a Lavagem de Dinheiro (AML)

O operador deverá estabelecer procedimentos e políticas AML, conforme exigido pelo órgão regulador, para assegurar que:

a) Os funcionários são treinados em AML e esse treinamento é mantido atualizado;
b) As contas de jogadores são monitoradas quando abertas e fechadas em períodos curtos e para depósitos e saques sem transações de apostas associadas; e
c) Transações agregadas em um período definido podem exigir uma verificação mais detalhada e deverão ser reportadas a organização relevante se excederem o limite estabelecido pelo órgão regulador.

A.8.3 Monitoramento do Provedor de Serviços de Localização

Quando é requerido pelo órgão regulador, o operador, que oferece apostas remotas, ou um provedor de serviços de localização de terceiros autorizado pelo órgão regulador deve:

a) Ter procedimentos para manter um feed de dados em tempo real de todas as verificações de localização e uma lista atualizada de riscos potenciais de fraude de localização (por exemplo, aplicativos de localização falsos, máquinas virtuais, programas de área de trabalho remota, etc.);
b) Oferecer um sistema de alerta para identificar acessos não autorizados ou indevidos;
c) Permitir auditorias periódicas para avaliar e medir sua capacidade contínua de detectar e mitigar os riscos existentes e emergentes de fraude de localização;
d) Garantir que o serviço de detecção de localização ou aplicativo usado para detecção de localização:
    i. Utilize bancos de dados de código fechado (IP, proxy, VPN, etc.) que serão atualizados com frequência e testados periodicamente quanto a precisão e confiabilidade; e
    ii. Passe por atualizações frequentes para manter recursos avançados de coleta de dados, compatibilidade com dispositivos e capacidades de prevenção de fraudes contra os riscos de fraude de localização.

Anexo B: Auditoria Operacional de Controle Técnicos de Segurança

B.1 Introdução

B.1.1 Declaração Geral

Este anexo estabelece controles técnicos de segurança que serão revisados em uma auditoria operacional como parte da avaliação do Sistema de Apostas de Eventos, incluindo, mas não limitado a, uma avaliação do sistema de segurança da informação (ISS), revisão dos processos operacionais que são críticos para conformidade, testes de penetração focados na infraestrutura externa e interna, bem como na transferência, armazenamento e/ou processamento de dados de jogadores e/ou informações confidenciais e quaisquer outros objetivos estabelecidos pelo órgão regulador. Os controles de segurança descritos neste apêndice aplicam-se aos seguintes componentes críticos do sistema:

a) Componentes que gravam, armazenam, processam, compartilham, transmitem ou recuperam informações confidenciais (por exemplo, números de validação, PINs, dados do jogador);
b) Componentes que geram, transmitem ou processam números aleatórios (RNG) usados para determinar o resultado dos jogos;
c) Componentes que armazenam resultados ou o estado atual da aposta de um jogador;
d) Pontos de entrada e saída dos componentes acima (outros sistemas que tenham a capacidade de se comunicar diretamente com os sistemas críticos principais); e
e) Redes de comunicação que transmitem informações confidenciais.

OBSERVAÇÃO: Também é reconhecido que os controles técnicos de segurança adicionais que não estão especificamente incluídos nesta norma serão relevantes e necessários para uma auditoria operacional, conforme determinado pelo operador e/ou órgão regulador dentro de suas regras, regulamentos e Padrões Mínimos de Controle Interno (MICS).

B.2 Operação e Segurança do Sistema

B.2.1 Procedimentos do Sistema

O operador será responsável por documentar e seguir os procedimentos relevantes do Sistema de Apostas de Eventos. Esses procedimentos devem incluir pelo menos o seguinte, conforme exigido pelo órgão regulador:

a) Procedimentos para monitorar os componentes críticos e a transmissão de dados de todo o sistema, incluindo comunicação, pacotes de dados, redes, bem como os componentes e transmissões de dados de quaisquer serviços de terceiros envolvidos, com o objetivo de garantir a integridade, confiabilidade e acessibilidade;
b) Procedimentos e padrões de segurança para a manutenção de todos os aspectos de segurança do sistema para garantir comunicações seguras e confiáveis, incluindo proteção contra hackers ou manipulação;

c) Procedimentos para definir, monitorar, documentar e relatar, investigar, responder e resolver incidentes de segurança, incluindo violações detectadas e *hackeamento* suspeito ou real ou adulteração do sistema;
d) Procedimento para monitorar e ajustar a utilização de recursos e manter um registro do funcionamento do sistema, incluindo uma função para compilar relatórios de desempenho;
e) Procedimentos para investigar, documentar e resolver o mau funcionamento, que abordam o seguinte:
   i. Determinar a causa do mau funcionamento;
   ii. Revisar registros, relatórios, logs e registros de vigilância;
   iii. Reparar ou substituir do componente crítico;
   iv. Verificar a integridade do componente crítico antes de restaurá-lo à operação;
   v. Apresentar um relatório de incidente ao órgão reguladore documentar a data, a hora e o motivo do mau funcionamento, juntamente com a data e a hora em que o sistema foi restaurado; e
   vi. Anular ou cancelar apostas e pagamentos se uma recuperação completa não for possível.

B.2.2 Localização Física dos Servidores

O(s) servidor(es) do Sistema de apostas de eventos deverão ser alojados em um ou mais locais seguros que poderão estar localizados localmente, dentro de um único local, ou poderá estar localizado remotamente, conforme permitido pelo órgão regulador. Além disso, os locais seguros deverão:

a) Ter proteção suficiente contra alteração, adulteração ou acesso não autorizado;
b) Ser dotado de sistema de vigilância que deverá atender aos procedimentos instituídos pelo órgão regulador;
c) Ser protegido por perímetros de segurança e por controles de entrada apropriados para garantir que o acesso seja restrito somente a pessoal autorizado e que quaisquer tentativas de acesso físico sejam registradas em um log seguro; e
d) Estar equipado com controles para fornecer proteção física contra danos causados por incêndios, inundações, furacões, terremotos e outras formas de desastres naturais ou causados pelo homem.

B.2.3 Controle de Acesso Lógico

O Sistema de Apostas de Eventos deve ser logicamente protegido contra acesso não autorizado por credenciais de autenticação permitidas pelo órgão regulador, como senhas, autenticação multifatorial, certificados digitais, PINs, biometria e outros métodos de acesso (por exemplo, tarja magnética, cartões de aproximação, cartões com chip).

a) Cada conta de usuário deverá ter sua própria credencial de autenticação individual, cuja criação e fornecimento deverá ser controlado por meio de um processo formal.
b) Os registros de credenciais de autenticação devem ser mantidos manualmente ou por sistemas que registram automaticamente as alterações de autenticação e forçam as alterações nas credenciais de autenticação.

c) O armazenamento de credenciais de autenticação deve ser seguro. Se as credenciais de autenticação for codificada por hardware em um componente do sistema, ela deverá ser criptografada.
d) O método substituto para falha de autenticação (por exemplo, senhas esquecidas) deverá ser tão seguro quanto o método principal.
e) Credenciais de autenticação perdidas ou comprometidas e credenciais de autenticação de usuários desativados deverão ser desativadas, protegidas ou destruídas assim que possível.
f) O sistema deverá ter vários níveis de acesso de segurança para controlar e restringir diferentes classes de acesso ao servidor, incluindo visualização, alteração ou exclusão de arquivos e diretórios críticos. Os procedimentos deverão estar em vigor para atribuir, revisar, modificar e remover direitos de acesso e privilégios para cada usuário, incluindo:
    i. Permitir a administração de contas de usuário para fornecer uma separação adequada de funções;
    ii. Limitar os usuários que possuem as permissões necessárias para ajustar os parâmetros críticos do sistema;
    iii. Adotar parâmetros de credencial de autenticação adequados, como por exemplo, comprimento mínimo e intervalo de expiração das credenciais;
g) Os procedimentos deverão estar em vigor para identificar e sinalizar contas suspeitas onde credenciais de autenticação possam ter sido roubadas.
h) Quaisquer tentativas de acesso lógico aos aplicativos do sistema ou sistemas operacionais deverão ser registradas em um log seguro.
i) O uso de programas utilitários que poderão substituir os controles do aplicativo ou do sistema operacional deverão ser restrito e rigidamente controlado.

OBSERVAÇÃO: Quando se utilizam senhas como uma credencial de autenticação, é recomendável que elas sejam alteradas pelo menos uma vez a cada 90 dias, tenham pelo menos 8 caracteres e contenham uma combinação de pelo menos dois dos seguintes critérios: letras maiúsculas e minúsculas, caracteres numéricos e/ou especiais.

B.2.4 Autorização do Usuário

O Sistema de Apostas de Eventos deverá implementar os seguintes requisitos de autorização do usuário:

a) Um mecanismo seguro e controlado deverá ser empregado para verificar se o componente crítico está sendo operado por um usuário autorizado de forma regular, conforme requerido pelo órgão regulador.
b) O uso de identificação automatizada do equipamento para autenticar conexões de localizações específicas e equipamentos deve ser documentado e deve ser incluído na revisão de acesso aos direitos e privilégios.
c) Qualquer informação de autorização comunicada pelo sistema para fins de identificação deverá ser obtida no momento da solicitação do sistema e não deve ser armazenada no componente do sistema.
d) O sistema deve ter a capacidade de notificar o administrador do sistema e bloquear o usuário ou informar no registro de auditoria, após um número definido de tentativas de autorização sem sucesso.

B.2.5 Programação do Servidor

O Sistema de Apostas de Eventos deverá ser suficientemente seguro para evitar quaisquer recursos de programação iniciados pelo usuário no servidor que poderá resultar em modificações no banco de dados. No entanto, será aceitável que os administradores de rede ou sistema executem manutenção autorizada da infraestrutura de rede ou solução de problemas de aplicativos com direitos de acesso suficientes. O servidor também deverá ser protegido da execução não autorizada de código móvel.

B.2.6 Procedimentos de Verificação

Deverá estabelecer procedimentos de verificação por solicitação de que os componentes críticos do programa de controle do Sistema de Apostas de Eventos no ambiente de produção sejam idênticos àqueles aprovados pelo órgão regulador.

a) As assinaturas dos componentes críticos do programa de controle deverão ser coletadas do ambiente de produção por meio de um processo a ser aprovado pelo órgão regulador.
b) O processo deverá incluir uma ou mais etapas analíticas para comparar as assinaturas atuais dos componentes críticos do programa de controle no ambiente de produção com as assinaturas das versões atuais aprovadas dos componentes críticos do programa de controle.
c) O resultado deste processo deve ser armazenado em um formato inalterável, que detalhe dos resultados da verificação para cada autenticação do programa de controle crítico e:
    i. Ser registrado em um histórico ou relatório do sistema que deverá ser armazenado por um período de noventa dias ou conforme especificado pelo órgão regulador;
    ii. Ser acessível pelo órgão regulador em formato que permitirá análise de registros de verificação por esta entidade; e,
    iii. Abranger parte dos registros do sistema que deverão ser recuperados no caso de desastre ou falha de equipamento ou software.
d) Qualquer falha na verificação de qualquer componente do sistema deve exigirá que uma notificação de falha de autenticação seja enviada ao operador e ao órgão regulador, se necessário.
e) Deverá haver um processo em vigor para responder as falhas de autenticação, incluindo a determinação da causa da falha e a execução das correções associadas ou reinstalações necessárias em tempo hábil.

B.2.7 Sistema Eletrônico de Retenção de Documentos

Relatórios exigidos por esta norma e pelo órgão regulador podem ser armazenados no sistema eletrônico de retenção de documentos, desde que o sistema:

a) Esteja devidamente configurado para manter a versão original junto com todas as versões subsequentes refletindo todas as alterações no relatório;
b) Mantenha uma assinatura única para cada versão do relatório, incluindo o original;
c) Retenha e reporte um histórico completo das alterações para todos os relatórios, incluindo quem (identificação do usuário) realizou as alterações e quando (data e hora);

d) Forneça um método de indexação completo para localizar e identificar facilmente o relatório, incluindo pelo menos o seguinte (que poderá ser inserido pelo usuário):
   i. Data e hora que o relatório foi gerado;
   ii. Aplicação ou sistema que gerou o relatório;
   iii. Título e descrição do relatório;
   iv. Identificação do usuário que gerou o relatório; e,
   v. Qualquer outra informação que possa ser útil para identificar o relatório e seu propósito;
e) Esteja configurado para limitar o acesso para modificar ou adicionar relatórios ao sistema por meio da segurança lógica de contas de usuário específicas;;
f) Esteja configurado para fornecer uma trilha de auditoria completa de todas as atividades da conta do usuário administrativo;
g) Esteja devidamente protegido por meio do uso de medidas de segurança lógicas (contas de usuário com acesso apropriado, níveis adequados de registro de eventos e documentação do controle de versão, etc.);
h) Está fisicamente protegido com todos os outros componentes críticos do Sistema de Apostas de Eventos; e,
i) Esteja equipado, baseado nas práticas recomendadas de redundância de hardware e software e processos de backup, para evitar a interrupção da disponibilidade de relatórios e perda de dados.

B.2.8 Gestão de Ativos

Todas os equipamentos que armazenam, processa ou transmite informações confidenciais, incluindo aqueles equipamentos que compõe o ambiente de operação do Sistema de Apostas de Eventos e/ou seus componentes, devem ser contabilizados e ter um proprietário nomeado.

a) Um inventário deve ser elaborado e mantido de todos os ativos que detêm itens controlados.
b) Deverá ser estabelecido um procedimento para adicionar novos ativos e remover ativos de serviço.
c) Uma política deverá ser incluída sobre o uso aceitável de ativos associados ao sistema e seu ambiente operacional;
d) Cada ativo deve ter um “proprietário” designado responsável por:
   i. Garantir que as informações e ativos sejam classificados de forma adequada em termos de sua criticidade, sensibilidade e valor; e,
   ii. Definir e revisar periodicamente as restrições e classificações de acesso.
e) Deverá existir um procedimento para garantir que a contabilidade registrada dos ativos seja comparada com os ativos reais em intervalos exigidos pelo órgão regulador e ações apropriadas deverão ser tomadas com respeito a discrepâncias.
f) A proteção contra cópia para evitar a duplicação ou modificação não autorizada do software poderá ser implementada desde que:
   i. O método de proteção contra cópia seja totalmente documentado e fornecido para o laboratório de teste independente, para verificar se a proteção funciona conforme descrito; ou,
   ii. O programa ou componente responsável pela aplicação da proteção contra cópia deverá ser verificado individualmente pela metodologia aprovada pelo órgão regulador.

B.3 Backup e Recuperação

B.3.1 Segurança dos Dados

O Sistema de Apostas de Eventos deve fornecer um método lógico para proteger os dados do jogador e dados da aposta, incluindo contabilidade, relatórios, eventos relevantes ou outra informação confidencial, a respeito de alteração, adulteração ou acesso não autorizado.

a) Métodos apropriados de tratamento de dados deverão ser implementados, incluindo validação de entrada e rejeição de dados corrompidos.
b) O número de estações de trabalho onde aplicativos críticos ou bancos de dados associados poderão ser acessados deverá ser limitado.
c) Criptografia ou proteção por senha ou qualquer outro tipo de segurança equivalente deverá ser utilizada para arquivos e diretórios que contenham dados. Se a criptografia não for utilizada, o operador deverá restringir os usuários de visualizar o conteúdo de tais arquivos e diretórios, e no mínimo, deverá prever a segregação das funções e responsabilidades do sistema, bem como o monitoramento e registro do acesso de qualquer pessoa a tais arquivos e diretórios.
d) O funcionamento normal de qualquer equipamento que contenha dados não deverá ter opções ou mecanismos que possam comprometer os dados.
e) Nenhum equipamento poderá ter um mecanismo no qual um erro acarretará no apagamento automático dos dados.
f) Nenhum equipamento que contenha dados em sua memória deverá permitir a remoção das informações, a menos que primeiro tenha transferido essas informações para o banco de dados ou outro(s) componente(s) seguro(s) do sistema.
g) Os dados devem ser armazenados em áreas do servidor que são criptografadas e seguras de acesso não autorizado, ambos externos e internos.
h) Os bancos de dados de produção contendo dados deverão residir em redes separadas dos servidores que hospedam qualquer interface do jogador.
i) Os dados deverão ser mantidos sempre, independentemente de o servidor estar ligado.
j) Os dados deverão ser armazenados de forma a evitar que sejam perdidos ao substituir peças ou módulos durante a manutenção normal.

B.3.2 Alteração dos Dados

A alteração de qualquer informação contábil, relatório ou eventos significativos não deverá ser permitida sem controles de acesso supervisionados. Se qualquer dado for alterado, as seguintes informações deverão ser documentadas ou registradas:

a) Número de identificação único para a alteração;
b) Qual dado foi alterado;
c) Valor do dado antes da alteração;
d) Valor dado depois da alteração;
e) Data/hora da alteração; e,
f) Usuário responsável pela alteração (identificação do usuário).

B.3.3 Frequência do Backup

A execução da rotina de backup deverá ser feita pelo menos uma vez por dia ou conforme especificado pelo órgão regulador, embora todos os métodos serão revisados caso a caso.

B.3.4 Mídia de Armazenamento do Backup

Logs de auditoria, bases de dados do sistema e quaisquer outros dados pertinentes do jogador e dados de apostas devem ser armazenados usando métodos de proteção razoáveis. O Sistema de Apostas de Eventos deve ser desenhado para proteger a integridade desses dados no evento de uma falha. Cópias redundantes desses dados devem ser mantidos no sistema com suporte aberto para backups e restaurações, para que nenhuma falha de qualquer parte do sistema possa causar a perda ou corrupção dos dados.

a) O backup deve ser feito em uma mídia física não volátil, ou uma implementação arquitetural equivalente, de modo que se o meio de armazenamento primário falhar, as funções do sistema e o processo de auditoria daquelas funções possam continuar sem perda de dados crítica.
b) Onde o órgão regulador permitir o uso de plataformas em nuvem, se o backup é armazenado em uma plataforma em nuvem, outra cópia pode ser armazenada em uma plataforma em nuvem diferente.
c) Se for utilizar unidades de disco rígido como mídia de backup, a integridade dos dados deve ser assegurada no evento de uma falha de disco. Métodos aceitáveis incluem, mas não são limitados, a vários discos rígidos em uma configuração RAID aceitável ou espelhamento de dados em dois ou mais discos rígidos.
d) Após a conclusão do processo de backup, a mídia de backup deverá ser imediatamente transferida para um local fisicamente separado do local que abriga os servidores e os dados dos quais está sendo feito backup (para armazenamento temporário e permanente).
    i. O local de armazenamento deverá ser protegido para impedir o acesso não autorizado e fornecer proteção adequada para prevenir a perda permanente de quaisquer dados.
    ii. Arquivos de dados de backup e componentes de recuperação de dados deverão ser gerenciados com pelo menos o mesmo nível de segurança e controles de acesso que o sistema.

NOTA: A distância entre os dois locais deve ser determinada baseada em potenciais ameaças e perigos ambientais, falhas de energia e outras interrupções, mas deve também considerar a potencial dificuldade de replicação de dados, além de poder acessar o site de recuperação dentro de um prazo razoável (Objetivo de Tempo de Recuperação).

B.3.5 Falhas do Sistema

O Sistema de Apostas de Eventos deve ter redundância e modularidade suficiente de modo que se qualquer componente único ou parte de um componente falha, as funções do sistema e o processo de auditoria dessas funções possam continuar sem perda de dados críticos. Quando dois ou mais componentes estão conectados:

a) O processo de todas as operações de jogo entre os componentes não deverão ser adversamente afetado pelo reinício ou recuperação de qualquer um dos componentes (por exemplo, as

transações não deverão ser perdidas ou duplicadas devido à recuperação de um ou outro componente); e
b) Na reinicialização ou recuperação, os componentes deverão sincronizar imediatamente o status de todas as transações, dados e configurações entre si.

B.3.6 Registro de Master Resets

O operador deverá ser capaz de identificar e lidar adequadamente com situações em que poderá ocasionar uma reinicialização geral em qualquer componente que afete as operações de aposta.

B.3.7 Requisitos de Recuperação

No caso de uma falha catastrófica quando o Sistema de Apostas de Eventos não puder ser reiniciado de nenhuma forma, deverá ser possível restaurar o sistema a partir do último backup e recuperá-lo totalmente. O conteúdo desse backup deverá conter as seguintes informações críticas, incluindo, mas não se limitando a:

a) As informações especificadas na seção intitulada “Informações a Serem Mantidas”;
b) Informações específicas do local, como configuração, contas de segurança, etc .;
c) Chaves de criptografia do sistema atual; e ,
d) Quaisquer outros parâmetros do sistema, modificações, reconfiguração (incluindo sites ou locais participantes), adições, fusões, exclusões, ajustes e alterações de parâmetros.

B.3.8 Suporte para Fonte de Alimentação Ininterrupta (UPS)

Todos os componentes do sistema deverão ser fornecidos com alimentação primária adequada. Quando o servidor for um aplicativo stand-alone, ele deverá ter uma fonte de alimentação ininterrupta (UPS) conectada e deverá ter capacidade suficiente para permitir um desligamento normal e que irá reter todos os dados do jogador e dados de apostas durante uma perda de energia. Será admissível que o sistema seja parte de uma rede suportada por um no-break que atenderá toda a rede, desde que o servidor esteja incluído como um dispositivo protegido pelo no-break. Deverá haver um sistema de proteção de sobretensão, se o servidor não estiver incorporado ao próprio no-break.

B.3.9 Plano de Continuidade e Recuperação em Caso de Desastre

Um plano de continuidade de negócios e recuperação de desastres deverá estar em vigor para recuperar as operações de apostas se o ambiente de produção do Sistema de Apostas de Eventos se tornar inoperante. O plano de continuidade dos negócios e recuperação em caso de desastres deve:

a) Incluir um método de armazenamento dos dados do jogador e dados das apostas para minimizar perdas. Se uma replicação assíncrona é usada, o método para recuperar os dados deve ser descrito ou a potencial perda de dados deve ser documentada;
b) Delinear as circunstâncias sob as quais ele será invocado; ;
c) Abordar o estabelecimento de um local de recuperação fisicamente separado do local de produção .

d) Conter guias de recuperação detalhando as etapas técnicas necessárias para restabelecer a funcionalidade de jogo no local onde será definido para que seja recuperado; e
e) Abordar os processos necessários para retomar as operações administrativas das atividades de jogo após a ativação do sistema recuperado considerando vários cenários apropriados para o contexto operacional do sistema

B.4 Comunicações

B.4.1 Declaração Geral

Esta seção tratará os vários métodos de comunicação com e sem fio, incluindo comunicações realizadas pela Internet ou em uma rede pública ou de terceiros, conforme permitido pelo órgão regulador.

B.4.2 Conectividade

Somente dispositivos autorizados deverão ter permissão para estabelecer comunicações entre qualquer componente do sistema. O Sistemae Apostas de Eventos deve fornecer um método para:

a) Inscrever e cancelar o registro de componentes do sistema;
b) Habilitar e desabilitar componentes específicos do sistema;
c) Certificar de que apenas os componentes do sistema registrados e habilitados, incluindo Dispositivos de Aposta, poderão participar nas operações de apostas; e,
d) Certificar de que a condição default para componentes deverá estar desabilitado.

B.4.3 Protocolo de Comunicação

Cada componente do Sistema de Apostas de Eventos deverá funcionar conforme indicado por um protocolo de comunicação seguro e documentado.

a) Todos os protocolos deverão usar técnicas de comunicação que tenham mecanismos adequados de detecção e recuperação de erros, que são projetados para evitar intrusão, interferência, espionagem e adulteração. Quaisquer implementações alternativas serão analisadas caso a caso e aprovadas pelo órgão regulador.
b) Todos as comunicações de dados críticos para a aposta ou para gerenciamento de conta de jogador deverão ser criptografados e autenticados.
c) As comunicações na rede segura só deverão ser possíveis entre componentes críticos aprovados que foram registrados e autenticados como válidos na rede. Nenhuma comunicação não autorizada com componentes e/ou pontos de acesso será permitida.

B.4.4 Comunicações pela Internet/Redes Públicas

Comunicações entre todos os componentes do sistema, incluindo Dispositivos de Apostas, que ocorrem através da internet/rede pública devem ser garantidas por um meio aprovado pelo órgão regulador. Dados do jogador, informações confidenciais, apostas, resultados, informações financeiras e informações de transação dos jogadores devem sempre ser criptografadas na internet/rede pública

e protegidas de transmissões incompletas, desvios errôneos, modificação de mensagem sem autorização, divulgação, duplicação ou reprodução.

B.4.5 Comunicações por Rede Local sem Fio (WLAN)

As comunicações de rede local sem fio (WLAN), quando permitidas pelo órgão regulador, deverão cumprir os requisitos jurisdicionais aplicáveis especificados para dispositivos sem fio e segurança de rede. Na ausência de normas jurisdicionais específicas, os "Requisitos de Dispositivo sem Fio" e "Requisitos de Segurança de Rede sem Fio" da norma GLI-26 para sistemas wireless deverão ser usados quando aplicável.

NOTA: Será mandatório que os operadores revisem e atualizem as políticas e procedimentos de controle interno para garantir que a rede esteja segura e que as ameaças e vulnerabilidades sejam devidamente tratadas. Recomenda-se a inspeção periódica e a verificação da integridade da WLAN.

B.4.6 Gestão de Segurança da Rede

As redes deverão ser logicamente separadas de modo que não haja tráfego em uma rede que não possa ser atendida pelo hosts no enlace onde ela está configurada. Os seguintes requisitos deverão ser aplicados:

a) Todas as funções de gerenciamento de rede deverão autenticar todos os usuários na rede e criptografar todas as comunicações de gerenciamento de rede.
b) A falha de qualquer item individual não deverá resultar em negação de serviço.
c) Um Sistema de Detecção de Invasão/Sistema de Prevenção de Invasão (IDS/IPS) deve ser instalado na rede e receber comunicações internas e externas, assim como detectar e prevenir:
   i. Ataques de Negação de Serviço distribuído (DDOS);
   ii. *Shellcode* para invadir a rede;
   iii. Falsificação (*spoofing)* do Protocolo de Resolução de Endereços (ARP); e,
   iv. Outros indicadores de ataque "*Man-In-The-Middle*" e deverá cortar as comunicações do imediatamente, quando detectado.
d) Além dos requisitos do item (c), um IDS/IPS instalado em uma WLAN deverá ser capaz de:
   i. Fazer a varredura da rede em busca de pontos de acesso não autorizados ou invasores ou dispositivos conectados a qualquer ponto de acesso na rede, pelo menos trimestralmente ou conforme definido pelo órgão regulador;
   ii. Desativar automaticamente quaisquer dispositivos não autorizados conectados ao sistema; e,
   iii. Manter um registro de histórico de todos os acessos wireless dos últimos noventa dias ou conforme especificado pelo órgão regulador. Este registro deverá conter informações completas e abrangentes sobre todos os dispositivos sem fio envolvidos e deverá ser capaz de ser reconciliado comtodos os outros dispositivos de rede dentro do local.
e) O Equipamento de Comunicação de Rede (NCE) deverá seguir os seguintes requisitos:
   i. O NCE deverá ser construído de forma a ser resistente a danos físicos ao hardware ou corrupção do firmware/software contido pelo uso normal.
   ii. O NCE deverá ser fisicamente protegido contra acessos não autorizados.
   iii. As comunicações de sistema via NCE deverão ser logicamente protegidas contra o acesso não

autorizado.
iv. O NCE com armazenamento limitado deve, se o log de auditoria estiver cheio, desabilitar todas as comunicações ou descarregar logs para um servidor de log dedicado.

f) Todos os hubs de rede, serviços e portas de conexões devem ser seguros para evitar acesso não autorizado à rede. Serviços não utilizados e portas não essenciais devem ser fisicamente bloqueadas ou desabilitadas por software quando possível.
g) Em ambientes virtualizados, servidores redundantes não devem ser executados sob o mesmo hipervisor.
h) Protocolos sem estado, como UDP (User Datagram Protocol), não deverão ser usados para informações confidenciais sem transporte com estado. Observe que, embora HTTP (Hypertext Transport Protocol) seja tecnicamente sem estado, se for executado em TCP (Transmission Control Protocol), que tem estado, será permitido.
i) Todas as mudanças na infraestrutura de rede (por exemplo, configuração do equipamento de comunicação de rede) deverão ser registradas.
j) Scanners de vírus e/ou programas de detecção deverão ser instalados no sistema. Esses programas deverão ser atualizados regularmente para verificar se há novas cepas de vírus.

B.5 Prestadores de Serviços Terceirizados

B.5.1 Comunicações com Terceiros

Quando comunicações com prestadores de serviços terceirizados forem implementadas, tais como programas de fidelidade do jogador, serviços financeiros (bancos, processadores de pagamentos, etc.), prestadores de serviços de localização, prestadores de serviços em nuvem, serviços estatísticos/ensaios e serviços de verificação de identidade, os seguintes requisitos se aplicam:

a) O Sistema de Apostas de Eventos deverá ser capaz de se comunicar com segurança com prestadores de serviços terceirizados usando criptografia e autenticação forte.
b) Todos os eventos de login envolvendo prestadores de serviços terceirizados deverão ser registrados em um arquivo de auditoria.
c) A comunicação com prestadores de serviços terceirizados não deverá interferir ou degradar funções normais do Sistema de Apostas de Eventos.
   i. Os dados do prestador de serviços terceirizados não deverão afetar as comunicações do jogador.
   ii. Conexões com prestadores de serviços terceirizados não devem usar a mesma infraestrutura de rede das conexões do jogador.
   iii. As apostas devem ser desconectadas em todas as conexões de rede, exceto para a rede de jogadores;
   iv. O sistema não deverá enviar pacotes de dados dos prestadores de serviços terceirizados diretamente para a rede dos jogadores e vice-versa.
   v. O sistema não deverá atuar como roteadores de IP entre as redes de jogadores e as de prestadores de serviços terceirizados.
d) Todas as transações financeiras devem ser reconciliadas com instituições financeiras e processadoras de pagamentos diárias ou conforme especificado pelo órgão regulador.

B.5.2 Serviços Terceirizados

As funções de segurança e responsabilidades dos prestadores de serviços terceirizados deverão ser definidas e documentada conforme exigido pelo órgão regulador. O Operador deverá ter políticas e procedimentos para gerenciá-los e monitorar sua adesão aos requisitos de segurança relevantes:

a) Acordos com prestadores de serviços terceirizados envolvendo acesso, processamento, comunicação ou gerenciamento do sistema e/ou seus componentes, ou adição de produtos ou serviços ao sistema e/ou seus componentes deverão atender todos os requisitos de segurança relevantes.
b) Os serviços, relatórios e registros fornecidos pelos prestadores de serviços terceirizados deverão ser monitorados e revisados anualmente ou conforme exigido pelo órgão regulador.
c) Mudanças nas normas que regem a prestação de serviços terceirizados, incluindo a manutenção e melhoria das políticas, procedimentos e controles de segurança existentes, deverão ser gerenciadas, levando em consideração a criticidade dos sistemas e processos envolvidos e reavaliação dos riscos.
d) Os direitos de acesso de prestadores de serviços terceirizados ao sistema e/ou aos seus componentes deverão ser removidos no término de seu contrato ou acordo ou ajustados em caso de alteração.

B.6 Controles Técnicos

B.6.1 Requisitos para o Domain Name Service (DNS)

Os seguintes requisitos se aplicarão aos servidores usados para resolver questões do Sistema de Nomes de Domínio (DNS) em associação com o Sistema de Apostas de Eventos.

a) O Operador deverá utilizar um servidor DNS primário seguro e um servidor DNS secundário seguro que deverão estar lógica e fisicamente separados um do outro.
b) O servidor DNS primário deverá estar fisicamente localizado em um data center seguro ou um host virtualizado em um hipervisor devidamente protegido ou equivalente.
c) O acesso lógico e físico ao(s) servidor(es) DNS deverá ser restrito ao pessoal autorizado.
d) Não deverão ser permitidas as transferências de zona para hosts arbitrários.
e) Um método para evitar o envenenamento do cache, como DNS Security Extensions (DNSSEC), será necessário.
f) Deverá ser utilizada a autenticação multifator.
g) Deverá ser estabelecido o bloqueio do registro, portanto, qualquer solicitação para alterar o(s) servidor(es) DNS deverá ser verificada manualmente.

B.6.2 Controles Criptográficos

Uma política sobre o uso de controles criptográficos para proteção das informações deverá ser desenvolvida e implementada.

a) Todos os dados e/ou informação confidencial devem ser criptografados se atravessar uma rede com baixo nível de confiança.

b) Os dados que não precisam ser ocultados, mas devem ser autenticados, deverão usar alguma forma de técnica de autenticação de mensagem.
c) A autenticação deve usar um certificado de segurança de uma organização aprovada.
d) O grau da criptografia utilizada deverá ser adequado à sensibilidade dos dados.
e) O uso de algoritmos de criptografia deverá ser revisado periodicamente para verificar se os algoritmos de criptografia atuais estão seguros.
f) Deverão ser implementadas alterações nos algoritmos de criptografia para corrigir pontos fracos assim que possível. Se tais alterações não estiverem disponíveis, o algoritmo deve ser substituído.
g) As chaves de criptografia deverão ser armazenadas em um meio de armazenamento seguro e redundante após serem criptografadas por meio de um método de criptografia diferente e/ou usando uma chave de criptografia diferente.

B.6.3 Gestão da Chave de Criptografia

A gestão das chaves de criptografia deverá seguir processos definidos e estabelecidos pelo operador e/ou pelo órgão regulador. Esses processos específicos devem cobrir o seguinte:

a) Obter ou gerar chaves de criptografia e armazená-las;
b) Gerenciar a expiração das chaves de criptografia, quando aplicável;
c) Revogar chaves de criptografia;
d) Alterar com segurança o conjunto de chaves de criptografia atual; e,
e) Poder recuperar dados criptografados com uma chave de criptografia revogada ou expirada por um período a ser determinado após a chave de criptografia se tornar inválida.

B.7 Acesso Remoto e Firewalls

B.7.1 Segurança do Acesso Remoto

O acesso remoto será definido como qualquer acesso de fora do sistema ou rede do sistema, incluindo qualquer acesso de outras redes dentro do mesmo local. O acesso remoto só deverá ser permitido se autorizado pelo órgão regulador e deverá:

a) Ser executado por meio de um método seguro;
b) Ter a opção de ser desabilitado;
c) Aceitar apenas as conexões remotas permitidas pelo aplicativo de firewall e pelas configurações do sistema;
d) Limitar-se apenas as funções do aplicativo necessárias para que os usuários realizem suas tarefas de trabalho:
    i. Nenhuma funcionalidade de administração de usuário remoto não autorizada deverá ser permitida (adição de usuários, alteração de permissões, etc.); e,
    ii. O acesso não autorizado ao sistema operacional ou a qualquer banco de dados que não seja a recuperação de informações, usando funções existentes, deverá ser proibido.

OBSERVAÇÃO: A segurança do acesso remoto será analisada caso a caso, juntamente com a implementação da tecnologia utilizada no momento e a aprovação do órgão regulador.

B.7.2 Procedimentos de Acesso Remoto e Contas de Convidados

Um procedimento para acesso remoto estritamente controlado deverá ser estabelecido. É reconhecido que o fornecedor poderá, se necessário, acessar o sistema e seus componentes associados remotamente para suporte ao produto e ao usuário ou atualizações/upgrades, conforme permitido pelo órgão regulador e pelo operador. Este acesso remoto deve usar contas de convidados específicas que são:

a) Continuamente monitorada pelo operador;
b) Desabilitada quando não estiver em uso; e
c) Restringida por meio de controles lógicos de segurança para acessar apenas os aplicativos e/ou bancos de dados necessários para o produto e suporte ao usuário ou para fornecer atualizações/upgrades.

B.7.3 Log de Atividades do Acesso Remoto

O aplicativo de acesso remoto deverá manter um registro de atividades que deverá ser atualizado automaticamente, descrevendo todas as informações do acesso remoto, incluindo:

a) Identificação do(s) usuário(s) que realizará e/ou autorizará o acesso remoto;
b) Endereços IP remotos, números de porta, protocolos e, quando possível, endereços MAC;
c) Data/Hora em que a conexão foi efetuada e duração da conexão; e,
d) Atividades efetuadas enquanto conectado, incluindo as áreas específicas acessadas e alterações feitas.

B.7.4 Firewall

Todas as comunicações, incluindo o acesso remoto, deverão passar por pelo menos um firewall aprovado a nível de aplicativo. Isso inclui conexões de e para qualquer host que não seja do sistema usado pelo operador.

a) O firewall deverá estar localizado no limite entre dois domínios de segurança diferentes.
b) Um dispositivo no mesmo domínio de broadcast que o host do sistema não poderá ter um recurso que permita o estabelecimento de um caminho de rede alternativo, que ignore o firewall.
c) Qualquer caminho de rede alternativo existente para fins de redundância também deverá passar por pelo menos um firewall a nível de aplicativo.
d) Apenas aplicativos relacionados ao firewall poderão residir no firewall.
e) Deverá ter um número limitado de contas de usuário cofiguradas no firewall (por exemplo, administradores de rede ou de sistema).
f) O firewall deverá rejeitar todas as conexões, exceto aquelas que foram especificamente aprovadas.
g) O firewall deverá rejeitar todas as conexões de destinos que não podem residir na rede de origem da mensagem (por exemplo, endereços RFC1918 no lado público de um firewall de internet).
h) O firewall somente deve permitir acesso remoto sobre protocolos de criptografia mais recentes.

B.7.5 Logs de Auditoria do Firewall

O aplicativo de firewall deve manter um log de auditoria e deve desabilitar todas as comunicações e gerar um erro se o log de auditoria ficar cheio. O log de auditoria deve conter:

a) Todas as mudanças efetuadas na configuração do firewall;
b) Todas as tentativas de conexão bem ou mal sucedidas através do firewall; e,
c) Os endereços IP de origem e destino, números de porta, protocolos e, quando possível, endereços MAC.

OBSERVAÇÃO: O parâmetro configurável 'tentativas de conexão malsucedidas' poderá ser utilizado para negar mais solicitações de conexão caso o limite predefinido seja excedido. O administrador do sistema também deverá ser notificado.

B.7.6 Revisão das Regras do Firewall

Se exigido pelo órgão regulador, as regras de firewall deverão ser revisadas periodicamente para verificar a condição de operação do firewall e a eficácia de sua configuração de segurança e do conjuntos de regras e deverá ser executadas em todos os firewalls internos e de perímetros.

B.8 Gestão de Mudanças

B.8.1 Considerações Gerais

Uma Política de Gerenciamento de Mudanças deverá ser selecionada pelo órgão regulador para lidar com as atualizações do Sistema de Apostas de Eventos e seus componentes baseados na frequência de atualizações do sistema e na tolerância de riscos determinada. Para sistemas que requerem atualizações frequentes, um programa de gerenciamento de mudanças baseado em risco poderá ser utilizado para proporcionar maior eficiência na implantação das atualizações. Programas de Gerenciamento de Mudanças baseados em risco normalmente incluem uma categorização das mudanças propostas com base no impacto regulatório e definem os procedimentos de certificação associados para cada categoria. O laboratório de teste independente avaliará o sistema e as modificações futuras de acordo com o Política de Gerenciamento de Mudanças selecionado pelo órgão regulador.

B.8.2 Procedimentos de Controle de Alterações do Programa

Os procedimentos de controle de alterações do programa deverão estar adequados para garantir que apenas as versões autorizadas dos programas sejam implementadas no ambiente de produção. Esses controles de mudança deverão incluir:

a) Um controle adequado de versão de software ou outro mecanismo para todos os componentes de software, código-fonte;
b) Manter registros de todas as novas instalações e / ou modificações no sistema, incluindo:
    i. A data da instalação ou da alteração;
    ii. Detalhes do motivo ou da natureza da instalação ou alteração, como novo software, reparo

do servidor, modificações significativas na configuração;
iii. Uma descrição dos procedimentos exigidos para implantar um componente novo ou modificado (conversão ou entrada de dados, procedimentos de instalação, etc.).
iv. A identidade do(s) usuário(s) que realizará esta instalação ou modificação;

c) Uma estratégia para reverter a última implementação (plano de reversão), se a instalação não for bem-sucedida, incluindo backups completos de versões anteriores do software e um teste de plano de reversão antes da implementação do ambiente de produção.
d) Uma política que trata dos procedimentos de mudanças emergenciais;
e) Procedimentos para teste e migração de mudanças;
f) Segregação de funções entre desenvolvedores, equipe de controle de qualidade, equipe de implantação e usuários; e,
g) Procedimentos para garantir que a documentação técnica e do usuário esteja atualizada após cada alteração implementada.

B.8.3 Ciclo de Vida de Desenvolvimento de Software

A aquisição e o desenvolvimento de novos softwares deverão seguir processos definidos e estabelecidos pelo operador e/ou pelo órgão regulador.

a) O ambiente de produção devera ser lógica e fisicamente separado dos ambientes de desenvolvimento e teste. Quando as plataformas em nuvem são usadas, nenhuma conexão direta poderá existir entre o ambiente de produção e qualquer outro ambiente.
b) A equipe de desenvolvimento deve ser impedida de ter acesso para fazer alterações de código dentro do ambiente de produção.
c) Deve haver um método documentado para verificar que um software de teste não está implantado no ambiente de produção.
d) Para evitar vazamentos de informações confidencial, deverá ser estabelecido um método documentado para assegurar que os dados brutos de produção não são usados em testes.
e) Toda a documentação relativa ao desenvolvimento de software e aplicativos deverá estar disponível e retida durante o seu ciclo de vida.

B.8.4 Correções

Todos os patches devem ser testados sempre que possível em um ambiente de desenvolvimento e de teste configurado identicamente ao ambiente de produção desejado. Sob circunstâncias em que os testes de patches não possam ser completamente realizados a tempo de atender o cronograma, de acordo com o nível de gravidade do alerta e, se autorizado, pelo órgão regulador, os testes de patches devem ser gerenciados por risco, seja por isolamento ou remoção do componente não testado da rede ou aplicando os patches e testando-os depois.

B.9 Teste de Segurança Periódica

B.9.1 Teste Técnicos de Segurança

Deverão ser realizados testes técnicos de segurança periodicamente no ambiente de produção, conforme requerido pelo órgão regulador, para garantir que não existem vulnerabilidades que

possam colocar em risco a segurança e operação do Sistema de Apostas de Eventos. Os testes devem consistir em um método de avaliação de segurança pelos meios de uma simulação de ataque por um terceiro seguindo uma metodologia reconhecida, e a análise de vulnerabilidade consistirá na identificação e quantificação passiva dos riscos potenciais do sistema. Tentativas de acesso não autorizado devem ser feitos até o mais alto nível de acesso possível e devem ser completadas com ou sem credenciais de autenticação disponíveis (testes de tipo caixa branca/caixa preta). Eles permitem que avaliações sejam feitas em relação aos sistemas operacionais e configuração de hardware, incluindo, mas não limitado a:

a) Varredura de porta UDP/TCP;
b) Identificação de emplilhamento e predição de sequência TCP para identificar sistemas operacionais e serviços;
c) Captura de normas do serviço público;
d) Varredura da Web usando scanners de vulnerabilidade HTTP e HTTPS; e,
e) Varredura de roteadores usando BGP (Border Gateway Protocol), BGMP (Border Gateway Multicast Protocol) e SNMP (Simple Network Management Protocol).

B.9.2 Avaliação de Vulnerabilidade

O objetivo da avaliação de vulnerabilidade é identificar vulnerabilidades, que poderão ser exploradas posteriormente durante o teste de penetração, fazendo consultas básicas relacionadas aos serviços em execução nos sistemas em questão. A avaliação deve incluir pelo menos as seguintes atividades:

a) Avaliação de Vulnerabilidade Externa - Os alvos deverão ser os dispositivos de rede e servidores que são acessíveis por um terceiro (uma pessoa ou uma empresa), por meio de um IP público (exposto publicamente), relacionado ao sistema a partir do qual será possível acessar as informações confidencias.
b) Avaliação de vulnerabilidade interna - os alvos deverão ser os servidores internos (dentro da DMZ ou na LAN se não houver DMZ) relacionados ao sistema a partir do qual poderá ser possível acessar as informações confidenciais. O teste de cada domínio de segurança na rede interna deverá ser realizado separadamente.

B.9.3 Testes de Penetração

O objetivo do teste de penetração deverá ser o de explorar quaisquer deficiências descobertas durante a avaliação de vulnerabilidade em quaisquer aplicativos expostos publicamente ou sistemas que hospedam aplicativos de processamento, transmissão e/ou armazenamento de informações confidenciais. Os teste de penetração deverá incluir pelo menos as seguintes atividades:

a) Teste de Penetração da Camada da Rede - O teste simulará as ações de um invasor real explorando as fraquezas na segurança da rede, examinando os sistemas em busca de qualquer fragilidade que possa ser usada por um invasor externo para interromper a confidencialidade, disponibilidade e/ou integridade da rede.
b) Teste de Penetração da Camada do Aplicativo - O teste deverá usar ferramentas para identificar pontos fracos nos aplicativos com varreduras autenticadas e não autenticadas, análise dos resultados para remover falsos positivos e teste manual para confirmar os resultados das

ferramentas e identificar o impacto dos pontos fracos.

B.9.4 Auditoria do Sistema de Gestão de Segurança da Informação (SGSI)

A auditoria do Sistema de Gerenciamento de Segurança da Informação (ISMS) deverá ser realizada, incluindo todas as localizações onde informações confidenciais são acessadas, processadas, transmitidas e/ou armazenadas. O ISMS será avaliado contra com os princípios de segurança de informação comum em relação à confidencialidade, integridade e disponibilidade, tal como as seguintes fontes ou equivalentes:

a) ISO/IEC 27001 Sistema de Gerenciamento de Segurança da Informação (ISMS);
b) Normas de Segurança de Dados da Indústria de Cartão de Pagamento (PCI-DSS); e,
c) Normas de Segurança da Associação Mundial de Loteria (WLA-SCS).

B.9.5 Auditoria de Serviços em Nuvem

Um operador utilizando um provedor de serviço em nuvem (CSP – Cloud Service Provider), conforme permitido pelo órgão regulador, para armazenar, transmitir ou processar informações confidenciais deve se submeter a auditoria específica, conforme requerido pelo órgão regulador. O CSP será avaliado contra os princípios de segurança da informação comuns em relação à provisão e uso de serviços em nuvem, tais como ISO/IEC 27017 e ISO/IEC 27018, ou equivalente.

a) Se informações confidenciais são armazenadas, processadas ou transmitidas em um ambiente em nuvem, os requisitos aplicáveis se aplicarão àquele ambiente, e constituirá de uma validação das infraestruturas CSP e uso deste ambiente pelo operador.
b) A designação de responsabilidades entre o CSP e o operador para gerenciar controles de segurança não isenta um operador da responsabilidade de assegurar que informações confidenciais são adequadamente protegidas, de acordo com os requisitos aplicáveis.
c) O CSP e o operador devem estar de acordo com as Políticas e procedimentos para todos os requisitos de segurança, e as responsabilidades da operação, gerenciamento e relatórios devem ser claramente definidos e compreendidos para cada requisito aplicável.

Glossário de Palavras-Chave

Acesso Não Autorizado – uma pessoa obtém acesso lógico ou físico sem permissão a uma rede, sistema, aplicativo, dados ou outro recurso.

Acesso Remoto – Qualquer acesso de fora do sistema ou da rede do sistema, incluindo qualquer acesso de outras redes dentro do mesmo local.

Administrador do Sistema – O(s) indivíduos(s) responsável por manter a operação do Sistema de Apostas de Eventos estável (incluindo software e infraestrutura de hardware e software aplicativo).

Algoritmo – Um conjunto finito de instruções inequívocas executadas em uma sequência prescrita para atingir um objetivo, especialmente uma regra matemática ou procedimento usado para calcular um resultado desejado. Os algoritmos são a base para a maior parte da programação de computadores.

Algoritmo Hash – uma função que converte uma string de dados em uma saída de string alfanumérica de comprimento fixo.

Ameaça – Qualquer circunstância ou evento com potencial de afetar adversamente as operações de rede (incluindo missão, funções, imagem ou reputação), ativos ou indivíduos por meio de um sistema ou por meio de acesso não autorizado, destruição, divulgação, modificação de informações e/ou negação de serviço. Além disso, o potencial de uma fonte de ameaça explorar com êxito uma vulnerabilidade do sistema.

Antivírus – Software usado para prevenir, detectar e remover vírus de computadores, incluindo malware, *worms* e cavalos de troia.

Aposta – Qualquer investimento de créditos ou dinheiro por parte do jogador em resultados de eventos.

Apostas de Probabilidades Fixas – Tipos de apostas no qual o valor a ser pago será fixado no momento em que a aposta for feita. Se as previsões estiverem corretas, as probabilidades são primeiro multiplicadas umas pelas outras e, em seguida, pelo valor da aposta.

Aposta em Evento Virtual – Uma forma de aposta que permite a colocação de apostas em esportes, competições e partidas cujos resultados são determinados exclusivamente por um Gerador de Números Aleatórios (RNG) aprovado.

Aposta em Jogo – Uma aposta que é colocada enquanto um evento está em andamento ou realmente acontecendo.

Aposta Parimutuel – Tipos de apostas em que apostas individuais são reunidas em um fundo. Os ganhos são calculados através da divisão do fundo entre todas as apostas ganhadoras.

Aposta Passada – Uma aposta que foi feita após o resultado de um evento ser aceito ou após um participante selecionado ter ganhado uma vantagem material (por exemplo, uma pontuação).

Aposta Remota – Apostas efetuadas utilizando Dispositivos de Apostas Remotas numa rede sem fios no local ou através da internet, dependendo da(s) implementação(ões) autorizada(s) pelo órgão regulador.

ARP - *Address Resolution Protocol* - O protocolo usado para converter endereços IP em endereços MAC para oferecer suporte a comunicação em uma rede local sem fio ou com fio.

Ataque "*Man-In-The-Middle*" – Um ataque em que o invasor retransmite secretamente e possivelmente altera a comunicação entre duas partes que acreditam estar se comunicando diretamente.

Autenticação – Verificar a identidade de um usuário, processo, pacote de software ou dispositivo, geralmente como um pré-requisito para permitir o acesso a recursos de um sistema.

Autenticação de Mensagem – Medida de segurança destinada a estabelecer a autenticidade de uma mensagem por meio de um autenticador na transmissão derivada de certos elementos predeterminados da própria mensagem.

Autenticação Multifator – Um tipo de autenticação que usa dois ou mais dos seguintes critérios para verificar a identidade de um usuário: Informações conhecidas apenas pelo usuário (por exemplo, uma senha padrão ou respostas a perguntas desafiadoras); Um item possuído por um usuário (por exemplo, um token eletrônico, um token físico ou um cartão de identificação); Dados biométricos de um usuário (por exemplo, impressões digitais, reconhecimento facial ou de voz).

Backup – Uma cópia de arquivos e programas feita para facilitar a recuperação, quando necessário.

Biometria – Uma entrada de identificação biológica, como impressões digitais ou a retina.

Bluetooth – Um protocolo de comunicações sem fio de baixa potência e curto alcance usado para interconexão de celulares, computadores e outros dispositivos eletrônicos, incluindo Dispositivos de Apostas. Conexões *bluetooth* tipicamente funcionam em distâncias de 10 metros ou menos e contam com ondas de rádio curto alcance para transmitir dados através do ar.

Certificado de Segurança – informações, geralmente armazenadas como um arquivo de texto, usadas pelo protocolo TSL (Transport Socket Layer) para estabelecer uma conexão segura. Um Certificado de Segurança contém informações sobre a quem ele pertence, de quem foi emitido, datas válidas, um número de série exclusivo ou outra identificação exclusiva que pode ser usada para verificar o conteúdo do certificado. Para uma conexão TSL ser criada, ambos os lados devem ter um Certificado de Segurança válido, que também é chamado de ID Digital.

Chave – Um valor usado para controlar operações criptográficas, como descriptografia, criptografia, geração de assinatura ou verificação de assinatura.

Chave de Criptografia – uma chave criptográfica que foi criptografada para disfarçar o valor do texto simples subjacente.

Código de Barras – Uma representação óptica de dados legível por máquina. Um exemplo é um código de barras encontrado nos registros de apostas impressos.

Código Móvel – código executável que se move de um computador para outro, incluindo código legítimo e código malicioso, como vírus de computador.

Comissão – Um valor retido e não distribuído pelo operador do valor total apostado em um jogo.

Componente Crítico – Qualquer subsistema no qual uma falha ou comprometimento pode levar a perda de direitos do jogador, receita do governo ou acesso não autorizado aos dados usados para gerar relatórios para o órgão regulador.

Conta do Jogador (também conhecido como "Conta de Aposta") – Uma conta mantida para um jogador onde as informações relativas ao jogo e transações financeiras são registradas em nome do jogador, incluindo, mas não se limitando a, depósitos, saques, apostas, ganhos e ajustes de saldo. O termo não inclui uma conta usada exclusivamente por um operador para rastrear pontos promocionais ou créditos ou benefícios semelhantes emitidos por um operador para um jogador que podem ser trocados por mercadorias e/ou serviços.

Controle de Acesso – O processo de conceder ou negar solicitações específicas para obter e usar informações confidenciais e serviços relacionados específicos de um sistema; e para entrar em instalações físicas específicas que abrigam uma rede crítica ou infraestrutura de sistema.

Controle da Versão – O método pelo qual um Sistema de Apostas de Eventos aprovado em evolução é verificado para estar operando em um estado aprovado.

Criptografia – A conversão de dados em uma forma, chamada de texto cifrado, que não pode ser facilmente compreendida por pessoas não autorizadas.

Cupom – Um instrumento de apostas que é usado primariamente para propósitos promocionais e que pode ser resgatado como créditos restritos ou irrestritos.

Cupom de Apostas – Um bilhete impresso ou mensagem eletrônica confirmando a aceitação de uma ou mais apostas.

Dados do Jogador – Informações confidenciais relacionadas a um jogador e que pode incluir itens tais como nome, data de nascimento, local de nascimento, CPF/RG, endereço, número de telefone, histórico de emprego e médico ou outras informações pessoais, conforme definido pelo órgão regulador.

DDOS - *Distributed Denial of Service* – Um tipo de ataque em que vários sistemas comprometidos, geralmente infectados por um programa de software destrutivo, são usados para atingir um único

sistema. As vítimas de um ataque DDOS consistem tanto no sistema de destino final quanto em todos os sistemas usados e controlados de forma maliciosa pelo hacker no ataque distribuído.

Dispositivo de Apostas – Um dispositivo eletrônico que converte comunicações do Sistema de Apostas de Eventos para uma forma humana interpretável e converte decisões humanas em formato de comunicação compreendida pelo Sistema de Apostas de Eventos.

Dispositivo de Aposta de Autoatendimento – Um quiosque que, no mínimo, será usado para a execução ou formalização de apostas feitas diretamente por um jogador e, se suportado, poderá ser usado para resgate de apostas vencedoras.

Dispositivo de Apostas POS, *Dispositivo de Apostas de Ponto de Venda* – Uma estação de atendimento que, no mínimo, será usada por um atendente para a execução ou formalização de apostas feitas em nome de um jogador.

Dispositivo de Aposta Remoto – Um dispositivo de propriedade de jogador operado em uma rede sem fio no local ou pela internet que, no mínimo, será usado para a execução ou formalização de apostas feitas diretamente pelo jogador. Exemplos de um Dispositivo de Apostas Remoto incluem um computador pessoal, telefone celular, tablet, etc.

Dividendos – O montante correspondente ao ganhador de uma aposta parimutuel.

DNS, *Domain Name Service* – O banco de dados da Internet distribuído globalmente que (entre outras coisas) mapeia os nomes de máquinas para números IP e vice-versa.

Domínio – um grupo de computadores e dispositivos em uma rede que são administrados como uma unidade com regras e procedimentos comuns.

DRP, *Disaster Recovery Plan* - Um plano para processar aplicativos críticos e prevenir a perda de dados no caso de uma grande falha de hardware ou software ou destruição de instalações.

Endereço IP - Endereço de Protocolo da Internet – Endereço de Protocolo da Internet - um número exclusivo para um computador que é usado para determinar onde as mensagens transmitidas na Internet devem ser entregues. O endereço IP é semelhante ao número da casa para o correio normal.

Envenenamento de Cache – Um ataque em que o invasor insere dados corrompidos no banco de dados de cache do serviço de nomes de domínio (DNS).

Evento – Ocorrência relativa a esportes, competições, jogos e outros tipos de atividades aprovadas pelo órgão regulador em quais apostas podem ser colocadas.

Evento Virtual de Apostas – Uma forma de aposta que permite fazer apostas em esportes, disputas e jogos cujos resultados são determinados somente por um Gerador de Número Aleatório (RNG) aprovado.

Firewall – Um componente de um sistema de computador ou rede projetado para bloquear o acesso ou tráfego não autorizado, ao mesmo tempo que permite a comunicação externa.

Geolocalização – Identifica a localização geográfica no mundo real de um dispositivo de reprodução remota conectado à Internet.

Gerenciamento de Chaves – Atividades que envolvem o manuseio de chaves criptográficas e outros parâmetros de segurança relacionados (por exemplo, senhas) durante todo o ciclo de vida das chaves, incluindo sua geração, armazenamento, estabelecimento, entrada e saída e zeragem.

Grupo de Funções – Um método de organizar contas de usuário em uma única unidade (por cargo) por meio do qual o acesso às funções do sistema pode ser modificado no nível da unidade e as alterações têm efeito para todas as contas de usuário atribuídas à unidade.

HTTP - *Hypertext Transport Protocol* - O protocolo subjacente usado para definir como as mensagens são formatadas e transmitidas e quais ações os servidores e navegadores devem realizar em resposta aos vários comandos.

IDS/IPS - Sistema de Detecção de Intrusão/Sistema de Prevenção de Intrusão - Um sistema que inspeciona todas as atividades de rede de entrada e saída e identifica padrões suspeitos que podem indicar um ataque de rede ou sistema de alguém tentando invadir ou comprometer um sistema. Usado em segurança de computador, a detecção de intrusão refere-se ao processo de monitoramento de atividades do computador e da rede e análise desses eventos para procurar sinais de intrusão em seu sistema.

Impressora – Um Dispositivo de Aposta periférico que imprime registros de apostas e/ou instrumentos de aposta.

Informações Confidenciais – Informações como dados dos jogadores, dados de apostas, números de validação, PINs, senhas, chaves e seeds de segurança e outros dados que devem ser tratados de maneira segura.

Instrumento de Apostas – Um documento virtual ou impresso de valor. também podendo ser um chip ou token e também cupons e vouchers. Um instrumento de aposta virtual é um token eletrônico trocado entre um dispositivo móvel de um jogador e o dispositivo de aposta que é usado para a inserção e resgate de crédito.

Integridade dos Dados – a propriedade de que os dados são precisos e consistentes e não foram alterados de maneira não autorizada no armazenamento, durante o processamento e durante o trânsito.

Interface do Usuário – Um aplicativo ou programa de interface através do qual o usuário visualiza e/ou interage com o Software de Apostas para comunicar suas ações ao Sistemas de Apostas de Eventos.

Internet – Um sistema interconectado de redes que conecta computadores em todo o mundo via TCP/IP.

Jailbreaking – Modificar um smartphone ou outro dispositivo eletrônico para remover restrições impostas pelo fabricante ou operadora para permitir a instalação de software não autorizado.

Jogada Grátis – Um modo que permite a um jogador participar em aposta sem colocar qualquer aposta financeira, principalmente para aprendizagem ou compreensão dos mecanismos de aposta.

Leitor de Código de Barras – Um dispositivo que é capaz de ler ou interpretar um código de barras. Isso pode se estender a alguns smartphones ou outros dispositivos eletrônicos que podem executar um aplicativo para ler um código de barras.

MAC - *Message Authentication Code* - Uma soma feita utilizando os dados para verificação criptográfica que usa uma chave simétrica com a finalidade de detectar modificações acidentais e intencionais dos dados.

Malware – Um programa que é inserido em um sistema, geralmente secretamente, com a intenção de comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicativos ou sistema operacional da vítima ou de incomodar ou interromper a vítima.

Mecanismo Físico – Software especializado que aproxima a lei da física, incluindo comportamentos como movimento, gravidade, força, aceleração, massa, etc., para elementos ou objetos de eventos virtuais. O mecanismo físico é usado para substituir elementos/objetos em eventos virtuais dentro de contextos do mundo físico ao renderizar computação gráfica ou simulações de vídeo.

Mercado – Um tipo de aposta (por exemplo, linha de dinheiro, spread, acima/abaixo) no qual oportunidade são construídas para apostas em um ou mais eventos.

NCE - Equipamento de Comunicação de Rede - um ou mais dispositivos que controlam a comunicação de dados em um sistema, incluindo, mas não se limitando a, cabos, switches, hubs, roteadores, pontos de acesso sem fio e telefones.

Operador – A pessoa ou entidade que executa um Sistema de Aposta em Eventos, usando capacidades tecnológicas de Sistema de Aposta em Eventos, assim com seus próprios procedimentos internos.

Parlay – Uma aposta única que liga duas ou mais apostas individuais e está dependente de todas essas apostas ganharem juntas.

Participante – O atleta, equipe ou outra entidade que compete em um evento.

Participante Virtual – O atleta ou outra entidade que compete em um evento virtual.

Perfecta (também conhecida como "*Exacta*") – Uma aposta em que o jogador escolhe o primeiro e o segundo colocado em uma competição na ordem correta.

PIN, *Número de Identificação Pessoal* – Um código numérico associado a um indivíduo e que permite acesso seguro a um domínio, conta, rede, sistema, etc.

Plano de Contingência – Política e procedimentos de gestão concebidos para manter ou restaurar as operações de apostas, possivelmente em um local alternativo, em caso de emergências, falhas do sistema ou desastres.

Política de Segurança – um documento que delineia a estrutura de gerenciamento de segurança e atribui claramente as responsabilidades de segurança e estabelece a base necessária para medir o progresso e a conformidade com segurança.

Porta – Uma entrada física ou um ponto de saída de um módulo que fornece acesso ao módulo para sinais físicos, representados por fluxos de informações lógicas (portas fisicamente separadas não compartilham o mesmo pino físico ou fio).

Postar em Linha – Um valor que estabelece o possível pagamento de uma aposta (por exemplo, linha de dinheiro + 175) ou as condições para uma aposta ser considerada ganha ou perdida (por exemplo, spread de ponto + 2,5).

Programa de Controle Crítico – Um programa de software que controla comportamentos relativos a qualquer padrão técnico aplicável e/ou requisito regulatório.

Programa de Detecção de Vírus – Software usado para prevenir, detectar e remover vírus de computador, incluindo malware, worms e cavalos de Tróia.

Programa de Fidelidade do Jogador – Um programa que fornece incentivo para os jogadores com base no volume de jogos ou receita recebida de um jogador.

Protocolo – Um conjunto de regras e convenções que especifica a troca de informações entre dispositivos, por meio de uma rede ou outra mídia.

Protocolo de Comunicação Seguro – um protocolo de comunicação que fornece a proteção adequada de confidencialidade, autenticação e integridade de conteúdo.

Protocolo Sem Estado – Um esquema de comunicação que trata cada solicitação como uma transação independente, não relacionada a nenhuma solicitação anterior, de forma que a comunicação consiste em pares independentes de solicitações e respostas.

Proxy – Um proxy é um aplicativo que "interrompe" a conexão entre o cliente e o servidor. O proxy aceita certos tipos de tráfego que entram ou saem de uma rede e os processa e encaminha. Isso fecha efetivamente o caminho direto entre as redes internas e externas. Tornando mais difícil para um invasor obter endereços internos e outros detalhes da rede interna.

Quinela – Aposta em que serão previstos os dois primeiros lugares de uma competição, mas não necessariamente na ordem de chegada.

Registro de Data/Hora – Um registro da data e hora do Sistema de Aposta em Eventos que é adicionado a uma mensagem no momento em que ela é criada.

Regras de Apostas – Qualquer informação escrita, gráfica ou de auditoria fornecida ao público em relação às apostas de eventos.

Risco – A probabilidade de uma ameaça ter sucesso em seu ataque contra uma rede ou sistema.

RNG Criptografado – Gerador de números aleatórios (RNG) resistente ao ataque ou ao comprometimento feito por hacker inteligente com recursos computacionais modernos que tenha conhecimento do código-fonte do RNG e/ou de seu algoritmo. RNGs criptografados não podem ser "quebrados" de nenhuma maneiro para prever valores futuros.

RNG, *Gerador de Números Aleatórios* – Um dispositivo computacional ou físico, algoritmo ou sistema projetado para produzir números de uma maneira indistinguível da seleção aleatória.

Rooting – Obtenção de acesso root ao código do sistema operacional para modificar o código do software no telefone celular ou outro Dispositivo de Aposta Remoto ou instalar softwares que o fabricante não permitiria a instalação.

Segurança da Informação – Proteger as informações e os sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de fornecer integridade, confidencialidade e disponibilidade.

Senha – uma sequência de caracteres (letras, números e outros símbolos) usada para autenticar uma identidade ou para verificar a autorização de acesso.

Servidor – uma instância em execução de software capaz de aceitar solicitações de clientes e do computador que executa esse software. Os servidores operam dentro de uma Arquitetura Cliente-Servidor, na qual "servidores" são programas de computador executados para atender as solicitações de outros programas ("clientes"). Neste caso, o "servidor" seria o Sistemas de Apostas de Eventos e os "clientes" seriam os Dispositivos de Apostas.

***Shellcode* –** Um pequeno pedaço de código usado como útil na exploração da segurança. O Shellcode explora a vulnerabilidade e permite que um invasor reduza a garantia de informações de um sistema.

Sistema de Aposta em Eventos – O hardware, software, firmware, tecnologias de comunicações, outros equipamentos, assim como procedimentos implementados pelo operador para permitir que o jogador participe na aposta, e, se suportado, o equipamento correspondente relacionado à exibição dos resultados da aposta e outras informações semelhantes necessárias para facilitar a participação do jogador. O sistema fornece ao jogador os meios para fazer e gerenciar as apostas. O sistema fornece ao operador os meios para revisar as contas dos jogadores, se suportadas, suspender eventos, gerar várias transações financeiras e de apostas e relatórios de contabilidade, inserir resultados para eventos e definir quaisquer parâmetros configuráveis.

Sistema de Apostas Externas – O sistema de hardware e software separados daquele que compreende o Sistemas de Apostas de Eventos, que podem executar recursos comuns de ofertas de apostas, configurações de apostas, relatórios, etc. O jogador inicialmente se comunica diretamente com o Sistemas de Apostas de Eventos que pode estar integrado com um ou mais Sistema de Apostas Externas.

Software de Apostas – O software usado para fazer a interface entre as apostas e transações financeiras com o Sistemas de Apostas de Eventos que, baseados no design, é baixado ou instalado no Dispositivo de Apostas, operado desde o Sistemas de Apostas de Eventos que é acessado pelo Dispositivo de Apostas ou uma combinação dos dois. Exemplos de Software de Apostas incluem pacotes de software de download proprietário, html, flash, etc.

TCP/IP - *Transmission Control Protocol/Internet Protocol* - O conjunto de protocolos de comunicação usado para conectar hosts na Internet.

Touch Screen – Um dispositivo de exibição de vídeo que também atua como um dispositivo de entrada do usuário usando locais de pontos de toque elétricos na tela.

Trifecta – Uma aposta na qual um jogador ganha ao selecionar os três primeiros finalistas de uma competição na ordem correta de chegada.

Trilha de Auditoria – Um registro que mostra quem acessou um sistema e quais operações o usuário realizou durante um determinado período.

Voucher – Um instrumento de aposta que pode ser resgatado em dinheiro ou usado para posteriormente resgatar créditos.

VPN - *Virtual Private Network* - Uma rede lógica estabelecida em uma rede física existente e que normalmente não inclui todos os nós presentes na rede física.

Vulnerabilidade – Software, hardware ou outros pontos fracos em uma rede ou sistema que podem fornecer uma "porta" para a introdução de uma ameaça.

Wi-Fi – A tecnologia padrão de rede local sem fio (WLAN) para conectar computadores e dispositivos eletrônicos entre si e/ou à Internet.