DIÁRIO OFICIAL DA UNIÃO
Publicado em: 03/05/2024 | Edição: 85-B | Seção: 1 - Extra B | Página: 1
Órgão: Ministério da Fazenda/Secretaria de Prêmios e Apostas

PORTARIA SPA/MF Nº 722, DE 2 DE MAIO DE 2024

Estabelece os requisitos técnicos e de segurança dos sistemas de apostas, bem como de suas plataformas de apostas esportivas e de jogos on-line, a serem utilizados por agentes operadores de loteria de apostas de quota fixa, de que tratam a Lei nº 13.756, de 12 de dezembro de 2018, e a Lei nº 14.790, de 29 de dezembro de 2023.

O SECRETÁRIO DE PRÊMIOS E APOSTAS DO MINISTÉRIO DA FAZENDA, no uso das atribuições que lhe confere o art. 55, inciso I, alínea "d", do Anexo I do Decreto nº 11.907, de 30 de janeiro de 2024, e tendo em vista o disposto no art. 29, § 3º, da Lei nº 13.756, de 12 de dezembro de 2018, no art. 7º, § 1º, inciso VII, da Lei nº 14.790, de 29 de dezembro de 2023, e no art. 6º, inciso V, da Portaria Normativa MF nº 1.330, de 26 de outubro de 2023, resolve:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria estabelece os requisitos técnicos e de segurança dos sistemas de apostas, bem como de suas plataformas de apostas esportivas e de jogos on-line, a serem utilizados por agentes operadores de loteria de apostas de quota fixa, de que tratam a Lei nº 13.756, de 12 de dezembro de 2018, e a Lei nº 14.790, de 29 de dezembro de 2023.

Art. 2º Para os fins desta Portaria, considera-se:

I - sistema de apostas: sistema informatizado gerido e disponibilizado pelos operadores aos apostadores que possibilita o cadastro dos apostadores, o gerenciamento de suas carteiras virtuais e outras funcionalidades necessárias para gerenciamento, operação e comercialização das apostas de quota-fixa;

II - plataforma de apostas: canal eletrônico integrado ao sistema de apostas utilizado para ofertar as apostas esportivas e os jogos on-line aos apostadores.

III - entidade certificadora: pessoa jurídica com capacidade operacional reconhecida pelo Ministério da Fazenda para testar e certificar equipamentos, programas, instrumentos e dispositivos que compreendem os sistemas de apostas, os estúdios de jogo ao vivo e os jogos on-line utilizados pelos operadores de loteria de apostas de quota fixa, observados os requisitos técnicos estabelecidos em regulamento específico;

IV - central de dados: local onde estão concentrados os sistemas computacionais do agente operador, como o sistema de armazenamento de dados;

V - plano de continuidade de Tecnologia da Informação: plano que abrange as estratégias necessárias à continuidade dos serviços de tecnologia da informação essenciais, como contingência, continuidade e recuperação;

VI - componente crítico: qualquer componente no qual uma falha ou comprometimento possa levar à perda de direitos do apostador, perda de receitas da União ou de destinatários legais, impedimento ou dificuldades de acesso do regulador às informações operacionais, ocorrência de acesso não autorizado aos dados do sistema de apostas, ou descumprimento das normas que regulamentam a operação de apostas de quota fixa no País; e

VII - terminal de apostas: dispositivo disponibilizado pelo agente operador no qual o apostador pode realizar apostas na modalidade física.

CAPÍTULO II

DOS REQUISITOS TÉCNICOS

Art. 3º Os sistemas de apostas, integrados pelas plataformas de apostas esportivas e de jogos on-line, utilizados pelos agentes operadores para exploração da modalidade lotérica das apostas de quota fixa deverão observar e implementar os requisitos técnicos estabelecidos nesta Portaria e em seus Anexos.

Art. 4º Os agentes operadores deverão manter o sistema de apostas e os respectivos dados em centrais de dados localizadas em território brasileiro, observadas as disposições da Lei nº 13.709, de 14 de agosto de 2018.

§1º Os sistemas e os dados de que trata o caput deste artigo poderão estar localizados fora do território nacional, em países que possuam Acordo de Cooperação Jurídica Internacional com o Brasil, em matéria civil e penal conjuntamente, desde que observado o inciso VIII do caput do art. 33 da Lei nº 13.709, de 2018, e os seguintes requisitos sejam atendidos cumulativamente:

I - o titular deverá autorizar, de modo específico e prévio, a transferência internacional de seus dados pessoais, cabendo ao agente operador prestar informações claras quanto à finalidade da operação;

II - a área técnica responsável do Ministério da Fazenda deverá ter acesso seguro e irrestrito, de forma remota e presencial, aos sistemas, às plataformas e aos dados da operação;

III - o agente operador deverá replicar, no Brasil, sua base de dados e de informações, que serão atualizadas de forma contínua, garantindo que todas as instâncias do banco de dados possuam o mesmo conteúdo, e que sejam testados periodicamente; e

IV - o agente operador deverá apresentar um plano de continuidade de negócios de Tecnologia da Informação, no caso da ocorrência de situações críticas que possam colocar em risco a operação e os dados, contendo, no mínimo:

a) mapeamento de cenários de perdas prováveis;

b) identificação, análise e avaliação dos riscos;

c) ações de prevenção e mitigação; e

d) designação de responsáveis.

§2º A central de dados utilizada deverá possuir a certificação ISO 27001.

Art. 5º Os canais eletrônicos utilizados pelo agente operador para ofertar apostas de quota fixa em meio virtual deverão utilizar registro de domínio "bet.br", conforme regulamento específico.

CAPÍTULO III

DA CERTIFICAÇÃO E DO RELATÓRIO DE AVALIAÇÃO PARA CERTIFICAÇÃO

Art. 6º Os agentes operadores deverão manter os sistemas de apostas, que compreendem as plataformas de apostas esportivas e de jogos on-line, certificados por entidade certificadora cuja capacidade operacional tenha sido reconhecida pela Secretaria de Prêmios e Apostas do Ministério da Fazenda, nos termos da Portaria MF/SPA nº 300, de 23 fevereiro de 2024.

§1º Os certificados emitidos pela entidade certificadora deverão atestar que os sistemas de apostas, incluindo as plataformas de apostas esportivas e de jogos on-line, estão em plena conformidade com os requisitos técnicos definidos nos Anexos I, II e III desta Portaria, inclusive em relação à integração entre seus módulos e plataformas.

§2º Nas situações em que os módulos e plataformas dos sistemas de apostas utilizados pelo agente operador não possuam a mesma versão de compilação e o mesmo fornecedor, será obrigatória a verificação da integração entre eles pelas entidades certificadoras cuja capacidade técnica tenha sido reconhecida pelo Ministério da Fazenda.

§3º Os sistemas de apostas, incluindo as plataformas de que trata o caput, deverão permanecer com certificados válidos durante todo o prazo de duração da autorização concedida.

§4º Os certificados emitidos pela entidade certificadora para os sistemas de apostas compreenderão as plataformas de apostas esportivas e de jogos on-line e deverão ser revalidados anualmente, e sempre que houver inclusão, alteração e exclusão de componentes críticos.

§5º O certificado revalidado nos termos do § 4º deverá ser encaminhado à Secretaria de Prêmios e Apostas do Ministério da Fazenda no prazo de até cinco dias úteis posteriores à expedição.

Art. 7º Os certificados devem ser emitidos especificamente para o Brasil pelas entidades certificadoras habilitadas pela Secretaria de Prêmios e Apostas do Ministério da Fazenda, nos termos da Portaria MF/SPA nº 300, de 23 fevereiro de 2024.

Art. 8º Os agentes operadores deverão apresentar, em até noventa dias após a publicação do ato de autorização pela Secretaria de Prêmios e Apostas do Ministério da Fazenda, relatório de avaliação para certificação dos requisitos técnicos definidos no Anexo IV desta Portaria emitido por entidade certificadora cuja capacidade operacional tenha sido reconhecida pela Secretaria de Prêmios e Apostas do Ministério da Fazenda.

Parágrafo único. Os relatórios de avaliação para certificação emitidos pela entidade certificadora para os sistemas de apostas e para as plataformas de apostas esportivas e de jogos on-line deverão ser revalidados anualmente.

CAPÍTULO IV

DA SUPERVISÃO E DA FISCALIZAÇÃO

Art. 9º As atividades de supervisão e de fiscalização dos sistemas de apostas, que compreendem as plataformas de apostas esportivas e de jogos on-line, serão disciplinadas em regulamento específico da Secretaria de Prêmios e Apostas do Ministério da Fazenda, respeitadas as competências dos demais órgãos e entidades governamentais e de defesa do consumidor.

Parágrafo único. Para a finalidade prevista no caput, o agente operador deverá, a qualquer tempo, conceder pleno acesso aos sistemas de apostas para as unidades e agentes de fiscalização da Secretaria de Prêmios e Apostas do Ministério da Fazenda.

Art. 10. Os agentes operadores deverão encaminhar à Secretaria de Prêmios e Apostas do Ministério da Fazenda os dados referentes às apostas, aos apostadores, às carteiras dos apostadores, às destinações legais e demais informações de sua operação, conforme periodicidade e formato estabelecidos no Manual SIGAP, disponibilizado no site https://www.gov.br/fazenda/pt-br/composicao/orgaos/secretaria-de-premios-e-apostas.

Parágrafo único. Sem prejuízo do disposto no caput, a Secretaria de Prêmios e Apostas do Ministério da Fazenda poderá, a qualquer tempo, solicitar informações adicionais ao operador.

Art. 11. Os sistemas de apostas, incluindo suas plataformas de apostas esportivas e de jogos on-line, serão submetidos a procedimentos de inspeção, conforme solicitação da Secretaria de Prêmios e Apostas do Ministério da Fazenda.

CAPÍTULO V

DOS TERMINAIS DE APOSTAS

Art. 12. Os agentes operadores com sistemas de apostas certificados, quando autorizados, poderão ofertar apostas que tenham por objeto eventos reais de temática esportiva, na modalidade física, por meio de terminais de apostas.

Parágrafo único. As apostas de quota fixa que tenham por objeto os eventos de jogo on-line somente poderão ser ofertadas em meio virtual.

Art. 13. Os terminais de apostas deverão estar sempre conectados e integrados ao sistema de apostas do operador, observados os requisitos técnicos estabelecidos nos Anexos I e II desta Portaria.

Parágrafo único. As apostas realizadas em terminais de apostas serão sempre precedidas dos procedimentos de identificação de que trata o art. 23 da Lei nº 14.790, de 2023, e obedecerão a todas as demais regras para a realização de apostas em meio virtual, inclusive as relativas às transações de pagamento, conforme regulamento específico da Secretaria de Prêmios e Apostas do Ministério da Fazenda.

CAPÍTULO VI

DOS JOGOS ON-LINE

Art. 14. Os jogos on-line a serem ofertados pelos agentes operadores deverão possuir fator de multiplicação do valor apostado que defina o montante a ser recebido pelo apostador, em caso de premiação, no momento da efetivação da aposta, para cada unidade de moeda nacional apostada, cujo resultado seja determinado pelo desfecho de evento futuro aleatório, a partir de um gerador randômico de números, de símbolos, de figuras ou de objetos definido no sistema de regras.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 15. Regulamento específico da Secretaria de Prêmios e Apostas do Ministério da Fazenda disciplinará as sanções aplicáveis ao agente operador em caso de descumprimento do disposto nesta Portaria.

Art. 16. Os requisitos técnicos dos estúdios de jogo ao vivo e dos jogos on-line a serem observados pelas entidades certificadoras de que trata a Portaria MF/SPA nº 300, de 2024, serão definidos em regulamento específico.

Art. 17. Esta Portaria entra em vigor na data da sua publicação.

REGIS ANDERSON DUDENA

ANEXO I

DO SISTEMA DE APOSTAS

Dos Requisitos Gerais

1. O sistema de apostas deve possuir um relógio interno que reflita a data e a hora sincronizados com o horário de Brasília - UTC-3, e forneça as seguintes informações:

a) marcação de tempo em todas as transações e eventos;

b) marcação de tempo de eventos significativos; e

c) relógio de referência para relatórios.

2. O sistema de apostas deverá garantir que a hora e as datas entre todos os seus componentes, incluindo as plataformas de apostas esportivas e de jogos on-line, estejam sincronizados.

3. O sistema de apostas deverá controlar comportamentos relativos a qualquer requisito definido pela Secretaria de Prêmios e Apostas do Ministério da Fazenda por meio de uma aplicação ou software, denominado de programa de controle.

4. O sistema de apostas deverá ser capaz de verificar se todos os componentes críticos do programa de controle são cópias autênticas dos componentes aprovados e instalados no sistema, pelo menos uma vez a cada 24 horas e sob demanda.

5. O mecanismo de autenticação do programa de controle deve:

a) utilizar 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 possam afetar as operações de apostas de quota fixa, incluindo, mas não se limitando a arquivos executáveis, bibliotecas, configurações de apostas ou do sistema, arquivos do sistema operacional, componentes que controlam o relatório do sistema necessário e elementos de banco de dados que afetam as operações do sistema; e

c) indicar falha de autenticação caso algum componente crítico do programa de controle seja considerado inválido.

6. Cada componente crítico do programa de controle deve permitir a verificação independente por terceiros, que deve operar independentemente de qualquer processo ou software de segurança dentro do sistema, cujo método de verificação de integridade deve ser aprovado pela entidade certificadora habilitada, antes da aprovação do sistema.

7. O sistema de apostas deve ser capaz de executar um desligamento normal e somente permitir o reinício automático após a execução, no mínimo, dos procedimentos a seguir:

a) conclusão, com sucesso, das rotinas de reinício do programa, incluindo autotestes;

b) autenticação de todos os componentes críticos do programa de controle, conforme item5; e

c) restabelecimento e autenticação da comunicação com todos os componentes necessários para a operação do sistema.

8. O sistema de apostas deverá poder suspender, sob demanda:

a) todas as atividades de aposta;

b) eventos individuais;

c) mercados individuais;

d) dispositivos de apostas individuais, se houver;

e) contas de apostadores individuais; e

f) temas de jogos individuais, tabelas de pagamento ou versões, como desktop, celular, tablet e similares.

Do gerenciamento de contas dos apostadores

Cadastro de contas

9. O sistema de apostas, por meio da plataforma de gerenciamento de contas de apostador, deverá coletar as informações do apostador antes da efetivação do cadastro.

10. Na etapa de cadastramento da conta do apostador, devem ser atendidos, no mínimo, os seguintes requisitos:

a) apenas apostadores maiores de dezoito anos podem se registrar; qualquer pessoa que informar uma data de nascimento que indique que é menor de idade terá a solicitação de registro da conta negada;

b) qualquer pessoa que indique uma informação diferente de seus documentos oficiais deverá ter seu registro de conta negado;

c) a verificação de identidade deve realizar o reconhecimento facial e ser realizada antes que um apostador tenha uma conta cadastrada;

d) a conta do apostador só pode ser ativada quando:

I. a verificação de idade e identidade, incluindo a validade do CPF e o reconhecimento facial, for concluída com sucesso;

II. a verificação de que o apostador não está em nenhuma lista de exclusão ou proibido de estabelecer ou manter uma conta for realizada;

III. o apostador tiver concordado com as políticas de privacidade e os termos e condições para realização de apostas;

IV. o apostador estiver ciente da vedação do acesso de terceiros à sua conta;

V. o apostador tiver autorizado o monitoramento e o registro de seus dados pelo agente operador e pela Secretaria de Prêmios e Apostas do Ministério da Fazenda; e

VI. o cadastro da conta do apostador estiver completo;

e) um apostador só poderá ter uma única conta ativa por vez no sistema de apostas de cada marca autorizada pela Secretaria de Prêmios e Apostas do Ministério da Fazenda; e

f) o sistema deve permitir a atualização de senhas ou outras credenciais de autenticação, de informações de registro e de contas bancárias utilizadas para transações financeiras de cada apostador, condicionada ao reconhecimento facial.

Acesso ao sistema de apostas

11. O sistema de apostas deve autenticar a entrada de qualquer apostador cadastrado no sistema por meio de usuário e senha ou por meio de biometria. Caso o sistema não reconheça o nome de usuário e/ou senha quando inseridos, uma mensagem explicativa deverá ser exibida ao apostador, solicitando a este que insira novamente as informações.

12. Nos casos em que o apostador esqueça seu nome de usuário e/ou senha, o sistema deverá oferecer um processo de autenticação multifatorial para a recuperação ou redefinição do usuário e/ou senha, sendo um dos fatores o reconhecimento facial.

13. Caso alguma atividade suspeita seja detectada, como por exemplo múltiplas tentativas malsucedidas de acesso, o sistema de apostas deverá bloquear a respectiva conta. Nesse caso, para que a conta seja desbloqueada, deverá ser realizado um processo de autenticação multifatorial, sendo um dos fatores o reconhecimento facial.

Inatividade do apostador

14. O sistema de apostas deverá exigir um novo processo de autenticação do apostador após um período de 30 minutos de inatividade em um dispositivo, não sendo permitida a realização de nenhuma aposta ou transação financeira até que o apostador seja autenticado novamente.

15. O sistema de apostas poderá oferecer, como forma de uma nova autenticação no mesmo dispositivo, acesso por biometria, que deverá ser testado pela entidade certificadora habilitada pela Secretaria de Prêmios e Apostas do Ministério da Fazenda.

16. O sistema de apostas deverá exigir do apostador uma autenticação multifatorial :

a) ao menos uma vez a cada 7 (sete) dias; ou

b) no primeiro acesso após um período de inatividade superior a 7 (sete) dias.

Limites e exclusões

17. O sistema de apostas deverá implementar corretamente quaisquer limitações e exclusões estabelecidas pelo apostador, pelo agente operador e pela Secretaria de Prêmios e Apostas do Ministério da Fazenda.

18. O sistema de apostas não deverá permitir ao apostador impor limites que sejam menos restritivos que aqueles estabelecidos pelo agente operador e pela Secretaria de Prêmios e Apostas do Ministério da Fazenda.

19. As limitações estabelecidas não devem ser afetadas por outros eventos de status internos.

Gerenciamento financeiro do apostador

20. O sistema de apostas deve fornecer confirmação ou negação de todas as transações realizadas pelo apostador.

21. O sistema de apostas deve garantir que todos os aportes e retiradas de recursos financeiros pelos apostadores sejam realizados exclusivamente por meio de transferência eletrônica entre a conta bancária cadastrada do apostador e a conta transacional do agente operador, ambas mantidas em instituições autorizadas a funcionar pelo Banco Central do Brasil, nos termos do art. 22 da Lei nº 14.790, de 2023.

22. O sistema de apostas deve garantir que os valores aportados na conta gráfica pelo apostador somente estejam disponíveis para realização das apostas após a confirmação da liquidação da operação pela instituição mantenedora da conta transacional, sendo mantida em um registro específico para auditoria.

23. O sistema de apostas não permitirá a realização de transações financeiras na conta gráfica do apostador que excedam os limites estabelecidos pelo apostador, pelo agente operador ou pela Secretaria de Prêmios e Apostas do Ministério da Fazenda.

24. O sistema de apostas não permitirá a realização de transferências de recursos entre contas de apostadores.

Extrato de conta

25. O sistema de apostas deverá prover um extrato dos últimos trinta e seis meses das movimentações da conta gráfica do apostador e um arquivo log com as transações efetuadas quando requerido. O extrato e o arquivo log deverão incluir informações suficientes para permitir ao apostador

conciliar as informações fornecidas pelo agente operador com seus extratos bancários, devendo incluir, no mínimo, os seguintes detalhes das transações financeiras, com registro de data e hora e com um identificador único da transação:

a) aportes na conta gráfica do apostador;

b) retiradas da conta gráfica do apostador;

c) recebimento de prêmios de apostas;

d) pagamento de imposto de renda sobre prêmios;

e) ajustes manuais ou modificações na conta gráfica do apostador, por exemplo, reembolso;

f) créditos adicionados ou removidos da conta gráfica do apostador relacionados a apostas;

g) meio de aporte e retirada: transferência eletrônica, PIX, cartão de débito, cartão pré- pago e book transfer;

h) identificação do usuário ou do dispositivo de apostas que processou a transação;

i) valor total das taxas pagas na transação, quando houver;

j) saldo total da conta antes e depois das transações; e

k) quaisquer outras movimentações realizadas na conta gráfica do apostador.

Dos programas de fidelidade

26. O sistema de apostas deve registrar todas as transações envolvendo programas de fidelidade eventualmente oferecidos ao apostador, considerando as vedações impostas pelo art. 29 da Lei nº 14.790, de 2023, e observada a regulamentação específica da Secretaria de Prêmios e Apostas do Ministério da Fazenda.

Dos requisitos de geolocalização

Prevenção de fraudes de localização

27. O sistema de apostas deverá detectar o uso de programas que possuam a capacidade de contornar a detecção da localização do apostador, como software de área de trabalho remota, rootkits, virtualização e quaisquer outros programas, e bloquear a tentativa de fraude dos dados de localização antes da conclusão de cada aposta.

28. O sistema de apostas deverá examinar e registrar o endereço IP em cada conexão de dispositivo remoto de apostas a uma rede para garantir que uma Virtual Private Network - VPN conhecida ou serviço de proxy não estejam em uso.

29. O sistema de apostas deverá detectar e bloquear dispositivos que indiquem adulteração em

nível de sistema, como rooting, jailbreak e similares.

30. O sistema de apostas deverá identificar e parar quaisquer ataques " Man-In-The-Middle" ou técnicas de hacking similares e prevenir a manipulação de código.

31. O sistema de apostas deverá monitorar e prevenir apostas realizadas por uma única conta de apostador a partir de locais geograficamente incompatíveis, como a identificação de locais nos quais foram feitas as apostas que seriam impossíveis de serem efetuadas deslocando-se em um curto intervalo de tempo.

Detecção da localização para apostas na internet

32. O sistema de apostas deverá possuir meios ou sistemas de detecção de geolocalização que determinem e monitorem dinamicamente a localização de um apostador tentando realizar uma aposta, e que bloqueiem tentativas não autorizadas.

33. Cada apostador deverá passar por uma checagem de localização prévia à realização da primeira aposta após acesso ao sistema de apostas em um dispositivo. As checagens subsequentes neste dispositivo devem ocorrer a cada 30 (trinta) minutos.

34. Um método de geolocalização deverá ser utilizado para fornecer a localização física do apostador e o raio de confiança associado. A entidade certificadora habilitada pela Secretaria de Prêmios e Apostas do Ministério da Fazenda validará o método de geolocalização utilizado.

35. Fontes acuradas de dados devem ser utilizadas pelo método de geolocalização para confirmar a localização do apostador.

Da manutenção dos dados

36. O sistema de apostas deverá manter e realizar o backup de todos os dados gravados pelo prazo mínimo de 5 (cinco) anos.

37. O sistema de apostas deverá possibilitar a exportação dos dados para fins de análise de dados e auditoria em formato XML, XLS e CSV, no mínimo.

38. O sistema de apostas deverá manter registro, em complemento às informações contidas no item 25 deste Anexo, das seguintes informações:

a) de apostas esportivas:

I. número de identificação único da aposta;

II. data e hora em que a aposta foi realizada;

III. identificação do endereço IP do dispositivo utilizado para a realização da aposta;

IV. Estado da Federação em que a aposta foi realizada;

V. status da aposta: em curso, não premiada, premiada, suspensa ou cancelada;

VI. motivo da suspensão ou cancelamento da aposta;

VII. montante total de recebimento de prêmios e status do prêmio: a pagar, pago ou prescrito;

VIII. ganho da aposta; e

IX. imposto de renda retido.

b) de mercados de apostas e eventos esportivos que foram objeto de apostas:

I. data e hora de início e término do período de apostas;

II. data e hora de início e término do evento;

III. data e hora em que os resultados foram confirmados;

IV. data e hora em que a aposta vencedora foi paga ao apostador;

V. quantidade de apostas e de apostadores;

VI. valor total de apostas realizadas;

VII. identificação do apostador, valor e data dos aportes financeiros;

VIII. identificação do evento da modalidade esportiva;

IX. status do evento: adiado, cancelado, suspenso, atrasado, em curso, finalizado ou não iniciado;

X. quota-fixa do mercado objeto da aposta;

XI. tipo do mercado apostado;

XII. valor total de prêmios pagos a apostadores;

XIII. identificação de cada apostador vencedor;

XIV. montante total de aportes;

XV. valor total de apostas suspensas e canceladas;

XVI. identificadores de evento e mercado;

c) do jogo on-line:

I. identificador de cada sessão de jogo on-line;

II. endereço IP utilizado para realizar a aposta;

III. data e hora do início e do fim da sessão de jogo on-line;

IV. status da sessão: premiada, não premiada, suspensa, cancelada;

V. quantidade de apostas;

VI. identificador da aposta no jogo on-line;

VII. quota fixa da aposta;

VIII. valor da aposta;

IX. valor total apostado;

X. ganho do apostador;

XI. tipo de jogo on-line;

XII. denominação do jogo on-line; e

XIII. número da certificação do jogo on-line;

d) de cada conta de apostador:

I. identificador único do apostador;

II. data e método de verificação de identidade, incluindo, quando aplicável, uma descrição do documento de identificação fornecido pelo apostador para confirmar sua identidade e a respectiva data de expiração;

III. dados criptografados do apostador, incluindo nome, nacionalidade, data de nascimento e CPF ou passaporte, em caso de apostador estrangeiro;

IV. data e hora de criação da conta;

V. data do aceite do apostador em relação aos termos e condições e à política de privacidade do operador;

VI. status do apostador: ativo, cancelado, suspenso, autoexcluído, pendente de verificação, excluído judicialmente, com cadastro pendente de atualização e validação anual, outro;

VII. data e hora de início e término da sessão do apostador;

VIII. motivo do encerramento da sessão do apostador: inatividade, encerramento voluntário, encerramento pelo operador ou outro motivo;

IX. data e hora de alterações no status do apostador;

X. período de pausa estabelecido;

XI. data e hora do estabelecimento do período de pausa;

XII. período de exclusão estabelecido;

XIII. data e hora do estabelecimento do período de exclusão;

XIV. período de exclusão judicial determinado;

XV. data e hora da determinação do período de exclusão judicial;

XVI. limites de aporte, gasto, tempo e perda estabelecidos;

e) do operador:

I. saldo das carteiras dos apostadores detido pelo operador;

II. saldo das contas transacionais do operador;

III. IRPF retido e recolhido;

IV. detalhamento das destinações legais, conforme estabelece o §1º-A do art. 30 da Lei nº 13.756, de 2018;

V. valor total do Gross Gaming Revenue - GGR.

39. Deverão ser mantidas e armazenadas no sistema de apostas as informações do meio utilizado para a realização da aposta em:

a) dispositivos móveis e computadores; e

b) pontos de venda física, com a identificação do terminal onde foi realizada a aposta.

40. O sistema de apostas deverá manter e armazenar informações sobre eventos diversos, incluindo:

a) tentativas de login malsucedidas;

b) erros do programa e incompatibilidades de autenticação;

c) períodos significativos de indisponibilidade de qualquer componente crítico do sistema;

d) grandes ganhos, individuais e agregados em um período, que excedam o valor definido em regulamento específico da Secretaria de Prêmios e Apostas do Ministério da Fazenda, incluindo informações de registro de apostas;

e) grandes apostas, únicas e agregadas em um período, que excedam o valor definido em regulamento específico da Secretaria de Prêmios e Apostas do Ministério da Fazenda, incluindo informações de registro de apostas;

f) falta de responsividade, anulações e correções do sistema;

g) alterações nos arquivos de dados ativos que ocorrerem fora da execução normal do programa e do sistema operacional;

h) alterações feitas na biblioteca de dados de download, incluindo a adição, a alteração ou a exclusão de software, quando suportado;

i) alterações no sistema operacional, banco de dados, rede, e nas políticas e parâmetros do aplicativo;

j) alterações de data e hora no servidor principal;

k) alterações nos critérios previamente estabelecidos para um evento ou mercado, não incluindo alterações nas quotas fixas de mercados ativos;

l) mudanças nos resultados de um evento ou mercado;

m) gerenciamento de conta de apostador:

I. ajustes no saldo da conta;

II. alterações feitas nos dados e em informações confidenciais do apostador registradas na conta;

III. desativação da conta;

IV. grandes transações financeiras, individuais e agregadas em um período, que excedam o valor definido em regulamento específico da Secretaria de Prêmios e Apostas do Ministério da Fazenda, incluindo informações sobre a transação;

n) perda irrecuperável de informações confidenciais;

o) qualquer outra atividade que exija intervenção do usuário e ocorra fora do escopo normal de operação do sistema; e

p) outros eventos significativos ou incomuns.

41. O sistema de apostas deverá manter e armazenar informações sobre cada conta de colaborador ou preposto do agente operador, incluindo:

a) nome e cargo ou posto;

b) identificação funcional;

c) lista completa e descrição das funções que cada grupo ou conta de usuário pode executar;

d) data e hora em que a conta foi criada;

e) data e hora do último acesso;

f) data e hora da última alteração de senha; e

g) data e hora em que a conta foi desabilitada ou desativada.

Das informações para relatórios

42) O sistema de apostas deverá fornecer informações sob demanda da Secretaria de Prêmios e Apostas do Ministério da Fazenda, além da transmissão diária e mensal de informações padronizadas acerca de apostadores, dos dados agregados do agente operador, das apostas e das carteiras de apostadores, conforme estabelecido no modelo de dados constante do Manual SIGAP.

ANEXO II

DA PLATAFORMA DE APOSTAS ESPORTIVAS

Dos requisitos gerais

1 - A plataforma de apostas esportivas integra o sistema de apostas e deve observar os mesmos requisitos de comunicação, segurança e demais controles técnicos do sistema.

Do software de apostas esportivas

2 - O software de apostas é utilizado na realização das apostas esportivas em eventos reais de temática esportiva por meio da plataforma de apostas esportivas, integrada ao sistema de apostas.

3 - O software de apostas, incluindo sua versão, deve ser identificado pela plataforma de apostas esportivas.

Validação do software

4 - O software de apostas instalado no dispositivo de aposta deverá conseguir autenticar que todos os componentes críticos nele contidos são válidos cada vez que o software é carregado para uso e sob demanda. Componentes críticos podem incluir, não se limitando a:

a) regras de apostas; e

b) elementos que controlam as comunicações entre o dispositivo de aposta, a plataforma de apostas esportivas e o sistema de apostas, ou outros componentes necessários para garantir o funcionamento adequado do software.

5 - No caso de falha na autenticação, o software deve impedir as operações de apostas e exibir uma mensagem de erro apropriada.

Dos requisitos da interface com o usuário

6 - A interface é definida como uma aplicação por meio da qual o usuário visualiza e interage com a plataforma de apostas esportivas. A interface deve observar os seguintes requisitos:

a) as funções de todos os botões, toque ou pontos de clique devem ser claramente indicadas dentro da área do botão, toque ou ponto de clique ou dentro do menu de ajuda. Não deve haver nenhuma funcionalidade disponível através de botões, pontos de toque ou clique na interface que não estejam documentados;

b) qualquer redimensionamento ou sobreposição da interface deve ser mapeado com precisão para refletir a exibição revisada e os pontos de toque ou clique;

c) as instruções da interface, 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; e

d) a exibição das instruções e informações deve ser adaptada à interface.

Impressora de registro de apostas

7 - Nos casos em que o dispositivo de apostas usar uma impressora para emitir os registros para o apostador, deverão constar as seguintes informações:

a) data e hora em que a aposta foi feita;

b) data e hora previstas para a realização do evento;

c) qualquer escolha de apostador envolvida na aposta;

d) valor total apostado;

e) número de identificação exclusivo ou código de barras da aposta;

f) identificação única do dispositivo de apostas que realizou o registro; e

g) identificador do local em que a aposta foi realizada.

Comunicação

8 - O software utilizado na plataforma integrada ao sistema de apostas deve ser programado de tal forma que possa se comunicar, de forma segura, apenas com componentes autorizados. Se a comunicação entre a plataforma e o dispositivo de apostas for perdida, o software deverá impedir outras operações e exibir uma mensagem de erro apropriada.

Dos dispositivos de apostas físicas

9 - As telas sensíveis ao toque devem ser precisas e suportar um método de calibração para manter essa precisão. Alternativamente, o hardware de exibição pode suportar autocalibração.

Dos dispositivos remotos de apostas

10 - Um apostador somente poderá realizar uma aposta utilizando saldo da sua conta gráfica, não sendo permitidas transações de apostas anônimas.

11 - O apostador pode baixar um aplicativo ou pacote de software integrado à plataforma de apostas esportivas ou acessá-la por meio de um navegador, desde que integrados ao sistema de apostas.

12 - A plataforma de apostas esportivas não deve permitir que os apostadores transfiram dados de qualquer natureza entre si, assim como executar funções de bate-papo, por meio da plataforma.

13 - A plataforma de apostas esportivas não deve alterar automaticamente quaisquer regras de firewall especificadas pelo dispositivo para abrir portas bloqueadas por um firewall de hardware ou software.

14 - O software de apostas não deve acessar nenhuma porta que não seja necessária para a comunicação entre o dispositivo de apostas remoto e o servidor que o conecta à plataforma de apostas esportivas e ao sistema de apostas.

15 - A integridade do software não poderá ser alterada por qualquer funcionalidade adicional que não seja de apostas.

16 - O software de apostas não deve ser usado para armazenar informações confidenciais.

Verificação de compatibilidade

17 - A plataforma de apostas esportivas deverá detectar quaisquer limitações de recursos ou incompatibilidades com o dispositivo de apostas utilizado pelo apostador que impeçam a operação adequada do software. Nesse caso, a plataforma deverá impedir as operações de apostas e exibir uma mensagem de erro.

Conteúdo do software

18 - O software de apostas não deve conter código malicioso ou funcionalidade considerada maliciosa.

Política de Cookies

19 - Os apostadores devem ser informados do uso de cookies na instalação do software de apostas ou no acesso por meio de navegadores de internet para realização das apostas. Quando os cookies forem necessários para as apostas, estas não podem ocorrer se a política de cookies não for aceita pelo apostador. Todos os cookies utilizados não devem conter código malicioso.

Acesso à informação

20 - A plataforma de apostas esportivas deverá ser capaz de exibir diretamente da interface do usuário ou de uma página acessível ao apostador:

a) regras de aposta e conteúdo;

b) informações de proteção ao apostador;

c) termos e condições;

d) política de privacidade;

e) telas de apostas e informações; e

f) exibição de resultados.

Das informações e da exibição das apostas

Disponibilização das regras de apostas

21 - O operador deverá manter e disponibilizar na plataforma de apostas esportivas regras atualizadas e compreensíveis de apostas, dos tipos de mercado e dos eventos oferecidos aos apostadores, além das regras e hipóteses relacionadas ao cancelamento e suspensão de apostas e eventos.

Informações dinâmicas de apostas

22 - O operador deverá exibir ao apostador as seguintes informações, independentemente da realização de apostas:

a) informações sobre os eventos e mercados disponíveis para apostas; e

b) probabilidades (odds) atualizadas e preços para os mercados disponíveis.

Oferta de recursos e funcionalidades

23- Dicas, sugestões e informações podem ser oferecidas ao apostador por meio do sistema e da plataforma de apostas esportivas, desde que observados os seguintes requisitos:

a) o apostador deve estar ciente de cada recurso e função disponível, a vantagem oferecida, e as opções existentes para a seleção;

b) quaisquer recursos que envolvam compra devem ter seu custo divulgado claramente; e

c) a disponibilidade e funcionalidade dos recursos devem permanecer estáveis e de forma isonômica para todos os apostadores.

Da realização de apostas

24 - A plataforma de apostas esportivas deverá observar as seguintes regras acerca da realização de uma aposta:

a) o método de realização de uma aposta deve ser simples, com todas as seleções identificadas. Quando a aposta envolver vários eventos, esses agrupamentos devem ser claramente identificados;

b) a plataforma deve permitir aos apostadores selecionarem o mercado no qual desejam apostar;

c) a plataforma não deve permitir que as apostas sejam realizadas automaticamente em nome do apostador sem seu prévio consentimento;

d) a plataforma deve permitir a revisão e a confirmação da seleção das apostas pelos apostadores antes que estas sejam enviadas;

e) a plataforma deve identificar as situações em que o apostador realizou uma aposta para a qual as probabilidades (odds) ou preços associados tenham sido modificados antes da efetivação da aposta e deve exibir uma notificação para confirmar a aposta com os novos valores;

f) uma indicação clara deve ser fornecida ao apostador 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) o saldo da conta gráfica do apostador deve ser prontamente acessível;

h) a plataforma não aceitará uma aposta que possa fazer com que o apostador tenha um saldo negativo; e

i) o saldo da conta gráfica do apostador deve ser debitado quando a aposta é aceita pela plataforma.

Apostas após o encerramento do período permitido

25 - A plataforma não permitirá a realização de apostas após o encerramento das ofertas.

Comprovante da aposta

26 - Após a conclusão de uma aposta, o apostador deverá ter acesso a um comprovante que contenha as seguintes informações:

a) data e hora em que a aposta foi feita;

b) data e hora em que se espera que o evento ocorra;

c) qualquer escolha do apostador envolvida na aposta;

d) valor total apostado;

e) número de identificação único da aposta; e

f) identificador do dispositivo que realizou a aposta.

Modo demonstração

27 - Caso o agente operador opte por fornecer na plataforma de apostas esportivas um modo gratuito de demonstração, no qual é permitido que um apostador simule a realização de apostas sem pagar, a plataforma deve replicar exatamente o mesmo comportamento da versão paga, vedada a indução do apostador ao erro sobre as chances e odds (probabilidades) disponíveis naquela versão.

Dos resultados

Exibição dos resultados

28 - A plataforma de apostas esportivas deverá:

a) fornecer os resultados das apostas de um apostador em qualquer mercado decidido assim que os resultados forem confirmados; e

b) disponibilizar qualquer alteração de resultado das apostas.

ANEXO III

DA PLATAFORMA DE JOGO ON-LINE

Dos Requisitos Gerais

1 - A plataforma de jogos on-line integra o sistema de apostas e deve observar os mesmos requisitos técnicos aplicáveis ao sistema.

2 - Os agentes operadores poderão ofertar na plataforma de jogos on-line somente os jogos on-line que atendam aos requisitos legais e do regulamento específico publicado pela Secretaria de Prêmios e Apostas do Ministério da Fazenda.

Do software de jogo on-line

3 - O software de jogo é utilizado para permitir que o apostador realize apostas por meio da plataforma de jogos on-line.

4 - O software de jogo, incluindo sua versão, deve ser identificado pela plataforma de jogos on-line.

Validação do software

5 - O software de jogo instalado no dispositivo de aposta deverá autenticar que todos os componentes críticos nele contidos são válidos cada vez que o software é carregado para uso e sob demanda. Componentes críticos podem incluir, não se limitando a:

a) regras de jogos;

b) informações da tabela de pagamento; e

c) elementos que controlam as comunicações entre o dispositivo de aposta, a plataforma de jogos on-line e o sistema de apostas, ou outros componentes que são necessários para garantir o funcionamento adequado do software.

6 - No caso de falha na autenticação, o software deve impedir as operações e exibir uma mensagem de erro.

Comunicação

7 - O software utilizado na plataforma de jogos on-line deve ser programado de tal forma que possa se comunicar apenas com componentes autorizados através de comunicações seguras. Se a comunicação entre a plataforma e o dispositivo for perdida, o software deverá impedir que outras apostas sejam efetuadas e exibir uma mensagem de erro.

Interações Cliente-Servidor

8 - A plataforma não deve permitir que os apostadores transfiram dados de qualquer natureza entre si, assim como executar funções de bate-papo, por meio da plataforma.

9 - O software não deve desabilitar automaticamente antivírus ou alterar quaisquer regras de firewall configuradas pelo dispositivo com a finalidade de abrir portas que estão bloqueadas por um firewall de hardware ou software.

10 - O software não deverá acessar nenhuma porta TCP/UDP que não seja necessária para a comunicação entre o dispositivo de jogo e o servidor.

11 - Caso o software inclua funcionalidades adicionais não relacionadas aos jogos on-line, essas não deverão alterar a integridade do software.

12 - O software não deve ser usado para armazenar informações confidenciais.

13 - O software não deve armazenar nenhuma lógica utilizada para gerar o resultado de qualquer jogo on-line. Todas as funções críticas, incluindo a geração de qualquer resultado, devem ser geradas pela plataforma e serem independentes do dispositivo de jogo remoto utilizado para realizar a aposta.

Verificação de compatibilidade

14 - A plataforma de jogos on-line deverá detectar quaisquer limitações de recursos ou incompatibilidades com o dispositivo de apostas utilizado pelo apostador que impeçam a operação adequada do software. Nesse caso, a plataforma deverá impedir as operações de apostas e exibir uma mensagem de erro.

Conteúdo do software

15 - O software de jogos não deve conter código malicioso ou funcionalidade considerada maliciosa.

Política de Cookies

16 - Os apostadores devem ser informados do uso de cookies na instalação do software de jogos ou no acesso aos sítios eletrônicos para jogar. Quando os cookies forem necessários para os jogos on-line, estes não podem ocorrer se a política de cookies não for aceita pelo apostador. Todos os cookies utilizados não devem conter código malicioso.

Acesso à informação

17 - A plataforma de jogos on-line deverá exibir diretamente da interface do usuário ou de uma página acessível ao apostador:

a) as regras e conteúdo dos jogos;

b) as informações de proteção ao apostador;

c) os termos e condições; e

d) a política de privacidade.

Dos requisitos do Gerador de Números Randômicos (RNG)

18. Os tipos de RNGs permitidos são os seguintes:

a) RNGs baseados em software: não utilizam dispositivos de hardware e derivam sua aleatoriedade principalmente de um algoritmo baseado em um computador ou em um software. Eles não incorporam aleatoriedade de hardware de forma significativa;

b) RNGs baseados em hardware: derivam sua aleatoriedade de eventos físicos de pequena escala, como retroalimentação de circuito elétrico, ruído elétrico, desintegração radioativa e rotação do fóton; e

c) RNGs mecânicos: geram resultados aleatórios de jogo mecanicamente, utilizando as leis da física por meio de rodilhos, embaralhadores e sopradores, por exemplo.

Requisitos do código fonte

19 - A entidade certificadora habilitada pela Secretaria de Prêmios e Apostas do Ministério da Fazenda deverá revisar o código-fonte de todo e qualquer algoritmo de aleatoriedade principal, algoritmos de escalonamento, algoritmos de embaralhamento e outros algoritmos ou funções que desempenham um papel crítico na geração do resultado aleatório selecionado para uso por um jogo.

Análise estatística

20 - A entidade certificadora habilitada pela Secretaria de Prêmios e Apostas do Ministério da Fazenda deverá utilizar testes estatísticos para avaliar os resultados gerados pelo RNG, selecionando testes adequados conforme o tipo de RNG que está sendo analisado e seu uso no jogo.

21 - Os testes estatísticos aplicados pela entidade certificadora serão avaliados em conjunto comparando a um nível de confiança de 99%, devendo incluir qualquer um ou mais dos seguintes métodos:

a) distribuição total ou Chi-Quadrado;

b) testes de sobreposição;

c) testes de coletor de tickets;

d) runs tests;

e) testes de correlação de interação;

f) testes de correlação serial; e

g) testes de duplicação.

Distribuição

22 - Cada seleção disponível de RNG deverá ter a mesma probabilidade de ser escolhida. Quando o design do jogo especificar uma distribuição não uniforme, o resultado deve estar de acordo com a distribuição desejada e observar os seguintes requisitos:

a) todos os algoritmos de escalonamento, mapeamento e embaralhamento utilizados deverão ser imparciais e verificados através de uma revisão de código-fonte, sendo permitido o descarte de valores de RNG neste contexto para eliminar a parcialidade; e

b) o resultado deverá ser testado contra a distribuição pretendida utilizando os testes estatísticos adequados.

Independência

23 - O conhecimento dos números sorteados em um sorteio não deve fornecer informações sobre os números que possam ser sorteados em um sorteio futuro. Se o RNG selecionar vários valores dentro de um único sorteio, conhecer um ou mais valores não deverá proporcionar informações sobre os outros valores, a menos que previsto na arquitetura do jogo e previamente autorizado pela Secretaria de Prêmios e Apostas do Ministério da Fazenda, observado o seguinte:

a) o RNG não deverá descartar ou modificar seleções baseadas em seleções anteriores, exceto se previsto pela arquitetura do jogo, como em funcionalidades sem troca; e

b) a apresentação do resultado deverá ser testada quanto à independência entre sorteios e, se aplicável, dentro de um mesmo sorteio, usando testes estatísticos apropriados.

Resultados Disponíveis

24 - O conjunto de resultados possíveis produzidos pela solução de RNG deverá ser suficientemente grande para garantir que todos os resultados estejam disponíveis em cada sorteio com a probabilidade adequada, independentemente dos resultados produzidos anteriormente, exceto quando previsto pela arquitetura do jogo e previamente autorizado pela Secretaria de Prêmios e Apostas do Ministério da Fazenda.

Do Monitoramento e Força do RNG

Força do RNG para Determinar Resultados

25 - O RNG utilizado para gerar os resultados do jogo em uma plataforma de jogo on-line deverá ser resistente a ataques hacker utilizando recursos computacionais modernos, e que possa ter conhecimento do código fonte do RNG.

Ataques Criptográficos ao RNG

26 - Um RNG criptografado não deverá ser comprometido por um hacker com conhecimento do código-fonte, sendo resistente aos seguintes tipos de ataque:

a) ataque cripto-analítico direto: dada uma sequência de valores anteriores gerados pelo RNG, deverá ser computacionalmente inviável prever ou estimar os valores futuros de um RNG. Isso deverá ser garantido através do uso adequado de um algoritmo criptografado reconhecido. Um RNG baseado em hardware ou um RNG mecânico poderá ser qualificado como um algoritmo criptografado, desde que passe no teste estatístico;

b) ataque de entrada conhecida: deverá ser inviável determinar computacionalmente ou estimar o estado do RNG após a propagação inicial. O RNG não deverá ser semeado apenas com base em um valor de tempo. Os fornecedores deverão garantir que os jogos não terão o mesmo seed inicial. Os métodos de propagação não devem comprometer a força criptográfica do RNG; e

c) ataque de extensão de comprometimento de estado: o RNG deverá modificar periodicamente seu estado por meio do uso de entropia externa, limitando a duração efetiva de qualquer tentativa de ataque bem-sucedida por um hacker.

Monitoramento de resultados dinâmicos para RNGs baseados em hardware

27 - Quando um RNG baseado em hardware for utilizado, deverá haver monitoramento dinâmico dos resultados por meio de testes estatísticos. Este processo deverá desativar o jogo quando um mau funcionamento ou alguma corrupção for detectada.

Do RNG Mecânico (dispositivo físico de aleatoriedade)

28 - O software de jogo estará limitado à operação de máquinas e à leitura e gravação de dados do resultado do jogo, não desempenhando um papel determinante na sua geração.

29 - Dispositivos que criam ou exibam fiel e mecanicamente o resultado do jogo gerado por um RNG de computador não serão considerados dispositivos físicos de aleatoriedade e deverão ser testados como RNGs quando a reprodução fiel do resultado gerado do RNG tenha sido garantida.

30 - Dispositivos físicos de aleatoriedade poderão incorporar RNGs em funções secundárias, como velocidade de rotação, que não precisarão ser avaliados em relação aos requisitos de RNG descritos. Porém, o dispositivo físico de aleatoriedade deverá ser testado como um todo.

31 - Os componentes aprovados de um dispositivo físico de aleatoriedade não poderão ser substituídos por componentes não aprovados.

Coleta de dados

32 - A entidade certificadora habilitada deverá coletar, pelo menos, 10.000 dados de resultados de jogos utilizando um método razoavelmente semelhante ao uso pretendido do dispositivo, quando em produção.

33 - A Secretaria de Prêmios e Apostas do Ministério da Fazenda poderá aceitar como resultados dos testes realizados pela entidade certificadora habilitada uma quantidade inferior de dados, que exigirá uma declaração sobre as limitações estatísticas causadas pelo teste reduzido no relatório de certificação.

Durabilidade

34 - Todas as peças mecânicas deverão ser construídas com materiais que evitem a degradação de qualquer componente ao longo de sua vida útil estimada.

35 - A entidade certificadora habilitada poderá recomendar um cronograma de substituição mais rigoroso do que o sugerido pelo fabricante do dispositivo, e sua inspeção periódica para garantir sua integridade.

Manipulação/Adulteração

36 - Os apostadores e atendentes de jogo não deverão manipular ou influenciar os dispositivos físicos de aleatoriedade fisicamente em relação à geração de dados de resultado do jogo, exceto se for projetado pela arquitetura do jogo, como no caso de um atendente de jogo pressionar um botão para parar uma roleta, ou se permitirem que um apostador faça isso.

ANEXO IV

DOS REQUISITOS GERAIS

1. Este anexo contém procedimentos e práticas relacionados às operações de apostas que serão verificadas pelas entidades certificadoras habilitadas pela Secretaria de Prêmios e Apostas do Ministério da Fazenda, nos termos do art. 8º desta Portaria, como parte da avaliação do sistema de apostas, da plataforma de apostas esportivas e da plataforma de jogos on-line.

Da operação e segurança do sistema

Procedimentos do sistema

2 - O operador será responsável por documentar, armazenar e seguir os procedimentos relevantes do sistema de apostas, da plataforma de apostas esportivas e da plataforma de jogos on-line, procedimento que deverá incluir, no mínimo, as seguintes exigências:

a) procedimentos de monitoramento dos componentes críticos e da 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, a confiabilidade e a acessibilidade do sistema;

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 e adulteração;

c) procedimentos para definir, monitorar, documentar, investigar, relatar, responder e resolver incidentes de segurança e adulterações do sistema, incluindo violações detectadas e invasões suspeitas ou reais;

d) procedimento de monitoramento e ajuste do consumo de recursos, mantendo um registro do desempenho do sistema, incluindo uma função para compilar relatórios de desempenho; e

e) procedimentos para investigar, documentar e resolver problemas de funcionamento, que abordem:

I. determinação da causa do mau funcionamento;

II. análise de registros, relatórios e registros de vigilância relevantes;

III. reparo ou substituição do componente crítico;

IV. verificação da integridade do componente crítico antes de restaurá-lo para operação;

V. produção de relatório de incidente para a Secretaria de Prêmios e Apostas do Ministério da Fazenda, e que documente a data, hora e motivo do mau funcionamento, juntamente com a data e a hora em que o sistema foi restaurado; e

VI. anulação ou cancelamento de apostas e pagamentos se uma recuperação completa não for possível.

Localização física dos servidores

3 - Os servidores do sistema de apostas devem estar alojados de forma segura em um ou mais locais, atendendo minimamente às seguintes exigências:

a) ter proteção suficiente contra alteração, adulteração ou acesso não autorizado;

b) estar equipada com um sistema de vigilância;

c) ser protegido por perímetros de segurança e por controles de entrada apropriados para garantir que o acesso seja restrito somente a pessoas autorizadas e que quaisquer acessos e 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.

Controle de acesso lógico

4 - O sistema de apostas deve ser logicamente protegido contra acesso não autorizado por credenciais de autenticação, como senhas, autenticação multifatorial, certificados digitais, PINs, biometria e outros métodos de acesso, observando os seguintes requisitos:

a) cada funcionário do operador deve ter sua própria credencial de autenticação individual, cuja concessão deve ser controlada por meio de um processo formal;

b) os registros de credenciais de autenticação devem ser mantidos 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 alguma credencial de autenticação for codificada em um componente do sistema, ela deverá ser criptografada;

d) um método de fallback para falha na autenticação, como senhas esquecidas, deve ser pelo menos tão forte quanto o método principal;

e) credenciais de autenticação perdidas ou comprometidas e credenciais de autenticação de usuários cancelados devem ser imediatamente desativadas, protegidas ou destruídas;

f) o sistema deve ter vários níveis de acesso de segurança para controlar e restringir diferentes classes de acesso ao servidor, incluindo a visualização, alteração ou exclusão de arquivos e diretórios críticos. Deverá haver procedimentos em vigor para atribuir, revisar, modificar e remover direitos e privilégios de acesso para cada usuário, incluindo:

I. permissão para administração de contas de usuário, para adequada separação de tarefas;

II. limitação dos usuários que possuam as permissões necessárias para ajustar os parâmetros críticos do sistema; e

III. aplicação de parâmetros de credenciais de autenticação adequados, como duração mínima e intervalos de expiração;

g) deverá haver procedimentos em vigor para identificar e sinalizar contas suspeitas onde credenciais de autenticação possam ter sido roubadas ou fraudadas;

h) quaisquer tentativas de acesso lógico às aplicações do sistema ou sistemas operacionais devem ser registradas em um arquivo log seguro;

i) o uso de programas utilitários que possam anular os controles do aplicativo ou do sistema operacional deve ser restrito e rigidamente controlado; e

j) quando as senhas forem usadas como uma credencial de autenticação, é recomendável que sejam alteradas, pelo menos, uma vez a cada 90 dias, tenham pelo menos 8 (oito) caracteres e contenham uma combinação dos seguintes critérios: letras maiúsculas e minúsculas, caracteres numéricos e/ou especiais.

Autorização de usuários

5 - O sistema de apostas deve implementar os seguintes requisitos de autorização de usuários:

a) um mecanismo seguro e controlado deve ser empregado para verificação e demonstração de que o componente do sistema está sendo operado por um usuário autorizado sob demanda ou de forma regular;

b) o uso de equipamentos automatizados de identificação para autenticar conexões locais e equipamentos específicos deve ser documentado e incluído na revisão de acesso aos direitos e privilégios;

c) qualquer informação de autorização comunicada pelo sistema para propósitos de identificação deve ser obtida na hora da solicitação e não armazenado no componente do sistema; e

d) o sistema deve permitir que notificações sejam enviadas ao administrador do sistema, e bloqueio do usuário ou entrada do rastro de auditoria, após um número definido de tentativas de autorização sem sucesso.

Programação de servidores

6 - O sistema de apostas e as plataformas de apostas esportivas e de jogos on-line devem ser suficientemente seguros para prevenir qualquer habilidade de programação iniciada pelo usuário no servidor que possa resultar em modificações na base de dados. No entanto, é aceita a realização de manutenção autorizada de infraestrutura de rede ou resolução de problemas de aplicações com direitos de acesso suficientes pela rede ou pelos administradores do sistema. O servidor também deve ser protegido de execução não autorizada de códigos móveis.

Procedimentos de verificação

7 - Deverão ser adotados procedimentos de verificação sob demanda para que os componentes do programa de controle crítico do sistema de apostas no ambiente de produção sejam idênticos àqueles certificados por entidade certificadora habilitada pela Secretaria de Prêmios e Apostas do Ministério da Fazenda, não se limitando a:

a) assinaturas dos componentes do programa de controle crítico serão recolhidas do ambiente de produção através do processo descrito no item 5 do Anexo I;

b) o procedimento deve incluir um ou mais passos analíticos para comparar as assinaturas atuais dos componentes do programa de controle crítico no ambiente de produção com as assinaturas das versões atuais aprovadas;

c) o resultado do procedimento deve ser armazenado em formato inalterável, que detalhe os resultados da verificação para cada autenticação do programa de controle crítico, devendo:

I. ser registrado em um arquivo log ou relatório do sistema que será armazenado por um período mínimo de 90 dias;

II. estar acessível pela Secretaria de Prêmios e Apostas do Ministério da Fazenda em um formato que permita análise dos registros de verificação; e

III. fazer parte dos registros do sistema que devem ser recuperados no evento de um desastre ou falha de equipamento ou software;

d) qualquer falha de verificação de qualquer componente do sistema exigirá uma notificação de falha de autenticação que será comunicada ao operador por meio de alertas, e à Secretária de Prêmios e Apostas do Ministério da Fazenda, quando requerido; e

e) deve haver um procedimento adotado para responder a toda e qualquer falha de autenticação, incluindo a determinação da causa da falha e o desempenho de correções associadas, bem como promover reinstalações necessárias em tempo hábil.

Inventário de ativos

8 - Todas as informações sensíveis de armazenamento, processamento e comunicação de ativos, incluindo aqueles que integram o ambiente de operação do sistema de apostas e seus componentes, devem ser contabilizados e ter um proprietário nomeado, observando os seguintes requisitos:

a) um inventário de todos os ativos deve ser elaborado e mantido pelo operador;

b) deve existir um procedimento para adicionar e remover ativos;

c) uma política deve estar incluída no uso aceitável de ativos associados ao sistema e seu ambiente de operação;

d) cada ativo deve ter um responsável designado para:

I. assegurar que as informações e os ativos são apropriadamente classificados nos termos de sua criticidade, sensibilidade e valor; e

II. definir e periodicamente revisar restrições de acesso e classificações;

e) um procedimento deve existir para assegurar que a contabilização registrada de ativos seja equivalente com os ativos atuais anualmente; e

f) a proteção contra cópia para impedir duplicação ou modificação não autorizada do software pode ser implementada, desde que o método de proteção utilizado seja documentado e fornecido para a entidade certificadora habilitada pela Secretaria de Prêmios e Apostas do Ministério da Fazenda para garantir que a proteção funciona conforme descrito.

Dos procedimentos de backup e restauração

Segurança dos dados

9 - O sistema de apostas, a plataforma de apostas esportivas e a plataforma de jogos on-line devem fornecer um significado lógico para proteger os dados do apostador e das apostas, incluindo contabilidade, evento significativo ou outra informação confidencial, contra alteração, adulteração ou acesso não autorizado, observados os seguintes requisitos:

a) métodos apropriados de manipulação de dados devem ser implementados, incluindo validação de entrada e rejeição de dados corrompidos;

b) o número de estações de trabalho onde aplicações críticas ou dados de base associadas podem ser acessadas deve ser limitado;

c) criptografia, proteção de senha ou segurança equivalente deve ser usada em arquivos e dados contendo diretórios. Caso contrário, o operador deve restringir a visualização de usuários aos conteúdos de tais arquivos e diretórios, promovendo o monitoramento e o registro de acesso de qualquer pessoa a eles;

d) a operação normal de qualquer equipamento que guarda dados não deve conter opção ou mecanismos que possam comprometer os dados;

e) nenhum equipamento deve ter um mecanismo em que um erro faça com que os dados sejam apagados automaticamente;

f) qualquer equipamento que guarde dados em sua memória não deve permitir a remoção da informação, a menos que tenha primeiro transferido informações para a base de dados ou outros componentes seguros do sistema;

g) os dados devem ser armazenados em áreas do servidor que sejam criptografadas e seguras contra acesso não autorizado;

h) a produção de bases de dados deve residir em redes separadas dos servidores que hospedam qualquer interface de usuário;

i) os dados devem ser mantidos o tempo todo, independentemente de o servidor estar sendo fornecido com energia; e

j) os dados devem ser armazenados de forma a evitar a perda de dados quando houver substituição de partes ou módulos durante manutenção de rotina.

Alteração de dados

10 - A alteração de qualquer contabilidade, relatório ou dado de evento significativo não deve ser permitida sem controle de acesso supervisionado. Quando houver alteração em qualquer dado, as seguintes informações devem ser documentadas ou inseridas em arquivos logs:

a) número de ID único para a alteração;

b) elemento de dado alterado;

c) valor do elemento de dado antes da alteração;

d) valor do elemento de dado após a alteração;

e) hora e data da alteração; e

f) identificação do usuário que realizou a alteração.

Frequência de backup

11 - A implementação do plano de backup deve ocorrer pelo menos uma vez ao dia.

Backup de mídia de armazenamento

12 - Arquivos de logs de auditoria, bases de dados do sistema e quaisquer outros dados pertinentes do apostador e de apostas devem ser armazenados mediante utilização de métodos de proteção razoáveis. O sistema de apostas deve ser projetado para proteger a integridade desses dados quando houver uma falha. Cópias redundantes desses dados devem ser mantidas 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, observados os seguintes requisitos:

a) o backup deve conter uma mídia física não volátil ou uma implementação arquitetural equivalente. Caso o meio de armazenamento primário falhe, as funções do sistema e o processo de auditoria daquelas funções continuarão sem perda de dados críticos;

b) caso o backup seja armazenado em uma plataforma em nuvem, outra cópia também pode ser armazenada em uma plataforma em nuvem diferente;

c) se as unidades de disco rígido forem usadas como mídia de backup, a integridade dos dados deve ser assegurada no evento de uma falha de disco. Métodos aceitáveis incluem, mas não se limitam, 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 respectiva mídia deve ser imediatamente transferida para um local separado do local de alojamento dos servidores e dados cujo backup foi realizado, por armazenamento temporário ou permanente, sendo que:

I. o local de armazenamento deve ser protegido para evitar acesso não autorizado e fornecer proteção adequada para prevenir a perda permanente de qualquer dado; e

II. os arquivos de dados de backup e componentes de recuperação de dados devem ser gerenciados com pelo menos o mesmo nível de segurança e controles de acesso do sistema; e

e) a distância entre as duas localizações deve ser determinada com base nas ameaças e riscos ambientais, falhas de energia, e outras interrupções, mas deve, também, considerar a dificuldade potencial da replicação dos dados, bem como estar apta a acessar o local de recuperação dentro de um tempo razoável.

Falhas no sistema

13 - O sistema de apostas deve ter redundância e modularidade suficiente de modo que, se qualquer componente único ou parte de um componente falhar, as funções do sistema e o processo de auditoria dessas funções possam continuar sem perda de dados críticos. Quando três ou mais componentes estão conectados:

a) as operações de apostas não devem ser afetadas adversamente pelo reinício ou recuperação de qualquer componente, como transações que não são perdidas ou duplicadas por causa da recuperação de um componente ou outro; e

b) após reiniciar ou recuperar determinado componente, eles devem imediatamente sincronizar o status de todas as transações, dados e configurações uns com os outros.

Contabilização de master resets - reinicialização principal

14 - O operador deve ser capaz de identificar e manipular apropriadamente a situação quando um master resetocorrer em qualquer componente que afete as operações de aposta.

Requisitos de recuperação

15 - No evento de uma falha catastrófica quando o sistema de apostas, ou qualquer componente ou plataforma, não puder ser redefinido de qualquer outra forma, deve ser possível restaurar o sistema do último ponto de backup e recuperá-lo totalmente. O conteúdo deste backup deve conter as seguintes informações críticas, incluindo, mas não se limitando a:

a) informações gravadas especificadas na seção "Da manutenção dos dados" do Anexo I desta Portaria;

b) informações específicas do local, como configurações e contas de segurança;

c) chaves de criptografia do sistema atual; e

d) quaisquer outros parâmetros do sistema, modificações, reconfigurações, adições, fusões, exclusões, ajustes e mudanças nos parâmetros.

Suporte de Fornecimento de Energia Ininterrupta (UPS)

16 - Todos os componentes do sistema devem ser fornecidos com energia primária adequada. Onde o servidor for um aplicativo independente, ele deve ter um Fornecimento de Energia Ininterrupta (UPS) conectada e ter capacidade suficiente para permitir um desligamento e retenção de todos os dados do apostador e dados de apostas durante uma perda de energia. É aceitável que o sistema possa compor uma rede que seja suportada por um UPS na qual o servidor esteja incluído como um dispositivo protegido pelo UPS.

Plano de continuidade do negócio e de recuperação em desastres

17 - Uma política de continuidade dos negócios e um plano de recuperação em desastres devem ser adotados para recuperação de operações de apostas se o ambiente de produção do sistema de apostas ou qualquer uma de suas plataformas tornar-se inoperável. A política de continuidade dos negócios e plano de recuperação em desastres devem:

a) direcionar o operador em relação à utilização do método de armazenamento dos dados do apostador e das apostas para minimizar perdas. Se uma replicação síncrona é usada, o método para recuperação dos dados deve ser descrito ou a potencial perda de dados deve ser documentada;

b) delinear as circunstâncias sob as quais serão invocados;

c) direcionar o operador no estabelecimento de uma recuperação local, fisicamente separada do local de produção;

d) conter guias de recuperação detalhando os passos técnicos exigidos para restabelecimento da funcionalidade da aposta na recuperação local; e

e) direcionar o operador em relação ao processo exigido para resumir operações administrativas de atividades de apostas após a ativação do sistema de recuperação para um alcance de cenários apropriados para o contexto operacional do sistema.

Das comunicações

Conectividade

18 - Somente dispositivos autorizados e certificados devem ser permitidos a estabelecer comunicações entre qualquer componente do sistema. O sistema de apostas deve fornecer um método para:

a) inscrever e cancelar a inscrição de componentes do sistema;

b) habilitar e desabilitar componentes específicos do sistema;

c) assegurar que somente os componentes habilitados do sistema, incluindo dispositivos de aposta, participem das operações de apostas; e

d) assegurar que a condição padrão para componentes deve ser "não registrado" e "desabilitada".

Protocolo de comunicação

19 - Cada componente do sistema de apostas deve funcionar conforme indicado por um protocolo de comunicação de segurança documentado, observados os seguintes requisitos:

a) todos os protocolos devem usar técnicas de comunicação que possuam detecção de erros apropriada e mecanismos de recuperação projetados para prevenir invasões, interferência, interceptações e adulterações;

b) todos os dados críticos de comunicação para gerenciamento de conta de apostador ou de apostas devem empregar criptografia e autenticação; e

c) a comunicação na rede segura deve somente ser possível entre componentes aprovados do sistema que tenham sido autenticados como válidos na rede. Comunicações não autorizadas para componentes e pontos de acesso não devem ser permitidas.

Comunicações via internet e redes públicas

20 - Comunicações entre qualquer componente do sistema, incluindo dispositivos de apostas, que ocorrem na internet e/ou em rede pública, devem ser seguras. Dados do apostador, informações sensíveis, apostas, resultados, informações financeiras e informações de transação dos apostadores devem sempre ser criptografadas e protegidas de transmissões incompletas, mau direcionamento, modificação não autorizada de mensagem, divulgação, duplicação ou repetição.

Comunicações via rede sem fio

21 - Comunicações de Rede de Área Local sem Fio Padrão (WLAN) devem ser seguras, e possíveis ameaças e vulnerabilidades direcionadas de acordo com a política de segurança dos dados do operador, devendo haver inspeção e verificação da integridade da WLAN periódicas.

Gerenciamento da segurança de rede

22- As redes devem ser logicamente separadas, de forma que não exista tráfego de rede em um link de rede que não possa ser atendido por hosts nesse link. Os seguintes requisitos se aplicam:

a) as funções de gerenciamento de rede devem autenticar todos os usuários na rede e criptografar todas as comunicações do gerenciamento;

b) a falha de qualquer item único não resultará na negação do serviço;

c) um Sistema de Detecção de Invasão/Sistema de Prevenção de Invasão (IDS/IPS) deve ser instalado na rede, que possa obedecer a ambas as comunicações internas e externas, assim como detectar e prevenir:

I. negação de Serviço Distribuído (DDoS);

II. shellcode de atravessamento da rede;

III. falsificador de Protocolo de Resolução de Endereços (ARP); e

IV. outros indicadores de ataque "Man-In-The-Middle" e cesse as comunicações imediatamente, se detectados;

d) além dos requisitos definidos na alínea (c) do item 22, um IDS/IPS instalado em uma WLAN deve ser capaz de:

I. escanear a rede em busca de pontos de acesso não autorizados ou de dispositivos conectados a qualquer ponto de acesso na rede, pelo menos trimestralmente;

II. desabilitar automaticamente qualquer dispositivo não autorizado conectado ao sistema; e

III. manter um arquivo de log de histórico de todos os acessos sem fio por pelo menos 90 dias, o qual deve conter informações completas e abrangentes sobre todos os dispositivos sem fio envolvidos e ser capaz de ser reconciliado com todos os outros dispositivos de rede dentro do site ou local;

e) o Equipamento de Comunicação de Rede (NCE) deve seguir os seguintes requisitos:

I. ser construído de tal forma a ser resistente a dano físico ao hardware ou corrupção do firmware/software nele contido pelo uso normal;

II. ser fisicamente protegido contra acesso não autorizado;

III. comunicações do sistema via NCE devem ser logicamente protegidas contra acesso não autorizado; e

IV. se o arquivo log de auditoria estiver cheio, o NCE deve desativar toda a comunicação ou descarregar logs para um servidor dedicado;

f) todos os hubs de rede, serviços e portas de conexões devem ser protegidos para evitar acesso não autorizado à rede. Serviços não usados e portas não essenciais devem ser fisicamente bloqueados e desabilitados por software quando possível;

g) em ambientes virtualizados, instâncias de servidores redundantes não devem ser executados no mesmo hipervisor;

h) protocolos sem estado, tais como UDP (Protocolo de Datagrama do Usuário), não devem ser usados para informações sensíveis sem transporte com estado. Embora o HTTP (Protocolo de Transporte de Hipertexto) seja tecnicamente sem estado, se ele for executado no TCP (Protocolo de Controle de Transmissão), que tem estado, será permitido;

i) todas as mudanças de infraestrutura de rede, como configuração de equipamento de comunicação de rede, devem ser registradas em arquivo logs; e

j) scanners de vírus e programas de detecção devem ser instalados em todo o sistema, e serem atualizados regularmente para escanear novos tipos de vírus.

Dos provedores de serviços

Comunicações de terceiros

23 - Quando comunicações com provedores de serviços terceirizados são implementadas, tais como programas de fidelidade do apostador, serviços financeiros, como instituições de pagamento, fornecedores de serviços em nuvem, serviços estatísticos e serviços de verificação de identidade, os seguintes requisitos são aplicáveis:

a) o sistema de apostas e as plataformas de apostas esportivas e de jogos on-line devem ser capazes de se comunicar seguramente com os provedores de serviços terceirizados usando criptografia e forte autenticação;

b) todos os eventos de login envolvendo provedores de serviços terceirizados devem ser registrados em um arquivo de auditoria;

c) a comunicação com provedores de serviços terceirizados não deve interferir ou degradar funções normais do sistema de apostas, observados os seguintes requisitos:

I os dados dos provedores de serviços terceirizados não devem afetar as comunicações dos apostadores;

II. conexões com provedores de serviços terceirizados não devem usar a mesma infraestrutura de rede das conexões do apostador;

III. as apostas devem ser desconectadas em todas as conexões de rede, exceto na rede de apostadores;

IV. o sistema não deve encaminhar pacotes de dados dos provedores de serviços terceirizados diretamente para a rede dos apostadores e vice-versa; e

V. o sistema não deve agir como roteador de IP entre a rede do apostador e os provedores de serviços terceirizados; e

d) todas as transações financeiras devem ser conciliadas com as instituições de pagamento diariamente.

Serviços de terceiros

24 - O operador deve possuir políticas e procedimentos para gerenciar e monitorar sua aderência aos seguintes requisitos de segurança:

a) contratos com prestadores de serviços terceirizados que envolvam o acesso, o processamento, a comunicação ou o gerenciamento do sistema e de seus componentes, ou a adição de produtos ou serviços ao sistema e a seus componentes, devem abranger todos os requisitos de segurança relevantes;

b) serviços, relatórios e registros fornecidos pelos provedores de serviços terceirizados devem ser monitorados e revisados anualmente;

c) alterações no fornecimento de prestadores de serviços terceirizados, incluindo a manutenção e o aprimoramento das políticas, dos procedimentos e dos controles de segurança existentes, devem ser gerenciadas, levando em conta a importância dos sistemas e processos envolvidos e a reavaliação dos riscos; e

d) direitos de acesso dos provedores de serviços terceirizados ao sistema e seus componentes devem ser removidos ao término do contrato ou acordo ou ajuste de alteração.

Dos Controles Técnicos

Requisitos de DNS

25 - Os seguintes requisitos se aplicam aos servidores usados para resolver consultas de Sistema de Nomes de Domínio (DNS) em associação com o sistema de apostas:

a) o operador deve utilizar um servidor DNS primário seguro e um servidor DNS secundário seguro que sejam logica e fisicamente separados um do outro;

b) o servidor DNS primário deve estar fisicamente localizado em uma central de dados segura ou em um host virtualizado em um hipervisor adequadamente seguro ou equivalente;

c) o acesso lógico e físico aos servidores DNS deve ser restrito ao pessoal autorizado;

d) as transferências de zonas para hosts arbitrários não devem ser permitidas;

e) é necessário um método para evitar o envenenamento do cache, como DNSSEC - Extensão de Segurança do DNS;

f) autenticação multifatorial deve estar em vigor; e

g) o bloqueio de registro deve estar em vigor e, portanto, qualquer solicitação de alteração dos servidores DNS precisará ser verificada manualmente.

Controles Criptográficos

26 - Uma política de uso de controles de criptografia deve ser desenvolvida e implementada para proteção da informação, observados os seguintes requisitos:

a) qualquer dado ou informação confidencial deve ser criptografada;

b) dados que não precisam ser ocultos, mas que devem ser autenticados, devem usar alguma técnica de autenticação de mensagens;

c) a autenticação deve usar um certificado de segurança de uma organização aprovada;

d) a classe de criptografia usada deve ser apropriada para a sensibilidade dos dados;

e) o uso de algoritmos de criptografia deve ser revisado periodicamente para verificar se são seguros;

f) alterações nos algoritmos de criptografia para correção de pontos fracos devem ser implementadas assim que possível. Se tais alterações não forem possíveis, o algoritmo deve ser substituído; e

g) as chaves de criptografia devem ser armazenadas em um meio de armazenamento seguro e redundante após serem criptografadas por meio de um método de criptografia diferente ou usando uma chave de criptografia diferente.

Gerenciamento da chave de criptografia

27 - O gerenciamento de chaves de criptografia deve seguir procedimentos que cubram minimamente o seguinte:

a) obtenção ou geração de chaves de criptografia e armazená-las;

b) gerenciamento da expiração das chaves de criptografia, quando aplicável;

c) revogação das chaves de criptografia;

d) alteração de forma segura da configuração da chave de criptografia atual; e

e) recuperação de dados criptografados com uma chave de criptografia revogada ou expirada para um período definido após a chave de criptografia se tornar inválida.

Do acesso remoto e firewalls

Segurança do acesso remoto

28 - Acesso remoto é definido como qualquer acesso de fora do sistema ou da rede do sistema, incluindo o acesso de outras redes dentro do mesmo local. O acesso remoto, se utilizado pelo operador, deve:

a) ser realizado por meio de um método seguro;

b) ter uma opção de ser desabilitado;

c) aceitar somente conexões remotas permitidas pelo aplicativo de firewall e pelas configurações do sistema; e

d) ser limitado a funções necessárias do aplicativo para que o usuário desempenhe seu trabalho, sendo proibido qualquer acesso não autorizado.

Procedimentos do acesso remoto e contas de convidados

29 - Um procedimento para acesso remoto controlado deve ser estabelecido. Um fornecedor pode, mediante autorização do operador, acessar o sistema e seus componentes associados remotamente para apoio ao produto e ao usuário ou atualizações e aprimoramentos. Este acesso remoto deve usar contas de convidados específicas que serão:

a) monitoradas continuamente pelo operador;

b) desabilitadas quando não estiverem em uso; e

c) restringidas através de controles de segurança lógica para acessar somente os aplicativos ou bases de dados necessários para o produto, o suporte ao usuário ou fornecer atualizações e aprimoramentos.

Registro de atividade do acesso remoto

30 - O aplicativo de acesso remoto deve manter um arquivo log de atividade atualizado automaticamente, que retrate todas as informações do acesso, inclusive:

a) identificação dos usuários que desempenham ou autorizam o acesso remoto;

b) endereços IP Remoto, números de portas, protocolos e, quando possível, endereços MAC;

c) data e hora em que a conexão foi feita e sua duração; e

d) atividade enquanto logado, incluindo as áreas específicas acessadas e alterações efetuadas.

Firewalls

31 - Todas as comunicações, incluindo o acesso remoto, devem passar através de, pelo menos, um firewall de nível de aplicação aprovado. Isso inclui conexões de e para qualquer host que não seja do sistema usado pelo operador, observado o seguinte:

a) o firewall deve estar localizado no limite de dois domínios de segurança diferentes;

b) um dispositivo no mesmo domínio de transmissão do host do sistema não deve ter um recurso que permita um caminho de rede alternativo que ultrapasse o firewall;

c) qualquer caminho de rede alternativo existente com o propósito de redundância também deve passar através de, pelo menos, um firewall de nível de aplicação;

d) somente aplicações relacionadas ao firewall podem residir nele;

e) somente um número limitado de contas de usuários pode estar presente no firewall, como administradores de rede ou sistema;

f) o firewall deve rejeitar todas as conexões, exceto aquelas que tenham sido especificamente aprovadas;

g) o firewall deve rejeitar todas as conexões de destinos que não residem na rede das quais as mensagens são originadas; e

h) o firewall só deve permitir o acesso remoto por meio dos protocolos de criptografia mais atualizados.

Registros de auditoria do firewall

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

a) data e hora de todos os registros;

b) todas as alterações de configuração do firewall;

c) todas as tentativas de conexão, bem-sucedidas ou não, através do firewall; e

d) fonte e destino de endereços IP remoto, números de portas, protocolos e, quando possível, endereços MAC.

Revisão das regras de firewall

33 - As regras do firewall devem ser periodicamente revisadas para verificação das condições de operação e a efetividade de suas configurações de segurança. Essa revisão deve ser realizada em todo o perímetro dos firewalls e nos firewalls internos.

Do gerenciamento das mudanças

Procedimentos do programa de controle de alterações

34 - Os procedimentos do programa de controle de alterações devem ser adequados para assegurar que somente versões autorizadas dos programas sejam utilizadas no ambiente de produção. Esses controles de alteração devem incluir:

a) um mecanismo ou controle de versão de software adequado para todos os componentes de software e códigos-fonte;

b) registros mantidos de todas as novas instalações e modificações do sistema, incluindo:

I. a data da instalação ou modificação;

II. detalhes do motivo ou natureza da instalação ou alteração, tal como novo software, reparo no servidor, modificações de configuração significativas;

III. uma descrição dos procedimentos exigidos para colocar o componente modificado ou novo em serviço; e

IV. a identidade do usuário que realizou a instalação ou modificação;

c) uma estratégia para reverter para a última implementação - plano de reversão - quando a instalação não for bem-sucedida, incluindo backups completos de versões anteriores do software e um teste do plano de reversão antes da implementação no ambiente de produção;

d) uma política estabelecendo procedimentos de alteração de emergência;

e) procedimentos de teste e migração de alterações;

f) segregação de funções entre desenvolvedores, equipe de certificação de qualidade, equipe de migração e usuários; e

g) procedimentos para assegurar que a documentação técnica e do usuário está atualizada após a alteração.

Ciclo de vida do desenvolvimento do software

35 - A aquisição e o desenvolvimento de um novo software devem observar, no mínimo, o seguinte:

a) o ambiente de produção deve ser lógico e fisicamente separado do desenvolvimento e do ambiente de teste. Quando sistemas em nuvem são usados, não poderão existir conexões diretas entre o ambiente de produção e qualquer outro ambiente;

b) a equipe de desenvolvimento deve ser impedida de ter acesso para promover alterações de código no 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 sensíveis, deve haver um método documentado para assegurar que os dados brutos de produção não sejam usados nos testes; e

e) todos os documentos relacionados ao desenvolvimento do software e da aplicação devem estar disponíveis e retidos pela duração do seu ciclo de vida.

Correções de erros

36 - Todas as correções de erro devem ser testadas, sempre que possível, em um ambiente de teste e desenvolvimento configurado de forma idêntica ao ambiente de produção alvo das correções. Sob circunstâncias em que os testes de correção de erros não possam ser cuidadosamente conduzidos a tempo de cumprir os cronogramas para o nível de gravidade do alerta e, se autorizado, o teste de correção de erros deve ser gerenciado por risco, seja isolando ou removendo o componente não testado da rede ou aplicando a correção e o teste após o fato.

Dos testes periódicos de segurança

Testes técnicos de segurança

37 - Testes técnicos periódicos de segurança no ambiente de produção devem ser realizados para garantir que não existam vulnerabilidades que coloquem em risco a segurança e a operação do sistema de apostas e das plataformas de apostas esportivas e de jogos on-line.

38 - Os testes devem consistir em um método de avaliação de segurança por meio de uma simulação de ataque por um terceiro seguindo uma metodologia conhecida, e a análise de vulnerabilidade consistirá na identificação e quantificação passiva do potencial risco do sistema.

39 - Tentativas de acesso não autorizado devem ser realizadas até o nível mais alto possível de acesso e devem ser completadas com ou sem credenciais de autenticação disponíveis, como testes de tipo caixa branca/caixa preta. Isso permite que avaliações sejam feitas em relação aos sistemas de operação e configuração de hardware, incluindo, mas não limitado a:

a) escaneamento de porta UDP/TCP;

b) Stack fingerprint e previsão de sequência TCP para identificar sistemas operacionais e serviços;

c) banner grabbing público;

d) varredura da web usando scanners de vulnerabilidade HTTP e HTTPS; e

e) varredura do roteador usando protocolo de roteamento de BGP (Border Gateway Protocol), o protocolo multicast de roteamento de -BGMP (Border Gateway Multicast Protocol) e o -SNMP (Simple Network Management Protocol).

Avaliação de vulnerabilidade

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

a) avaliação de vulnerabilidade externa - Os alvos são dispositivos de rede e servidores acessíveis por terceiros, pessoas naturais ou empresas, por meio de IP público, relacionados ao sistema pelo qual é possível o acesso a informações sensíveis; e

b) avaliação de vulnerabilidade interna - Os alvos são servidores internos relacionados ao sistema pelo qual é possível acessar informações sensíveis. O teste de cada domínio de segurança na rede interna deve ser realizado separadamente.

Teste de penetração

41 - O objetivo do teste de penetração é explorar quaisquer pontos fracos descobertos durante a avaliação de vulnerabilidade em quaisquer aplicativos ou sistemas expostos publicamente que hospedem aplicativos que processem, transmitam e/ou armazenem informações confidenciais. O teste de penetração deve incluir pelo menos as seguintes atividades:

a) teste de penetração da camada de rede - o teste imita as ações de um agressor real que explora pontos fracos na segurança da rede, examinando sistemas em busca de qualquer ponto fraco que possa ser usado por um agressor externo para perturbar a confidencialidade, disponibilidade e/ou integridade da rede; e

b) teste de penetração da camada do aplicativo - o teste usa ferramentas para identificar pontos fracos nos aplicativos com varreduras autenticadas e não autenticadas, análise dos resultados para remover falsos positivos e testes manuais para confirmar os resultados das ferramentas e identificar o

impacto dos pontos fracos.

42 - A auditoria do Sistema de Gerenciamento de Segurança da Informação (ISMS) deve ser realizada, incluindo todos os locais onde as informações confidenciais acessadas, processadas, transmitidas e armazenadas. O ISMS será revisado em comparação com os princípios comuns de segurança da informaçãoem 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) Padrões de Segurança de Dados Industriais de Cartão de Pagamento (PCI-DSS); e

c) Padrões de Segurança da Associação Mundial de Loterias (WLA-SCS).

43 - Um operador fazendo uso de provedor de serviço em nuvem (CSP), armazenando, transmitindo ou processando informações sensíveis, deve se submeter a auditoria específica. O CSP será revisado em comparação aos princípios comuns de segurança da informação em relação à provisão e ao uso de serviços em nuvem, tais como ISO/IEC 27017 e ISO/IEC 27018, ou equivalentes, observado o seguinte:

a) se informações sensíveis são armazenadas, processadas ou transmitidas em um ambiente em nuvem, os requisitos apropriados se aplicarão àquele ambiente, e envolverão tipicamente a validação de ambas as infraestruturas CSP e uso do operador daquele ambiente;

b) a alocação de responsabilidade entre o CSP e o operador para gerenciar controles de segurança não isenta o operador da responsabilidade de assegurar que informações sensíveis estejam apropriadamente protegidas, de acordo com os requisitos aplicáveis; e

c) políticas e procedimentos claros devem ser acordados entre o CSP e o operador para todos os requisitos de segurança, e as responsabilidades pela operação, gerenciamento e relatórios devem ser claramente definidas e compreendidas para cada requisito aplicável.

ANEXO V

GLOSSÁRIO

Acesso Não Autorizado - Quando 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 - Os indivíduos responsáveis por manter a operação estável do Sistema de Apostas, incluindo infraestrutura de software e hardware e software de aplicativo.

Algoritmo - Um conjunto finito de instruções não ambíguas executadas em uma sequência prescrita para atingir um objetivo, especialmente uma regra ou procedimento matemático usado para computar um resultado desejado. Os algoritmos são a base da maior parte da programação de computadores.

Algoritmo de Hash - Função que converte uma cadeia de dados em uma saída de cadeia alfanumérica de comprimento fixo.

Ameaça - Qualquer circunstância ou evento com potencial para afetar negativamente as operações de rede, incluindo missão, funções, imagem ou reputação, ativos ou indivíduos por meio de um sistema via acesso não autorizado, destruição, divulgação, modificação de informações e/ou negação de serviço. Além disso, consiste na possibilidade de uma fonte de ameaça explorar com sucesso uma vulnerabilidade do sistema.

Antivírus - Software usado para prevenir, detectar e remover vírus de computador, inclusive malware, worms e cavalos de Troia.

ARP, Protocolo de Resolução de Endereço - O protocolo usado para traduzir endereços IP em endereços MAC para dar suporte à comunicação em uma rede local com ou sem fio.

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

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

Autenticação de Mensagem - Uma medida de segurança projetada para estabelecer a autenticidade de uma mensagem por meio de um autenticador dentro da transmissão, derivado de certos elementos predeterminados da própria mensagem.

Autenticação Multifatorial - Um tipo de autenticação que usa dois ou mais dos seguintes elementos para verificar a identidade de um usuário: informações conhecidas apenas pelo usuário, como uma senha, um padrão ou respostas a perguntas de desafio; um item possuído por um usuário, como um token eletrônico, um token físico ou um cartão de identificação; dados biométricos de um usuário, como impressões digitais, reconhecimento facial ou de voz.

Backup - Uma cópia de arquivos e programas feita para facilitar recuperação, se necessário.

Banner grabbing - técnica usada para obter informações de um sistema ou serviço de rede, capturando o banner exibido na resposta do servidor.

Biometria - Uma entrada de identificação biológica, tal como impressões digitais ou retina.

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

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

Código Móvel - Código executável que se move de um computador para outro, incluindo tanto o código legítimo quanto o código malicioso, como vírus de computador.

Chave - Valor usado para controlar operações criptográficas, como descriptografia, criptografia, geração ou verificação de assinaturas.

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

Conta do Apostador - Uma conta mantida para um apostador em que as informações relativas a apostas e transações financeiras são registradas em nome do apostador.

Controle de Acesso - Processo de conceder ou negar solicitações para obter e usar informações sensíveis e serviços relacionados específicos de um sistema; e entrar em instalações físicas específicas que hospedam redes críticas ou infraestrutura de sistemas.

Criptografia - A conversão de dados em um formato, chamado de texto cifrado, que não pode ser facilmente compreendida por pessoas não autorizadas.

Dados do Apostador - Informações confidenciais sobre um apostador, que podem incluir itens como nome completo, data de nascimento, local de nascimento, endereço, número de telefone ou outras informações pessoais.

DDoS, Ataque de Negação de Serviço - Tipo de ataque em que vários sistemas comprometidos, geralmente infectados com um software destrutivo, são usados para atingir um único sistema. As vítimas de um ataque DDoS consistem tanto no sistema alvo final quanto em todos os sistemas maliciosamente usados e controlados pelo hacker no ataque distribuído.

Digest - processo no qual um documento, uma mensagem, uma palava-chave ou outro item de dados é condensado em um resumo de tamanho fixo curto.

Dispositivo de Apostas - Um dispositivo eletrônico que converte as comunicações do Sistema de Apostas, da plataforma de apostas esportivas e da plataforma de jogos on-line em uma forma interpretável por humanos e converte decisões humanas em formato de comunicação compreendido pelo Sistema de Apostas e pelas plataformas, permitindo as operações de apostas em quota fixa diretamente pelo apostador. Exemplos de um dispositivo de apostas incluem computador, telefone celular e tablet.

DNS, Domain Name Service - serviço de nomes de domínio - O banco de dados da Internet distribuído globalmente que mapeia 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.

Endereço IP - Endereço de Protocolo de Internet - número atribuído a cada dispositivo, como computador, impressora, smartphone conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação. Um endereço IP serve a duas funções principais: identificação de interface de hospedeiro ou de rede e endereçamento de localização.

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 relacionada a esportes, competições, jogos em que as apostas podem ser feitas.

Evento significativo - Ocorrência que possui um potencial de impacto para a operação e que frequentemente leva a consequências e mudanças, como tentativas de acesso mau sucedidas, períodos de inatividade do sistema, grandes apostas, grandes ganhos e mudanças em algum componente crítico do sistema.

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

Geolocalização - Identificação da localização geográfica no mundo real de um dispositivo de apostas remoto conectado à Internet.

Gerenciamento de Chave - Atividades que envolvem o manuseio de chaves criptográficas e outros parâmetros de segurança relacionados, como senhas, durante todo o ciclo de vida das chaves, incluindo sua geração, armazenamento, estabelecimento, entrada e saída, e zeragem.

Hipervisor - Um hipervisor, ou monitor de máquina virtual, é um software, firmware ou hardware que cria e roda máquinas virtuais.

HTTP - Protocolo de Transferência de Hipertexto - O protocolo subjacente usado para definir como as mensagens são formatadas e transmitidas, e quais ações os servidores e navegadores devem executar em resposta a vários comandos.

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 em trânsito.

Internet - Um sistema interconectado de redes que conecta computadores em todo o mundo por meio do protocolo TCP/IP.

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

Impressora - Um Dispositivo de Aposta periférico que imprime registros de apostas e instrumentos de aposta.

Informações Sensíveis - Informações como dados do apostador, dados de apostas, números de validação, PINs, senhas, seeds e chaves seguras e outros dados que devem ser tratados de forma segura.

Interface do Usuário - Um aplicativo ou programa de interface por meio do qual o usuário visualiza e interage com o Software de Apostas e com as plataformas de apostas esportivas e de jogos on-line para comunicar suas ações ao Sistema de Apostas.

Jailbreaking - Modificação de um smartphone ou outro dispositivo eletrônico para remover restrições impostas pelo fabricante ou operador para permitir a instalação de software não autorizado.

Leitor de Código de Barras - Um dispositivo 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 - Código de Autenticação de Mensagem - Código de segurança que pode ser anexado a mensagens ou solicitações enviadas por um usuário com o objetivo de autenticar a mensagem.

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

Mecanismo de Física - Software especializado que aproxima as leis da física, incluindo comportamentos como movimento, gravidade, velocidade, aceleração, massa e outros, para os elementos ou objetos de um evento virtual. O mecanismo de física é utilizado para colocar os elementos/objetos do evento virtual no contexto do mundo físico ao renderizar gráficos de computador ou simulações de vídeo.

Mercado - São as diferentes opções que um jogador tem para fazer suas apostas em um jogo ou evento esportivo, como no vencedor de um jogo de futebol.

Método de fallback - Estratégia ou solução alternativa utilizada para lidar com erros ou falhas de sistemas, processos ou interfaces, permitindo que o sistema continue funcionando de maneira adequada.

Modo Demonstração - Um modo de jogo que permite que um apostador participe de apostas sem fazer nenhuma aposta financeira, principalmente com o objetivo de aprender ou entender a mecânica das apostas.

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

PIN - Número de Identificação Pessoal - Um código numérico associado a um indivíduo e que permite o acesso seguro a um domínio, conta, rede ou sistema, por exemplo.

Plano de Contingência - Política e procedimentos de gerenciamento projetados para manter ou restaurar as operações de apostas possivelmente em um local alternativo, no caso de emergências, falhas no sistema ou desastres.

Plano de Recuperação em Desastres - Plano para processar aplicativos essenciais e evitar a perda de dados no caso de uma falha grave de hardware ou software ou destruição das instalações.

Política de Segurança - Um documento que delineia a estrutura de gerenciamento de segurança e atribui claramente responsabilidades de segurança e estabelece a base necessária para medir de forma confiável o progresso e a conformidade.

Porta - Um ponto físico de entrada ou saída de um módulo que fornece acesso a este para sinais físicos, representados por fluxos de informações lógicas.

Programa de Controle Crítico - Um programa de software que controla comportamentos relativos a qualquer norma técnica e/ou requisito regulatório aplicável.

Programa de fidelidade do apostador - Um programa que oferece incentivos aos apostadores com base no volume de jogo ou na receita recebida de um apostador.

Programas Utilitários - Programas utilizados para agregar funcionalidades específicas relacionadas ao gerenciamento de sistemas.

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 e Segurança - Um protocolo de comunicação que fornece a proteção adequada de confidencialidade, autenticação e proteção da integridade do conteúdo.

Protocolo sem estado - Um esquema de comunicação que trata cada solicitação como uma transação independente que não está relacionada a nenhuma solicitação anterior, de modo 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 determinados tipos de tráfego que entram ou saem de uma rede, processa-o e o encaminha. Isso efetivamente fecha o caminho direto entre as redes interna e externa, tornando mais difícil a obtenção de endereços internos e outros detalhes da rede interna por um invasor.

Rastro de Auditoria - um registro que mostra quem acessou um sistema e quais operações o usuário realizou durante um determinado período.

Registro de Apostas - Um bilhete impresso ou mensagem eletrônica confirmando a aceitação de uma ou mais apostas.

Registro de data e hora - Um registro do valor atual da data e hora do sistema de apostas que é adicionado a uma mensagem no momento em que esta é criada.

Regras de Apostas - Qualquer informação escrita, gráfica e auditiva fornecida ao público com relação a operações de apostas.

Risco - A probabilidade de uma ameaça ser bem-sucedida em seu ataque contra uma rede ou sistema.

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

RNG Criptográfico - Gerador de números aleatórios - RNG que seja resistente a ataques ou comprometimento por um invasor inteligente com recursos computacionais modernos que tenha conhecimento do código-fonte do RNG e/ou seu algoritmo. Os RNGs criptográficos não podem ser "quebrados" de forma viável para prever valores futuros.

Rooting - Obter acesso à raiz do código do sistema operacional para modificar o código do software no telefone celular ou outro dispositivo de apostas remoto ou instalar software que o fabricante não permitiria que fosse instalado.

Segurança da Informação - Processo de proteção de informações e sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição não autorizados, a fim de proporcionar 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 de software em execução que é capaz de aceitar solicitações de clientes e o computador que executa esse software. Os servidores operam em uma arquitetura cliente-servidor, na qual "servidores" são programas de computador executados para atender às solicitações de outros programas - "clientes". Nesse caso, o "servidor" seria o Sistema de Apostas em Eventos e os "clientes" seriam os Dispositivos de Apostas.

Shellcode - Um pequeno trecho de código usado como carga útil na exploração da segurança. O shellcode explora vulnerabilidade e permite que um invasor reduza a garantia de informações de um sistema.

Software de Apostas - O software usado para participar de apostas e transações financeiras com o Sistema de Apostas e com as plataformas de apostas esportivas e de jogos on-line que, com base no design, é baixado ou instalado no Dispositivo de Apostas.

Stack fingerprinting - Coleta sistemática de informações sobre um determinado dispositivo remoto para fins de identificação e rastreamento.

TCP/IP - Protocolo de Controle de Transmissão/Protocolo de Internet - É um conjunto de protocolos que possibilita a comunicação entre computadores e servidores.

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

Vírus - Um programa autorreplicante, normalmente com intenção maliciosa, que é executado e se espalha modificando outros programas ou arquivos.

VPN - Rede Virtual Privada - Rede de comunicações privada construída sobre uma rede de comunicações pública, como a Internet, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados.

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 de rede local sem fio - WLAN padrão para conectar computadores e dispositivos eletrônicos entre si e/ou à Internet.