GLI®

FRAMEWORK DE SEGURANÇA PARA JOGOS

GLI-GSF-1

SEGURANÇA DA INFORMAÇÃO EM JOGOS (GIS) AUDITORIA DE CONTROLES – CONTROLES COMUNS

Versão 1.1 – Publicada em 30 de setembro de 2025

Conteúdo

1. INTRODUÇÃO

1.1. Declaração Geral

A integridade e precisão da operação de um Ambiente de Produção de Jogos (GPE) dependem fortemente dos procedimentos operacionais, configurações e da infraestrutura de rede. Com ameaças emergentes às operações de jogos, os órgãos reguladores dependem fortemente da expertise de uma Empresa Independente de Segurança (ISF) qualificada para realizar avaliações de segurança em jogos como um complemento essencial ao teste e certificação dos Componentes Críticos do Sistema de um GPE por um Laboratório de Testes Independente (ITL).

a. Este módulo do Framework de Segurança para Jogos da GLI, GLI-GSF-1, estabelece os Controles comuns de Segurança da Informação de Jogos (GIS) necessários para auditar o Sistema de Gerenciamento de Segurança da Informação de Jogos (GISMS) de uma Empresa de Jogos, a fim de garantir uma gestão eficaz da segurança no GPE de uma Empresa de Jogos.
b. Esses Controles GIS comuns se aplicam aos GPEs usados em todas as formas de jogo, como jogos de cassino, loteria, apostas em eventos e jogos interativos.
c. Este módulo pode ser usado junto com o GLI-GSF-2, que fornece um parâmetro para conduzir avaliações de Segurança Técnica de Jogos (GTS) do GPE de uma Empresa de Jogos.
d. Dependendo do tipo de Empresa de Jogos, módulos adicionais do GLI-GSF também podem se aplicar.

NOTA: Todo o Framework de Segurança para Jogos da GLI (GLI-GSF) está disponível gratuitamente na www.gaminglabs.com.

1.2. Empresa de Jogos e Função de Gestão de Dados Sensíveis

Garantir a segurança de um GPE é uma responsabilidade coletiva que abrange as múltiplas entidades que compõem a Empresa de Jogos, como o operador, e seus fornecedores, fabricantes, fornecedores, prestadores de serviços e outras entidades que têm papel na supervisão ou operação de um GPE ou na prestação de serviços integrantes à sua função. Cada entidade desempenha um papel crucial na manutenção da confidencialidade, integridade, disponibilidade e responsabilidade do ambiente, especialmente quando estão envolvidos dados sensíveis, que consistem no mínimo nos seguintes aspectos, conforme aplicável:

a. Registros de auditoria e bancos de dados do sistema registrando informações usadas para determinar resultados, pagamento, resgate e rastreamento das informações dos usuários;
b. Informações contábeis e de eventos significativos relacionadas aos Componentes Críticos do Sistema do GPE;
c. RNG seed e qualquer outra informação que afete os resultados de jogos e apostas;
d. Chaves de criptografia, onde a implementação escolhida requer transmissão de chaves;
e. Números de validação associados a contas de patronos, instrumentos de apostas e quaisquer outras transações de jogo;
f. Transferências de fundos para e de contas de patronos, contas de pagamento eletrônico e para fins de jogos;
g. Pacotes de software dentro do GPE;
h. Qualquer dado de localização relacionado à atividade de funcionários ou usuários (por exemplo, gerenciamento de contas, jogos online, etc.);
i. Qualquer uma das seguintes informações registradas para qualquer funcionário ou usuário:
    i. número de identificação governamental (número de seguridade social, número de identificação do contribuinte, número de passaporte ou equivalente);
    ii. informações financeiras pessoais (números de instrumentos de crédito ou débito, números de conta bancária, etc.);
    iii. Credenciais de autenticação em relação a qualquer conta de usuário ou conta patrona;
    iv. Qualquer outra informação pessoal identificável (PII) que precise ser mantida confidencial; e
j. Quaisquer outros dados considerados sensíveis pelo Órgão Regulador ou pela Empresa de Jogos.

NOTA: Este documento não tem a intenção de definir quais entidades são responsáveis por atender a cada Controle GIS. É responsabilidade das múltiplas entidades que compõem a Empresa de Jogos concordar sobre a responsabilidade.

1.3. Ambiente de Produção de Jogos (GPE)

Um GPE refere-se ao ambiente operacional onde atividades de jogos e serviços relacionados são conduzidos, gerenciados e entregues aos usuários de forma ao vivo ou em tempo real. Ela abrange a infraestrutura física e virtual, sistemas de jogo, softwares e processos necessários para facilitar diversas formas de jogo, como jogos de cassino, loteria, apostas em eventos e jogos interativos. O GPE também abrange os sistemas backend, aplicações de negócios e infraestrutura que se conectam e/ou apoiam as atividades de jogos. Características principais de um GPE incluem:

a. Componentes Críticos do Sistema: Isso inclui dispositivos de rede, servidores, dispositivos computacionais, componentes virtuais, hardware e plataformas de software que suportam a execução de atividades de jogo, como dispositivos de jogo, mesas de jogo, sistemas de jogos, sistemas de loteria, sistemas de apostas em eventos e sistemas ou aplicativos interativos de jogo.
b. Módulos Criptográficos: Módulos criptográficos usados dentro do GPE são responsáveis pelas funções criptográficas, incluindo a criptografia e descriptografia de dados sensíveis, utilizando algoritmos que atendem aos padrões atuais aceitos pela indústria, como ISO/IEC 19790, FIPS 140-2 ou equivalente.
c. Processamento de Transações: O GPE processa transações monetárias relacionadas a atividades de jogo, incluindo apostas, pagamentos, depósitos, saques e transações financeiras com patronos.
d. Medidas de Segurança: Medidas robustas de segurança são implementadas para salvaguardar a confidencialidade, integridade, disponibilidade e responsabilidade dos Componentes Críticos do Sistema, dados sensíveis, transações financeiras e informações dos usuários contra acesso não autorizado, fraude, manipulação e ameaças cibernéticas.
e. Gestão de Riscos: O GPE emprega práticas de gestão de riscos para identificar, avaliar, mitigar e monitorar riscos associados às operações de jogos, incluindo riscos operacionais, financeiros, regulatórios e tecnológicos.
f. Operação Contínua: Um GPE normalmente opera 24 horas por dia, 7 dias por semana, para atender à demanda dos clientes e maximizar a geração de receita. Isso exige alta disponibilidade, confiabilidade e resiliência da infraestrutura e dos sistemas para minimizar o tempo de inatividade e as interrupções.
g. Monitoramento e Controle: Mecanismos de monitoramento, vigilância e controle em tempo real estão em vigor para supervisionar atividades de jogo, detectar anomalias, garantir conformidade com regras e regulamentos e responder prontamente a incidentes, fraudes ou outros problemas relacionados a GIS.
h. Conformidade Regulatória: A conformidade com regulamentos de jogos, requisitos de licenciamento e padrões do setor é essencial em um GPE para garantir jogo justo, proteção dos usuários, práticas responsáveis de jogo e cumprimento das obrigações legais e regulatórias.

1.4. Sistema de Gerenciamento de Segurança da Informação em Jogos (GISMS)

Um GISMS é um framework estruturado e um conjunto de processos projetados para proteger os dados sensíveis, ativos e Componentes Críticos do Sistema de uma Empresa de Jogos dentro de seu GPE contra acesso, divulgação, alteração ou destruição não autorizada. Ela abrange políticas, procedimentos, controles e práticas de gestão de riscos especificamente adaptadas aos desafios únicos e requisitos regulatórios da indústria de jogos, envolvendo a identificação de riscos de GIS, a implementação de controles e salvaguardas apropriados, monitoramento e avaliação contínuos das medidas de segurança, e melhoria contínua para se adaptar às ameaças e requisitos de conformidade em evolução.

1.5. Propósito do Framework

Garantir a segurança e integridade das atividades de jogos é fundamental para preservar a confiança e a confiança pública no setor. Portanto, cassinos, loterias, operações de apostas em eventos, operações de jogos interativos e outras empresas de jogos devem estabelecer e manter um arcabouço claramente definido e documentado para conquistar e preservar a confiança pública em suas operações. O objetivo é alinhar o GIS de forma que as operações de jogos possam funcionar como outras operações de comércio eletrônico, garantindo um ambiente seguro e estável com as características seguras das operações em indústrias paralelas.

1.6. Normas e Diretrizes de Segurança Consultadas

Cada módulo do GLI-GSF é baseado em padrões e diretrizes de segurança comumente usados que fornecem uma base aceita pela indústria para desenvolver práticas eficazes de gestão de GIS. A GLI reconhece e agradece aos Órgãos Reguladores e outros participantes do setor que reuniram regras, regulamentos, normas técnicas e outros documentos que foram influentes no desenvolvimento deste documento.

1.7. Adoção e Observância

Este módulo do GLI-GSF pode ser adotado total ou parcialmente por qualquer Órgão Regulador que deseje implementar um conjunto abrangente de Controles Comuns de GIS.

2. AUDITORIAS DE CONTROLE DE GIS

2.1. Visão Geral da Auditoria

A Auditoria de Controles GIS é realizada com o objetivo de identificar quaisquer casos reais ou potenciais de não conformidade, vulnerabilidades ou fraquezas, garantindo que a confidencialidade, integridade, disponibilidade e responsabilidade das informações sob o controle da Empresa de Jogos sejam preservadas. Essa metodologia depende fortemente da segurança em camadas para reduzir o risco aos sistemas de computador e rede, fornecendo redundância e reforçando o modelo geral de segurança, já que várias camadas de segurança precisam ser violadas antes que um armazenamento de dados sensíveis seja acessado.

NOTA: O foco das orientações GIS detalhadas no GLI-GSF-1 está nos controles comuns de segurança da informação para jogos; outros métodos de avaliação são discutidos nos módulos de suporte do GLI-GSF.

2.2. Métodos de Auditoria

A Auditoria de Controles GIS utiliza uma variedade de métodos de auditoria, incluindo os seguintes métodos, cujos resultados são usados para apoiar a determinação da eficácia do Controle GIS ao longo do tempo:

a. Entrevista: Um tipo de método de auditoria caracterizado pelo processo de conduzir discussões com indivíduos ou grupos dentro de uma Empresa de Jogos para facilitar a compreensão, alcançar esclarecimentos ou levar à localização de evidências.
b. Examinar: Um tipo de método de auditoria caracterizado pelo processo de verificar, inspecionar, revisar, observar, estudar ou analisar um ou mais objetos de avaliação para facilitar a compreensão, obter esclarecimentos ou obter evidências.
c. Teste: Um tipo de método de auditoria caracterizado pelo processo de exercitar um ou mais objetos de auditoria sob condições especificadas para comparar o comportamento real com o esperado.

2.3. Tarefas de Auditoria

A seguir estão as atividades de Auditoria de Controle de GIS de alto nível sugeridas. O Apêndice detalha os controles mínimos comuns de GIS com mais detalhes. Os usuários deste documento são direcionados ao Apêndice deste módulo para garantir que nenhum Controle GIS necessário seja negligenciado. Os Controles GIS listados no Apêndice não são exaustivos e podem ser incluídos Controles GIS adicionais com base nos requisitos regulatórios e no escopo da auditoria.

2.3.1. Revisão de Documentação Submetida

A ISF primeiro avalia os Controles de GIS existentes da Empresa de Jogos, coletando e revisando a documentação relevante para melhor compreender e avaliar aspectos pertinentes do GPE em relação ao GIS geral, e para determinar se a documentação complementa adequadamente os controles técnicos. Um exemplo de parte da documentação que deve ser revisada inclui, mas não se limita a:

a. Política de GIS;
b. Controle de Acesso ao Usuário e Baseado em Funções (RBAC);

c. Procedimentos de Desenvolvimento e Testes;
d. Acordos de Nível de Serviço (SLAs);
e. Política sobre o uso de serviços de rede;
f. Controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos;
g. Política de Backup de Dados;
h. Procedimentos estabelecidos para que a mídia seja descartada de forma segura e protegida;
i. Procedimentos para o manuseio e armazenamento de dados sensíveis (para proteger contra divulgação ou uso indevido não autorizado);
j. Programa de Gestão de Mudanças;
k. Procedimentos para monitoramento do uso de instalações de processamento de informações;
l. Políticas, planos operacionais e procedimentos para atividades de teletrabalho;
m. Política sobre o uso de controles criptográficos; e
n. Diagrama de rede.

2.3.2. Entrevistas com Pessoal-chave

Após coletar e revisar a documentação relevante, a ISF entrevista os principais funcionários (usuários, administradores e gestão) para identificar práticas não documentadas e obter feedback. Como parte do processo de entrevista, o ISF discute as práticas reais em uso e, ao longo das outras fases da avaliação, identifica os procedimentos em uso com base nos resultados técnicos da avaliação. Essas informações permitem que a ISF identifique lacunas processuais e boas práticas que não estão totalmente documentadas nas políticas e procedimentos formais. Além disso, o ISF avalia o nível de consciência dos usuários durante as entrevistas para determinar se usuários fora da função de TI possuem um nível adequado de compreensão de GIS e seu papel na proteção de informações e outros ativos críticos. Os seguintes principais profissionais responsáveis por estabelecer a política de GIS e se candidatar devem ser entrevistados, no mínimo.

a. Pessoa com responsabilidade geral pela operação de jogos;
b. Oficial de conformidade;
c. Oficial de segurança da informação;
d. Equipe operacional; e
e. Desenvolvedores de software.

2.3.3. Avaliação de Controles Administrativos

A ISF realiza testes e avaliações para avaliar a eficácia e adequação dessas medidas administrativas na mitigação de riscos e na garantia do cumprimento dos requisitos de segurança. Essa avaliação normalmente aborda os seguintes tópicos:

a. Políticas, Normas e Diretrizes;
b. Segurança Organizacional;
c. Treinamento de Conscientização em Segurança;
d. Gestão de Operações;
e. Atualizações de Patches e Gerenciamento;
f. Monitoramento do Acesso e Uso do Sistema;
g. Procedimentos de Mudança de Programa;
h. Classificação e Controle de Ativos; e
i. Planejamento de contingência.

2.3.4. Avaliação de Controles Técnicos

A ISF realiza testes e avaliações para avaliar a eficácia e adequação dessas salvaguardas técnicas na mitigação de riscos e proteção de dados sensíveis. Essa avaliação normalmente aborda os seguintes tópicos:

a. Projeto de Infraestrutura;
b. Levantamento em Rede e Testes de Penetração;
c. Segurança de Rede e Comunicações;
d. Controles de Acesso Lógico;
e. Segurança de Sistemas Operacionais (SO);

f. Controles de Software Malicioso;
g. Projeto e Configuração de Banco de Dados;
h. Controles Criptográficos;
i. Monitoramento do Sistema;
j. Relatórios e registros;
k. Controles de Desenvolvimento de Sistemas; e
l. Planos de Continuidade do Negócio e Recuperação de Desastres.

2.3.5. Avaliação de Controles Físicos e Ambientais

A ISF realiza testes e avaliações para avaliar a eficácia e adequação desses controles na proteção contra ameaças físicas, riscos ambientais e acesso não autorizado a áreas sensíveis. Essa avaliação normalmente aborda os seguintes tópicos:

a. Segurança de Localização e Instalações;
b. Segurança e Monitoramento do Perímetro;
c. Controles de Acesso Físico;
d. Segurança de Equipamentos;
e. Detecção de Intrusão;
f. Sistemas de Alarme;
g. Sistemas de Vigilância;
h. Aquecimento, Ventilação e Ar-Condicionado;
i. Sistemas de Energia;
j. Controle de Energia, Telecomunicações e Meio Ambiente;
k. Detecção e Supressão de Incêndios; e
l. Resposta de emergência.

2.3.6. Avaliação do Plano de Resposta a Incidentes GIS

A ISF realiza testes e avaliações para avaliar a eficácia e adequação do plano de resposta a incidentes GIS da Empresa de Jogos, identificar possíveis fraquezas ou deficiências do plano, possibilitar atualizações e melhorias regulares do plano e manter a preparação e resiliência organizacional em relação a incidentes de GIS. Os métodos da ISF para realizar essa avaliação podem incluir, mas não se limitam a, preenchimento de checklist, exercícios de apresentação ou de mesa, simulações e exercícios abrangentes.

2.3.7. Avaliação de Risco

A ISF realiza uma Avaliação de Risco para identificar não conformidades a qualquer Controle de GIS aplicável e quaisquer ameaças e vulnerabilidades potenciais que possam não estar explicitamente listadas no GLI-GSF, mas tenham sido observadas durante a auditoria e possam constituir um risco. A ISF deve usar um sistema de pontuação apropriado para segurança nos jogos (por exemplo, CVSS, ISO/IEC 31010, etc.) para atribuir níveis de gravidade (menor ou maior) a não conformidades, vulnerabilidades e ameaças, permitindo a priorização de respostas e recursos. O sistema de pontuação utilizado pela ISF deve ser identificado no relatório de Auditoria de Controles GIS.

2.3.8. Revisão dos Resultados de Auditorias Anteriores

O ISF pode revisar e aproveitar os resultados de auditorias anteriores conduzidas por ISFs devidamente credenciados e qualificados contra o GLI-GSF, ou outros padrões como ISO/IEC 27001, o Quadro de Cibersegurança do NIST (CSF), ou equivalentes nos últimos seis meses ou outro período especificado pelo Órgão Regulador. O escopo e a aplicabilidade da auditoria alavancada devem ser os mesmos que estão sendo avaliados para esta auditoria. Esse tipo de alavancagem deve ser registrado no relatório de Auditoria de Controles GIS.

2.4. Frequência de Auditoria

2.4.1. Auditoria Inicial

A Empresa de Jogos deve ter uma Auditoria de Controles GIS realizada por um ISF dentro de noventa dias após o início das operações de jogo dentro dessa jurisdição, a menos que o Órgão Regulador tenha informado o contrário. Qualquer adiamento da Auditoria de Controles GIS, conforme solicitado pela Empresa de Jogos, juntamente com um cronograma atualizado, deve ser autorizado pelo Órgão Regulador.

NOTA: Recomenda-se que os órgãos reguladores permitam flexibilidade para os cronogramas de auditoria de controles GIS para empresas de jogos multijurisdicionais, permitindo a consolidação de auditorias de múltiplas jurisdições em um cronograma comum.

2.4.2. Auditoria Anual

A Empresa de Jogos deve, como regra, ter outra Auditoria de Controles GIS realizada por um ISF dentro de doze meses após a Auditoria anterior de Controles GIS, a menos que o Órgão Regulador tenha orientado o contrário. Qualquer adiamento da Auditoria de Controles GIS, conforme solicitado pela Empresa de Jogos, juntamente com um cronograma atualizado, deve ser autorizado pelo Órgão Regulador.

NOTA: Recomenda-se que os órgãos reguladores permitam flexibilidade para os cronogramas de auditoria de controles GIS para empresas de jogos multijurisdicionais, permitindo a consolidação de auditorias de múltiplas jurisdições em um cronograma comum.

2.4.3. Auditorias Adicionais

O Órgão Regulador ou Empresa de Jogos pode solicitar auditorias adicionais de Controle GIS para serem realizadas por um ISF após quaisquer mudanças críticas no GPE que possam afetar a segurança do GPE, que permitam acesso a dados sensíveis e/ou Componentes Críticos do Sistema, ou quaisquer outras alterações que impactem o fluxo de dados ou a postura de segurança. Essas auditorias podem focar especificamente nas mudanças críticas e nos Componentes Críticos do Sistema afetados por essas mudanças.

2.5. Relatórios de Auditoria

Os resultados de uma Auditoria de Controles GIS identificam para as Empresas de Jogos quais áreas das operações devem ser consideradas melhorias e recomendam estratégias para melhorar essas áreas. O relatório de Auditoria de Controles GIS deve ser submetido ao Órgão Regulador até, no máximo, noventa dias após a conclusão da Auditoria de Controles GIS, a menos que o Órgão Regulador tenha orientado o contrário. O relatório de Auditoria de Controles GIS deve incluir todos os seguintes elementos:

a. Resumo Executivo:
   i. O nome e as informações de contato da Empresa de Jogos.
   ii. Uma breve visão geral do modelo de negócios da Empresa de Jogos, atividades de jogos oferecidas, provedores de serviços utilizados, localização, número de funcionários, site, certificações e uma descrição em alto nível da infraestrutura de TI (incluindo data centers, serviços em nuvem, etc.).
b. Detalhes da Auditoria de Controles GIS:
   i. O nome da ISF, a filiação à empresa, as informações de contato e as qualificações e experiência dos indivíduos que realizaram a Auditoria de Controles GIS.
   ii. A(s) data(s) da Auditoria de Controles GIS, incluindo a data do pedido, a data de início, a data de conclusão e a data do relatório.
c. Escopo da Auditoria de Controles GIS:
   i. Uma visão geral de alto nível do trabalho realizado, especificando os ambientes (por exemplo, desenvolvimento, produção) operacionais e os Controles GIS contra os quais a Auditoria de Controles GIS foi conduzida.
   ii. Identificação de Componentes Críticos do Sistema e ativos revisados, detalhando como esses componentes e ativos foram selecionados como parte da Auditoria de Controles GIS.

iii. Ferramentas e técnicas específicas utilizadas durante a Auditoria de Controles GIS, incluindo nomes de softwares, versões e sites oficiais das ferramentas empregadas.

d. Metodologia:
   i. Uma descrição detalhada da abordagem de auditoria, incluindo perguntas baseadas em consulta, observação, evidências, pessoas-chave entrevistadas.
   ii. Quaisquer limitações ou exclusões na Auditoria de Controles GIS, com justificativas (por exemplo, certos sistemas estavam fora do escopo devido a requisitos de negócio).

e. Evidências Coletadas:
   i. Documentação revisada, incluindo nomes , datas e versões.
   ii. Pessoal entrevistado, com funções, locais, nomes, datas e versões das entrevistas.
   iii. Evidências (por exemplo, capturas de tela, logs) que ilustram claramente as não conformidades identificadas, incluindo comandos e ferramentas usadas para descobrir essas questões.
   iv. Técnicas de amostragem usadas para verificar a postura de segurança, incluindo o tamanho e a natureza da amostra.

f. Descobertas e Resultados:
   i. Um resumo das não conformidades descobertas, categorizadas pela gravidade (por exemplo, menor, maior).
   ii. Uma explicação detalhada de cada não conformidade, apoiada por evidências (por exemplo, capturas de tela, logs).
   iii. Uma auditoria do impacto ou risco potencial associado a cada não conformidade identificada, considerando o ambiente específico da Empresa de Jogos.
   iv. Passos recomendados de remediação para cada não conformidade identificada, com níveis de prioridade e prazos sugeridos para mitigação.
   v. A resposta da Empresa de Jogos às descobertas e resultados, incluindo as medidas recomendadas para remediação.

2.6. Remediação

Se o relatório de Auditoria de Controles GIS da ISF recomendar remediação, a Empresa de Jogos deve fornecer ao Órgão Regulador e à ISF, se exigido pelo Órgão Regulador, um plano de remediação e quaisquer planos de mitigação de riscos que detalhem as ações e o cronograma da Empresa de Jogos para implementar as etapas de remediação. O plano de remediação deve ser submetido dentro de trinta dias após a conclusão da auditoria, salvo indicação em contrário pelo órgão regulador.

a. Cada não conformidade deve ser resolvida pelo processo de remediação da Empresa de Jogos, incluindo:
   i. Ações tomadas para determinar a extensão e conter a não conformidade específica.
   ii. Investigação da causa raiz para determinar as causas mais básicas da não conformidade.
   iii. Ações tomadas para corrigir a não conformidade e, em resposta à causa raiz, eliminar a recorrência da não conformidade.

b. As medidas de remediação para resolver cada grande não conformidade identificada devem ser realizadas imediatamente e o Órgão Regulador e a ISF, se solicitados pelo Órgão Regulador, devem ser notificados das ações tomadas em até trinta dias, salvo especificação em contrário pelo Órgão Regulador. Se solicitado pelo Órgão Regulador, o ISF deve realizar uma auditoria de acompanhamento dentro de um prazo razoável especificado no plano de remediação para confirmar as ações tomadas, avaliar sua eficácia e determinar se as não conformidades foram resolvidas.

c. As medidas de remediação para tratar cada menor não conformidade identificada devem ser documentadas e enviadas pela Empresa de Jogos ao Órgão Regulador e à ISF, se exigido pelo Órgão Regulador, para revisão em até trinta dias, salvo indicação em contrário pelo Órgão Regulador. Se as ações forem consideradas satisfatórias, elas devem ser acompanhadas na próxima auditoria agendada.

d. Uma vez tomadas as medidas de remediação, a Empresa de Jogos deve fornecer ao Órgão Regulador e à ISF, se solicitado pelo Órgão Regulador, documentação comprovando a conclusão.

e. A Empresa de Jogos deve manter registros de remediação, incluindo evidências objetivas, por pelo menos cinco anos, salvo indicação em contrário pelo Órgão Regulador.

f. Para qualquer incidente de GIS identificado durante a auditoria pela ISF, ou auto-relatado pela Empresa de Jogos, que atinja ou exceda o limite definido de reporte de incidentes de GIS, a Empresa de Jogos deve:
   i. Enviar um relatório de incidente de GIS ao Órgão Regulador;

ii. Incluir análise da causa raiz, medidas de contenção e ações preventivas como parte do plano de remediação;
iii. Atualizar sua classificação de incidentes e procedimentos de resposta se forem identificadas deficiências nas definições de limiar ou nos caminhos de escalonamento; e
iv. Forneça documentação ao Órgão Regulador e à ISF, se necessário, demonstrando a conclusão de todas as ações de remediação associadas ao incidente que deve ser reportado.

2.7. Empresa Independente de Segurança (ISF)

A Auditoria de Controles GIS deve ser realizada por indivíduos com qualificações suficientes, o que GISnifica que a ISF deve empregar pessoas suficientemente qualificadas, competentes e experientes. Salvo especificação em contrário pelo Órgão Regulador, esses indivíduos devem:

a. Ter formação educacional relevante ou, de outras formas, fornecer qualificações relevantes na avaliação de GPEs;
b. Obter e manter certificações suficientes para demonstrar proficiência e expertise como profissional de segurança qualificado por órgãos de certificação reconhecidos, nacional ou internacionalmente. As seguintes certificações podem demonstrar adequação para concluir a Auditoria de Controles GIS:
   i. ISO/IEC 27001 Auditor Principal;
   ii. Auditor Certificado de Sistemas de Informação (CISA);
   iii. Gerente Certificado em Segurança da Informação (CISM);
   iv. Profissional Certificado em Segurança de Sistemas de Informação (CISSP);
c. Ter pelo menos cinco anos de experiência realizando auditorias de segurança da informação na indústria de jogos ou, quando aceitável para o Órgão Regulador, outra experiência relevante em auditoria dos controles de segurança de um setor semelhante;
d. Não ser funcionário da Empresa de Jogos, da empresa-mãe da Empresa de Jogos, ou de quaisquer outras entidades que hospedam, controlem ou operem o GPE; e
e. Atenda a quaisquer outras qualificações prescritas pelo Órgão Regulador.

NOTA: Nada aqui está destinado a proibir a equipe qualificada do Órgão Regulador de atuar como ISF, desde que sejam independentes da Empresa de Jogos que está sendo auditada.

3. CONTROLES ALTERNATIVOS DE GIS E EXCEÇÕES

3.1. Controles Alternativos de GIS

Reconhece-se que os controles GIS aplicáveis a uma empresa de jogos podem variar dependendo de seu tamanho, estrutura de propriedade, escopo e complexidade das operações, estratégia corporativa e perfil de risco. O Órgão Regulador pode, a seu critério, aprovar a implementação de Controles GIS alternativos em substituição daqueles listados no Apêndice, mediante solicitação da Empresa de Jogos.

a. Para cada Controle GIS enumerado para o qual a Empresa de Jogos deseja usar um Controle GIS alternativo, a Empresa de Jogos deve demonstrar como o Controle GIS alternativo:
   i. Protege a integridade dos jogos oferecidos pela Empresa de Jogos;
   ii. Protege os ativos críticos usados em conexão com o GPE; e
   iii. Alcança um nível de segurança e integridade suficiente para cumprir o propósito do Controle GIS que pretende substituir.
b. Uma Empresa de Jogos só pode implementar um Controle de GIS alternativo após aprovação do órgão regulador.
c. A prova da aprovação do Órgão Regulador para o Controle Alternativo de GIS deve ser fornecida à ISF e avaliada como parte da Auditoria Anual de Controle GIS.

NOTA: É responsabilidade do Órgão Regulador determinar quando é aceitável ou permitido que uma Empresa de Jogos utilize Controles GIS alternativos.

3.2. Pequenas Empresas de Jogos

O Órgão Regulador pode, a seu critério, permitir que uma pequena Empresa de Jogos seja isenta do cumprimento dos Controles de GIS listados no Apêndice, desde que:

a. A receita bruta anual de jogos da pequena Empresa de Jogos não excede um limite estabelecido pelo Órgão Regulador; e
b. A pequena empresa de jogos implementa controles alternativos de GIS que atendem aos requisitos da seção anterior.

NOTA: Nada aqui está destinado a proibir o Órgão Regulador de usar critérios alternativos ou adicionais para definir uma pequena Empresa de Jogos.

3.3. Empresas de Jogos Beneficentes

O Órgão Regulador pode, a seu critério, permitir que uma Empresa de Jogos de Caridade seja isenta do cumprimento dos Controles GIS listados no Apêndice, desde que:

a. Todos os lucros são para benefício de uma organização beneficente;
b. A Empresa de Jogos de Caridade é operada inteiramente pelos funcionários ou voluntários da organização, e não por operadores independentes em benefício de uma organização beneficente;
c. A receita bruta anual de jogos da empresa beneficente de jogos não ultrapassa um limite estabelecido pelo Órgão Regulador; e
d. A empresa beneficente de jogos implementa controles alternativos de GIS que atendem aos requisitos da seção anterior.

NOTA: Nada aqui está destinado a proibir o Órgão Regulador de usar critérios alternativos ou adicionais para definir uma Empresa de Jogos de Caridade.

3.4. Exceções ISF

O Órgão Regulador pode, a seu critério, permitir que uma pequena Empresa de Jogos ou uma Empresa de Jogos de Caridade utilize uma função de auditoria interna ou um funcionário qualificado dentro da Empresa de Jogos ou de uma unidade de negócios, subsidiária ou entidade afiliada da mesma empresa-mãe da Empresa de Jogos que está sendo auditada, que é independente da Empresa de Jogos como ISF, para suas Auditorias de Controle GIS. Nesses casos, a função de auditoria interna ou o funcionário qualificado que atua como ISF deve:

a. Operar independentemente das operações e funções de TI que estão sendo auditadas;
b. Ser gerenciado e supervisionado por pessoal que não tenha responsabilidade operacional pela Empresa de Jogos sob auditoria;
c. Demonstrar independência operacional suficiente para evitar conflitos de interesse e preservar a integridade da Auditoria de Controles GIS;
d. Garantir que indivíduos que realizam ou supervisionam a Auditoria de Controles GIS não estejam envolvidos na gestão, operação ou funções de segurança da Empresa de Jogos;
e. Implementar controles rigorosos para garantir que nenhuma informação relacionada à auditoria seja compartilhada de forma inadequada dentro da estrutura corporativa mais ampla;
f. Divulgue sua relação com a Empresa de Jogos no relatório de Auditoria de Controles GIS e forneça uma explicação por escrito das salvaguardas em vigor para garantir a independência; e
g. Cumprir requisitos de objetividade e integridade equivalentes aos aplicados aos ISFs.

NOTA: É responsabilidade do Órgão Regulador determinar quando é aceitável ou permitido que uma pequena Empresa de Jogos ou Empresa de Jogos de Caridade realize a Auditoria de Controles GIS nessas circunstâncias. O Órgão Regulador mantém a discricionariedade para determinar se tais arranjos internos atendem aos requisitos de independência caso a caso.

APÊNDICE: CONTROLES DE SEGURANÇA DA INFORMAÇÃO EM JOGOS (GIS)

Os Controles de Segurança da Informação de Jogos (GIS), conforme especificado neste Apêndice, indicam a qual Grupo de Implementação de Jogos (GIG) o Controle GIS se aplica. Para auxiliar empresas de jogos de todos os tamanhos, os GIGs são divididos em três grupos, com base no perfil de risco e nos recursos que uma empresa de jogos possui para implementar o GLI-GSF. Cada GIG identifica um conjunto de controles GIS que eles precisam implementar. O GIG2 se baseia no GIG1, e o GIG3 é composto por todos os controles GIS.

GIG	Descrição do Grupo de Implementação de Jogos (GIG)
GIG1	O GLI-GSF define o Grupo de Implementação 1 (GIG1) como higiene essencial para a segurança dos jogos e representa um padrão mínimo emergente de GIS para todas as empresas de jogos. Os controles GIS incluídos no GIG1 são o que toda Empresa de Jogos deveria aplicar para se defender dos ataques mais comuns. Uma GIG1 Empresa de Jogos normalmente tem conhecimento limitado em segurança para se dedicar à proteção de ativos e pessoal críticos. Uma preocupação comum da Empresa de Jogoss é manter suas operações de jogos operacionais, pois elas têm tolerância limitada para o tempo de inatividade. A criticidade dos dados sensíveis que eles tentam proteger é baixa e está principalmente relacionada às informações dos funcionários e financeiras. Os controles GIS selecionados para o GIG1 devem ser implementáveis com conhecimento limitado em segurança de jogos e visam impedir ataques gerais e não direcionados. Esses controles GIS também são tipicamente projetados para funcionar em conjunto com hardware e software comercial comercial de pequenos ou escritórios em casa (COTS).
GIG2	Os Controles GIS selecionados para o GIG2 podem ajudar as equipes de segurança a lidar com a complexidade operacional crescente. Alguns controles GIS dependerão de tecnologia de nível empresarial para jogos e expertise especializada para serem instalados e configurados corretamente. Uma Empresa de Jogos GIG2 emprega indivíduos responsáveis por gerenciar e proteger a infraestrutura do GPE. Essas Empresas de Jogos normalmente apoiam múltiplos departamentos com diferentes perfis de risco baseados na função e missão do cargo. Pequenas unidades de Empresas de Jogos podem enfrentar ônus de conformidade regulatória. A GIG2 Empresa de Jogoss frequentemente armazena e processa dados sensíveis e pode suportar interrupções curtas no serviço. Uma grande preocupação é a perda de confiança pública caso ocorra uma violação. Todas as Empresas de Jogos que operam operações de jogos físicos nas quais o GPE se comunica continuamente por internet/redes públicas (por exemplo, loterias, cassinos com sistemas externos, apostas esportivas de varejo, etc.) devem ser tratadas como Empresas de Jogos GIG2, salvo indicação em contrário pelo Órgão Regulador.
GIG3	Uma GIG3 Empresa de Jogos geralmente emprega especialistas em segurança de jogos que se especializam nas diferentes facetas da segurança em jogos (por exemplo, gestão de riscos, testes de penetração, segurança de aplicações). Os ativos críticos de uma GIG3 Empresa de Jogos contêm dados ou funções sensíveis que estão sujeitos à supervisão regulatória e de conformidade. Uma Empresa GIG3 Gaming deve abordar a disponibilidade e responsabilidade dos serviços, bem como a integridade e confidencialidade de dados sensíveis. Ataques bem-sucedidos podem causar danos significativos às Informações Pessoais Identificáveis (PII). Os controles GIS selecionados para o GIG3 devem reduzir ataques direcionados de adversários sofisticados e reduzir o impacto dos ataques zero-day. Todas as Empresas de Jogos que operam operações de jogos online (por exemplo, jogos interativos, apostas em eventos online, etc.) devem ser tratadas como Empresas de Jogos GIG3, salvo indicação em contrário pelo Órgão Regulador.

A. Adotado de Controles Críticos de Segurança CIS

Para estabelecer uma linha de base clara e razoável para os Controles GIS, o GLI-GSF incorpora por referência os seguintes controles do Center for Internet Security (CIS) Critical Security Controls, Versão 8.1, que devem ser atendidos por cada Empresa de Jogos (Enterprise). A coluna do lado direito indica o Grupo de Implementação de Jogos (GIG) aplicável ao qual o Controle CIS se aplica.

NOTA: O documento completo de Controles Críticos de Segurança da CEI está disponível gratuitamente em www.cisecurity.org.

CIS-1	Inventário e Controle de Ativos Corporativos	GIG
CIS-1.1	Estabelecer e Manter um Inventário Detalhado de Ativos Corporativos	GIG1
CIS-1.2	Endereçar Ativos Não Autorizados	GIG1
CIS-2	Inventário e Controle de Ativos de Software	GIG
CIS-2.1	Estabelecer e Manter um Inventário de Software	GIG1
CIS-2.2	Assegurar Que o Software Autorizado Seja Atualmente Suportado	GIG1
CIS-2.3	Endereçar o Software Não Autorizado	GIG1
CIS-3	Proteção de Dados	GIG
CIS-3.1	Estabelecer e Manter um Processo de Gestão de Dados	GIG1
CIS-3.2	Estabelecer e Manter um Inventário de Dados	GIG1
CIS-3.4	Aplicar Retenção de Dados	GIG1
CIS-3.5	Descartar Dados com Segurança	GIG1
CIS-3.6	Criptografar Dados em Dispositivos de Usuário Final	GIG1
CIS-3.7	Estabelecer e Manter um Esquema de Classificação de Dados	GIG2
CIS-3.9	Criptografar Dados em Mídia Removível	GIG2
CIS-3.10	Criptografar Dados Sensíveis em Trânsito	GIG2
CIS-3.11	Criptografar Dados Sensíveis em Repouso	GIG2
CIS-3.14	Registrar o Acesso a Dados Sensíveis	GIG3
CIS-4	Configuração Segura de Ativos Corporativos e Software	GIG
CIS-4.1	Estabelecer e Manter um Processo de Configuração Segura	GIG1
CIS-4.2	Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede	GIG1
CIS-4.4	Implementar e Gerenciar um Firewall Nos Servidores	GIG1
CIS-4.6	Gerenciar com segurança os ativos e software corporativos	GIG1
CIS-4.7	Gerenciar contas padrão nos ativos e software corporativos	GIG1
CIS-4.8	Desinstalar ou desativar serviços desnecessários nos ativos e software corporativos	GIG2
CIS-4.9	Configurar servidores DNS confiáveis nos ativos corporativos	GIG2
CIS-4.10	Impor o bloqueio automático de dispositivos nos dispositivos portáteis do usuário final	GIG2
CIS-5	Gestão de Contas	GIG
CIS-5.1	Estabelecer e Manter um Inventário de Contas	GIG1
CIS-5.2	Usar Senhas Exclusivas	GIG1
CIS-5.3	Desabilitar Contas Inativas	GIG1
CIS-5.4	Restringir Privilégios de Administrador a Contas de Administrador Dedicadas	GIG1
CIS-5.5	Estabelecer e Manter um Inventário de Contas de Serviço	GIG2
CIS-5.6	Centralizar a Gestão de Contas	GIG2

CIS-6	Gestão do Controle de Acesso	GIG
CIS-6.1	Estabelecer um Processo de Concessão de Acesso	GIG1
CIS-6.2	Estabelecer um Processo de Revogação de Acesso	GIG1
CIS-6.3	Exigir MFA para Aplicações Expostas Externamente	GIG1
CIS-6.4	Exigir MFA para Acesso Remoto à Rede	GIG1
CIS-6.5	Exigir MFA para Acesso Administrativo	GIG1
CIS-6.7	Centralizar o Controle de Acesso	GIG2
CIS-6.8	Definir e Manter o Controle de Acesso Baseado em Funções	GIG3
CIS-7	Gestão Contínua de Vulnerabilidades	GIG
CIS-7.1	Estabelecer e Manter um Processo de Gestão de Vulnerabilidade	GIG1
CIS-7.2	Estabelecer e Manter um Processo de Remediação	GIG1
CIS-7.3	Executar a Gestão Automatizada de Patches do Sistema Operacional	GIG1
CIS-7.4	Executar a Gestão Automatizada de Patches de Aplicações	GIG1
CIS-7.5	Realizar Varreduras Automatizadas de Vulnerabilidade em Ativos Corporativos Internos	GIG2
CIS-7.6	Realizar Varreduras Automatizadas de Vulnerabilidade em Ativos Corporativos Expostos Externamente	GIG2
CIS-7.7	Corrigir Vulnerabilidades Detectadas	GIG2
CIS-8	Gestão de Registros de Auditoria	GIG
CIS-8.1	Estabelecer e Manter um Processo de Gestão de Log de Auditoria	GIG1
CIS-8.2	Coletar Logs de Auditoria	GIG1
CIS-8.3	Garantir o Armazenamento Adequado do Registro de Auditoria	GIG1
CIS-8.4	Padronizar a Sincronização de Tempo	GIG2
CIS-8.5	Coletar Logs de Auditoria Detalhados	GIG2
CIS-8.9	Centralizar os Logs de Auditoria	GIG2
CIS-8.11	Conduzir revisões de Log de Auditoria	GIG2
CIS-8.12	Colete Logs do Provedor de Serviços	GIG3
CIS-9	Proteções de e-mail e Navegador Web	GIG
CIS-9.1	Garantir o Uso Apenas de Navegadores e Clientes de e-mail Suportados Plenamente	GIG1
CIS-9.2	Usar Serviços de Filtragem de DNS	GIG1
CIS-9.7	Implantar e Manter Proteções Anti-malware de Servidor de e-mail	GIG3
CIS-10	Defesas Contra Malware	GIG
CIS-10.1	Instalar e Manter um Software Anti-Malware	GIG1
CIS-10.2	Configurar Atualizações Automáticas de Assinatura Anti-Malware	GIG1
CIS-10.6	Gerenciar o Software Anti-Malware de Maneira Centralizada	GIG2
CIS-10.7	Usar Software Anti-Malware Baseado em Comportamento	GIG2
CIS-11	Recuperação de Dados	GIG
CIS-11.1	Estabelecer e Manter um Processo de Recuperação de Dados	GIG1
CIS-11.2	Executar Backups Automatizados	GIG1
CIS-11.3	Proteger os Dados de Recuperação	GIG1
CIS-11.4	Estabelecer e Manter uma Instância Isolada de Dados de Recuperação	GIG1
CIS-11.5	Testar os Dados de Recuperação	GIG2

CIS-12	Gestão da Infraestrutura de Rede	GIG
CIS-12.1	Assegurar Que a Infraestrutura de Rede Esteja Atualizada	GIG1
CIS-12.2	Estabelecer e Manter uma Arquitetura de Rede Segura	GIG2
CIS-12.3	Gerenciar Infraestrutura de Rede com Segurança	GIG2
CIS-12.4	Estabelecer e Manter Diagrama(s) de Arquitetura	GIG2
CIS-12.6	Usar Protocolos de Comunicação e Gestão de Rede Seguros	GIG2
CIS-13	Monitoramento e Defesa da Rede	GIG
CIS-13.1	Centralizar o Alerta de Eventos de Segurança	GIG2
CIS-13.2	Implantar uma Solução de Detecção de Intrusão Baseada em Host	GIG2
CIS-13.3	Implantar uma Solução de Detecção de Intrusão de Rede	GIG2
CIS-13.4	Realizar Filtragem de Tráfego Entre Segmentos de Rede	GIG2
CIS-13.7	Implantar uma Solução de Prevenção de Intrusão Baseada em Host	GIG3
CIS-13.8	Implantar uma Solução de Prevenção de Intrusão de Rede	GIG3
CIS-13.9	Implantar Controle de Acesso No Nível de Porta	GIG3
CIS-13.10	Executar Filtragem da Camada de Aplicação	GIG3
CIS-14	Conscientização Sobre Segurança e Treinamento de Competências	GIG
CIS-14.1	Estabelecer e Manter um Programa de Conscientização de Segurança	GIG1
CIS-14.2	Treinar Membros da Força de Trabalho para Reconhecer Ataques de Engenharia Social	GIG1
CIS-14.3	Treinar Membros da Força de Trabalho nas Melhores Práticas de Autenticação	GIG1
CIS-14.4	Treinar a Força de Trabalho nas Melhores Práticas de Tratamento de Dados	GIG1
CIS-14.6	Treinar Membros da Força de Trabalho no Reconhecimento e Comunicação de Incidentes de Segurança	GIG1
CIS-14.9	Conduzir Treinamento de Competências e Conscientização de Segurança para Funções Específicas	GIG2
CIS-15	Gestão de Provedor de Serviços	GIG
CIS-15.1	Estabelecer e Manter um Inventário de Provedores de Serviços	GIG1
CIS-15.2	Estabelecer e manter uma Política de Gestão de Provedores de Serviços	GIG2
CIS-15.3	Classificar Provedores de Serviços	GIG2
CIS-15.4	Garantir que os Contratos do Provedor de Serviços Incluam Requisitos de Segurança	GIG2
CIS-15.5	Avaliar Provedores de Serviços	GIG3
CIS-15.6	Monitorar Provedores de Serviços	GIG3
CIS-15.7	Descomissionar com Segurança os Provedores de Serviços	GIG3
CIS-16	Segurança de Aplicações	GIG
CIS-16.1	Estabelecer e Manter um Processo Seguro de Desenvolvimento de Aplicações	GIG2
CIS-16.2	Estabelecer e Manter um Processo para Aceitar e Endereçar Vulnerabilidades de Software	GIG2
CIS-16.3	Executar Análise de Causa Raiz em Vulnerabilidades de Segurança	GIG2
CIS-16.4	Estabelecer e Gerenciar um Inventário de Componentes de Software de Terceiros	GIG2
CIS-16.5	Usar Componentes de Software de Terceiros Atualizados e Confiáveis	GIG2
CIS-16.6	Estabelecer e Manter um Sistema de Classificação de Gravidade e Processo para Vulnerabilidades de Aplicações	GIG2
CIS-16.8	Separar Sistemas de Produção e Não Produção	GIG2
CIS-16.9	Treinar Desenvolvedores em Conceitos de Segurança de Aplicações e Codificação Segura	GIG2
CIS-16.12	Implementar Verificações de Segurança em Nível de Código	GIG2
CIS-16.13	Realizar Teste de Invasão de Aplicação	GIG3

CIS-17	Gestão de Respostas a Incidentes	GIG
CIS-17.1	Designar Pessoal para Gerenciar Tratamento de Incidentes	GIG1
CIS-17.2	Estabelecer e Manter Informações de Contato para Relatar Incidentes de Segurança	GIG1
CIS-17.3	Estabelecer e Manter um Processo Corporativo para Relatar Incidentes	GIG1
CIS-17.4	Estabelecer e Manter um Processo de Resposta a Incidentes	GIG2
CIS-17.5	Atribuir Funções e Responsabilidades Chave	GIG2
CIS-17.6	Definir Mecanismos de Comunicação Durante a Resposta a Incidente	GIG2
CIS-17.7	Conduzir Exercícios de Resposta a Incidentes Rotineiros	GIG2
CIS-17.8	Conduzir Análises Pós-Incidente	GIG2
CIS-17.9	Estabelecer e Manter Limites de Incidentes de Segurança	GIG3
CIS-18	**Testes de Invasão**	**GIG**
CIS-18.1	Estabelecer e Manter um Programa de Teste de Invasão	GIG2
CIS-18.2	Realizar Testes de Invasão Externos Periódicos	GIG2
CIS-18.3	Corrigir as Descobertas do Teste de Invasão	GIG2
CIS-18.4	Validar as Medidas de Segurança	GIG3
CIS-18.5	Realizar Testes de Invasão Internos Periódicos	GIG3

B. Controles Comuns Adicionais de GIS

Além dos Controles Críticos de Segurança CIS adotados anteriormente, os seguintes Controles GIS adicionais se aplicam aos GPEs usados em todas as formas de jogos. A coluna do lado direito indica o Grupo de Implementação de Jogos (GIG) aplicável ao qual o Controle GIS se aplica.

GIS-1	Funções do Programa de Controle Crítico do GPE	GIG
GIS-1.1	**Relógio Interno GPE**	
GIS-1.1.1	O GPE deve manter um clock interno que reflita a data e hora atuais, que deve ser usado para fornecer o carimbo de hora de todas as transações, mudanças de configuração e eventos significativos, além de servir como relógio de referência para relatórios usando o Protocolo de Tempo de Rede (NTP) ou equivalente.	**GIG1**
GIS-1.1.2	Alterações na data e hora do relógio interno, ou nas fontes de tempo aprovadas, devem ser registradas em um registro de auditoria, indicando: a. A data e hora das mudanças; b. Motivo e descrição das mudanças, incluindo valores iniciais e finais; e c. IDs(s) de conta de usuário que realizou e/ou autorizou as alterações.	**GIG1**
GIS-1.2	**Verificação de Assinatura do Programa de Controle Crítico**	
GIS-1.2.1	Programas de Controle Crítico devem ser identificados e documentados para que a Empresa de Jogos possa verificar a integridade do GPE.	**GIG1**
GIS-1.2.2	A Empresa de Jogos deve ser capaz de verificar os Programas de Controle Crítico como idênticos aos aprovados pelo Órgão Regulador por meio de um procedimento de verificação de assinatura, que deve ser aprovado pelo Órgão Regulador e realizado: a. Em intervalos regulares apropriados ao GPE, com cadência de verificação definida com base em limiares baseados em risco (por exemplo, na implantação, reinicialização do sistema e varreduras periódicas de linha de base) b. Sob demanda; e c. Conforme exigido pelo Órgão Regulador.	**GIG1**
GIS-1.2.3	O procedimento de verificação de assinatura deve empregar um algoritmo de hash criptográfico que produza um digest de mensagem de pelo menos 128 bits. Outras metodologias de teste devem ser revisadas caso a caso.	**GIG1**
GIS-1.2.4	Deve haver um processo para responder a falhas de verificação de assinatura, incluindo determinar a causa da falha e realizar as correções ou reinstalações associadas do Programa de Controle Crítico necessárias em tempo hábil.	**GIG1**
GIS-1.3	**Ferramentas Independentes de Verificação de Terceiros**	
GIS-1.3.1	Quando uma ferramenta independente de verificação de terceiros é usada para verificação de assinaturas, tal ferramenta deve operar independentemente de qualquer processo ou software de segurança dentro do GPE.	**GIG1**
GIS-2	**Segurança da Informação em Jogos (GIS)**	**GIG**
GIS-2.1	**Programa de Análise e Supervisão de Riscos em GIS**	
GIS-2.1.1	A Empresa de Jogos deve estabelecer e manter um programa de análise e supervisão de riscos GIS para identificar e minimizar fontes de risco operacional, por meio do desenvolvimento de Controles GIS apropriados e do desenvolvimento do GPE, que sejam confiáveis, seguros e possuam capacidade escalável adequada.	**GIG1**
GIS-2.1.2	O programa da Empresa de Jogos de análise e supervisão de riscos GIS em relação às suas operações e ao GPE deve abordar as seguintes categorias de análise e supervisão de risco GIS: a. Avaliação, mitigação e monitoramento de riscos de segurança e tecnologia; b. planejamento e investimento de capital em segurança e tecnologia; c. supervisão do conselho diretor e da gestão da tecnologia e segurança do GPE; d. Manutenção de um registro de riscos; e. Auditorias de Controles GIS e Avaliações GTS; f. Remediação de deficiências de auditorias de controles GIS e avaliações GTS; e g. Quaisquer outros elementos de gestão de riscos e governança incluídos nas melhores práticas geralmente aceitas.	**GIG1**

GIS-2.1.3	Ao abordar as categorias de análise e supervisão de riscos em GIS, a Empresa de Jogos deve seguir padrões e melhores práticas geralmente aceitos no que diz respeito ao desenvolvimento, operação, confiabilidade, segurança e capacidade do GPE.	**GIG1**
GIS-2.2	**Política de GIS**	
GIS-2.2.1	Uma política de GIS deve ser definida e implementada para descrever a abordagem da Empresa de Jogos para gerenciar o GIS e sua implementação, além de garantir que os riscos sejam identificados, mitigados e garantidos por planos de contingência.	**GIG1**
GIS-2.2.2	A política de GIS deve conter uma disposição que exija revisão pelo menos anualmente ou em intervalos planejados exigidos pelo Órgão Regulador e quando ocorrem mudanças GISnificativas nos processos do GPE ou da Empresa de Jogos que alterem o perfil de risco do sistema.	**GIG1**
GIS-2.2.3	A política de GIS deve ser aprovada pela administração e comunicada e reconhecida pelo pessoal relevante dentro da Empresa de Jogos.	**GIG1**
GIS-2.2.4	A política de GIS deve delimitar os papéis e responsabilidades de segurança do pessoal relevante dentro da Empresa de Jogos para a operação, serviço e manutenção do GPE, juntamente com suas informações de contato. Algunsdesses papéis e responsabilidades de segurança podem ser atribuídos com base em Avaliações de Risco realizadas pela Empresa de Jogos.	**GIG1**
GIS-2.2.5	Deve haver um processo disciplinar claro e formal para agir quando funcionários ou outras pessoas violarem a política de GIS.	**GIG1**
GIS-2.3	**Política de Controle de Acesso**	
GIS-2.3.1	Uma política de controle de acesso deve ser estabelecida e documentada com base nos requisitos de negócios e segurança para acesso físico e lógico ao GPE, incluindo acesso remoto.	**GIG1**
GIS-2.3.2	A política de controle de acesso deve ser revisada pelo menos anualmente ou conforme exigido pela Empresa de Jogos e/ou pelo Órgão Regulador.	**GIG1**
GIS-2.3.3	Deve existir um procedimento formal de registro e desregistro de usuários para conceder e revogar o acesso ao GPE.	**GIG1**
GIS-2.3.4	A alocação e o uso dos direitos e privilégios de acesso dos usuários devem ser restritos e controlados com base nos requisitos comerciais e no princípio do privilégio mínimo.	**GIG2**
GIS-2.3.5	O pessoal deve ter acesso apenas aos serviços ou instalações que foi especificamente autorizado a utilizar.	**GIG1**
GIS-2.3.6	A administração deve usar um processo formal para revisar e confirmar os direitos e privilégios de acesso dos usuários pelo menos uma vez por ano ou conforme exigido pela Organização de Jogos e/ou pelo Órgão Regulador.	**GIG2**
GIS-2.4	**Requisitos de Triagem e Monitoramento de Pessoal**	
GIS-2.4.1	A Empresa de Jogos deve realizar verificações de antecedentes em todos os candidatos antes de iniciar o emprego. Essas verificações devem estar em conformidade com as leis locais aplicáveis, padrões éticos e regulamentos observados pelo Órgão Regulador.	**GIG1**
GIS-2.4.2	Verificações de antecedentes devem ser realizadas anualmente para o pessoal existente que tenha acesso físico e lógico ao GPE, incluindo acesso remoto. A frequência e a profundidade dessas verificações devem ser adequadas ao papel do indivíduo, à sensibilidade dos dados acessados e ao nível de risco associado às suas responsabilidades.	**GIG1**
GIS-2.4.3	O escopo e o rigor das verificações de antecedentes devem ser proporcionais à classificação das informações acessadas pelo cargo, à influência do cargo dentro da Empresa de Jogos e ao impacto potencial na integridade do GPE e das operações de jogo.	**GIG1**
GIS-2.4.4	A Empresa de Jogos deve estabelecer e manter uma política e procedimento documentados para verificação de segurança, a fim de garantir a confiabilidade das pessoas cujos papéis possam afetar a integridade do GPE e das operações de jogo.	**GIG1**
GIS-2.4.5	Uma política formal e procedimentos associados devem ser implementados para monitorar a atividade do GPE pelo pessoal. Esse monitoramento deve visar detectar e investigar comportamentos que possam comprometer a integridade dos jogos.	**GIG1**
GIS-2.4.6	Todas as políticas de triagem e monitoramento de pessoal devem ser elaboradas para equilibrar os direitos de privacidade individuais com a obrigação da Empresa de Jogos de proteger a integridade do GPE e das operações de jogo.	**GIG1**
GIS-2.5	**Código de Conduta de Pessoal**	
GIS-2.5.1	A Empresa de Jogos deve emitir um código de conduta para todos os funcionários para reconhecimento e aceitação quando inicialmente contratados.	**GIG1**

GIS-2.5.2	O código de conduta deve incluir declarações que: a. Garantir que os funcionários estejam cientes de suas obrigações de cumprir todas as políticas e procedimentos da Empresa de Jogos; b. Especifique que a infração ou outras violações do código de conduta ou das políticas e procedimentos mencionados podem levar a ações disciplinares; c. Exigir que os empregados declarem conflitos de interesse no emprego assim que ocorrerem. Exemplos específicos de conflito de interesses podem ser citados dentro do código de conduta; e d. Aborde disposições anticorrupção, incluindo hospitalidade e presentes fornecidos por, ou dados a, pessoas ou entidades com as quais a Empresa de Jogos realiza negócios.	**GIG1**
GIS-2.6	**Atribuição de Responsabilidades e Funções em GIS**	
GIS-2.6.1	As responsabilidades e deveres de GIS do pessoal e da Empresa de Jogos devem ser efetivamente documentados, implementados e comunicados ao pessoal relevante, incluindo aqueles que permanecem válidos após a demissão ou mudança de emprego.	**GIG2**
GIS-2.6.2	Um fórum de GIS composto por gestões deve ser formalmente estabelecido para monitorar e revisar a política de GIS a fim de garantir sua adequação, adequação e eficácia contínuas, manter atas formais das reuniões e se reunir pelo menos a cada seis meses ou em intervalos regulares exigidos pelo Órgão Regulador.	**GIG2**
GIS-2.6.3	Deve existir uma função de GIS responsável por desenvolver e implementar estratégias e planos de ação de segurança de acordo com o Empreendimento de Jogos como um todo.	**GIG2**
GIS-2.6.4	A função de GIS deve estar envolvida na revisão de todas as tarefas e processos necessários relacionados aos aspectos de GIS da Empresa de Jogos, incluindo, mas não se limitando a, a proteção de informações e dados sensíveis, comunicações, infraestrutura virtual e física, pessoal e segurança operacional geral.	**GIG2**
GIS-2.6.5	A função de GIS deve reportar à gestão de nível executivo no que diz respeito à gestão de riscos de segurança.	**GIG2**
GIS-2.6.6	Para evitar conflito de interesses entre operações e gestão de riscos de segurança, a função de GIS deve ser independente da função de TI, salvo autorização em contrário pelo Órgão Regulador.	**GIG2**
GIS-2.6.7	A função de GIS deve ter as competências, estar suficientemente capacitada e ter acesso a todos os recursos necessários para permitir uma avaliação, gestão e redução adequadas de riscos.	**GIG2**
GIS-2.6.8	O chefe da função de GIS deve ser membro do fórum de GIS e ser responsável por recomendar políticas e mudanças em GIS.	**GIG2**
GIS-2.7	**Programa de Privacidade de Informações Pessoais Identificáveis (PII)**	
GIS-2.7.1	A Empresa de Jogos deve estabelecer e manter um programa de privacidade para fornecer proteções técnicas e organizacionais adequadas para as PII coletadas ou processadas pela Empresa de Jogos.	**GIG1**
GIS-2.7.2	O programa de privacidade deve considerar a justiça e transparência geral de como a Empresa de Jogos processa as PII dos indivíduos e protege essas informações em conformidade com quaisquer regulamentos e padrões locais de privacidade observados pelo Órgão Regulador.	**GIG1**
GIS-2.7.3	A Empresa de Jogos deve deGISnar uma ou mais pessoas com responsabilidade primária pelo deGISn, implementação e avaliação contínua de procedimentos e práticas relacionados à segurança e ao processamento de PII.	**GIG1**
GIS-2.7.4	A Empresa de Jogos deve estabelecer procedimentos para determinar a natureza e o escopo de todas as PII coletadas e processadas pela Empresa de Jogos, incluindo os tipos de informações coletadas e processadas, fontes de coleta e propósitos de uso.	**GIG1**
GIS-2.7.5	A Empresa de Jogos deve seguir e disponibilizar publicamente um aviso de privacidade para informar as pessoas sobre as atividades de processamento de PII da Empresa de Jogos, incluindo, sem limitações, a. Informações relacionadas ao propósito da coleta de PII; b. Se as PII serão compartilhadas ou vendidas para outras entidades; e c. A forma de exercer os direitos individuais, se aplicável.	**GIG1**
GIS-2.7.6	Se uma Empresa de Jogos utiliza tomada de decisão automatizada, deve estabelecer procedimentos para a governança desse processo, garantindo que os direitos legais do indivíduo não sejam violados.	**GIG1**

GIS-2.8	**Garantindo Transações Financeiras dentro do GPE**	
GIS-2.8.1	Os métodos de pagamento usados para transações financeiras no GPE devem ser protegidos contra uso fraudulento.	**GIG1**
GIS-2.8.2	A Empresa de Jogos deve coletar apenas os dados sensíveis estritamente necessários para a transação financeira.	**GIG1**
GIS-2.8.3	Devem existir processos para verificar a proteção de dados sensíveis diretamente relacionados a cada transação financeira dentro do GPE, incluindo quaisquer PII fornecidas pelo patrono ou dados relacionados ao pagamento.	**GIG1**
GIS-2.8.4	Quaisquer canais de comunicação dentro do GPE que transmitam detalhes das transações financeiras devem ser seguros e empregar criptografia e autenticação forte para proteger contra interceptação.	**GIG1**
GIS-3	**Operação e Segurança do GPE**	**GIG**
GIS-3.1	**Procedimentos de Segurança**	
GIS-3.1.1	A Empresa de Jogos deve monitorar os Componentes Críticos do Sistema e a transmissão de dados de todo o GPE, incluindo comunicação, pacotes de dados, redes, aplicações, bem como os componentes e transmissões de dados de quaisquer serviços de Provedor de Serviços envolvidos, com o objetivo de garantir confidencialidade, integridade, disponibilidade e responsabilidade, além de identificar comportamentos anômalos.	**GIG2**
GIS-3.1.2	A Empresa de Jogos deve monitorar e ajustar a capacidade e o consumo de recursos do GPE para garantir que a disponibilidade seja mantida.	**GIG1**
GIS-3.1.3	A Empresa de Jogos deve manter um registro de auditoria do desempenho do GPE, incluindo uma função para compilar relatórios de desempenho.	**GIG2**
GIS-3.1.4	A Empresa de Jogos deve monitorar seu GPE para detectar, prevenir, mitigar e responder a ataques e compromissos técnicos ativos e passivos comuns.	**GIG1**
GIS-3.1.5	A Empresa de Jogos deve estabelecer procedimentos para coletar e analisar inteligência de ameaças, e agir adequadamente sobre ela.	**GIG2**
GIS-3.1.6	A Empresa de Jogos deve estabelecer procedimentos para monitorar, gerenciar e responder centralmente a atividades, exceções, falhas e eventos adversos dos usuários.	**GIG2**
GIS-3.2	**Falas no GPE**	
GIS-3.2.1	Após a detecção de uma falha, a Empresa de Jogos deve iniciar uma investigação para determinar a causa raiz da falha.	**GIG1**
GIS-3.2.2	A investigação deve envolver uma análise minuciosa dos registros relevantes, relatórios, registros de auditoria e registros de vigilância associados ao Componente Crítico do Sistema afetado.	**GIG1**
GIS-3.2.3	Com base nas descobertas documentadas da investigação, devem ser tomadas ações apropriadas para reparar ou substituir os Componentes Críticos do Sistema responsáveis pela falha.	**GIG1**
GIS-3.2.4	Antes de restaurar os Componentes Críticos do Sistema para operação, atividades de verificação devem ser realizadas para garantir sua integridade e funcionalidade.	**GIG1**
GIS-3.2.5	De acordo com os requisitos regulatórios, a Empresa de Jogos deve apresentar um relatório de falha ao órgão regulador apropriado, documentando os detalhes da falha.	**GIG1**
GIS-3.3	**Gestão de Incidentes em GIS**	
GIS-3.3.1	A Empresa de Jogos deve estabelecer e manter um plano de resposta a incidentes de GIS que inclua: a. Procedimentos para detectar, monitorar, registrar, classificar, escalar, reportar, investigar, responder e resolver vários tipos de incidentes de GIS, incluindo violações detectadas e suspeitas ou manipulações reais ou hackeadas com o GPE; b. Definiu prazos de resposta a incidentes de GIS para detecção, escalonamento e resolução; c. Requisitos de documentação para todas as etapas do tratamento de incidentes em GIS; d. Comunicação interna e externa e compartilhamento de informações sobre incidentes de GIS; e e. Definição e classificação de incidentes de GIS e limites para incidentes de GIS reportáveis (por exemplo, baseados em impacto, urgência ou componentes e dados afetados).	**GIG1**

GIS-3.3.2	A Empresa de Jogos deve manter mecanismos para garantir que incidentes de GIS sejam consistentemente avaliados de acordo com a metodologia de classificação de incidentes de GIS e os limites para incidentes de GIS que podem ser reportados. Esses limiares mínimos definidos de denúncia estabelecem os tipos e a gravidade dos incidentes que exigem notificação formal e ações de resposta. A Empresa de Jogos pode adotar ou adaptar modelos de gravidade e categorização de incidentes a partir de estruturas já estabelecidas.	**GIG1**
GIS-3.3.3	A Empresa de Jogos deve implementar mecanismos técnicos e processuais apropriados para: a. Monitorar continuamente o GPE para incidentes de GIS; b. Detectar e registrar todos os incidentes suspeitos ou reais de GIS; e c. Escalar automaticamente ou manualmente incidentes de GIS que atendam ou excedam os limites definidos.	**GIG1**
GIS-3.3.4	Todos os incidentes de GIS devem ser investigados, respondidos e resolvidos dentro de um prazo estabelecido, aprovado pelo Órgão Regulador e formalmente documentado.	**GIG1**
GIS-3.3.5	No caso de um incidente de GIS que comprometa a segurança ou integridade de dados sensíveis ou Componentes Críticos do Sistema, a Empresa de Jogos deve: a. Notifique prontamente os indivíduos afetados, o Órgão Regulador e outras autoridades relevantes sobre a violação, conforme necessário; e b. Forneça detalhes ao Órgão Regulador e a outras autoridades relevantes sobre a natureza do incidente GIS, os dados e componentes impactados, os riscos potenciais e as medidas tomadas para mitigar o impacto, além das ações de recuperação, incluindo planos para prevenir a recorrência.	**GIG1**
GIS-3.3.6	A Empresa de Jogos deve demonstrar, por meio de documentação e registros, que: a. Todos os incidentes de GIS aplicáveis foram reportados de acordo com suas políticas e requisitos regulatórios; b. O plano de resposta e os controles são implementados e testados de forma eficaz; e c. Logs, relatórios e ações tomadas durante o tratamento de incidentes estão disponíveis para auditoria e revisão regulatória.	**GIG1**
GIS-3.3.7	O plano de resposta a incidentes de GIS deve incluir procedimentos documentados para lidar com incidentes de GIS.	**GIG1**
GIS-3.3.8	Procedimentos devem ser estabelecidos para a recuperação controlada de incidentes de GIS, incluindo a restauração dos sistemas afetados e dados sensíveis a um estado conhecido de bom estado.	**GIG1**
GIS-3.3.9	O conhecimento adquirido com Incidentes de GIS deve ser usado para fortalecer e aprimorar os controles de GIS.	**GIG1**
GIS-3.4	**Localização Física dos Servidores**	
GIS-3.4.1	Os servidores GPE, dados sensíveis, informações e outros ativos associados devem estar alojados em um ou mais locais seguros que podem estar localizados localmente, dentro de um único local ou local, ou podem estar localizados remotamente fora do local ou local, conforme permitido pelo Órgão Regulador.	**GIG1**
GIS-3.4.2	Cada local seguro deve ter proteção suficiente contra alterações, manipulações ou acessos não autorizados.	**GIG1**
GIS-3.4.3	Cada local seguro deve estar equipado com um sistema de vigilância que atenda aos procedimentos estabelecidos pelo Órgão Regulador.	**GIG1**
GIS-3.4.4	Medidas de segurança para trabalhar em locais seguros devem ser projetadas e implementadas.	**GIG1**
GIS-3.4.5	Perímetros de segurança devem ser definidos e usados para proteger cada local seguro.	**GIG1**
GIS-3.4.6	Cada local seguro deve ser protegido por controles de entrada adequados para garantir que o acesso seja restrito apenas a pessoal autorizado.	**GIG1**
GIS-3.4.7	Para o acesso físico a cada local seguro, deve ser utilizado um processo auditável de MFA, a menos que o local seguro esteja sempre com pessoal.	**GIG1**
GIS-3.4.8	Dispositivos de acesso a cada local seguro, como deslizamento magnético, cartões de proximidade, chips embutidos, fobs, chaves, devem: a. ser controlada por pessoal autorizado; e b. Não identificar o usuário ou o local ao qual ele tem acesso, incluindo seu nome ou endereço.	**GIG1**

GIS-3.4.9	Todas as tentativas de acesso físico a cada local seguro devem ser registradas em um registro de auditoria, indicando: a. A data e hora da tentativa de acesso; b. Identificação do indivíduo que tenta acessar; c. Identificação do local ou local seguro acessado; d. Indicação de se a tentativa de acesso foi bem-sucedida ou não; e e. Se a tentativa de acesso foi bem-sucedida, a duração do acesso.	**GIG1**
GIS-3.4.10	Cada local seguro deve estar equipado com controles para fornecer proteção física contra danos causados por incêndio, enchente e outras ameaças ambientais e formas de desastre natural ou causado pelo homem (por exemplo, furacão, terremoto, etc.).	**GIG1**
GIS-3.4.11	O GPE deve ser protegido contra surtos de energia, falhas e outras interrupções causadas por falhas nas concessionárias de apoio.	**GIG1**
GIS-3.4.12	Cabos que transportam energia, dados ou que suportam Componentes Críticos do Sistema devem ser protegidos contra interceptação, interferência, riscos ambientais ou outros danos.	**GIG1**
GIS-3.4.13	Todos os Componentes Críticos do Sistema devem ser fornecidos com energia primária adequada.	**GIG1**
GIS-3.4.14	Quando o servidor é uma aplicação independente, ele deve ter uma Fonte de Alimentação Ininterrupta (UPS) conectada e capacidade suficiente para permitir um desligamento gradual, mantendo todos os dados sensíveis durante uma queda de energia. É aceitável que o sistema possa ser um componente de uma rede suportada por um nobreak de rede geral, desde que o servidor esteja incluído como um dispositivo protegido pelo nobreak. Um sistema de proteção contra surtos deve estar em uso se não estiver incorporado ao próprio nobreak.	**GIG1**
GIS-3.5	**Controle de Acesso Lógico**	
GIS-3.5.1	O GPE deve ser logicamente protegido contra acessos não autorizados por meio de credenciais de autenticação permitidas pelo Órgão Regulador, como senhas, MFA, certificados digitais, PINs, biometria e outros métodos de acesso.	**GIG1**
GIS-3.5.2	Cada conta de usuário deve ter sua própria credencial de autenticação individual, cuja provisão deve ser controlada por meio de um processo formal.	**GIG1**
GIS-3.5.3	Os usuários devem ter acesso apenas às funcionalidades e recursos adequados para seu papel e responsabilidades dentro do GPE.	**GIG1**
GIS-3.5.4	Não deve ser possível modificar os parâmetros críticos do sistema do GPE, incluindo as políticas e parâmetros para sistemas operacionais, bancos de dados, redes e aplicações (por exemplo, configurações de auditoria, configurações de complexidade de senha, níveis de segurança do sistema, atualizações manuais de bancos de dados, etc.), sem um processo seguro autorizado. Alterações nos parâmetros críticos do sistema devem ser registradas em um registro de auditoria, indicando: a. A data e hora das mudanças; b. Parâmetros críticos do sistema alterados; c. Motivo e descrição das mudanças, incluindo valores iniciais e finais; e d. IDs(s) de conta de usuário que realizou e/ou autorizou as alterações.	**GIG1**
GIS-3.5.5	O uso de contas padrão e contas genéricas deve ser limitado. Quando usados, os motivos de seu uso devem ser formalmente documentados e revisados anualmente.	**GIG1**
GIS-3.5.6	Os registros das credenciais de autenticação devem ser mantidos manualmente ou por sistemas que registram automaticamente as mudanças de autenticação e forçam alterações nas credenciais de autenticação.	**GIG1**
GIS-3.5.7	Quaisquer credenciais de autenticação armazenadas no sistema devem ser criptografadas ou hasheadas para outros algoritmos criptográficos autorizados.	**GIG1**
GIS-3.5.8	Um método de reserva para redefinir credenciais de autenticação (por exemplo, senhas esquecidas) deve ser pelo menos tão forte quanto o método principal. Um processo MFA deve ser empregado para esses fins.	**GIG2**
GIS-3.5.9	Credenciais de autenticação perdidas ou comprometidas e de usuários encerrados devem ser desativadas, protegidas ou destruídas o mais rápido possível.	**GIG1**

GIS-3.5.10	O sistema deve ter múltiplos níveis de acesso de segurança para controlar e restringir diferentes classes de acesso ao GPE, incluindo visualização, alteração ou exclusão de arquivos e diretórios críticos. Procedimentos devem existir para atribuir, revisar, modificar e remover direitos e privilégios de acesso a cada usuário, incluindo: a. Permitindo que a administração das contas de usuário proporcione uma separação adequada de funções. b. Limitar os usuários que possuem as permissões necessárias para ajustar parâmetros críticos do sistema. c. A aplicação de parâmetros adequados de credenciais de autenticação, como duração mínima e intervalos de validade.	**GIG1**
GIS-3.5.11	Um Provedor de Serviços da Empresa de Jogos pode, conforme necessário, acessar o GPE e seus componentes associados usando uma conta de usuário dedicada para suporte ao produto e ao usuário ou atualizações/atualizações, conforme permitido pelo Órgão Regulador e pela Empresa de Jogos. As contas dedicadas de usuários devem ser: a. Restrito por controles lógicos para acessar apenas a(s) aplicação(s) e/ou banco de dados necessários para o produto e suporte ao usuário ou fornecer atualizações/atualizações; b. Monitorado continuamente pela Empresa de Jogos; c. Desativado quando não estiver em uso e imediatamente após o propósito para o qual a conta foi criada não é mais necessário; e d. Identificado de forma única para o indivíduo que acessa o GPE. Contas genéricas e contas compartilhadas para Provedores de Serviço são proibidas.	**GIG1**
GIS-3.5.12	Devem existir procedimentos para identificar e sinalizar contas suspeitas de usuários, a fim de evitar seu uso não autorizado, o que inclui: a. Ter notificação do administrador do sistema e bloqueio do usuário, após um máximo de três tentativas incorretas de autenticação; b. Sinalização de contas suspeitas onde credenciais de autenticação podem ter sido roubadas; e c. Invalidando contas e transferindo informações críticas armazenadas para uma nova conta.	**GIG1**
GIS-3.5.13	Qualquer tentativa lógica de acesso às aplicações do sistema ou sistemas operacionais deve ser registrada em um registro de auditoria, indicando: a. A data e hora da tentativa de acesso; b. ID da conta de usuário; c. Endereço IP do indivíduo que tenta acessar; d. Indicação de se a tentativa de acesso foi bem-sucedida ou não; e e. Se a tentativa de acesso foi bem-sucedida, a duração do acesso.	**GIG1**
GIS-3.5.14	O uso de programas utilitários que podem sobrescrever controles de aplicação ou sistema operacional deve ser restrito e rigidamente controlado.	**GIG1**
GIS-3.5.15	Vacâncias, sobreposições, correções ou quaisquer outras atividades que exijam intervenção do usuário e ocorram fora do escopo normal de operação do sistema devem ser registradas em um registro de auditoria, indicando: a. A data e o horário das atividades; b. Componentes afetados pelas atividades; c. Razão e descrição das atividades, incluindo valores iniciais e finais; e d. ID(s) de conta de usuário que realizou e/ou autorizou as atividades.	**GIG1**
GIS-3.5.16	Para cada conta de usuário, as informações a serem mantidas e respaldadas pelo GPE devem incluir: a. ID da conta de usuário; b. Nome e título ou cargo individual; c. Lista completa e descrição das funções que cada grupo ou conta de usuário pode executar; d. A data e hora da criação da conta; e. A data e hora do último acesso, incluindo o endereço IP; f. A data e hora da última mudança de senha; g. A data e hora em que a conta foi desativada/desativada; h. Descrição dos direitos de acesso ou da participação em grupo da conta, se aplicável; e i. Os status atuais e anteriores da conta de usuário (por exemplo, ativo, inativo, fechado, suspenso, etc.).	**GIG1**

GIS-3.5.17	Deve existir um processo para que o pessoal autorizado mude, bloqueie, desative ou remova uma conta de usuário em tempo hábil em caso de uso não autorizado da conta, ou suspensão, rescisão ou mudança de função ou responsabilidade do usuário.	**GIG1**
GIS-3.5.18	Somente pessoal autorizado terá acesso a contas de usuário inativas ou fechadas.	**GIG1**
GIS-3.6	**Autenticação e Autorização do Usuário**	
GIS-3.6.1	Deve ser empregado um mecanismo seguro e controlado que possa verificar se o Componente Crítico do Sistema está sendo acessado por pessoal autorizado sob demanda e regularmente, conforme exigido pelo Órgão Regulador.	**GIG1**
GIS-3.6.2	As sessões ativas de usuário devem ser encerradas se a autorização do usuário tiver excedido um número configurável de tentativas fracassadas.	**GIG1**
GIS-3.6.3	Qualquer informação de autorização comunicada pelo sistema para fins de identificação deve ser obtida no momento da solicitação ao sistema e não armazenada no Componente Crítico do Sistema.	**GIG2**
GIS-3.6.4	Quando as sessões de usuário são rastreadas para autorização, as informações de autorização devem sempre ser criadas aleatoriamente, na memória, e devem ser removidas após o término da sessão do usuário.	**GIG2**
GIS-3.6.5	Restrições sobre tempos de conexão, como, mas não necessariamente limitadas, os tempos de espera das sessões do usuário, devem ser usadas para fornecer segurança adicional para aplicações de alto risco, como acesso remoto.	**GIG1**
GIS-3.6.6	As sessões de usuário devem ser configuradas para expirar automaticamente após um período definido de inatividade, conforme determinado pela administração. Salvo especificação em contrário pelo Órgão Regulador, o período de inatividade não deve exceder: a. Para dispositivos eletrônicos portáteis (por exemplo, dispositivos móveis para usuários finais), 5 minutos; e b. Para todos os outros sistemas e dispositivos, 15 minutos.	**GIG1**
GIS-3.7	**Programação de Servidores**	
GIS-3.7.1	O GPE deve ser suficientemente seguro para evitar qualquer capacidade de programação iniciada não autorizada pelo usuário no servidor que possa resultar em modificações no banco de dados. No entanto, é aceitável que administradores de rede ou sistema realizem manutenção autorizada da infraestrutura de rede ou solução de problemas de aplicações com direitos de acesso suficientes.	**GIG1**
GIS-3.8	**Nuvem e Ambientes Virtualizados**	
GIS-3.8.1	Se dados sensíveis forem armazenados, processados ou transmitidos em uma nuvem ou ambiente virtualizado, os Controles GIS apropriados devem se aplicar a esse ambiente. Isso normalmente envolve validar tanto a infraestrutura do ambiente de nuvem ou virtualização quanto o uso das instâncias de servidor dentro desse ambiente.	**GIG2**
GIS-3.8.2	Instâncias redundantes de servidor em um ambiente em nuvem ou virtualizado devem ser implantadas em hipervisores separados para evitar um único ponto de falha.	**GIG2**
GIS-3.9	**Uso Opcional de um Sistema Eletrônico de Retenção de Documentos (EDRS)**	
GIS-3.9.1	O EDRS deve ser configurado corretamente para manter a versão original junto com todas as versões subsequentes que refletam todas as alterações nos relatórios ou logs de auditoria armazenados em um formato alterável.	**GIG1**
GIS-3.9.2	O EDRS deve manter uma assinatura única para cada versão do log de auditoria, incluindo a original.	**GIG1**
GIS-3.9.3	O EDRS deve manter um registro de auditoria das alterações em todos os relatórios, incluindo o ID da conta de usuário realizado pelas alterações, a data e hora em que as alterações ocorreram e o que foi alterado.	**GIG1**
GIS-3.9.4	O EDRS deve fornecer um método de indexação completa para facilitar a localização e identificação do log de auditoria, incluindo pelo menos o seguinte (que pode ser inserido pelo usuário): a. Data e hora da geração do log de auditoria; b. Componente crítico do sistema gerando o log de auditoria; c. Título e descrição do registro de auditoria; d. ID da conta de usuário de quem está gerando o registro de auditoria; e e. Qualquer outra informação que possa ser útil para identificar o registro de auditoria e seu propósito.	**GIG1**

GIS-3.9.5	O EDRS deve ser configurado para a. Limitar o acesso para modificar ou adicionar relatórios ou logs de auditoria ao sistema por meio da segurança lógica de contas específicas de usuário; e b. Forneça um registro de auditoria de toda a atividade da conta administrativa de usuários.	**GIG1**
GIS-3.9.6	O EDRS deve ser devidamente protegido usando medidas físicas e lógicas de segurança (contas de usuário com acesso apropriado, níveis adequados de registro de eventos, e o controle de versões documentado, etc.).	**GIG1**
GIS-3.9.7	O EDRS deve estar equipado para evitar a interrupção da disponibilidade dos registros e a perda de dados por meio de redundância de hardware e software, melhores práticas e processos de backup.	**GIG1**
GIS-4	**Integridade dos Dados**	**GIG**
GIS-4.1	**Gerenciamento de Dados Sensíveis**	
GIS-4.1.1	A Empresa de Jogos deve oferecer uma abordagem em camadas para a segurança dos GPE para garantir o armazenamento e processamento seguros de dados sensíveis usando métodos razoáveis de proteção.	**GIG1**
GIS-4.1.2	A Empresa de Jogos deve implementar uma política para manter dados sensíveis por pelo menos cinco anos, salvo especificação em contrário pelo Órgão Regulador, e de acordo com as regulamentações e padrões locais de retenção de dados observados pelo Órgão Regulador.	**GIG1**
GIS-4.1.3	Métodos apropriados para lidar com dados sensíveis devem ser implementados, incluindo validação de entrada e rejeição de dados sensíveis corrompidos.	**GIG2**
GIS-4.1.4	Criptografia ou segurança equivalente deve ser usada para arquivos e diretórios contendo dados sensíveis. Se a criptografia não for utilizada, a Empresa de Jogos deve restringir os usuários de visualizar o conteúdo desses arquivos e diretórios, que, no mínimo, devem prever a segregação das funções e responsabilidades do sistema, bem como o monitoramento e registro do acesso por qualquer pessoa a tais arquivos e diretórios.	**GIG2**
GIS-4.1.5	Alterações autorizadas aos arquivos de dados ao vivo e tabelas de banco de dados do GPE que ocorram fora da execução normal do programa e do sistema operacional devem ser registradas em um registro de auditoria, indicando: a. A data e hora das alterações; b. Os arquivos de dados ao vivo e as tabelas de banco de dados afetados pelas alterações; c. Motivo e descrição das alterações, incluindo arquivos de dados em tempo real e tabelas de banco de dados antes e depois das alterações; e d. IDs de conta de usuário que realizou e/ou autorizou a alteração.	**GIG1**
GIS-4.1.6	O GPE deve fornecer um meio lógico para proteger e proteger dados sensíveis contra alterações, manipulações ou acessos não autorizados, tanto externos quanto internos.	**GIG1**
GIS-4.1.7	A operação normal de qualquer Componente Crítico do Sistema que contenha dados sensíveis não deve ter opções ou mecanismos que possam comprometer os dados sensíveis.	**GIG1**
GIS-4.1.8	Componentes Críticos do Sistema não devem ter um mecanismo pelo qual um erro faça com que os dados sensíveis sejam automaticamente apagados.	**GIG1**
GIS-4.1.9	Qualquer Componente Crítico do Sistema que contenha dados sensíveis em sua memória não deve permitir a remoção das informações, a menos que tenha transferido essas informações para o banco de dados associado ou outro(s) componente(s) seguro(s) do GPE.	**GIG1**
GIS-4.1.10	A Empresa de Jogos deve proteger a confidencialidade, integridade, disponibilidade e responsabilidade dos dados sensíveis quando mantidos em repouso em servidores, aplicações críticas e bancos de dados associados contendo dados sensíveis, incluindo limitar o número de estações de trabalho onde podem ser acessados.	**GIG2**
GIS-4.1.11	A criptografia deve ser aplicada para proteger a confidencialidade, integridade, disponibilidade e responsabilidade dos dados sensíveis quando estão em uso, quando armazenados em computadores portáteis (por exemplo, laptops, dispositivos USB, etc.) e quando permanecem em repouso em estações de trabalho.	**GIG2**
GIS-4.1.12	Dados sensíveis que não precisam ser ocultos, mas devem ser autenticados, devem usar algum tipo de técnica de autenticação de mensagens.	**GIG2**
GIS-4.1.13	A autenticação deve usar um certificado de segurança de uma autoridade confiável, contendo informações sobre a quem pertence, por quem foi emitido, datas válidas, um número de série único ou outra identificação única que possa ser usada para verificar o conteúdo do certificado.	**GIG1**

GIS-4.1.14	Bancos de dados de produção contendo dados sensíveis devem residir em redes separadas dos servidores que hospedam interfaces de patrono.	**GIG1**
GIS-4.1.15	Dados sensíveis devem ser mantidos o tempo todo, independentemente de o servidor estar sendo alimentado ou não.	**GIG1**
GIS-4.1.16	Medidas de prevenção de vazamento de dados sensíveis devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que processem, armazenem ou transmitam dados sensíveis.	**GIG2**
GIS-4.1.17	Dados sensíveis devem ser armazenados de forma a evitar a perda dos dados ao substituir peças ou módulos durante a manutenção normal.	**GIG1**
GIS-4.1.18	A alteração de quaisquer dados sensíveis não deve ser permitida sem controles de acesso supervisionados. Caso algum dado sensível seja alterado, as seguintes informações devem ser documentadas ou registradas: a. A data e hora da alteração; b. Identificação dos dados sensíveis alterada; c. Motivo e descrição da alteração dos dados sensíveis, incluindo valores iniciais e finais; e d. IDs de conta de usuário que realizou e/ou autorizou a alteração.	**GIG1**
GIS-4.1.19	Qualquer perda irrecuperável de dados sensíveis deve ser registrada em um registro de auditoria, indicando; a. A data e hora da perda; b. Identificação dos dados sensíveis perdidos; e c. Motivo e descrição dos dados sensíveis perdidos.	**GIG1**
GIS-4.1.20	O mascaramento de dados sensíveis deve ser aplicado de acordo com a política de controle de acesso da Empresa de Jogos e políticas relacionadas, com base nos requisitos comerciais e de segurança, e em conformidade com as regulamentações e padrões aplicáveis exigidos pelo Órgão Regulador.	**GIG1**
GIS-4.1.21	Acordos de confidencialidade ou confidencialidade (NDAs) alinhados aos requisitos sensíveis de proteção de dados da Empresa de Jogos devem ser identificados, formalmente documentados, revisados anualmente e executados por todo o pessoal relevante.	**GIG1**
GIS-4.1.22	A Empresa de Jogos deve implementar controles para garantir a exclusão segura de dados regulamentados ou sensíveis, de acordo com as leis, regulamentos, padrões e exigências contratuais aplicáveis. Os processos de exclusão devem ser verificáveis, auditáveis e comprovadamente eficazes para proteger contra recuperação não autorizada.	**GIG1**
GIS-4.2	**Implementação do Processo de Backup**	
GIS-4.2.1	A implementação do processo de backup deve ocorrer pelo menos diariamente ou conforme especificado pelo Órgão Regulador, embora todos os métodos devam ser revisados caso a caso.	**GIG1**
GIS-4.2.2	Dados sensíveis, aplicações críticas e bancos de dados associados devem ser respaldados com salvaguardas de imutabilidade para evitar alterações ou exclusões, garantindo a integridade do GPE.	**GIG1**
GIS-4.2.3	Cópias espelhadas ou redundantes de dados sensíveis devem ser mantidas no GPE com suporte aberto para backups e restauração.	**GIG1**
GIS-4.2.4	O backup deve estar contido em um meio físico não volátil, ou em uma implementação arquitetônica equivalente.	**GIG1**
GIS-4.2.5	Se os HHDs forem usados como armazenamento de backup, a integridade dos dados deve ser garantida em caso de falha no disco.	**GIG1**
GIS-4.2.6	Após a conclusão do processo de backup, o armazenamento de backup é imediatamente transferido para um local fisicamente separado do local que abriga os servidores e dados sensíveis que estão sendo feitos backup (para armazenamento temporário e permanente).	**GIG1**
GIS-4.2.7	O local de armazenamento de backup deve ser protegido para evitar acessos não autorizados e oferece proteção adequada para evitar a perda permanente de quaisquer dados sensíveis.	**GIG1**
GIS-4.2.8	Se o backup for armazenado em uma plataforma em nuvem, outra cópia pode ser armazenada em uma plataforma ou região em nuvem diferente.	**GIG2**
GIS-4.2.9	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 GPE.	**GIG1**
GIS-4.2.10	A Empresa de Jogos deve implementar controles para garantir que um backup falhe, havendo um plano claro de ação para resolver a falha.	**GIG1**
GIS-4.2.11	De acordo com o processo de backup acordado, arquivos de dados de backup e componentes de recuperação de dados devem ser mantidos, protegidos e testados pelo menos anualmente ou conforme especificado pelo Órgão Regulador.	**GIG2**

GIS-4.3	**Falha do Sistema e Recuperação**	
GIS-4.3.1	O GPE deve ter redundância e modularidade suficientes para que, se qualquer Componente Crítico do Sistema ou parte de um componente falhar, as funções do GPE e o processo de auditoria dessas funções possam continuar sem perda ou corrupção de dados sensíveis.	**GIG1**
GIS-4.3.2	Períodos significativos de indisponibilidade de qualquer Componente Crítico do Sistema (qualquer período de tempo de operações é interrompido para todos os usuários e/ou transações não podem ser concluídas com sucesso para nenhum usuário) devem ser registrados em um registro de auditoria, indicando; a. Identificação do componente indisponível; b. A data e hora em que o componente ficou indisponível; c. Motivo e descrição da indisponibilidade dos componentes; e d. A data e hora em que o componente voltou a estar disponível.	**GIG1**
GIS-4.3.3	Quando dois ou mais Componentes Críticos do Sistema são conectados, deve haver um procedimento para que os componentes sejam testados após a instalação, mas antes do uso em um GPE.	**GIG1**
GIS-4.3.4	O processo de todas as operações de jogo entre os Componentes Críticos do Sistema não deve ser prejudicado pela reinicialização ou recuperação de qualquer componente (por exemplo, transações não devem ser perdidas ou duplicadas devido à recuperação de um componente ou outro).	**GIG1**
GIS-4.3.5	Ao reiniciar ou recuperar, os Componentes Críticos do Sistema devem sincronizar imediatamente o status de todas as transações, dados sensíveis e configurações entre si.	**GIG1**
GIS-4.4	**Plano de Continuidade dos Negócios e Recuperação de Desastres**	
GIS-4.4.1	Um plano de continuidade de negócios e recuperação de desastres deve estar em vigor para recuperar as operações de jogo caso o GPE seja tornado inoperante, incluindo, mas não se limitando a: a. restauração de backup de dados; b. Restauração do programa; e c. Restauração de hardware redundante ou de backup.	**GIG1**
GIS-4.4.2	O plano de continuidade de negócios e recuperação de desastres deve considerar desastres incluindo, mas não se limitando a, aqueles causados por clima, água, enchentes, incêndios, derramamentos e acidentes ambientais, destruição maliciosa, atos de terrorismo, guerra e contingências como greves, epidemias, pandemias, etc.	**GIG1**
GIS-4.4.3	O plano de continuidade do negócio e recuperação de desastres deve abordar o método de armazenamento de dados sensíveis para minimizar perdas. Se for usada a replicação assíncrona, o método para recuperar informações deve ser descrito ou a possível perda de informação deve ser documentada.	**GIG2**
GIS-4.4.4	O plano de continuidade do negócio e recuperação de desastres deve delinear as circunstâncias sob as quais será invocado.	**GIG1**
GIS-4.4.5	O plano de continuidade do negócio e recuperação de desastres deve tratar do estabelecimento de um local de recuperação fisicamente separado do local de produção. A distância entre os dois locais deve ser determinada com base em potenciais ameaças e perigos ambientais, falhas de energia e outras interrupções, mas também deve considerar a dificuldade potencial de replicação dos dados, bem como a possibilidade de acessar o local de recuperação dentro de um tempo razoável.	**GIG3**
GIS-4.4.6	O plano de continuidade de negócios e recuperação de desastres deve conter guias de recuperação detalhando as etapas técnicas necessárias para restabelecer a funcionalidade de jogos no local de recuperação e deve definir o seguinte: c. Um Objetivo de Ponto de Recuperação (RPO), para garantir que dados sensíveis possam ser restaurados a um ponto aceitável no tempo; e d. Um Objetivo de Tempo de Recuperação (RTO), para garantir que a restauração seja concluída dentro de um período aceitável.	**GIG1**
GIS-4.4.7	O plano de continuidade do negócio e recuperação de desastres deve abordar os processos necessários para retomar as operações administrativas das atividades de jogo após a ativação do sistema recuperado para uma variedade de cenários apropriados ao contexto operacional do sistema.	**GIG1**

GIS-4.4.8	O plano de continuidade do negócio e recuperação de desastres deve ser testado pelo menos anualmente ou conforme especificado pelo órgão regulador. Os resultados dos testes devem ser documentados.	**GIG1**
GIS-5	**Comunicações**	**GIG**
GIS-5.1	**Protocolo de Comunicação**	
GIS-5.1.1	Cada Componente Crítico do Sistema do GPE deve funcionar conforme indicado por um protocolo de comunicação seguro documentado.	**GIG1**
GIS-5.1.2	Todos os protocolos devem usar técnicas de comunicação que possuam mecanismos adequados de detecção e recuperação de erros, projetados para evitar intrusões, interferências, escutas, alterações não autorizadas e adulteração. Quaisquer implementações alternativas devem ser analisadas caso a caso e aprovadas pelo Órgão Regulador.	**GIG1**
GIS-5.1.3	Todas as comunicações críticas de dados sensíveis devem empregar criptografia e autenticação para garantir integridade.	**GIG1**
GIS-5.1.4	As comunicações na rede segura só devem ser possíveis entre Componentes Críticos do Sistema autorizados que tenham sido registrados e autenticados como válidos na rede. Não é permitida comunicação não autorizada para componentes e/ou pontos de acesso.	**GIG1**
GIS-5.1.5	As comunicações devem ser reforçadas para serem imunes a todos os possíveis ataques de mensagens malformadas.	**GIG1**
GIS-5.1.6	A falha nas comunicações não deve afetar a integridade dos dados sensíveis.	**GIG1**
GIS-5.1.7	Após uma interrupção ou desligamento do sistema, a comunicação com todos os Componentes Críticos do Sistema necessários para a operação do GPE não deve ser estabelecida e autenticada até que a rotina de retomada do programa, incluindo quaisquer autotestes, seja concluída com sucesso.	**GIG1**
GIS-5.2	**Comunicações pela Internet/Redes Públicas**	
GIS-5.2.1	As comunicações entre quaisquer Componentes Críticos do Sistema que ocorram por internet/redes públicas devem ser protegidas contra atividades fraudulentas, disputas contratuais e divulgação e modificação não autorizadas por meio da criptografia dos pacotes de dados ou utilizando um protocolo de comunicação seguro para garantir a confidencialidade, integridade, disponibilidade e responsabilidade da transmissão.	**GIG1**
GIS-5.2.2	Dados sensíveis devem sempre ser criptografados pela internet/rede pública e protegidos contra transmissões incompletas, roteamento incorreto, modificação não autorizada de mensagens, divulgação, duplicação ou reprodução.	**GIG1**
GIS-5.3	**Comunicações de Rede Local Sem Fio (WLAN)**	
GIS-5.3.1	O uso de comunicações WLAN deve ser seguro e usado apenas quando apropriado e não em áreas onde possa ser potencialmente prejudicial.	**GIG1**
GIS-5.3.2	As comunicações entre dispositivos sem fio na WLAN devem usar protocolos projetados para proteger, autenticar e criptografar redes sem fio.	**GIG1**
GIS-5.3.3	A Autenticação Multifator (MFA) deve ser exigida no nível da rede sem fio e do dispositivo.	**GIG1**
GIS-5.3.4	Esquemas de autenticação que utilizam Infraestrutura de Chave Pública (PKI) devem exigir validação de certificados, idealmente em ambas as direções (por exemplo, certificados de cliente).	**GIG1**
GIS-5.3.5	Padrões Avançados de Criptografia (AES) ou equivalentes com um mínimo de criptografia de 256 bits devem ser usados para suportar serviços de integridade e confidencialidade.	**GIG1**
GIS-5.3.6	A Chave Mestra Pairwise (PMK) utilizada deve ter uma vida útil de vinte e quatro horas ou menos. Alternativamente, é aceitável que o PMK seja alterado durante o tempo de inatividade pré-programado de manutenção de acordo com os Controles GIS adotados pela Empresa de Jogos.	**GIG1**
GIS-5.3.7	A Chave Mestra de Grupo (GMK) utilizada deve ter uma vida útil de oito horas ou menos.	**GIG1**
GIS-5.3.8	A Privacidade Equivalente por Cabo (WEP) não deve ser utilizada. Se não for possível para o GPE usar o protocolo WPA2, a implementação do WEP como método seguro de criptografia e autenticação deve ser revisada caso a caso.	**GIG1**
GIS-5.3.9	Um dos seguintes protocolos de tunelamento criptografado ou equivalente deve ser utilizado para garantir a comunicação de todos os dados sensíveis pela WLAN: a. Protocolo de Autenticação Protegida Extensível (EAP Protegido ou PEAP); b. Protocolo de Autenticação Extensível - Segurança da Camada de Transporte (EAP-TLS); c. Protocolo de Autenticação Extensível - Segurança da Camada de Transporte Tunelada (EAP-TTLS);	**GIG1**

	d. Rede Privada Virtual (VPN) com L2TP/IPsec; e. Protocolo de Tunelamento Ponto a Ponto (PPTP); ou f. Camada de Soquetes Seguros (SSL).	
GIS-5.3.10	Os protocolos de tunelamento criptografados devem ser autenticados contra o Protocolo Leve de Acesso a Diretórios (LDAP), Remote Authentication Dial In User Service (RADIUS), servidores Kerberos ou Microsoft Active Directory ou equivalentes, bem como bancos de dados locais armazenados no controlador seguro do gateway.	**GIG1**
GIS-5.4	**Pontos de Acesso Sem Fio (WAP)**	
GIS-5.4.1	Um WAP permite que dispositivos sem fio se conectem a uma rede cabeada usando transporte sem fio (por exemplo, Wi-Fi) e retransmitam dados entre o(s) dispositivo(s) sem fio e o restante da rede.	**GIG1**
GIS-5.4.2	O login e senha padrão de administração devem ser alterados do padrão de fábrica para um valor seguro controlado pela Empresa de Jogos.	**GIG1**
GIS-5.4.3	A senha padrão da rede deve ser alterada do padrão de fábrica para um valor seguro controlado de acordo com a Empresa de Jogos.	**GIG1**
GIS-5.4.4	O Identificador do Conjunto de Serviços (SSID) deve ser alterado do padrão de fábrica para um valor seguro que não contenha nenhuma referência ao nome do local, fabricante ou qualquer outra referência que possa ser facilmente discernida.	**GIG1**
GIS-5.4.5	O acesso às funções administrativas do WAP deve ser restrito a conexões do lado cabeado da rede utilizando um protocolo seguro com uma conta de usuário privilegiada definida pela Empresa de Jogos.	**GIG1**
GIS-5.4.6	Se o roteador suportar autenticação WPA2, todos os WAPs devem estar compatíveis com IEEE 802.11 e configurados com o Modo Empresarial ativado ou com uma chave pré-compartilhada forte.	**GIG1**
GIS-5.5	**Equipamento de Comunicação de Rede (NCE)**	
GIS-5.5.1	A Empresa de Jogos deve fornecer um local seguro para a colocação, operação e uso da NCE.	**GIG1**
GIS-5.5.2	A NCE deve ser instalada de acordo com um plano definido e os registros de todas as NCE instaladas devem ser mantidos.	**GIG1**
GIS-5.5.3	A NCE deve ser construída de forma a ser resistente a danos físicos ao hardware ou corrupção do software contido pelo uso normal.	**GIG1**
GIS-5.5.4	A NCE deve ser fisicamente protegida contra acessos não autorizados.	**GIG1**
GIS-5.5.5	As comunicações GPE via NCE devem ser logicamente protegidas contra acessos não autorizados.	**GIG1**
GIS-5.5.6	O NCE com armazenamento interno limitado deve, se o log de auditoria ficar cheio, desabilitar toda comunicação ou transferir os logs de auditoria para um servidor dedicado de logs de auditoria.	**GIG1**
GIS-5.6	**Sistema de Detecção de Intrusões/Sistema de Prevenção de Intrusão (IDS/IPS)**	
GIS-5.6.1	Um IDS/IPS deve ser instalado, incluindo um ou mais componentes capazes de ouvir tanto comunicações internas quanto externas, bem como detectar ou impedir: a. Ataques de Negação de Serviço Distribuída (DDoS); b. Shellcode da travessia da rede; c. Protocolo de Resolução de Endereços (ARP) falsificação; e d. Outros indicadores de ataque "Man-In-The-Middle" e cortam comunicações imediatamente se detectados.	**GIG1**
GIS-5.6.2	O IDS/IPS deve escanear a rede em busca de pontos de acesso ou dispositivos não autorizados ou não autorizados ou não autorizados conectados a qualquer ponto de acesso na rede pelo menos trimestralmente ou conforme especificado pelo Órgão Regulador.	**GIG2**
GIS-5.6.3	O IDS/IPS deve desabilitar automaticamente qualquer dispositivo não autorizado ou desonesto conectado ao GPE.	**GIG2**
GIS-5.6.4	O IDS/IPS deve manter um registro de auditoria para acesso, que deve: a. Conter informações completas e abrangentes sobre todos os dispositivos envolvidos, incluindo a hora e data, o nome e o identificador de hardware de todos os dispositivos que solicitam acesso à rede; e b. Ser capaz de ser reconciliado com todos os outros dispositivos de rede dentro do GPE.	**GIG1**

GIS-5.7	**Gerenciamento de Segurança de Rede**	
GIS-5.7.1	A Empresa de Jogos deve revisar e atualizar políticas e procedimentos para garantir que a rede seja segura e que ameaças e vulnerabilidades sejam tratadas de acordo.	**GIG1**
GIS-5.7.2	As redes devem ser logicamente separadas de modo que não haja tráfego de rede em um enlace de rede que não possa ser atendido por hosts nesse link.	**GIG1**
GIS-5.7.3	Todas as funções de gerenciamento de rede devem autenticar todos os usuários na rede e criptografar todas as comunicações de gerenciamento de rede.	**GIG1**
GIS-5.7.4	A falha de qualquer item isolado não pode resultar em negação de serviço.	**GIG1**
GIS-5.7.5	Todos os pontos de entrada e saída da rede devem ser identificados, gerenciados, controlados e monitorados 24 horas por dia, 7 dias por semana.	**GIG2**
GIS-5.7.6	Todos os hubs de rede, serviços e portas de conexão devem ser protegidos para evitar acessos não autorizados à rede.	**GIG1**
GIS-5.7.7	Serviços não utilizados e portas não essenciais devem ser fisicamente bloqueados ou desativados pelo software sempre que possível.	**GIG1**
GIS-5.7.8	Protocolos criptográficos aprovados devem ser usados para dados sensíveis que ofereçam autenticação, confidencialidade, integridade, disponibilidade e responsabilidade, como TLS (Transport Layer Security) ou HTTPS (Hypertext Transport Protocol Secure). Protocolos sem estado, como o UDP (User Datagram Protocol), não devem ser usados sem transporte com estado. Em vez disso,	**GIG1**
GIS-5.7.9	Todas as alterações na infraestrutura de rede devem ser registradas em um registro de auditoria, indicando: a. A data e hora das mudanças; b. Motivo e descrição das mudanças, incluindo valores iniciais e finais; e c. IDs(s) de conta de usuário que realizou e/ou autorizou as alterações.	**GIG1**
GIS-5.8	**Teletrabalho e Computação Móvel**	
GIS-5.8.1	O teletrabalho só deve ser permitido em circunstâncias em que a segurança do endpoint possa ser assegurada. Funcionários que trabalham remotamente devem usar dispositivos gerenciados pela Empresa de Jogos, conectar-se apenas por métodos seguros aprovados e proteger tanto o acesso físico quanto digital a dados sensíveis.	**GIG1**
GIS-5.8.2	Uma política formal deve estar em vigor, e medidas de segurança de apoio devem ser adotadas para proteger contra os riscos do uso de computação móvel e facilidades de comunicação.	**GIG1**
GIS-6	**Provedores de Serviços**	**GIG**
GIS-6.1	**Relacionamentos com Provedores de Serviços**	
GIS-6.1.1	A alocação de responsabilidade entre um Provedor de Serviços e as outras entidades dentro da Empresa de Jogos para gerenciar os Controles GIS não isenta uma Empresa de Jogos da responsabilidade de garantir que dados sensíveis estejam devidamente protegidos conforme os requisitos aplicáveis.	**GIG1**
GIS-6.1.2	Quando dados sensíveis são compartilhados com Provedores de Serviços, devem existir acordos formais de processamento de dados que declarem os direitos e obrigações de cada parte em relação à proteção dos dados sensíveis, incluindo: a. O tema e a duração do processamento; b. A natureza e o propósito do processamento; c. O tipo de dados a serem processados; d. Como os dados são armazenados; e. O detalhe da segurança em torno dos dados; f. Os meios usados para transferir os dados de uma Empresa de Jogos para outra; g. Os meios usados para recuperar dados sobre determinados indivíduos; h. O método para garantir que um cronograma de retenção seja seguido; i. Os meios usados para excluir ou descartar os dados; e j. As categorias de dados.	**GIG1**
GIS-6.2	**Comunicações com Provedores de Serviço**	
GIS-6.2.1	O GPE deve ser capaz de se comunicar de forma segura com os Provedores de Serviços usando criptografia e autenticação forte.	**GIG1**
GIS-6.2.2	Todos os eventos de login envolvendo Provedores de Serviço devem ser registrados em um registro de auditoria.	**GIG1**

GIS-6.2.3	A comunicação com os Provedores de Serviço não deve interferir ou degradar as funções normais do GPE.	**GIG1**
GIS-6.2.4	Os dados do Provedor de Serviço não devem afetar as comunicações dos usuários.	**GIG1**
GIS-6.2.5	Os Provedores de Serviço devem estar em uma rede segmentada separada dos segmentos de rede que hospedam conexões de usuários.	**GIG1**
GIS-6.2.6	Jogos devem ser desativados em todas as conexões de rede, exceto aquelas dentro do GPE.	**GIG1**
GIS-6.2.7	O GPE não deve rotear pacotes de dados dos Provedores de Serviço diretamente para o GPE e vice-versa.	**GIG1**
GIS-6.2.8	O GPE não deve atuar como roteador IP entre o GPE e os Provedores de Serviço.	**GIG1**
GIS-6.2.9	Provedores de Serviço Não Autorizados devem ser impedidos de visualizar ou alterar dados sensíveis.	**GIG1**
GIS-7	**Controles Técnicos**	**GIG**
GIS-7.1	**Requisitos do Serviço de Nomes de Domínio (DNS)**	
GIS-7.1.1	A Empresa de Jogos deve utilizar um servidor DNS primário seguro e um servidor DNS secundário seguro, que sejam logicamente e fisicamente separados entre si, aumentando a resiliência contra pontos únicos de falha e potenciais ataques.	**GIG2**
GIS-7.1.2	O servidor DNS primário deve estar fisicamente localizado em um data center seguro ou em um host virtualizado em um hipervisor devidamente protegido ou equivalente para evitar acessos não autorizados.	**GIG2**
GIS-7.1.3	O acesso lógico e físico aos servidores DNS deve ser restrito a pessoal autorizado por meio da Autenticação Multifator (MFA), garantindo que apenas usuários autenticados possam acessar os servidores DNS e que os registros DNS sejam mantidos seguros contra alterações maliciosas e não autorizadas.	**GIG2**
GIS-7.1.4	Transferências de zona para hospedeiros arbitrários devem ser desautorizadas. Essa restrição impede que partes não autorizadas acessem ou repliquem dados da zona DNS, reduzindo o risco de exposição ou manipulação de dados.	**GIG2**
GIS-7.1.5	É necessário um método para prevenir envenenamento do cache, como as Extensões de Segurança DNS (DNSSEC).	**GIG2**
GIS-7.1.6	O bloqueio do registro do lado do cliente deve estar em funcionamento, então qualquer solicitação para mudar de servidor(es) DNS, precisará ser verificada manualmente.	**GIG2**
GIS-7.2	**Controles Criptográficos**	
GIS-7.2.1	Uma política sobre o uso de controles criptográficos para a proteção de dados sensíveis deve ser desenvolvida e implementada, garantindo que todos os controles criptográficos utilizem módulos criptográficos para execução e proteção seguras.	**GIG1**
GIS-7.2.2	O grau de criptografia utilizado deve ser apropriado à sensibilidade dos dados.	**GIG1**
GIS-7.2.3	O uso de métodos de criptografia deve ser revisado pelo menos anualmente ou conforme especificado pelo órgão regulador para verificar se os algoritmos de criptografia atuais e os comprimentos das chaves estão seguros.	**GIG1**
GIS-7.2.4	O método de criptografia deve incluir o uso de diferentes chaves de criptografia para que os algoritmos de criptografia possam ser alterados ou substituídos para corrigir fraquezas o mais rápido possível. Outras metodologias devem ser revisadas caso a caso.	**GIG1**
GIS-7.2.5	O gerenciamento das chaves de criptografia ao longo de todo o seu ciclo de vida deve seguir processos definidos estabelecidos pela Empresa de Jogos.	**GIG1**
GIS-7.2.6	A Empresa de Jogos deve estabelecer procedimentos para obter ou gerar chaves de criptografia, garantindo que apenas pessoal autorizado esteja envolvido no processo.	**GIG1**
GIS-7.2.7	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 e/ou usando uma chave de criptografia diferente.	**GIG1**
GIS-7.2.8	Procedimentos devem ser estabelecidos para monitorar as datas de expiração das chaves de criptografia, quando aplicável.	**GIG1**
GIS-7.2.9	Procedimentos devem ser definidos para revogar prontamente as chaves de criptografia em caso de comprometimento, perda ou acesso não autorizado.	**GIG1**
GIS-7.2.10	Procedimentos devem ser estabelecidos para alterar com segurança o conjunto de chaves de criptografia atual, incluindo a geração de novas chaves e a aposentadoria de chaves antigas.	**GIG1**

GIS-7.2.11	A Empresa de Jogos deve implementar procedimentos para recuperar dados protegidos com chaves de criptografia revogadas ou expiradas por um período definido após as chaves se tornarem inválidas.	**GIG1**
GIS-7.3	**Endurecimento de Componentes Críticos do Sistema**	
GIS-7.3.1	Configurações críticas de Componentes do Sistema devem ser estabelecidas, documentadas, implementadas, monitoradas e revisadas.	**GIG1**
GIS-7.3.2	Os procedimentos de configuração para Componentes Críticos do Sistema devem abordar todas as vulnerabilidades de segurança conhecidas e ser consistentes com as melhores práticas aceitas pela indústria para reforço do sistema.	**GIG1**
GIS-7.3.3	A adequação e eficácia das medidas tomadas para endurecer os Componentes Críticos do Sistema devem ser avaliadas pelo menos anualmente ou conforme especificado pelo Órgão Regulador e, se apropriado, mudanças devem ser feitas para melhorar o endurecimento.	**GIG2**
GIS-7.3.4	Todos os parâmetros padrão ou de configuração padrão devem ser removidos de todos os Componentes Críticos do Sistema quando um risco de segurança é apresentado.	**GIG1**
GIS-7.3.5	Apenas uma função primária deve ser implementada por servidor para evitar que funções que exigem diferentes níveis de segurança coexistam no mesmo servidor.	**GIG1**
GIS-7.3.6	Recursos adicionais de segurança devem ser implementados para quaisquer serviços, protocolos ou daemons necessários considerados inseguros.	**GIG1**
GIS-7.3.7	Os parâmetros de segurança do sistema devem ser configurados para evitar uso indevido.	**GIG1**
GIS-7.3.8	Todas as funcionalidades desnecessárias devem ser removidas, como scripts, drivers, recursos, subsistemas, sistemas de arquivos e servidores web desnecessários.	**GIG1**
GIS-7.4	**Geração e Armazenamento de Relatórios ou Logs de Segurança**	
GIS-7.4.1	Relatórios ou logs de segurança devem ser pré-definidos e gerados em cada Componente Crítico do Sistema para monitorar e corrigir anomalias, falhas e alertas.	**GIG1**
GIS-7.4.2	Relatórios ou registros de segurança devem ser protegidos contra adulteração e acesso não autorizado.	**GIG2**
GIS-7.4.3	Relatórios ou registros de segurança devem ser revisados pelo menos a cada noventa dias ou conforme especificado pelo Órgão Regulador.	**GIG1**
GIS-8	**Acesso Remoto e Firewalls**	**GIG**
GIS-8.1	**Segurança de Acesso Remoto**	
GIS-8.1.1	A segurança do acesso remoto deve ser revisada caso a caso, em conjunto com a implementação da tecnologia atual e a aprovação do Órgão Regulador.	**GIG1**
GIS-8.1.2	Os métodos de acesso remoto devem ser devidamente protegidos e gerenciados.	**GIG1**
GIS-8.1.3	O GPE deve ter a capacidade de habilitar ou desativar o acesso remoto, e o estado padrão deve ser configurado como desativado.	**GIG1**
GIS-8.1.4	O acesso remoto deve aceitar apenas as conexões remotas permitidas pela aplicação do firewall e pelas configurações do sistema.	**GIG1**
GIS-8.1.5	O acesso remoto deve ser limitado apenas às funções da aplicação necessárias para que os usuários desempenhem suas funções de trabalho.	**GIG1**
GIS-8.1.6	Não é permitida nenhuma funcionalidade não autorizada de administração remota de usuários (adicionar usuários, alterar permissões, etc.).	**GIG1**
GIS-8.1.7	O acesso remoto não autorizado ao sistema operacional ou a qualquer banco de dados que não seja a recuperação de informações usando funções existentes é proibido.	**GIG1**
GIS-8.1.8	O GPE deve manter um registro de auditoria que retraga todas as informações e atividades de acesso remoto. Os logs de acesso remoto devem incluir, no mínimo, o seguinte: a. ID(s) de conta de usuário que realizou e/ou autorizou o acesso remoto, incluindo verificação de autorização; b. Endereços IP Remotos, Números de Porta, Protocolos e, quando possível, Endereços MAC; c. Hora e data da conexão e duração da conexão; d. Motivo do acesso remoto e descrição do trabalho a ser realizado; e e. Atividade enquanto estiver logado, incluindo as áreas específicas acessadas e as alterações feitas.	**GIG1**

GIS-8.2	**Segurança de Firewall**	
GIS-8.2.1	Todas as comunicações, incluindo o acesso remoto, devem passar por pelo menos um firewall aprovado em nível de aplicação. Isso inclui conexões para e de qualquer host não do sistema usado pela Empresa de Jogos.	**GIG1**
GIS-8.2.2	O firewall deve estar localizado na fronteira de quaisquer dois domínios de segurança diferentes.	**GIG1**
GIS-8.2.3	Um dispositivo no mesmo domínio de broadcast do host do sistema não deve ter uma funcionalidade que permita estabelecer um caminho alternativo de rede que contorne o firewall.	**GIG2**
GIS-8.2.4	Qualquer caminho alternativo de rede existente para fins de redundância também deve passar por pelo menos um firewall em nível de aplicação.	**GIG1**
GIS-8.2.5	Apenas aplicações relacionadas ao firewall podem residir no firewall.	**GIG1**
GIS-8.2.6	As contas de usuário no firewall devem ser limitadas (por exemplo, apenas administradores de rede ou sistema).	**GIG1**
GIS-8.2.7	O firewall deve rejeitar todas as conexões, exceto aquelas que foram especificamente aprovadas.	**GIG1**
GIS-8.2.8	O firewall deve rejeitar todas as conexões de destinos que não podem residir na rede de onde a mensagem se originou (por exemplo, endereços RFC1918 no lado público de um firewall de internet).	**GIG1**
GIS-8.2.9	O firewall deve permitir apenas acesso remoto usando criptografia e autenticação forte.	**GIG1**
GIS-8.2.10	O firewall deve ser capaz de registrar as seguintes informações em um log de auditoria de forma a preservar e proteger as informações contra perdas ou alterações: a. Todas as mudanças na configuração do firewall; b. Todas as tentativas de conexão bem-sucedidas e não bem-sucedidas através do firewall; e c. Os endereços IP de origem e destino, números de porta, protocolos e, quando possível, endereços MAC.	**GIG1**
GIS-8.2.11	Para tentativas de conexão malsucedidas pelo firewall, um parâmetro configurável pode ser utilizado para negar novas solicitações de conexão e notificar o administrador do sistema caso o limite predefinido seja ultrapassado.	**GIG1**
GIS-9	**Revisão de Ativos Críticos e Gestão de Mudanças**	**GIG**
GIS-9.1	**Gestão de Ativos**	
GIS-9.1.1	Todos os ativos físicos ou lógicos que abrigam, processam ou comunicam dados sensíveis, incluindo aqueles que compõem o GPE, devem ser contabilizados.	**GIG1**
GIS-9.1.2	Devem existir procedimentos para adicionar novos ativos e remover ativos do serviço.	**GIG1**
GIS-9.1.3	Deve haver uma política sobre o uso aceitável dos ativos associados ao GPE.	**GIG1**
GIS-9.1.4	O proprietário deGISnado de cada ativo deve: a. Garantir que as informações e os ativos sejam devidamente classificados com base em seus requisitos de confidencialidade, integridade, disponibilidade e responsabilidade; e b. Defina restrições e classificações de acesso com base nos critérios de classificação estabelecidos e no princípio do privilégio mínimo.	**GIG1**
GIS-9.1.5	Deve existir um procedimento para garantir que a responsabilidade registrada pelos ativos seja comparada com os ativos reais pelo menos anualmente ou em intervalos exigidos pelo Órgão Regulador, e que ações apropriadas sejam tomadas em relação a discrepâncias.	**GIG1**
GIS-9.1.6	Para garantir sua confidencialidade, integridade, disponibilidade e responsabilidade contínua das informações, os ativos devem ser devidamente mantidos, inspecionados e mantidos pelo menos anualmente ou em intervalos regulares exigidos pelo Órgão Regulador para garantir que estejam livres de defeitos ou mecanismos que possam interferir em sua operação.	**GIG1**
GIS-9.1.7	Os meios de armazenamento devem ser gerenciados ao longo de seu ciclo de vida de aquisição, uso, transporte e descarte, de acordo com o esquema de classificação e os requisitos de manuseio da Empresa de Jogos.	**GIG1**
GIS-9.1.8	Os bens devem ser descartados de forma segura e segura utilizando procedimentos documentados.	**GIG1**
GIS-9.1.9	Dados sensíveis armazenados em Componentes Críticos do Sistema, dispositivos ou qualquer outro meio de armazenamento devem ser excluídos quando não forem mais necessários.	**GIG1**
GIS-9.1.10	Antes de descartar ou reutilizar, os ativos contendo mídia de armazenamento devem ser verificados para garantir que qualquer software licenciado, bem como dados sensíveis, tenham sido removidos ou sobrescritos com segurança (ou seja, não apenas excluídos).	**GIG1**

GIS-9.2	**Registro de Ativos Críticos (CAR)**	
GIS-9.2.1	Um CAR deve ser desenvolvido e mantido para quaisquer ativos que afetem a funcionalidade do GPE ou influenciem a forma como dados sensíveis são armazenados/tratados pelo ambiente.	**GIG1**
GIS-9.2.2	A estrutura do CAR deve incluir componentes de hardware e software, bem como as inter-relações e dependências desses componentes.	**GIG1**
GIS-9.2.3	Os seguintes itens mínimos devem ser documentados no CAR para cada ativo: a. Um ID único atribuído a cada ativo individual; b. O nome/definição de cada ativo; c. Um número de versão do ativo listado; d. Identificação das características do ativo (por exemplo, componente do sistema, banco de dados, máquina virtual, hardware); e. O "proprietário" responsável pelo ativo; f. A localização geográfica dos ativos de hardware; e g. Códigos de relevância sobre o papel do ativo no cumprimento ou garantia dos critérios de classificação.	**GIG1**
GIS-9.2.4	Os critérios de classificação são os seguintes: a. Confidencialidade de dados sensíveis (por exemplo, informações de identificação e transações); b. Integridade do sistema, especificamente de qualquer ativo que afete a funcionalidade do sistema e/ou influencie como dados sensíveis são armazenados e/ou manuseados; c. Disponibilidade de dados sensíveis; e d. Responsabilidade pela atividade do usuário e quanta influência o ativo tem sobre a atividade do usuário.	**GIG1**
GIS-9.2.5	Cada um dos critérios de classificação deve receber um código de relevância com: a. 1 - Sem Relevância: O ativo não pode ter impacto negativo nos critérios; b. 2 - Alguma Relevância: O ativo pode impactar os critérios; ou c. 3 - Relevância Substancial: Os critérios estão relacionados ou dependem do ativo.	**GIG1**
GIS-9.3	**Programa de Gestão de Mudanças (CMP)**	
GIS-9.3.1	Um CMP deve ser implementado para lidar com atualizações do GPE e seus Componentes Críticos do Sistema, com base na propensão para atualizações frequentes do sistema e na tolerância ao risco escolhida. Para um GPE que exige atualizações frequentes, um CMP baseado em risco pode ser utilizado para proporcionar maior eficiência na implantação de atualizações. CMPs baseados em risco normalmente incluem uma categorização das mudanças propostas com base no impacto regulatório e definem procedimentos de certificação associados para cada categoria.	**GIG1**
GIS-9.3.2	Os procedimentos de mudança de programas devem ser adequados para garantir que apenas versões autorizadas dos programas e modificações sejam implementadas no GPE.	**GIG1**
GIS-9.3.3	Um mecanismo de controle de versão de software apropriado deve estar em vigor para todos os componentes do software, código-fonte e controles binários.	**GIG1**
GIS-9.3.4	Um Registro de Gerenciamento de Mudanças (CML) deve ser mantido de todas as novas instalações e/ou modificações no sistema, incluindo: a. A data da instalação ou modificação; b. Detalhes sobre o motivo ou natureza da instalação ou alteração, como novo software, reparo de servidores, modificações GISnificativas na configuração; c. O(s) componente(s) a ser alterado(s) incluindo o número de identificação único do CAR, informações de versão e, se o componente a ser alterado for hardware, a localização física desse componente; d. A identidade do(s) usuário(s) que realizam a instalação ou modificação; e e. A identidade do(s) usuário(s) responsável por autorizar a instalação ou modificação.	**GIG1**
GIS-9.3.5	A completude da LMC deve ser verificada pelo menos trimestralmente ou conforme especificado pelo Órgão Regulador.	**GIG1**
GIS-9.3.6	Uma estratégia deve ser estabelecida para cobrir o potencial de uma instalação malsucedida ou um problema de campo com uma ou mais mudanças implementadas. a. Quando uma parte externa, como uma App Store, é parte interessada no processo de lançamento, essa estratégia deve abranger o gerenciamento dos lançamentos por meio de uma parte externa. Essa estratégia pode considerar a gravidade do problema.	**GIG1**

	b. Caso contrário, essa estratégia deve cobrir a reversão da última implementação (plano de rollback), incluindo backups completos de versões anteriores de software e um teste do plano de rollback antes da implementação no GPE.	
GIS-9.3.7	Uma política que aborde procedimentos de mudança emergencial deve estar em vigor. Mudanças emergenciais devem ser aprovadas, testadas, documentadas e monitoradas.	**GIG1**
GIS-9.3.8	Procedimentos devem estar em vigor para testes e migração de mudanças, incluindo a identificação do pessoal autorizado para aprovação antes da liberação.	**GIG1**
GIS-9.3.9	Deve haver segregação de deveres dentro do processo de dispensação.	**GIG1**
GIS-9.3.10	A documentação técnica e do usuário deve ser mantida, como manuais e guias do usuário, descrevendo os sistemas em uso e a operação, incluindo hardware.	**GIG1**
GIS-9.3.11	Procedimentos devem estar em prática para garantir que a documentação técnica e do usuário seja atualizada como resultado de uma mudança.	**GIG1**
GIS-9.3.12	Mudanças dentro do GPE devem ser revisadas quanto ao risco-impacto antes ou após a implementação para determinar sua criticidade. Quaisquer mudanças categorizadas como críticas serão submetidas a Auditorias Adicionais de Controles GIS e Avaliações GTS realizadas por um ISF, conforme descrito na seção "Auditorias Adicionais" deste documento e na seção "Avaliações Adicionais" dentro do GLI-GSF-2. Essas auditorias e avaliações podem se concentrar especificamente nas mudanças críticas e nos Componentes Críticos do Sistema afetados por essas mudanças.	**GIG1**
GIS-9.4	**Ciclo de Vida do Desenvolvimento do Sistema**	
GIS-9.4.1	A aquisição e o desenvolvimento de novos softwares devem seguir processos definidos estabelecidos pela Empresa de Jogos e/ou pelo Órgão Regulador.	**GIG1**
GIS-9.4.2	O GPE deve estar logicamente e fisicamente separado dos ambientes de desenvolvimento e testes, de modo que nenhuma conexão direta entre o GPE e qualquer outro ambiente possa existir.	**GIG1**
GIS-9.4.3	A delegação de responsabilidades deve ser estabelecida, quando aplicável.	**GIG1**
GIS-9.4.4	A Empresa de Jogos deve estabelecer e documentar um método para desenvolver software de forma segura, que inclua o cumprimento dos padrões da indústria e das melhores práticas para programação.	**GIG1**
GIS-9.4.5	Considerações de GIS devem ser integradas ao longo de todo o ciclo de vida do desenvolvimento de software, desde a coleta inicial de requisitos até a implantação e manutenção.	**GIG1**
GIS-9.4.6	A metodologia de teste documentada deve incluir disposições para a. Verifique se o software de teste não está implantado no GPE; b. Selecionar, proteger e gerenciar adequadamente os dados de teste; e c. Evite o uso de dados sensíveis reais ou outros dados brutos de produção nos testes.	**GIG1**
GIS-9.4.9	Toda a documentação relacionada ao desenvolvimento de software e aplicações deve estar disponível e mantida durante todo o seu ciclo de vida.	**GIG1**
GIS-9.5	**Gerenciamento de Patches**	
GIS-9.5.1	A Empresa de Jogos deve ter políticas de gerenciamento de patches aprovadas pelo Órgão Regulador, seja desenvolvida e apoiada pela Empresa de Jogos.	**GIG1**
GIS-9.5.2	A Empresa de Jogos deve monitorar e aplicar patches a todos os Componentes Críticos do Sistema envolvidos na coleta, processamento, armazenamento e transmissão de dados sensíveis.	**GIG1**
GIS-9.5.3	Sempre que possível, todos os patches devem ser testados em um ambiente de desenvolvimento e testes configurado idênticamente ao GPE alvo.	**GIG1**
GIS-9.5.4	Em circunstâncias em que os testes de patch não podem ser realizados a tempo para cumprir os prazos do nível de gravidade do alerta, então os testes de patch devem ser gerenciados pelo risco, seja isolando ou removendo o componente não testado da rede, seja aplicando o patch e testando depois.	**GIG1**
GIS-9.6	**Software Desenvolvido/Modificado Internamente**	
GIS-9.6.1	Se o código-fonte do software for desenvolvido ou modificado internamente (software desenvolvido/modificado internamente), um processo é adotado para gerenciar o desenvolvimento ou modificação do software.	**GIG1**

GIS-9.6.2	Nenhum desenvolvimento ou modificação de software desenvolvido/modificado internamente pode começar sem autorização prévia da gestão de TI. As aprovações para iniciar o trabalho no software são documentadas.	**GIG1**
GIS-9.6.3	O software desenvolvido/modificado internamente não deve ser implementado ou utilizado em qualquer capacidade operacional até que o software tenha passado pelos procedimentos necessários de mudança de programa.	**GIG1**
GIS-9.6.4	A Empresa de Jogos deve demonstrar que a devida diligência foi realizada em todas as etapas do desenvolvimento e implementação do software desenvolvido internamente. Isso inclui: a. Um plano de projeto documentado; b. Requisitos técnicos e funcionais definidos; c. Protocolos de teste; d. Avaliações de segurança; e e. Procedimentos de verificação de software.	**GIG1**
GIS-9.6.5	Procedimentos operacionais detalhados devem ser desenvolvidos para: a. Como o software desenvolvido e modificado internamente é utilizado; b. Quais controles existem para garantir a precisão dos resultados; c. Quais relatórios são gerados; e d. Como as disputas são resolvidas;	**GIG1**
GIS-9.6.6	Uma função independente tanto da função de TI quanto dos usuários finais do software desenvolvido/modificado internamente deve ser responsável por verificar regularmente e após qualquer atualização ou alteração de configuração.	**GIG1**
GIS-9.6.7	Software desenvolvido/modificado internamente deve incluir ou estar sujeito a procedimentos que gerem e preservem: a. Arquivos de log abrangentes; b. histórico de acesso dos usuários; e c. Mude o rastreamento.	**GIG1**
GIS-9.6.8	O acesso ao software desenvolvido ou modificado internamente deve ser restrito por: a. Mecanismos internos de controle de acesso; ou b. Fiscalização externa via permissões de rede e controles GIS.	**GIG1**
GIS-9.6.9	Os direitos de acesso para o software desenvolvido/modificado internamente devem ser documentados e revisados pelo menos trimestralmente.	**GIG1**
GIS-9.6.10	Relatórios gerados pelo software desenvolvido ou modificado internamente devem: a. Ser arquivado de acordo com as políticas de retenção de dados do Órgão Regulador; b. Esteja disponível para inspeção; e c. Inclua dados resumidos e exceções quando aplicável.	**GIG1**
GIS-9.6.11	O software desenvolvido/modificado internamente deve incluir um plano separado de backup e recuperação de desastres documentado e testado. O plano deve incluir: a. Frequência de backups de dados; b. Armazenamento seguro fora do local ou baseado em nuvem; e c. Procedimentos de restauração.	**GIG1**
GIS-9.6.12	Softwares desenvolvidos/modificados internamente usados em qualquer função que possa afetar os resultados para os patronos (por exemplo, promoções, acompanhamento de fidelidade, sorteios) devem incluir um método documentado para: a. Revisão de registros relevantes; b. Reconstruir o comportamento de software desenvolvido/modificado internamente; e c. Reportando as conclusões ao Órgão Regulador.	**GIG1**
GIS-9.6.13	Para manutenção e mitigação do risco de rotatividade de pessoal, a Empresa de Jogos deve possuir: a. Documentação suficiente para permitir suporte contínuo ao software desenvolvido/modificado internamente na ausência do desenvolvedor original; b. Um plano de sucessão para suporte e desenvolvimento contínuos; e c. Procedimentos de controle de versão para gerenciar atualizações.	**GIG1**

DEFINIÇÕES DE TERMOS

Mandato	Descrições
Acesso	Capacidade de usar qualquer recurso de GPE.
Controle de Acesso	O processo de conceder ou negar solicitações específicas para obter e usar dados sensíveis e serviços relacionados específicos a um sistema; e para entrar em instalações físicas específicas que abrigam infraestrutura crítica de rede ou sistema.
Protocolo de Resolução de Endereços (ARP)	O protocolo usado para traduzir endereços IP em endereços MAC para suportar comunicação em uma rede local sem fio ou cabeada.
Controles Administrativos	Políticas, procedimentos e diretrizes implementados por uma Empresa de Jogos para gerenciar seus GISMS.
Padrões Avançados de Criptografia (AES)	Uma cifra de bloco simétrica que pode criptografar (cifrar) e descriptografar (decifrar) informações.
Algoritmo	Um conjunto finito de instruções inequívocas executadas em uma sequência prescrita para alcançar um objetivo, especialmente uma regra ou procedimento matemático usado para calcular um resultado desejado. Algoritmos são a base da maior parte da programação de computadores.
Aplicação	Software de computador projetado para ajudar o usuário a realizar uma tarefa específica.
Registro de Auditoria	Um registro auditável de ações, eventos ou mudanças dentro de um GPE, capturando detalhes como atividades dos usuários, tentativas de acesso, alterações e operações do sistema para garantir segurança, conformidade e responsabilidade durante um determinado período.
Autenticação	Verificar a identidade de um usuário, processo, pacote de software ou dispositivo, geralmente como pré-requisito para permitir o acesso aos recursos do GPE.
Credenciais de Autenticação	Quaisquer senhas, autenticação multifator, certificados digitais, PINs, biometria, perguntas e respostas de segurança, e quaisquer outros métodos de acesso à conta (por exemplo, deslizamento magnético, cartões de proximidade, chips embutidos).
Disponibilidade	Garantir acesso e uso oportuno e confiável das informações.
Reserva	Uma cópia de arquivos e programas feitos para facilitar a recuperação, se necessário.
Biometria	Uma entrada de identificação biológica, como impressões digitais, padrões da retina, dados de reconhecimento facial ou impressões de voz.
Aplicações de Negócios	Aplicativos que operam como um serviço compartilhado para que os usuários coletem, processem, mantenham e utilizem, compartilhem, disseminem ou descartem dados sensíveis dentro do GPE para fins de auditoria de conformidade e resposta a incidentes GIS.
Plano de Continuidade dos Negócios e Recuperação de Desastres	Um plano para processar aplicações críticas e prevenir a perda de dados em caso de falha grave de hardware ou software ou destruição de instalações.
Envenenamento de cache	Um ataque em que o atacante insere dados corrompidos no banco de dados de cache do Serviço de Nomes de Domínio (DNS).
Conforme	A política e as evidências analisadas foram consideradas totalmente em conformidade com a GLI-GSF.
Confidencialidade	Preservar restrições autorizadas ao acesso e divulgação de informações, incluindo meios para proteger a privacidade pessoal e informações proprietárias.
Plano de Contingência	Política e procedimentos de gestão projetados para manter ou restaurar as operações de jogo, possivelmente em um local alternativo, em caso de emergências, falhas de sistema ou desastres.
Programa de Controle Crítico	Programas de software que controlam comportamentos relativos a qualquer padrão técnico e/ou requisito regulamentar aplicável, como executáveis, bibliotecas, configurações de jogos ou de sistema, arquivos do sistema

Mandato	Descrições
	operacional, componentes que controlam relatórios necessários do sistema e elementos de banco de dados que afetam jogos ou operações do sistema.
Componente Crítico do Sistema	Qualquer hardware, software, programas críticos de controle, tecnologia de comunicação, outros equipamentos ou componentes implementados em um GPE para permitir a participação do usuário em jogos, e cujo fracasso ou comprometimento podem levar à perda de direitos do usuário, receita do governo ou acesso não autorizado a dados usados para gerar relatórios para o Órgão Regulador. Exemplos de Componentes Críticos do Sistema incluem, mas não se limitam a: • Componentes que gravam, armazenam, processam, compartilham, transmitem ou recuperam dados sensíveis. • Componentes que podem impactar a segurança de dados sensíveis ou do GPE. • Componentes que geram, transmitem ou processam números aleatórios usados para determinar o resultado de jogos e eventos. • Componentes que armazenam resultados ou o estado atual do jogo, aposta ou fundos disponíveis do cliente. • Pontos de entrada e saída dos componentes acima, incluindo outros sistemas que se comunicam diretamente com os Componentes Críticos do Sistema. • Tecnologia de comunicação e redes que transmitem dados sensíveis, incluindo equipamentos de comunicação de rede (NCE) e controles de segurança de rede. • Componentes que fornecem serviços de segurança, incluindo servidores de autenticação, servidores de controle de acesso, sistemas de gerenciamento de informações e eventos de segurança (SIEM), sistemas de segurança física, sistemas de vigilância, sistemas de autenticação multifator (MFA), sistemas anti-malware/antivírus. • Componentes que facilitam a segmentação, incluindo controles internos de segurança de rede. • Componentes de virtualização como máquinas virtuais, switches/roteadores virtuais, appliances virtuais, aplicativos/desktops virtuais e hipervisores. • Infraestrutura e componentes em nuvem, tanto externos quanto on-premiss, incluindo instâncias de containers ou imagens, nuvens privadas virtuais, gerenciamento de identidade e acesso baseado em nuvem, componentes residentes no local ou na nuvem, malhas de serviços com aplicações conteinerizadas e ferramentas de orquestração de containers. • Tipos de servidores incluem web, aplicação, banco de dados, autenticação, e-mail, proxy, Protocolo de Tempo de Rede (NTP) e Serviço de Nomes de Domínio (DNS). • Dispositivos para usuários finais, como computadores, laptops, estações de trabalho, estações administrativas, tablets e dispositivos móveis. • Aplicações, softwares e componentes de software, aplicações serverless, incluindo todas as compras, assinaturas (por exemplo, Software como Serviço), personalizadas e aplicações internas, incluindo aplicações internas e externas (por exemplo, Internet). • Ferramentas, repositórios de código e sistemas que implementam gerenciamento de configuração de software ou para implantação de objetos no GPE ou em componentes que possam impactar o GPE. • Redes e sistemas corporativos que se conectam ao GPE e a partir dos quais atacantes poderiam se mover lateralmente para dentro do GPE (por exemplo, redes de cassinos corporativos e redes corporativas de operadores online). • Qualquer outro componente considerado crítico para o GPE pelo Órgão Regulador ou pela Empresa de Jogos.

Mandato	Descrições
Módulo Criptográfico	Hardware, software, firmware ou combinação deles que implementam funções criptográficas como criptografia, descriptografia, assinaturas, hashing e gerenciamento de chaves. O principal objetivo de um módulo criptográfico é fornecer processamento e armazenamento seguros de chaves e operações.
Integridade dos Dados	A propriedade de que os dados são tanto precisos quanto consistentes e não foram alterados de forma não autorizada no armazenamento, durante o processamento e durante o trânsito.
Negação de Serviço Distribuída (DDoS)	Um tipo de ataque em que múltiplos sistemas comprometidos, geralmente infectados por um programa de software destrutivo, são usados para atingir um único sistema. As vítimas de um ataque DDoS consistem tanto no sistema final alvo quanto em todos os sistemas usados e controlados maliciosamente pelo hacker no ataque distribuído.
Domínio	Um grupo de computadores e dispositivos em uma rede que são administrados como uma unidade com regras e procedimentos comuns.
Serviço de Nomes de Domínio (DNS)	O banco de dados global da internet que (entre outras coisas) mapeia nomes de máquinas para números IP e vice-versa.
Criptografia	A conversão de dados em uma forma chamada texto cifrado, que não pode ser facilmente compreendida por pessoas não autorizadas. Quando a criptografia não é possível devido a uma limitação tecnológica ou de desempenho, outras medidas de proteção razoáveis devem ser implementadas em seu lugar e revisadas caso a caso.
Chave de Criptografia	Uma chave que foi criptografada para disfarçar o valor do texto simples subjacente.
Aplicações Externas	Aplicações que são públicas e podem ser descobertas por meio de reconhecimento e varredura de rede a partir da internet pública fora da rede da Empresa de Jogos. Isso não se aplica a aplicações destinadas ao uso dos usuários.
Ativos Empresariais Externos Expostos	Ativos que são públicos e podem ser descobertos por meio de reconhecimento do Domain Name Service (DNS) e varredura de rede a partir da internet pública fora da rede da Empresa de Jogos. Isso não se aplica a ativos destinados ao uso do usuário.
Firewall	Um componente de um sistema ou rede de computadores projetado para bloquear acessos ou tráfego não autorizados, permitindo ainda assim comunicação externa.
Empresa de Jogos	Um operador, e quaisquer fornecedores, fabricantes, fornecedores, prestadores de serviços e/ou outras entidades que tenham papel na supervisão da operação de um GPE, ou na prestação de serviços integrantes à sua função, incluindo a gestão de dados sensíveis.
Segurança da Informação em Jogos (GIS)	Proteger dados sensíveis e Componentes Críticos do Sistema contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizada, a fim de garantir confidencialidade, integridade, disponibilidade e responsabilidade.
Sistema de Gerenciamento de Segurança da Informação em Jogos (GISMS)	Um sistema de gestão definido e documentado que consiste em um conjunto de políticas, processos e sistemas para gerenciar riscos aos dados sensíveis, ativos e Componentes Críticos do Sistema de uma Empresa de Jogos dentro de um GPE, com o objetivo de garantir níveis aceitáveis de risco GIS.
Ambiente de Produção de Jogos (GPE)	O ambiente operacional onde atividades de jogos e serviços relacionados são conduzidos, gerenciados e entregues aos usuários de forma ao vivo ou em tempo real. Ela abrange a infraestrutura física e virtual, sistemas de jogos, softwares e processos necessários para facilitar várias formas de jogo e/ou gerenciar dados sensíveis, bem como os sistemas e infraestrutura backend que interfazem e/ou apoiam as atividades de jogo.
Sistemas de Jogos	Componentes Críticos do Sistema que são relativos a qualquer padrão técnico e/ou requisito regulatório aplicável para atividades de jogos.

Mandato	Descrições
Gateway	Qualquer dispositivo, sistema ou aplicativo de software que possa desempenhar a função de traduzir dados de um formato para outro. A principal característica de um gateway é que ele converte o formato dos dados, não os dados em si.
Controle GIS	A salvaguarda ou contramedida empregada pela Empresa de Jogos para proteger a confiabilidade, segurança ou capacidade do GPE ou a confidencialidade, integridade, disponibilidade e responsabilidade de seus dados sensíveis, a fim de permitir que a Empresa de Jogos cumpra suas responsabilidades legais e regulatórias.
Incidente de GIS	Uma ocorrência que realmente ou potencialmente coloque em risco a confidencialidade, integridade, disponibilidade ou responsabilidade de um GPE ou dos dados sensíveis que o GPE processa, armazena ou transmite, ou que constitua uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitável. Exemplos de incidentes de GIS reportáveis incluem, mas não se limitam a: • Acesso não autorizado a dados sensíveis ou Componentes Críticos do Sistema. • Execução de código malicioso ou infecção por ransomware dentro do GPE. • Perda, roubo ou divulgação não autorizada de PII. • Quedas ou interrupções do sistema que afetam a integridade ou disponibilidade das operações de jogo por um período definido (por exemplo, mais de 15 minutos). • Detecção de adulteração, manipulação ou tentativa de comprometimento de software ou hardware de jogos. • Tentativas repetidas ou sistêmicas de login falhadas indicam um ataque de força bruta. • Comprometimento ou uso indevido de credenciais administrativas ou certificados de segurança. • Alterações de configuração de segurança feitas fora dos processos autorizados de gerenciamento de mudanças.
Plano de Resposta a Incidentes de GIS	A documentação de um conjunto pré-determinado de instruções ou procedimentos quando um ataque cibernético malicioso é encontrado contra o GPE de uma Empresa de Jogos.
Política de GIS	Um documento que delineia a estrutura de gestão de segurança e atribuísse claramente responsabilidades de segurança e estabelecesse a base necessária para medir de forma confiável o progresso e a conformidade.
Membros do Grupo	Um método de organizar contas de usuário em uma única unidade (por posição de trabalho), pelo qual o acesso às funções do sistema pode ser modificado no nível da unidade e as mudanças entram em vigor para todas as contas de usuário atribuídas à unidade.
Algoritmo de Hash	Uma função que converte uma string de dados em uma saída de string alfanumérica de comprimento fixo.
Protocolo de Transporte de Hipertexto (HTTP)	O protocolo subjacente usado para definir como as mensagens são formatadas e transmitidas, e quais ações servidores e navegadores devem tomar em resposta a vários comandos.
Hub	Conecta dispositivos em uma rede de par trançado. Um hub não realiza nenhuma tarefa além de regenerar sinais.
Integridade	Proteger contra modificações ou destruições indevidas de informações e inclui garantir a não repúdio e autenticidade das informações.
Internet	Um sistema interconectado de redes que conecta computadores ao redor do mundo via TCP/IP.
Endereço de Protocolo de Internet (Endereço IP)	Um número único para um computador usado para determinar onde as mensagens transmitidas pela Internet devem ser entregues. O endereço IP é análogo ao número da casa para correspondência postal comum.

Mandato	Descrições
Sistema de Detecção de Intrusão/ Sistema de Prevenção de Intrusão (IDS/IPS)	Um sistema que inspeciona toda a atividade de rede de entrada e saída e identifica padrões suspeitos que possam indicar um ataque à rede ou sistema de alguém tentando invadir ou comprometer um sistema. Usado em segurança informática, a detecção de intrusões refere-se ao processo de monitorar atividades de computadores e redes e analisar esses eventos para buscar sinais de intrusão no GPE.
Segurança de IP (IPSec)	Um conjunto de protocolos para proteger comunicações IP autenticando e criptografando cada pacote IP de um fluxo de dados. O IPsec também inclui protocolos para estabelecer autenticação mútua entre agentes no início da sessão e negociação de chaves de criptografia a serem usadas durante a sessão.
Kerberos	Um protocolo de autenticação em rede projetado para fornecer autenticação forte para aplicações cliente/servidor usando criptografia por chave secreta.
Chave	Um valor usado para controlar funções criptográficas, como criptografia, descriptografia, assinaturas, hashing, etc.
Gestão de Chaves	Atividades envolvendo o manuseio de chaves de criptografia e outros parâmetros de segurança relacionados (por exemplo, senhas) durante todo o ciclo de vida das chaves, incluindo sua geração, armazenamento, estabelecimento, entrada e saída, e zeroização.
Segurança em Camadas	Uma abordagem de defesa que utiliza múltiplas proteções independentes em todo o sistema, como firewalls, autenticação, criptografia e monitoramento, de modo que um atacante precise contornar várias camadas antes de acessar dados sensíveis ou Componentes Críticos do Sistema.
Principais Não-Conformidades	Uma falha fundamental (sistemática) foi identificada que afeta um ou mais Controles de GIS e GISnifica que as políticas gerais de segurança, controles, processos ou práticas de gestão de riscos da Gaming Enterprise não podem ser seguidos. Pode ser qualquer uma: • Um número de pequenas não conformidades contra um controle pode representar uma falha total do sistema e, portanto, ser considerada uma grande não conformidade; • Qualquer não conformidade que resulte no provável envio de um produto não conforme ou em uma falha que comprometa GISnificativamente a confidencialidade, integridade, disponibilidade ou responsabilidade de dados sensíveis ou Componentes Críticos do Sistema; • Uma condição que possa resultar na falha ou reduzir materialmente a usabilidade, segurança ou confiabilidade dos produtos ou serviços para seu propósito pretendido; ou • Uma não conformidade que o julgamento e a experiência indicam provavelmente resultará na falha do sistema, reduzirá materialmente sua capacidade de garantir processos e produtos controlados, ou levará a ações regulatórias de fiscalização, perdas financeiras substanciais ou danos à confiança pública se não for remediada. Tais não conformidades normalmente não podem ser corrigidas sem exigir uma reforma abrangente ou ação emergencial imediata para remediar.
Falha	Quando um Componente Crítico do Sistema não funciona como deveria.
Malware	Um programa que é inserido em um sistema, geralmente de forma encoberta, com a intenção de comprometer a confidencialidade, integridade, disponibilidade ou responsabilidade dos dados, aplicativos ou sistema operacional da vítima, ou de incomodar ou perturbar a vítima de alguma forma.
Ataque "Homem-No-Meio"	Um ataque em que o atacante secretamente transmite e possivelmente altera a comunicação entre duas partes que acreditam estar se comunicando diretamente. Também conhecido como ataque "On-Path".
Autenticação de Mensagens	Uma medida de segurança projetada para estabelecer a autenticidade de uma mensagem por meio de um autenticador dentro da transmissão derivada de certos elementos predeterminados da própria mensagem.

Mandato	Descrições
Código de Autenticação de Mensagem (MAC)	Uma soma de verificação criptográfica em dados que utiliza uma chave simétrica para detectar modificações acidentais e intencionais dos dados.
Menor Não Conformidade	Um Controle GIS não foi abordado ou não está em conformidade com o GLI-GSF (não sistemático), e esse julgamento e experiência indicam que provavelmente não resultará na falha do sistema ou reduzirá sua capacidade de garantir processos ou produtos controlados. Pode ser qualquer uma: • Uma falha em alguma parte do sistema em relação a um controle; ou • Um único lapso observado em seguir um item do sistema; • Um desvio limitado ou isolado que não representa uma ameaça imediata ou GISnificativa à segurança ou integridade do GPE; ou • Um lapso processual, deficiência documental ou um controle que está em vigor, mas parcialmente implementado ou seguido de forma inconsistente. Tais não conformidades normalmente podem ser corrigidas sem exigir uma reforma completa ou ação emergencial imediata para remediar.
Autenticação Multifator (MFA)	Um tipo de autenticação que utiliza dois ou mais dos seguintes elementos para verificar a identidade de um usuário: • Informações conhecidas apenas pelo usuário (por exemplo, senha, PIN ou respostas a perguntas de segurança); • Um item possuído por um usuário (por exemplo, um token eletrônico, um token físico ou um cartão de identificação); e • Dados biométricos do usuário (por exemplo, impressões digitais, padrões de retina, dados de reconhecimento facial ou impressões de voz).
Equipamento de Comunicação de Rede (NCE)	Tecnologia de comunicações que controla a comunicação de dados em um sistema, incluindo, mas não se limitando a, NICs, cabos, switches, pontes, hubs, roteadores, pontos de acesso (WAPs) e telefones, dispositivos de rede VoIP, appliances de rede e outros aparelhos de segurança.
Observação	Uma constatação que vale destacar para possíveis melhorias que atendam às melhores práticas do setor.
Senha	Uma sequência de caracteres (letras, números e outros símbolos) usada para autenticar uma identidade ou para verificar a autorização de acesso.
Informações pessoais identificáveis (PII)	Dados sensíveis que poderiam ser usados para identificar uma pessoa específica. Exemplos incluem nome legal, data de nascimento, local de nascimento, número de identificação do governo (número de seguro social, número de identificação do contribuinte, número de passaporte ou equivalente), informações financeiras pessoais (números de instrumentos de crédito ou débito, números de conta bancária, etc.) ou outras informações pessoais, se definidas pelo Órgão Regulador.
Número de Identificação Pessoal (PIN)	Um código numérico associado a um indivíduo que permite acesso seguro a um domínio, conta, rede, sistema, etc.
Controles Físicos e Ambientais	As medidas implementadas para proteger os ativos físicos, instalações e condições ambientais que abrigam os sistemas e infraestrutura do Ambiente de Produção de Jogos.
Porto	Um ponto físico de entrada ou saída de um módulo que fornece acesso ao módulo para sinais físicos, representado por fluxos lógicos de informação (portas fisicamente separadas não compartilham o mesmo pino ou fio físico).
Protocolo	Um conjunto de regras e convenções que especifica a troca de informações entre dispositivos, por meio de uma rede ou outro meio.
Órgão Regulador	O órgão governamental ou equivalente que regula ou controla as operações dos jogos.
Acesso Remoto	Qualquer acesso de fora do sistema ou da rede do sistema, incluindo qualquer acesso de outras redes dentro do mesmo local ou local.
Risco	A probabilidade de uma ameaça ser bem-sucedida em seu ataque contra uma rede ou sistema dentro do GPE.
Avaliação de Riscos	Identificar, analisar e priorizar ameaças e vulnerabilidades às operações ou ativos de uma Empresa de Jogos, ou a indivíduos ou outras entidades,

Mandato	Descrições
	resultantes da comprometimento da confidencialidade, integridade, disponibilidade e responsabilidade de dados sensíveis ou da confiabilidade, segurança ou capacidade do GPE.
Roteador	Conecta redes entre si. Um roteador usa o endereço de rede configurado por software para tomar decisões de encaminhamento.
Protocolo de Comunicação Segura	Um protocolo de comunicação que oferece a confidencialidade, autenticação e proteção da integridade do conteúdo adequadas.
Certificado de Segurança	Informações, frequentemente armazenadas como um arquivo de texto, são usadas pelo Protocolo da Camada de Soquete de Transporte (TSL) para estabelecer uma conexão segura. Para que uma conexão TSL seja criada, ambos os lados devem possuir um Certificado de Segurança válido.

Dados Sensíveis	Informações que precisam ser tratadas de maneira segura, incluindo, mas não se limitando a, conforme aplicável:
	• Registros de auditoria e bancos de dados do sistema registrando informações usadas para determinar resultado, pagamento, resgate e o rastreamento das informações dos usuários;
	• Informações contábeis e de eventos significativos relacionadas aos Componentes Críticos do Sistema do GPE;
	• RNG seed e qualquer outra informação que afete os resultados de jogos e apostas;
	• Chaves de criptografia, onde a implementação escolhida requer transmissão de chaves;
	• Números de validação associados a contas de patronos, instrumentos de apostas e quaisquer outras transações de jogo;
	• Transferências de fundos para e de contas de patronos, contas de pagamento eletrônico e para fins de jogos;
	• Pacotes de software dentro do GPE;
	• Qualquer dado de localização relacionado à atividade de funcionários ou usuários (por exemplo, gerenciamento de contas, jogos online, etc.);
	• Qualquer uma das seguintes informações registradas para qualquer funcionário ou usuário:
	  • número de identificação governamental (número de seguridade social, número de identificação do contribuinte, número de passaporte ou equivalente);
	  • informações financeiras pessoais (números de instrumentos de crédito ou débito, números de conta bancária, etc.);
	  • Credenciais de autenticação em relação a qualquer conta de usuário ou conta patrona;
	  • Qualquer outra informação pessoal identificável (PII) que precise ser mantida confidencial; e
	• Quaisquer outros dados considerados sensíveis pelo Órgão Regulador ou pela Empresa de Jogos.

Servidor	Uma instância em execução de software capaz de aceitar solicitações de clientes e do computador que executa tal software. Servidores operam dentro de uma Arquitetura Cliente-Servidor, na qual "servidores" são programas de computador executados para atender aos pedidos de outros programas ("clientes").
Provedores de Serviços	Entidades que oferecem plataformas, softwares e serviços para Empresas de Jogos. Exemplos incluem consultores de TI, provedores de serviços gerenciados, plataformas de Software como Serviço (SaaS) e provedores de serviços em nuvem. Provedores e fornecedores terceirizados também são considerados Provedores de Serviço.
Identificador de Conjunto de Serviços (SSID)	Um nome que identifica uma determinada LAN sem fio IEEE 802.11.

Mandato	Descrições
Código de shell	Um pequeno pedaço de código usado como carga útil na exploração da segurança. O shellcode explora vulnerabilidades e permite que o atacante reduza a garantia de informações do sistema.
Verificação de Assinatura	Garantindo, por meio de verificação de assinaturas eletrônicas, que qualquer pacote de software seja uma cópia autêntica do software criado por seu fabricante e, se aplicável, uma cópia exata do software conforme certificado pelo Laboratório de Testes Independente (ITL).
Engenharia Social	Uma tentativa de enganar alguém para revelar informações (por exemplo, uma senha) que podem ser usadas para atacar sistemas ou redes. Ataques de engenharia social incluem intrusões não técnicas em um GPE usando informações adquiridas por interação humana e dependem de truques que se aproveitam de um indivíduo desconhecido com tecnologias e protocolos emergentes.
Código-fonte	Uma lista de texto dos comandos a serem compilados ou montados em um programa executável de computador.
Protocolo Sem Estado	Um esquema de comunicação que trata cada requisição como uma transação independente, sem relação com qualquer requisição anterior, de modo que a comunicação consiste em pares independentes de requisições e respostas.
Administrador de Sistema	O(s) indivíduo(s) responsável por manter a operação estável do GPE (incluindo infraestrutura de software e hardware e software de aplicação).
Controles Técnicos	Os mecanismos de segurança implementados nos sistemas e infraestrutura do Gaming Production Environment para proteger contra acessos não autorizados, vazamentos de dados e outras ameaças à segurança.
Ameaça	Qualquer circunstância ou evento com potencial para impactar negativamente as operações da rede (incluindo missão, funções, imagem ou reputação), ativos ou indivíduos por meio de um sistema por meio de acesso não autorizado, destruição, divulgação, modificação de informações e/ou negação de serviço; o potencial de uma fonte de ameaça explorar com sucesso uma vulnerabilidade específica; qualquer perigo potencial para uma rede que alguém ou algo possa identificar como vulnerável e, portanto, tentar explorar.
Carimbo de Tempo	Um registro do valor atual da data e hora que é adicionado a uma mensagem no momento em que a mensagem é criada.
Acesso Não Autorizado	Uma pessoa obtém acesso lógico ou físico sem permissão a uma rede, sistema, aplicativo, dado ou outro recurso.
Protocolo de Datagrama do Usuário (UDP)	Um protocolo de transporte que não garante a entrega. Assim, é mais rápido, mas menos confiável.
Fornecedores	Provedores de serviços que integram aplicações empresariais e outras soluções auxiliares no GPE de uma empresa de jogos, que não afeta diretamente componentes ou atividades reguladas de jogos.
Controle de Versão	O método pelo qual os Componentes Críticos do Sistema aprovados em evolução são verificados como operando em um estado aprovado.
Rede Privada Virtual (VPN)	Uma rede lógica estabelecida sobre uma rede física existente e que normalmente não inclui todos os nós presentes na rede física.
Vírus	Um programa autorreplicante, tipicamente com intenção maliciosa, que roda e se espalha modificando outros programas ou arquivos.
Scanner de Vírus	Software usado para prevenir, detectar e remover vírus de computador, incluindo malwares, worms e cavalos de Troia.
Vulnerabilidade	Software, hardware ou outras fraquezas em uma rede ou sistema que podem servir de "porta" para a introdução de uma ameaça.
Protocolo Equivalente Com Cabo (WEP)	Um algoritmo facilmente quebrado e, portanto, obsoleto para proteger redes sem fio IEEE 802.11. Originalmente, ele foi projetado para permitir o mesmo nível de proteção de uma conexão com fio, mas falhas logo foram descobertas após sua adoção, tornando-o pouco melhor do que nenhuma proteção.

Mandato	Descrições
Ponto de Acesso Sem Fio (WAP)	Fornece capacidades de rede para dispositivos de rede sem fio. Um WAP é frequentemente usado para se conectar a uma rede cabeada, atuando assim como um elo entre as partes cabeadas e sem fio da rede.
Wi-Fi	A tecnologia padrão de rede local sem fio (WLAN) para conectar computadores e dispositivos eletrônicos entre si e/ou à internet.
Acesso Protegido por Wi-Fi (WPA)	O sucessor do WEP. Sua autenticação pode ser quebrada em certas circunstâncias, mas frases de acesso suficientemente complexas são seguras o suficiente para a maioria dos usos.
Estação de trabalho	Uma interface para que pessoal autorizado acesse as funções reguladas do GPE.