GLI®

FRAMEWORK DE SEGURANÇA PARA JOGOS

GLI-GSF-1

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

Versão 1.1 – Publicada em 30 de setembro de 2025

Conteúdo

1. INTRODUÇÃO 3

1.1. DECLARAÇÃO GERAL 3

1.2. EMPRESA DE JOGOS E FUNÇÃO DE GESTÃO DE DADOS SENSÍVEIS 3

1.3. AMBIENTE DE PRODUÇÃO DE JOGOS (GPE) 3

1.4. SISTEMA DE GERENCIAMENTO DE SEGURANÇA DA INFORMAÇÃO EM JOGOS (GISMS) 3

1.5. PROPÓSITO DO FRAMEWORK 4

1.6. NORMAS E DIRETRIZES DE SEGURANÇA CONSULTADAS 4

1.7. ADOÇÃO E OBSERVÂNCIA 4

2. AUDITORIAS DE CONTROLE DE GIS ONLINE (OGIS) 4

2.1. VISÃO GERAL DA AUDITORIA 4

2.2. MÉTODOS DE AUDITORIA 4

2.3. TAREFAS DE AUDITORIA 4

2.4. FREQUÊNCIA DE AUDITORIA 5

2.5. RELATÓRIOS DE AUDITORIA 5

2.6. REMEDIAÇÃO 5

2.7. EMPRESA INDEPENDENTE DE SEGURANÇA (ISF) 5

APÊNDICE: CONTROLES DE SEGURANÇA DA INFORMAÇÃO EM JOGOS ONLINE (OGIS) 6

DEFINIÇÕES DE TERMOS 11

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) adicionais ao GLI-GSF-1, 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 utilizado em operações de jogos online, por meio de website de jogos, aplicação móvel ou outra plataforma digital, para oferecer jogos interativos, jogos de estúdio ao vivo, loteria pela internet, apostas online em eventos ou qualquer outra forma de jogo online.
b. Este módulo destina-se a ser avaliado em conjunto com o GLI-GSF-1, que fornece os Controles GIS comuns necessários para auditar o GISMS de uma Empresa de Jogos.
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. Para informações adicionais, consulte a seção “Papel da Empresa de Jogos e do Gerenciamento de Dados Sensíveis” do GLI-GSF-1.

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 online 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 online, tais como jogos interativos (iGaming), loteria interativa (iLottery), apostas online em eventos e jogos de estúdio ao vivo. O GPE também abrange os sistemas backend, aplicações de negócios e infraestrutura que se conectam e/ou apoiam as atividades de jogos online. Características principais de um GPE são descritas na seção “Ambiente de Produção de Jogos (GPE)” do GLI-GSF-1.

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 online é fundamental para preservar a confiança e a confiança pública no setor. Portanto, Empresas de Jogos que oferecem jogos online 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 GIS aplicáveis a jogos online, em conjunto com os Controles GIS comuns do GLI-GSF-1.

2. AUDITORIAS DE CONTROLE DE GIS ONLINE (OGIS)

2.1. Visão Geral da Auditoria

A Auditoria de Controles OGIS 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-5 está nos controles específicos de segurança da informação para jogos online, aplicáveis adicionalmente aos controles comuns de segurança da informação para jogos previstos no GLI-GSF-1. 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

O Apêndice detalha os Controles OGIS mínimos em maior granularidade. Os usuários deste documento devem consultar o Apêndice deste módulo, bem como o Apêndice do GLI-GSF-1, para assegurar que nenhum Controle GIS necessário seja negligenciado. Os Controles OGIS listados no Apêndice não são exaustivos e, além dos Controles GIS comuns do GLI-GSF-1, Controles GIS adicionais podem ser incluídos com base nos requisitos regulatórios e no escopo da avaliação.

NOTA: Informações sobre as atividades de alto nível da Auditoria de Controles OGIS podem ser encontradas na seção "Tarefas de Auditoria" do GLI-GSF-1, incluindo, mas não se limitando a, revisão documental, entrevistas, avaliação de controles, avaliação do plano de resposta a incidentes GIS e avaliação de risco.

2.4. Frequência de Auditoria

As Auditorias de Controles OGIS devem ser realizadas por uma ISF conforme a "Frequência de Auditoria" expressa no GLI-GSF-1. Isso pode incluir auditorias adicionais solicitadas pelo Órgão Regulador ou pela Empresa de Jogos, focadas especificamente em alterações críticas no GPE que possam afetar sua segurança, permitir acesso a dados sensíveis e/ou Componentes Críticos do Sistema, ou impactar de qualquer outra forma o fluxo de dados ou a postura de segurança.

NOTA: O Órgão Regulador ou a Empresa de Jogos também pode solicitar uma varredura de vulnerabilidades ou testes de Segurança Técnica de Jogos (GTS) especificamente sobre alterações críticas e os Componentes Críticos do Sistema afetados por essas alterações. Consulte o GLI-GSF-2 para informações adicionais.

2.5. Relatórios de Auditoria

Os resultados de uma Auditoria de Controles OGIS identificam para as Empresas de Jogos quais áreas das operações devem ser consideradas melhorias e recomendam estratégias para melhorar essas áreas. relatório da Auditoria de Controles OGIS deve atender aos requisitos para "Relatórios de Auditoria" especificados no GLI-GSF-1.

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.

NOTA: Para informações adicionais, consulte a seção "Remediação" do GLI-GSF-1.

2.7. Empresa Independente de Segurança (ISF)

A Auditoria de Controles OGIS deve ser realizada por indivíduos com qualificações suficientes, o que significa que a ISF deve empregar profissionais suficientemente qualificados, competentes e experientes. Salvo especificação em contrário pelo Órgão Regulador, esses indivíduos devem atender às qualificações especificadas para uma "Empresa Independente de Segurança (ISF)" no GLI-GSF-1.

APÊNDICE: CONTROLES DE SEGURANÇA DA INFORMAÇÃO EM JOGOS ONLINE (OGIS)

Além dos Controles GIS comuns especificados no GLI-GSF-1 para Empresas de Jogos GIG3, os seguintes Controles GIS adicionais se aplicam aos GPEs de Empresas de Jogos que oferecem jogos online.

OGIS-1	Verificação de Assinatura de Programas Críticos de Controle
OGIS-1.1	**Procedimento e Registro de Verificação de Assinatura**
OGIS-1.1.1	As assinaturas dos Programas Críticos de Controle devem ser obtidas do GPE por meio de um procedimento de verificação de assinatura, que deve ser executado nas seguintes condições: a. Mediante instalação ou atualização de quaisquer Programas Críticos de Controle; b. Mediante inicialização do sistema ou recuperação de um estado de desligamento; c. No mínimo, uma vez a cada 24 horas durante as operações normais; e d. Mediante solicitação, sob demanda.
OGIS-1.1.2	O procedimento de verificação de assinatura deve incluir uma ou mais etapas analíticas para comparar as assinaturas atuais dos Programas Críticos de Controle no GPE com as assinaturas das versões atualmente aprovadas.
OGIS-1.2	**Registro de Auditoria de Verificação**
OGIS-1.2.1	A saída do procedimento de verificação de assinatura deve ser registrada em um log de auditoria de verificação, que compõe parte dos dados sensíveis que devem ser recuperados em caso de desastre ou falha de equipamento ou software.
OGIS-1.2.2	O log de auditoria de verificação deve detalhar o seguinte para cada verificação de assinatura: a. A data e hora da verificação; b. A identificação de cada Programa Crítico de Controle verificado; c. Os resultados de assinatura esperados e gerados, incluindo indicação de qualquer erro de programa ou incompatibilidade de assinatura; e d. Quando realizada sob demanda, o ID da conta de usuário que iniciou o procedimento de verificação.
OGIS-1.2.3	O log de auditoria de verificação deve estar acessível ao Órgão Regulador em um formato que permita a análise de cada verificação pelo Órgão Regulador.
OGIS-1.3	**Falha de Verificação**
OGIS-1.3.1	Qualquer falha de verificação de assinatura de qualquer Programa Crítico de Controle deve exigir que uma notificação da falha de verificação seja comunicada à Empresa de Jogos.
OGIS-1.3.2	Quando exigido pelo Órgão Regulador, a Empresa de Jogos deve reportar a falha de verificação de assinatura e as ações corretivas tomadas ao Órgão Regulador sem atraso indevido.
OGIS-2	**Administração de Back Office**
OGIS-2.1	**Aplicação de Autenticação Multifator (MFA)**
OGIS-2.1.1	As Aplicações de Administração de Back Office devem suportar a aplicação de MFA para todas as contas privilegiadas utilizadas por indivíduos para acessar as aplicações, quando possível. Isso inclui contas administrativas, operacionais, de sistema e de suporte com permissões elevadas.
OGIS-2.1.2	Quando a MFA for aplicada, ela deve utilizar pelo menos dois fatores de autenticação distintos, por exemplo, senha e token de hardware, para reduzir o risco de acesso não autorizado decorrente de credenciais comprometidas.
OGIS-2.1.3	Quando a implementação de MFA não for possível, por exemplo, em contas de serviço, as contas privilegiadas devem possuir controles compensatórios, tais como autenticação forte, gerenciamento de contas privilegiadas, controles de acesso condicional e monitoramento adicional.
OGIS-2.2	**Monitoramento do Acesso de Suporte de Fornecedores**
OGIS-2.2.1	Todo acesso de fornecedores às Aplicações de Administração de Back Office, seja remoto ou presencial, para fins de manutenção, solução de problemas ou suporte, deve ser estritamente controlado, monitorado e registrado em log pela Empresa de Jogos.
OGIS-2.2.2	O acesso de fornecedores deve ser concedido somente de forma temporária, conforme necessário, por meio de canais de comunicação seguros.
OGIS-2.2.3	Todas as atividades de fornecedores realizadas durante esse acesso devem ser totalmente registradas em log e auditáveis para assegurar responsabilização e apoiar monitoramento, análise e revisão forense.

OGIS-2.2.4	Todas as alterações no acesso de fornecedores, incluindo adições, modificações ou remoções, devem ser formalmente documentadas e registradas para manter uma trilha auditável das atividades de gerenciamento de acesso.
OGIS-2.2.5	O GPE deve incluir um mecanismo para revogar imediatamente o acesso de fornecedores no caso de um incidente GIS, assegurando a mitigação rápida de potenciais riscos de segurança ou operacionais.
OGIS-2.3	**Controles de Acesso Baseados em Função (RBAC) e Princípio do Menor Privilégio**
OGIS-2.3.1	As Aplicações de Administração de Back Office devem implementar RBAC para atribuir permissões com base nas responsabilidades de trabalho dos usuários. Alterações no RBAC devem ser documentadas e registradas.
OGIS-2.3.2	O acesso deve seguir o princípio do menor privilégio, assegurando que os usuários tenham apenas as permissões mínimas necessárias para desempenhar suas funções.
OGIS-2.3.3	As Aplicações de Administração de Back Office devem aplicar segregação de funções para impedir que o mesmo indivíduo execute tarefas conflitantes, por exemplo, iniciar e aprovar transações.
OGIS-2.4	**Restrições de Acesso à Rede**
OGIS-2.4.1	O acesso às Aplicações de Administração de Back Office deve ser restrito a redes confiáveis e autorizadas, implementando pelo menos um dos seguintes controles para aplicar essa restrição: lista de permissões de IP, firewalls, segmentação de rede ou acesso seguro por Rede Privada Virtual (VPN). a. Redes públicas e dispositivos não confiáveis devem ter o acesso explicitamente negado. b. Todo o tráfego não explicitamente autorizado deve ter o acesso implicitamente negado. c. Soluções zero trust devem verificar continuamente a confiabilidade de usuários e dispositivos antes de conceder acesso, assegurando que nenhuma confiança implícita seja concedida com base na localização da rede ou em outros fatores presumidos. d. Quando a implementação dos controles acima não for viável devido à configuração do produto, controles compensatórios adicionais devem ser aplicados e documentados.
OGIS-2.4.2	Os controles de acesso à rede devem ser revisados e atualizados regularmente para assegurar alinhamento contínuo com a postura de segurança da Empresa de Jogos.
OGIS-2.5	**Gerenciamento de Sessões e Contas**
OGIS-2.5.1	As Aplicações de Administração de Back Office devem ser configuradas para proibir logins simultâneos da mesma conta de usuário em múltiplos dispositivos ou sessões.
OGIS-2.5.2	Quando tecnicamente viável, as sessões ativas existentes devem ser encerradas quando uma tentativa de login duplicado for realizada, a fim de prevenir acesso simultâneo não autorizado e proteger a integridade da conta.
OGIS-3	**Integridade do Lado do Servidor e Segurança de Programação**
OGIS-3.1	**Validação da Lógica de Jogo no Lado do Servidor**
OGIS-3.1.1	Toda lógica crítica de jogo e transições de estado, por exemplo, pontuação, atualizações de saldo e resolução de vitória/perda, devem ser validadas no lado do servidor, independentemente da entrada do cliente.
OGIS-3.1.2	As entradas recebidas do website de jogos, aplicação móvel ou outra plataforma digital devem ser verificadas quanto à integridade, autenticação e consistência lógica antes que qualquer alteração de estado seja aplicada.
OGIS-3.2	**Controle de Execução e Restrições de Código Externo**
OGIS-3.2.1	A Empresa de Jogos deve implementar e manter mecanismos robustos projetados para prevenir a execução de código potencialmente prejudicial ou não autorizado introduzido por meio de dispositivos móveis, mídia removível ou outras fontes externas.
OGIS-3.2.2	A Empresa de Jogos deve restringir servidores críticos para executar somente aplicações aprovadas e verificadas, bloqueando a execução de todo código não aprovado ou não autorizado, por exemplo, implementação de lista de permissões de aplicações que permita somente a execução de aplicações de software pré-aprovadas ou “whitelisted” em um sistema.
OGIS-3.2.3	A Empresa de Jogos deve aplicar políticas que desabilitem ou limitem a capacidade de executar código a partir de dispositivos externos ou não confiáveis, incluindo a desativação de recursos de execução automática e a restrição da execução de scripts.

OGIS-3.3	**Aplicação de Políticas**
OGIS-3.3.1	A Empresa de Jogos deve estabelecer e aplicar políticas que regulamentem o uso de dispositivos móveis e mídias externas em servidores que executam Programas de Controle Crítico (Critical Control Programs - CCPs), por exemplo, permitindo que apenas dispositivos móveis gerenciados se conectem à rede e bloqueando o uso de unidades USB em servidores críticos. Essas medidas podem incluir soluções de Mobile Device Management (MDM), controles de acesso à rede (Network Access Controls - NAC) ou restrições em nível de servidor para prevenir conexões não autorizadas ou transferências indevidas de dados.
OGIS-3.3.2	A Empresa de Jogos deve restringir ou proibir a conexão e o uso de dispositivos móveis e mídias externas não autorizados, de modo a prevenir a introdução de código não confiável ou malicioso.
OGIS-3.3.3	A Empresa de Jogos deve definir procedimentos e métodos seguros para a introdução de qualquer código externo, software ou atualização, garantindo sua integridade e conformidade com os padrões de segurança aplicáveis.
OGIS-3.3.4	A Empresa de Jogos deve estabelecer requisitos para autenticação, varredura (scanning) e validação de dispositivos antes que qualquer mídia externa ou código externo seja autorizado em Componentes Críticos do Sistema.
OGIS-3.4	**Monitoramento do GPE e Resposta a Incidentes do GIS**
OGIS-3.4.1	Mecanismos de monitoramento contínuo devem ser implementados para detectar, alertar e registrar quaisquer tentativas de execução de código não autorizado, apoiando a resposta tempestiva, a análise e a investigação forense de potenciais incidentes de segurança do GIS.
OGIS-3.4.2	A Empresa de Jogos deve possuir procedimentos estabelecidos para tratar prontamente quaisquer Incidentes GIS relacionados a código móvel ou ameaças executáveis externas.
OGIS-3.5	**Segurança de Ambientes em Nuvem e Virtualizados**
OGIS-3.5.1	Cada instância de servidor implantada em um ambiente em nuvem ou virtualizado deve ser dedicada a uma única função crítica (por exemplo, o servidor de banco de dados não deve hospedar serviços web ou de aplicação). Essa abordagem assegura a segregação lógica de funções, limita o raio de impacto de potenciais incidentes de segurança e está alinhada ao princípio do menor privilégio.
OGIS-3.5.2	A Empresa de Jogos deve implementar controles técnicos e administrativos para impor a segregação de funções entre instâncias de servidor por meio do isolamento de funções. Isso inclui o uso de máquinas virtuais, contêineres ou serviços distintos para cada função (por exemplo, banco de dados, aplicação e servidor web), bem como a aplicação de configurações, controles de acesso e monitoramento específicos para cada carga de trabalho.
OGIS-4	**Mecanismos de Proteção de Aplicações**
OGIS-4.1	**Comunicação Segura em Aplicações Móveis**
OGIS-4.1.1	As aplicações móveis devem assegurar comunicação segura entre o cliente e o servidor. Isso pode ser alcançado por meio de fixação de certificado SSL/TLS ou medidas equivalentes, tais como monitoramento de transparência de certificados ou frameworks de fixação dinâmica, que fornecem proteção comparável contra ataques “Man-In-The-Middle” e, ao mesmo tempo, suportam o gerenciamento seguro de certificados ou chaves de criptografia.
OGIS-4.1.2	As aplicações móveis devem ser projetadas para encerrar imediatamente as conexões de rede se o certificado fixado ou a chave de criptografia não corresponder ao valor esperado.
OGIS-4.1.3	Todas as falhas de validação de certificado ou chave de criptografia devem ser registradas em log para apoiar monitoramento, análise e investigação forense, assegurando a rastreabilidade de incidentes GIS e potenciais comprometimentos do sistema.
OGIS-4.2	**Detecção de Jailbreak/Root em Dispositivos Móveis**
OGIS-4.2.1	Como parte de uma estratégia de defesa em camadas, aplicações móveis podem implementar detecção de jailbreak (iOS) e root (Android) para prevenir a execução em dispositivos comprometidos. A detecção deve abranger técnicas, ferramentas e anomalias comuns do sistema indicativas de adulteração.
OGIS-4.2.2	Se for determinado que um dispositivo móvel está com root ou jailbreak, a aplicação deve restringir o acesso a funcionalidades sensíveis ou encerrar sua operação.

OGIS-4.3	**Ofuscação de Código para Aplicações Móveis**
OGIS-4.3.1	A base de código da aplicação móvel deve implementar ofuscação de código para proteção contra engenharia reversa. Isso inclui, mas não se limita a: a. Renomear classes, variáveis e métodos para identificadores não descritivos; b. Modificar fluxos de controle para tornar a lógica do programa mais difícil de acompanhar; e c. Aplicar criptografia de strings ou ocultar recursos críticos.
OGIS-4.3.2	Os processos de ofuscação de códigos devem ser integrados ao pipeline automatizado de build para assegurar que cada build de produção seja devidamente ofuscado antes do liberação.
OGIS-4.3.3	Mecanismos de tamper-detection devem ser implementados para alertar o pessoal autorizado caso a aplicação móvel seja alterada após a distribuição, assegurando a integridade ao longo de todo o ciclo da vida do software.
OGIS-4.4	**Detecção e Prevenção de Password Stuffing Attacks**
OGIS-4.4.1	A Empresa de Jogos deve implementar mecanismos para detectar padrões consistentes com passwordsl stuffing, tais como tentativas de login em alto volume usando credenciais variadas a partir de um único endereço IP ou dispositivo.
OGIS-4.4.2	Medidas preventivas devem ser aplicadas nos endpoints de autenticação (por exemplo, desafios CAPTCHA, limitação de taxa, políticas de bloqueio de contas, lógica de detecção de password stuffing, entre outras.).
OGIS-4.5	**Solução de Mitigação de Bots**
OGIS-4.5.1	O GPE deve integrar uma solução de mitigação de bots para detectar e bloquear tráfego automatizado que tente executar ações abusivas, fraudulentas ou não autorizadas.
OGIS-4.5.2	A solução de mitigação de bots deve incluir análise comportamental, device fingerprinting e mecanismos de desafio-resposta para diferenciar usuários humanos de scripts automatizados.
OGIS-4.6	**Segurança de API**
OGIS-4.6.1	Todas as APIs que dão suporte ao gaming website, à aplicação móvel ou a outra plataforma digital devem aderir às boas práticas do OWASP API Security Top 10, incluindo autenticação, limitação de taxa, validação de dados e tratamento de erros.
OGIS-4.6.2	A Empresa de Jogos deve realizar regularmente testes de segurança de API, incluindo durante a fase de desenvolvimento, por exemplo, testes de penetração e análise estática/dinâmica, e implantar API gateways ou Web Application Firewalls (WAFs) para aplicar políticas de segurança de API e monitorar o tráfego em tempo real.
OGIS-4.7	**Arquitetura de Segurança**
OGIS-4.7.1	Os segmentos de rede que compõem a infraestrutura do gaming website, da aplicação móvel ou de outra plataforma digital devem ser isolados entre si.
OGIS-4.7.2	A comunicação entre segmentos deve ser explicitamente restrita apenas aos protocolos, hosts e serviços necessários para a funcionalidade operacional.
OGIS-4.7.3	Em uma rede zero trust, todo o tráfego entre segmentos deve ser autenticado, autorizado e monitorado continuamente para prevenir acesso não autorizado e movimentação lateral dentro da rede.
OGIS-4.7.4	O gaming website, a aplicação móvel ou outra plataforma digital deve ser protegida por um WAF ou controle equivalente que forneça proteção comparável contra ataques baseados na web, incluindo, mas não se limitando a, ataques de injeção, cross-site scripting e outras ameaças comuns da camada de aplicação.
OGIS-4.7.5	O WAF ou controle equivalente deve ser monitorado regularmente quanto a eventos de interesse e atualizado para assegurar que os vetores de ataque mais recentes estejam configurados para monitoramento.
OGIS-5	**Controles de Proteção contra Negação de Serviço Distribuída (DDoS)**
OGIS-5.1	**Limitação de Taxa em Múltiplas Camadas e Throttling**
OGIS-5.1.1	A limitação de taxa deve ser aplicada em múltiplas camadas da arquitetura do GPE para identificar e aplicar throttling a padrões abusivos de requisição e mitigar a degradação do serviço: a. Camada de rede: firewalls e ingress controllers devem aplicar limites para conexões ou pacotes por origem, por exemplo, por endereço IP. b. Camada de API gateway: os API gateways devem, quando possível, limitar o número de chamadas por cliente, incorporando tratamento de rajadas e mecanismos de back-off. c. Camada de aplicação: a lógica da aplicação deve detectar e suprimir uso excessivo ou abusivo de endpoints específicos para prevenir exaustão de recursos.

OGIS-5.1.2	A limitação de taxa deve ser adaptativa em relação a padrões variáveis de tráfego e à carga do sistema, e todas as violações de limites definidos devem ser registradas em log para fins de monitoramento, análise e investigação forense.
OGIS-5.2	**Ofuscação de IP e Mitigação de DDoS**
OGIS-5.2.1	Os endereços IP públicos dos servidores de jogos, APIs, painéis administrativos e outros Componentes Críticos do Sistema devem ser ofuscados para evitar o alvo direto à infraestrutura. Essa ofuscação pode ser realizada por meio de, mas não se limita a: a. Proxies reversos, Redes de Distribuição de Conteúdo (CDNs) ou balanceadores de carga baseados em nuvem (por exemplo, posicionar uma CDN à frente de um servidor de jogos para processar as solicitações enquanto oculta o endereço IP do servidor de origem); e b. Tradução de Endereços de Rede (NAT) e redes sobrepostas (por exemplo, utilizar endereçamento IP privado combinado com NAT, ou implementar redes sobrepostas definidas por software, para mascarar a localização real de origem e o endereçamento dos servidores de backend).
OGIS-5.2.2	Serviços terceirizados de proteção contra DDoS devem ser integrados ao GPE para aumentar a resiliência e manter a disponibilidade. A integração deve fornecer as seguintes capacidades: a. Detectar e absorver ataques volumétricos, de protocolo e de camada de aplicação, por exemplo, identificando automaticamente e bloqueando solicitações HTTP excessivas direcionadas a uma API; b. Assegurar que o tráfego malicioso seja filtrado antes de alcançar o GPE, por exemplo, utilizando centros de limpeza de tráfego para filtrar o tráfego; c. Manter a continuidade dos negócios por meio de failover automático e redes globais de borda, por exemplo, redirecionando o tráfego para edge node alternativos caso um node regional esteja sob ataque; e d. Validar acordos de nível de serviço (SLAs) e procedimentos de resposta a incidentes GIS com os Prestadores de Serviços, por exemplo, testando periodicamente o failover e os tempos de resposta conforme os SLAs contratuais.

DEFINIÇÕES DE TERMOS

Termo	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.
Controles Administrativos	Políticas, procedimentos e diretrizes implementados por uma Empresa de Jogos para gerenciar seus GISMS.
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	Verificação da identidade de um usuário, processo, pacote de software ou dispositivo, frequentemente como pré-requisito para permitir acesso a recursos no 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, cartões magnéticos, cartões de proximidade e cartões com chip incorporado.
Disponibilidade	Garantir acesso e uso tempestivos e confiáveis da informação.
Aplicação de Administração de Back Office	Um sistema de software seguro e centralizado utilizado pela Empresa de Jogos e pelos Órgãos Reguladores para gerenciar, monitorar e dar suporte às funções operacionais, financeiras, de conformidade e de atendimento ao cliente de um GPE, tais como sistemas de verificação de identidade, prevenção à lavagem de dinheiro e relatórios regulatórios.
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.
Confidencialidade	Preservar restrições autorizadas ao acesso e divulgação de informações, incluindo meios para proteger a privacidade pessoal e informações proprietárias.
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 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.

Termo	Descrições
	• 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.
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.

Termo	Descrições
Chave de Criptografia	Uma chave que foi criptografada para disfarçar o valor do texto simples subjacente.
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.
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.
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.
Integridade	Proteger contra modificações ou destruições indevidas de informações e inclui garantir a não repúdio e autenticidade das informações.

Termo	Descrições
Endereço de Protocolo de Internet (Endereço IP)	Número único de um computador usado para determinar para onde as mensagens transmitidas pela Internet devem ser entregues. O endereço IP é análogo ao número de uma residência no correio postal comum.
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.
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.
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.
Código Móvel	Código executável que se move de computador para computador, incluindo tanto código legítimo como código malicioso, como vírus de computador.
Microservice	Pequeno componente independente de software que executa uma função específica dentro de um sistema maior. Cada microsserviço opera de forma independente, comunica-se com outros por meio de conexões seguras e pode ser atualizado ou substituído sem interromper todo o sistema.
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.
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.

Termo	Descrições
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.
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, resultantes da comprometimento da confidencialidade, integridade, disponibilidade e responsabilidade de dados sensíveis ou da confiabilidade, segurança ou capacidade do GPE.

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.
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).

Termo	Descrições
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.
Acesso Não Autorizado	Uma pessoa obtém acesso lógico ou físico sem permissão a uma rede, sistema, aplicativo, dado ou outro recurso.
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.
Vulnerabilidade	Software, hardware ou outras fraquezas em uma rede ou sistema que podem servir de "porta" para a introdução de uma ameaça.