GLI®

FRAMEWORK DE SEGURANÇA PARA JOGOS

GLI-GSF-2

AVALIAÇÃO DE SEGURANÇA TÉCNICA DE JOGOS (GTS)

Versão 1.0 – Publicada em 7 de fevereiro 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-2 estabelece um parâmetro para a realização de avaliações de Segurança Técnica em Jogos (GTS) do GPE de uma Empresa de Jogos.
b. Esses Testes GTS 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-1, que fornece 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
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 garantir o 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 Metodologias de Teste GTS.

2. AVALIAÇÕES GTS

2.1. Visão Geral da Avaliação

A Avaliação GTS 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 GTS detalhada no GLI-GSF-2 está em testes técnicos de segurança para jogos; outros métodos de avaliação são discutidos nos módulos de suporte do GLI-GSF.

2.2. Métodos de Avaliação

Uma Avaliação GTS utiliza uma variedade de métodos de avaliação, incluindo os seguintes, cujos resultados são usados para apoiar a determinação da segurança de um GPE:

a. Entrevista: Um tipo de método de avaliação 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 avaliação 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 avaliação caracterizado pelo processo de exercitar um ou mais objetos de avaliação sob condições especificadas para comparar o comportamento real com o esperado.

2.3. Tarefas de Avaliação

A seguir estão as atividades de avaliação de alto nível da GTS sugeridas. O Apêndice detalha os requisitos mínimos do Teste GTS com mais detalhes. Os usuários deste documento são direcionados ao Apêndice para garantir que nenhum Teste GTS necessário seja negligenciado. Os Testes GTS listados no Apêndice não são exaustivos e podem ser incluídos Testes GTS adicionais com base nos requisitos regulatórios e no escopo da Avaliação GTS. As Avaliações GTS devem abranger mais do que varreduras automatizadas e incorporar técnicas manuais de Teste de Penetração.

2.3.1. Avaliação de Vulnerabilidade

A ISF realiza uma Avaliação de Vulnerabilidades dos sistemas, sites da internet, aplicativos móveis, redes internas, externas e sem fio da Empresa de Jogos, com o objetivo de identificar vulnerabilidades ou potenciais vulnerabilidades de dispositivos, sistemas e aplicações que transferem, armazenam ou processam dados sensíveis conectados ou presentes nas redes. As Avaliações de Vulnerabilidade incluem a identificação e quantificação passiva de riscos potenciais dentro do GPE.

2.3.2. Teste de Penetração

A ISF realiza um Teste de Penetração dos sistemas, sites da internet, aplicativos móveis e redes internas, externas e sem fio da Empresa de Jogos para confirmar se vulnerabilidades identificadas em dispositivos, sistemas e aplicações são suscetíveis a comprometimento. Simplesmente executar uma Varredura de Vulnerabilidade e fornecer esses resultados não é suficiente para cumprir os requisitos do Teste de Penetração. Deve haver algum tipo de verificação manual e/ou exploração. Os testes de penetração incluem:

a. Avaliação da segurança tanto dos ambientes externos quanto internos do GPE.
b. Identificar fraquezas que poderiam ser exploradas por atacantes para obter acesso não autorizado, interromper operações ou exfiltrar dados sensíveis.
c. Simulando cenários de ataque potenciais para entender o impacto das vulnerabilidades na postura de segurança do GPE.
d. Validando os resultados das Avaliações de Vulnerabilidade por meio de técnicas manuais de testes.

2.3.3. Avaliação de Risco

A ISF realiza uma Avaliação de Risco para identificar não conformidades a qualquer Teste GTS 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 (crítico, alto risco, médio ou baixo risco) 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.

2.4. Frequência de Avaliação

2.4.1. Avaliação Inicial

A Empresa de Jogos deve ter uma Avaliação GTS realizada por um ISF dentro de noventa dias após o início das operações de jogo dentro dessa jurisdição, salvo aviso contrário pelo Órgão Regulador. Qualquer adiamento da Avaliação GTS solicitado pela Empresa de Jogos, juntamente com um cronograma atualizado, deve ser autorizado pelo Órgão Regulador.

NOTA: Recomenda-se que um Órgão Regulador permita flexibilidade para os cronogramas de avaliação GTS para empresas de jogos multijurisdicionais, permitindo a consolidação das avaliações de múltiplas jurisdições em um cronograma comum.

2.4.2. Avaliação Anual

A Empresa de Jogos deve, como regra, realizar outra Avaliação GTS por um ISF dentro de doze meses após a Avaliação GTS anterior, a menos que o Órgão Regulador tenha orientado o contrário. Qualquer adiamento desta avaliação conforme solicitado pela Empresa de Jogos, juntamente com um cronograma atualizado, deve ser autorizado pelo Órgão Regulador.

NOTA: Recomenda-se que um Órgão Regulador permita flexibilidade para os cronogramas de avaliação GTS para empresas de jogos multijurisdicionais, permitindo a consolidação das avaliações de múltiplas jurisdições em um cronograma comum.

2.4.3. Avaliações Adicionais

A Empresa de Jogos deve, como regra, ter Avaliações GTS adicionais realizadas por um ISF após quaisquer mudanças críticas dentro do GPE, como atualizações e modificações de infraestrutura ou aplicação, ou a instalação de novos Componentes Críticos do Sistema. A determinação do que constitui uma "mudança crítica" baseia-se no processo de Avaliação de Risco da Empresa de Jogos, na configuração específica do GPE e nos requisitos do Órgão Regulador. No entanto, qualquer mudança que possa afetar a segurança do GPE ou permitir o acesso a dados sensíveis e/ou Componentes Críticos do Sistema pode ser considerada uma "mudança crítica" pela Empresa de Jogos.

2.5. Relatórios de Avaliação

Os resultados de uma Avaliação GTS identificam para as Empresas de Jogos quais áreas das operações devem ser consideradas melhorias e recomendam estratégias para melhorar essas áreas. O relatório de Avaliação GTS deve ser submetido ao Órgão Regulador até, no máximo, noventa dias após a conclusão da Avaliação GTS, a menos que o Órgão Regulador tenha informado o contrário. O relatório de avaliação da GTS deve incluir o seguinte:

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 Avaliação GTS:
   i. O nome da ISF, a filiação à empresa, as informações de contato e as qualificações e experiência dos indivíduos que realizaram a Avaliação GTS.
   ii. A(s) data(s) da Avaliação GTS, incluindo a data do pedido, a data de início, a data de conclusão e a data do relatório.
c. Escopo da Avaliação GTS:
   i. Uma visão geral de alto nível dos testes realizados, especificando os ambientes (por exemplo, desenvolvimento, produção) e os tipos de sistemas testados (por exemplo, aplicações web, redes, bancos de dados, sistemas operacionais).
   ii. Identificação de Componentes Críticos do Sistema e ativos revisados, detalhando como esses componentes e ativos foram selecionados como parte da Avaliação GTS.
   iii. Ferramentas e técnicas específicas utilizadas durante a Avaliação GTS, incluindo nomes de softwares, versões e sites oficiais das ferramentas empregadas.
d. Metodologia:
   i. Uma descrição detalhada da metodologia de Teste de Penetração ou do framework de Avaliação de Vulnerabilidade aplicada (por exemplo, OWASP, OSSTMM).
   ii. Quaisquer limitações ou exclusões na Avaliação GTS, 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 vulnerabilidades 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 de cada vulnerabilidade descoberta, categorizada por gravidade (por exemplo, crítica, alto risco, médio, baixo risco).
   ii. Uma explicação detalhada de cada vulnerabilidade, apoiada por evidências (por exemplo, capturas de tela, logs).
   iii. Uma avaliação do impacto ou risco potencial associado a cada vulnerabilidade identificada, considerando o ambiente específico da empresa de jogos.
   iv. Passos de remediação recomendados para cada vulnerabilidade identificada, com níveis de prioridade e prazos sugeridos para mitigação.
   v. Passos recomendados de remediação para cada vulnerabilidade identificada, com níveis de prioridade e prazos sugeridos para mitigação.
   vi. A resposta da Empresa de Jogos às descobertas e resultados, incluindo as medidas recomendadas para remediação.

2.6. Remediação

Se o relatório de Avaliação GTS 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.

a. Cada vulnerabilidade deve ser resolvida pelo processo de remediação da Empresa de Jogos, incluindo:
   i. Ações tomadas para determinar a extensão e conter a vulnerabilidade específica.
   ii. Investigação da causa raiz para determinar as causas mais básicas da vulnerabilidade.
   iii. Ações tomadas para corrigir a vulnerabilidade e, em resposta à causa raiz, eliminar a recorrência da vulnerabilidade.
b. As medidas de remediação para resolver cada vulnerabilidade crítica ou de alto risco 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 indicação em contrário pelo Órgão Regulador. Se solicitado pelo Órgão Regulador, o ISF deve realizar uma avaliação de acompanhamento dentro de um prazo razoável especificado no plano de remediação para confirmar as ações tomadas, avaliar sua eficácia e determinar se as vulnerabilidades foram resolvidas.
c. As medidas de remediação para tratar cada vulnerabilidade identificada de risco médio ou baixo devem ser documentadas e enviadas pela Empresa de Jogos ao Órgão Regulador e à ISF, se exigido pelo Órgão Regulador, para revisão dentro de trinta dias, salvo especificação em contrário pelo Órgão Regulador. Se as ações forem consideradas satisfatórias, elas devem ser acompanhadas na próxima avaliação 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.

2.7. Empresa Independente de Segurança (ISF)

A Avaliação GTS deve ser realizada por indivíduos com qualificações suficientes, o que significa que a ISF deve contratar 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 Avaliação GTS:
   i. Profissional Certificado em Segurança Ofensiva (OSCP);
   ii. Hacker Ético Certificado (CEH);
   iii. Certificações em Garantia Global da Informação (GIAC): Testador de Penetração Certificado GIAC (GPEN), Testador de Penetração de Aplicações Web GIAC (GWAPT), Pesquisador de Exploits GIAC e Testador Avançado de Penetração (GXPN);
   iv. certificação da Autoridade Nacional para Cibersegurança (NCSC) do Serviço de Verificação de Saúde de TI (CHECK);
   v. Esquema Tigre: Testador de Segurança Sênior, Testador de Segurança Qualificado;
   vi. Fornecedor Aprovado de Escaneamento (ASV);
c. Ter pelo menos cinco anos de experiência realizando avaliações técnicas de segurança na indústria de jogos ou, quando aceitável para o Órgão Regulador, outra experiência relevante avaliando a segurança de uma indústria similar; e
d. 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 avaliada.

3. VARREDURAS RECORRENTES DE VULNERABILIDADES

3.1. Cadência dos Escaneamentos

Salvo especificação em contrário pelo Órgão Regulador, Varreduras de Vulnerabilidades internas e externas da rede devem ser realizadas pelo menos trimestralmente e após quaisquer mudanças críticas dentro do GPE. Qualquer adiamento da Varredura de Vulnerabilidades conforme solicitado pela Empresa de Jogos, juntamente com um cronograma atualizado, deve ser autorizado pelo Órgão Regulador.

NOTA: Recomenda-se que um Órgão Regulador permita flexibilidade para cronogramas de Varredura de Vulnerabilidades para Empresas de Jogos multijurisdicionais, permitindo a consolidação de varreduras para múltiplas jurisdições em um cronograma comum.

3.2. Requisitos para Scanners

Scanners de vulnerabilidades devem ser usados para testar e identificar vulnerabilidades de dispositivos internos de rede, aplicações e defesas perimetral de rede, bem como para cumprir o plano e padrões de segurança. Scanners de vulnerabilidades devem ter a capacidade de lidar com as seguintes tarefas mínimas:

a. Não Disruptivo: O scanner deve ser configurado para evitar métodos de teste disruptivos que possam causar travamentos do sistema, reinicializações ou interferir em serviços de rede como Domain Name Service (DNS), roteamento ou comutação.
b. Descoberta do Host: O scanner deve identificar com precisão sistemas ativos, incluindo aqueles que não respondem aos requisições padrão de eco ("ping") do Protocolo de Mensagens de Controle de Controle da Internet (ICMP).
c. Descoberta de Serviços: O scanner deve realizar uma varredura minuciosa de portas em todas as portas do Protocolo de Controle de Transmissão (TCP) e portas do Protocolo de Datagramas de Usuário (UDP), garantindo cobertura abrangente de serviços como protocolos de autenticação, servidores de banco de dados e outros componentes críticos de infraestrutura.
d. Impressão Digital do Sistema Operacional e do Serviço: O scanner deve identificar com precisão os sistemas operacionais e as versões dos serviços para ajudar a priorizar os esforços de remediação de forma eficaz.
e. Independência da Plataforma: O scanner deve ser compatível com todas as plataformas comumente usadas, garantindo ampla aplicabilidade.
f. Precisão: O scanner deve relatar tanto vulnerabilidades confirmadas quanto potenciais com alto nível de certeza, garantindo que até mesmo riscos potenciais sejam considerados nas determinações de conformidade.
g. Consideração do Balanceador de Carga: Em ambientes que utilizam balanceadores de carga, o scanner deve levar em conta possíveis inconsistências de configuração e garantir que todos os endereços IP relevantes sejam devidamente escaneados.
h. Requisitos Específicos de Componentes: O scanner deve ser capaz de detectar vulnerabilidades em vários componentes, garantindo cobertura completa de todos os riscos potenciais de segurança. Componentes chave incluem:
    i. Firewalls e roteadores: Escaneie vulnerabilidades e problemas de configuração que possam comprometer a segurança da rede.
    ii. Sistemas Operacionais: Detectar exploits conhecidos e garantir que os sistemas estejam adequadamente atualizados.
    iii. Servidores de Banco de Dados: Identificar qualquer acesso aberto da Internet e detectar vulnerabilidades conhecidas.
    iv. Servidores Web: Teste vulnerabilidades e problemas de configuração, incluindo navegação por diretórios.
    v. Servidores de Aplicação: Detectar a presença de vulnerabilidades em servidores de aplicações e suas configurações.
    vi. Scripts Web Comuns: Identifique vulnerabilidades em scripts como CGI, ASP e PHP.
    vii. Contas Integradas: Detectar contas e senhas padrão, reportando quaisquer vulnerabilidades desse tipo.
    viii. Servidores DNS: Detectar vulnerabilidades, incluindo problemas com transferências de zonas DNS.

ix. Servidores de E-mail: Identifique vulnerabilidades específicas para configurações de servidores de e-mail.
x. Componentes de Virtualização: Detectar vulnerabilidades em hosts virtuais, máquinas e hipervisores.
xi. Aplicações Web: Detectar vulnerabilidades como SQL Injection e Cross-Site Scripting (XSS), especialmente em aplicações web personalizadas.
xii. Outras Aplicações: Escaneie vulnerabilidades em vários aplicativos, como mídia de streaming ou servidores proxy.
xiii. Serviços Comuns: Identificar vulnerabilidades em serviços como compartilhamento de arquivos e e-mail.
xiv. Pontos de Acesso Sem Fio (WAPs): Detectam vulnerabilidades e configurações incorretas em redes sem fio.
xv. Portas dos fundos/Malware: Identifique a presença de softwares maliciosos como rootkits e trojans.
xvi. SL/TLS: Detectar protocolos e configurações criptográficas inseguras, garantindo conformidade com padrões rigorosos de criptografia.
xvii. Protocolos Anônimos de Concordância de Chaves: Identificar e relatar o uso de protocolos criptográficos inseguros que não possuem autenticação de servidor.
xviii. Acesso Remoto: Detectar configurações inseguras de acesso remoto que possam comprometer o ambiente.

3.3. Tarefas de Varredura

As Varreduras de Vulnerabilidade Internas devem ser realizadas sob a perspectiva de uma varredura credenciada. Varreduras de Vulnerabilidades Externas podem ser realizadas a partir de uma perspectiva de varredura não credenciada.

3.4. Identificação de vulnerabilidades

Um processo deve ser estabelecido para identificar vulnerabilidades, usando fontes externas confiáveis para informações sobre vulnerabilidades, e usar um sistema de pontuação apropriado para segurança em jogos (por exemplo, CVSS, ISO/IEC 31010, etc.), para atribuir um nível de gravidade (crítico, alto risco, médio ou baixo risco) às vulnerabilidades de segurança recém-descobertas. O sistema de pontuação utilizado deve ser identificado nos resultados de varredura.

3.5. Resultados de Varredura

A Empresa de Jogos deve submeter a verificação das Varreduras de Vulnerabilidades ao Órgão Regulador e incluir um plano de remediação e quaisquer planos de mitigação de riscos para essas vulnerabilidades que não possam ser resolvidas. Se exigido pelo Órgão Regulador, as re-varreduras devem ocorrer até que cada vulnerabilidade crítica ou de alto risco seja resolvida e/ou aceita por meio de um programa formal de aceitação de riscos. Todas as vulnerabilidades verificadas devem ser corrigidas pela Empresa de Jogos e documentadas em um relatório fornecido ao Órgão Regulador.

3.6. Qualificações de Escaneamento

As Varreduras de Vulnerabilidades trimestrais devem ser realizadas por um ISF, a equipe qualificada do Órgão Regulador atuando como ISF, ou por meio de um funcionário qualificado da Empresa de Jogos atuando como ISF, que é separado, em termos organizacionais, da função que implementa mudanças no GPE.

APÊNDICE: TESTES DE SEGURANÇA TÉCNICA EM JOGOS (GTS)

A. Metodologias de Teste GTS

O Teste GTS deve consistir em uma avaliação da segurança do GPE por meio de uma simulação de ataque por um ISF, seguindo metodologias conhecidas de Avaliação de Vulnerabilidades e Testes de Penetração, conforme prescrito pelo Manual de Metodologia de Testes de Segurança de Código Aberto (OSSTMM), o Projeto de Segurança de Aplicações Web Abertas (OWASP), o Padrão de Execução de Testes de Penetração (PTES), o Guia Técnico do Instituto Nacional de Padrões e Tecnologia (NIST) para Testes e Avaliação de Segurança da Informação (SP800-115). e outras especificações conforme necessário. Essas metodologias garantem que as informações coletadas durante os Testes GTS tenham detalhes suficientes para avaliar com precisão as áreas de exposição ao risco e seu impacto potencial no GPE.

NOTA: Espera-se que testes relacionados à segurança de rede, sistema e servidor sejam realizados no GPE ao vivo. Para evitar qualquer interrupção nos serviços ativos, testes relacionados à segurança de aplicações podem ser realizados em um ambiente não de produção (por exemplo, ambiente de desenvolvimento, ambiente de testes, etc.) que espelhe de perto a configuração do GPE para garantir resultados precisos.

A.1. Testes de Caixa Branca

O Teste White Box é realizado com pleno conhecimento da arquitetura interna do GPE, incluindo acesso ao código-fonte, configurações de rede e documentação detalhada. Essa abordagem permite um exame minucioso do funcionamento interno do sistema, possibilitando a identificação de vulnerabilidades que podem não ser aparentes por meio de testes externos.

A.2. Testes da Caixa Cinza

O Teste da Caixa Cinza combina elementos tanto do Teste da Caixa Branca quanto do Teste da Caixa Preta. A ISF tem conhecimento parcial da estrutura interna do GPE, frequentemente refletindo a perspectiva de um usuário com privilégios elevados, mas não acesso administrativo completo. Essa abordagem simula um cenário em que um atacante possui algum conhecimento interno e visa testar controles GIS com uma perspectiva semi-privilegiada.

A.3. Testes em Caixa Preta

O Teste Black Box é realizado sem qualquer conhecimento prévio da arquitetura interna do GPE. A ISF aborda o sistema como um atacante externo, tentando identificar e explorar vulnerabilidades sem qualquer informação privilegiada. Esse tipo de teste é crucial para simular cenários de ataque no mundo real.

B. Avaliações de Vulnerabilidade

As Avaliações de Vulnerabilidades são um processo crítico para identificar vulnerabilidades usando bancos de dados de vulnerabilidades atualizados, que podem ser explorados posteriormente durante Testes de Penetração por meio de consultas básicas relacionadas a serviços em execução nos sistemas a partir dos quais é possível acessar dados sensíveis. Dadas as janelas de teste limitadas, o ISF deve ter visibilidade total e a capacidade de contornar certas proteções, incluindo todos os serviços de aprimoramento de segurança dos Provedores de Serviço (por exemplo, Redes de Entrega de Conteúdo, Inspeção Profunda de Pacotes, Proteção contra Negação de Serviço, Firewalls de Aplicações Web, etc.) para permitir uma avaliação mais precisa e abrangente, removendo obstáculos que poderiam mascarar vulnerabilidades. As Avaliações de Vulnerabilidades podem ser realizadas usando scanners automatizados de vulnerabilidades.

B.1. Avaliação de Vulnerabilidades da Camada Interna de Rede

O objetivo da Avaliação de Vulnerabilidades da Camada Interna de Rede é identificar vulnerabilidades de segurança na infraestrutura interna do GPE. Esta Avaliação de Vulnerabilidades tem como objetivo descobrir vulnerabilidades que podem ser exploradas por ameaças internas, contas comprometidas ou atacantes que tenham obtido acesso à rede interna por meio de violações externas ou movimentos laterais.

a. Os alvos desta Avaliação de Vulnerabilidade são os sistemas voltados internamente, que incluem:
   i. Servidores dentro da DMZ ou LAN.
   ii. Estações de trabalho e outros dispositivos de rede conectados ao GPE.
   iii. Aplicações e serviços que lidam com dados sensíveis ou operações críticas.

b. A ISF deve realizar uma série de atividades projetadas para identificar e mapear a rede interna, enumerar sistemas e descobrir vulnerabilidades de segurança:
   i. Levantamento de Rede: Mapeamento completo da rede interna para detectar hosts ativos, arquitetura de rede e dispositivos conectados. Essa fase ajuda a definir a superfície interna de ataque.
   ii. Varredura de Portas: Identificação de portas abertas em sistemas internos, revelando serviços potencialmente expostos que atacantes podem explorar.
   iii. Identificação do Sistema (Enumeração): Detecção de sistemas operacionais, tipos de dispositivos e serviços em execução na rede. Isso inclui identificar todos os dispositivos e sistemas críticos de infraestrutura no ambiente interno.
   iv. Enumeração de Serviços: Coleta de informações detalhadas sobre serviços e aplicações em execução para entender suas versões, configurações e vulnerabilidades associadas.
   v. Varredura Não Credenciada: Essas Varreduras de Vulnerabilidades simulam um atacante sem acesso interno ou credenciais de autenticação válidas. Eles são usados para identificar portas abertas, serviços e vulnerabilidades básicas visíveis para qualquer pessoa que tenha acesso à rede.
   vi. Varredura com Credenciais: Essas Varreduras de Vulnerabilidades utilizam credenciais de autenticação válidas para realizar uma inspeção mais detalhada dos sistemas internos. Eles são usados para revelar insights mais profundos sobre níveis de patch, fraquezas na configuração, controles GIS ausentes e permissões inadequadas, fornecendo uma análise mais abrangente dos potenciais vetores de ataque.
   vii. Encontrando Validação e Eliminação de Falsos Positivos: O ISF deve tentar validar os achados das Varreduras de Vulnerabilidades para garantir que os problemas relatados sejam precisos. Isso inclui a verificação manual dos detalhes das vulnerabilidades para confirmar sua legitimidade e a remoção de falsos positivos dos resultados, garantindo que apenas riscos reais e acionáveis sejam reportados.

c. Para garantir uma cobertura completa, o ISF deve avaliar diferentes camadas da rede e da pilha tecnológica, incluindo segurança em nível de host, rede e aplicação em nível de segurança:
   i. Varredura de Portas e Serviços: A ISF deve escanear todos os sistemas e estações de trabalho para identificar portas abertas e serviços em execução que possam fornecer pontos de entrada para atacantes.
   ii. Teste de VLAN da Camada 2: A ISF deve avaliar a configuração das VLANs, garantindo que estejam devidamente segmentadas e seguras. Isso inclui testes para sub-redes ou dispositivos não intencionais que compartilham o mesmo domínio de broadcast.
   iii. Teste de Rede da Camada 3: O ISF deve avaliar as VLANs que se conectam a zonas públicas ou à DMZ da Internet, garantindo que não haja exposição indevida dos sistemas internos a ameaças externas.
   iv. Enumeração Abrangente de Vulnerabilidades: A ISF deve enumerar todos os computadores internos e dispositivos de rede para fornecer um inventário detalhado das vulnerabilidades presentes na rede. Isso inclui tanto sistemas ativos quanto componentes de infraestrutura passiva, como switches, roteadores e firewalls.

d. O uso da varredura credenciada oferece uma visão mais profunda das configurações internas e da postura de segurança. Uma abordagem amostral de 20%-30% do inventário do GPE pode ser utilizada para as varreduras, focando em sistemas de alto risco ou naqueles que lidam com dados sensíveis. A varredura credenciada avalia configurações como:
   i. Permissões de Usuário: Garantir que os controles de acesso sejam devidamente aplicados e que não haja privilégios excessivos concedidos a usuários não administrativos.
   ii. Gerenciamento de Patches: Identificar sistemas que estão sem patches ou atualizações críticas de segurança.
   iii. Fraquezas de Configuração: Revelar configurações incorretas que podem expor dados sensíveis ou permitir acesso não autorizado.

B.2. Avaliação de Vulnerabilidade da Camada Externa de Rede

O objetivo da Avaliação de Vulnerabilidades da Camada Externa de Rede é identificar vulnerabilidades de segurança dentro da infraestrutura externa do GPE. A Avaliação de Vulnerabilidades da Camada Externa de Rede tem como objetivo descobrir vulnerabilidades que possam ser exploradas por ameaças externas, usuários não autorizados ou atacantes que visem sistemas acessíveis publicamente.

a. Os alvos da Avaliação de Vulnerabilidade da Camada Externa de Rede são os sistemas voltados para o exterior, que incluem:
    i. Servidores e dispositivos acessíveis por endereços IP públicos.
    ii. Aplicações e serviços expostos à internet que lidam ou transmitem dados sensíveis.
    iii. Firewalls públicos e dispositivos de rede que protegem o ambiente interno do GPE.
b. A ISF deve realizar uma série de atividades projetadas para identificar e mapear a rede externa, enumerar sistemas expostos e descobrir vulnerabilidades de segurança:
    i. Levantamento de Rede: Mapeamento completo da rede externa para detectar hosts ativos, arquitetura de rede e dispositivos conectados. Essa fase ajuda a definir a superfície externa de ataque.
    ii. Varredura de Portas: Identificação de portas abertas em sistemas externos, revelando serviços potencialmente expostos que atacantes podem explorar.
    iii. Identificação do Sistema (Enumeração): Detecção de sistemas operacionais, tipos de dispositivos e serviços rodando na rede externa. Isso inclui identificar todos os dispositivos e sistemas críticos de infraestrutura expostos à internet.
    iv. Enumeração de Serviços: Coleta de informações detalhadas sobre serviços e aplicações em execução para entender suas versões, configurações e vulnerabilidades associadas;
    v. Varredura Não Credenciada: Essas Varreduras de Vulnerabilidades simulam um atacante sem acesso interno ou credenciais de autenticação válidas. Eles são usados para identificar portas abertas, serviços e vulnerabilidades básicas visíveis para qualquer pessoa que tenha acesso à rede.
    vi. Encontrando Validação e Eliminação de Falsos Positivos: O ISF deve tentar validar os achados das Varreduras de Vulnerabilidades para garantir que os problemas relatados sejam precisos. Isso inclui a verificação manual dos detalhes das vulnerabilidades para confirmar sua legitimidade e a remoção de falsos positivos dos resultados, garantindo que apenas riscos reais e acionáveis sejam reportados.
c. Dadas as janelas de teste limitadas, o ISF deve ter visibilidade total e a capacidade de contornar certas proteções, incluindo todos os serviços de aprimoramento de segurança dos Provedores de Serviço (por exemplo, Redes de Entrega de Conteúdo, Inspeção Profunda de Pacotes, Proteção contra Negação de Serviço, Firewalls de Aplicações Web, etc.) para permitir uma avaliação mais precisa e abrangente, removendo obstáculos que poderiam mascarar vulnerabilidades. Isso garante que a postura de segurança do GPE seja avaliada com precisão e que nenhuma vulnerabilidade crítica seja negligenciada.

B.3. Avaliação de Vulnerabilidades na Camada de Aplicação

O objetivo da Avaliação de Vulnerabilidades da Camada de Aplicação é identificar vulnerabilidades de segurança em aplicações web, móveis e desktop associadas ao GPE. A Avaliação de Vulnerabilidades da Camada de Aplicação utiliza principalmente métodos automatizados de varredura, complementados por validação manual para garantir precisão. Possíveis vulnerabilidades de segurança podem incluir falhas na validação de entrada, autenticação, gerenciamento de sessões e outras áreas comuns de preocupação.

a. Os objetivos da Avaliação de Vulnerabilidades da Camada de Aplicação são as aplicações expostas a usuários externos (B2C) e portais administrativos internos (B2B) como parte do GPE, que incluem:
    i. Aplicativos voltados ao público acessíveis por usuários e usuários externos.
    ii. Serviços web, APIs e outros componentes essenciais das operações do GPE.
    iii. Integrações business-to-business (B2B), como feeds de dados para odds, dados de correspondência e resultados; Esses serviços devem ser seguros para evitar acessos não autorizados e vazamentos de dados.
    iv. Portais de gerenciamento de back-office usados por parceiros, afiliados ou operadores.
b. O ISF deve realizar uma série de atividades projetadas para identificar e mapear a estrutura, incluindo todas as URLs e pontos de entrada acessíveis, além de descobrir vulnerabilidades de segurança.

c. A ISF deve usar ferramentas automatizadas padrão da indústria para escanear as aplicações em busca de vulnerabilidades. Essas ferramentas são projetadas para detectar uma ampla gama de problemas comuns de segurança, incluindo vulnerabilidades de injeção (e.g. SQL Injection, Cross-Site Scripting (XSS), Command Injection), falhas de autenticação e gerenciamento de sessões, configurações incorretas de segurança e componentes e bibliotecas de aplicações desatualizados:
d. Após a varredura automatizada, o ISF deve validar manualmente os resultados para garantir a precisão e remover falsos positivos. Essa etapa confirma que apenas vulnerabilidades genuínas são relatadas, fornecendo uma visão geral confiável da postura de segurança da aplicação

C. Testes de Penetração

Testes de Penetração são um processo crítico para avaliar a segurança do GPE, simulando a perspectiva do atacante ao identificar e explorar vulnerabilidades que possam comprometer a confidencialidade, integridade e disponibilidade do GPE. Testes de penetração permitem que a ISF valide as vulnerabilidades identificadas durante as Varreduras de Vulnerabilidades e avalie a eficácia dos controles GIS existentes em cenários de ataque do mundo real.

C.1. Teste de Penetração da Camada Interna de Rede

O objetivo do Teste de Penetração da Camada Interna de Rede é explorar vulnerabilidades identificadas dentro da infraestrutura interna do GPE. O Teste de Penetração da Camada Interna de Rede simula um atacante que já conquistou uma posição na rede interna. O objetivo do Teste de Penetração da Camada Interna de Rede é descobrir vulnerabilidades que possam ser exploradas por ameaças internas, contas comprometidas ou atacantes que tenham violado o perímetro externo.

a. Os alvos do Teste de Penetração da Camada Interna de Rede são os sistemas voltados internamente, que incluem:
    i. Servidores dentro da DMZ ou LAN.
    ii. Estações de trabalho e outros dispositivos de rede conectados ao GPE.
    iii. Aplicações e serviços que lidam com dados sensíveis ou operações críticas.
b. Durante o Teste de Penetração da Camada Interna de Rede, o ISF deve realizar as seguintes atividades-chave:
    i. Reconhecimento e Coleta de Informações:
        1. Levantamento de Rede: Mapeamento da rede interna para identificar hosts ativos, arquitetura de rede e dispositivos conectados, definindo a superfície interna de ataque.
        2. Identificação do Sistema (Enumeração): Identificação de sistemas operacionais, tipos de dispositivos e serviços em execução na rede, com foco em componentes críticos de infraestrutura.
    ii. Varredura interna de rede:
        1. Varredura de Portas: Identificação de portas abertas em sistemas internos para detectar possíveis pontos de entrada.
        2. Enumeração de Serviços: Coleta de informações detalhadas sobre serviços em execução para avaliar suas configurações e vulnerabilidades associadas.
    iii. Identificação de Vulnerabilidades:
        1. Varredura Interna de Vulnerabilidades: Comparar sistemas e serviços identificados com vulnerabilidades conhecidas para destacar patches ausentes, configurações incorretas e falhas de software.
        2. Revisão de Configuração e Controle de Acesso: Avaliação de permissões de usuários, controles de acesso e configurações do sistema para identificar possíveis falhas de segurança.
    iv. Simulação de Ataque:
        1. Tentativas Iniciais de Exploração: Tentar explorar vulnerabilidades identificadas para obter acesso não autorizado dentro da rede interna.
        2. Escalonamento de privilégios e movimento lateral: Testar oportunidades para escalar privilégios e se mover lateralmente dentro da rede para acessar sistemas e dados adicionais.

v. Testes de Segmentação e Isolamento:
    1. Eficácia das VLANs: Avaliar quão bem VLANs e segmentação previnem violações e limitam o movimento lateral.
    2. Medidas de Isolamento: Avaliação das técnicas de isolamento para garantir que contenham efetivamente ameaças e restrinjam acessos não autorizados.
vi. Validação de Controle de Acesso:
    1. Restrição de Movimento Lateral: Garantir que os controles de acesso estejam configurados para evitar movimentos laterais não autorizados dentro da rede.
    2. Proteção Crítica do Sistema: Verificar se os controles de acesso bloqueiam efetivamente o acesso não autorizado a sistemas-chave

C.2. Teste de Penetração na Camada Externa de Rede

O objetivo do Teste de Penetração da Camada de Rede Externa é explorar vulnerabilidades identificadas dentro da infraestrutura voltada para o exterior do GPE. O Teste de Penetração da Camada de Rede Externa simula um ataque de um ator de ameaça externa que tenta invadir o GPE através de seus sistemas voltados para o exterior. O objetivo do Teste de Penetração na Camada Externa de Rede é descobrir vulnerabilidades que possam ser exploradas por atacantes externos para obter acesso não autorizado, interromper operações ou exfiltrar dados sensíveis.

a. Os alvos do Teste de Penetração da Camada de Rede Externa são os sistemas voltados para o exterior, que incluem:
    i. Servidores e dispositivos acessíveis por endereços IP públicos.
    ii. Aplicações e serviços expostos à internet que lidam ou transmitem dados sensíveis.
    iii. Firewalls públicos e dispositivos de rede que protegem o ambiente interno do GPE.
b. Durante o Teste de Penetração da Camada Externa de Redes, a ISF deve realizar as seguintes atividades-chave:
    i. Reconhecimento e Coleta de Informações:
        1. Descoberta baseada em domínio: Identificação de informações publicamente disponíveis relacionadas ao GPE, incluindo nomes de domínio, endereços IP e serviços associados.
        2. Perfil de Rede: Mapeamento da superfície externa de ataque, incluindo a identificação da topologia da rede, serviços ativos e possíveis pontos de entrada.
    ii. Varredura de Rede Externa:
        1. Varredura de Portas: Identificação de portas abertas em sistemas voltados para externamente para detectar possíveis pontos de entrada.
        2. Enumeração de Serviços: Coleta de informações detalhadas sobre serviços expostos, como versões e configurações de software, para avaliar potenciais vulnerabilidades.
    iii. Identificação de Vulnerabilidades:
        1. Varredura de Vulnerabilidades: Comparar sistemas e serviços descobertos com bancos de dados de vulnerabilidades atualizados para identificar fraquezas exploráveis.
        2. Revisão de Configuração e Patches: Avaliação das configurações do sistema para detectar vulnerabilidades de segurança, como software desatualizado, configurações fracas ou serviços expostos.
    iv. Simulação de Ataque:
        1. Tentativas Iniciais de Exploração: Tentar explorar vulnerabilidades identificadas para obter acesso não autorizado a sistemas voltados para o exterior.
        2. Escalonamento de privilégios: Se o acesso inicial for obtido, tente escalar privilégios para obter níveis mais altos de acesso.
        3. Teste de Movimento Lateral: Teste de oportunidades de movimento lateral que possam permitir que um atacante se aprofunde na rede a partir do sistema externo comprometido.
    v. Teste de Bypass:
        1. Avaliação de Defesa do Perímetro: Testando a eficácia das defesas perimetrais, incluindo Firewalls de Aplicações Web (WAF), tentando contorná-las.
        2. Ataques Sofisticados Simulados: Simulação de técnicas avançadas de ataque para avaliar o quanto as medidas de segurança resistem a ameaças sofisticadas.

C.3. Teste de Penetração na Camada de Aplicação

O objetivo do Teste de Penetração da Camada de Aplicação é explorar vulnerabilidades identificadas em todos os tipos de aplicações associadas ao GPE, incluindo aplicações web, aplicativos móveis e aplicativos desktop. O Teste de Penetração da Camada de Aplicação simula cenários de ataque reais para avaliar a resiliência da aplicação contra acessos não autorizados, vazamentos de dados e outras atividades maliciosas. O Teste de Penetração da Camada de Aplicação envolve uma abordagem estruturada, que inclui varredura automatizada como etapa preliminar, seguida de testes manuais aprofundados em áreas centrais de segurança para explorar e validar vulnerabilidades de segurança. O Teste de Penetração da Camada de Aplicação deve seguir os Guias de Teste de Segurança OWASP aplicáveis e deve avaliar as aplicações para o Top 10 do OWASP.

a. Os alvos do Teste de Penetração da Camada de Aplicação são as aplicações expostas a usuários externos (B2C) e portais administrativos internos (B2B) como parte do GPE, que incluem:
    i. Aplicativos voltados ao público acessíveis por usuários e usuários externos.
    ii. Serviços web, APIs e outros componentes essenciais das operações do GPE.
    iii. Integrações business-to-business (B2B), como feeds de dados para odds, dados de correspondência e resultados; Esses serviços devem ser seguros para evitar acessos não autorizados e vazamentos de dados.
    iv. Portais de gerenciamento de back-office usados por parceiros, afiliados ou operadores.
b. Durante o Teste de Penetração da Camada de Aplicação, o ISF deve realizar as seguintes atividades-chave:
    i. Reconhecimento e Coleta de Informações:
        1. Perfil de Aplicações: Colete informações detalhadas sobre a arquitetura da aplicação, incluindo linguagens de programação, frameworks, tecnologias de banco de dados, protocolos de comunicação backend, bibliotecas de terceiros e controles GIS.
        2. Engenharia Reversa: Descompile o aplicativo para examinar o código-fonte, APIs e componentes de terceiros em busca de segredos codificados, exposição de dados sensíveis ou configurações inseguras.
    ii. Testes de Autenticação:
        1. Fiscalização da Política de Credenciais: Revise a política de credenciais da aplicação e garanta que ela cumpra os requisitos de complexidade (comprimento, caracteres e rotação periódica).
        2. Segurança do Armazenamento de Credenciais: Avalie a segurança dos mecanismos de armazenamento de credenciais, garantindo que estejam corretamente hasheados e salgados.
        3. Avaliação de Autenticação Multifator (MFA): Avalie a segurança, eficácia e implementação adequada da MFA e teste possíveis técnicas de bypass.
        4. Resiliência em Ataques por Força Bruta: Teste a resiliência contra ataques de força bruta, incluindo bloqueio de contas e implementações de CAPTCHA.
        5. Autenticação baseada em tokens: Teste a segurança dos tokens de autenticação (JWTs, tokens OAuth) usados pela aplicação para interagir com serviços backend.
    iii. Validação de Autorização:
        1. Testes de Controle de Acesso Baseado em Funções (RBAC): Teste a aplicação de funções em toda a aplicação, garantindo que usuários com diferentes níveis de permissão possam acessar apenas áreas, funções e dados autorizados apropriados para suas funções.
        2. Teste de Escalonamento de Privilégios: Teste vulnerabilidades de escalonamento de privilégios, incluindo escalonamento horizontal e vertical explorando endpoints da API, funcionalidades de aplicações ou configurações backend inseguras.
        3. Teste de Bypass de Autorização: Tente burlar controles de autorização por meio de manipulação de URLs, manipulação de parâmetros ou referências diretas a objetos. Tente acessar áreas não autorizadas usando diferentes níveis de privilégio.
    iv. Testes de Gerenciamento de Sessões:
        1. Revisão do Manuseio de Sessão: Colete e analise cookies de sessão, cabeçalhos e tokens do lado do servidor para possíveis usos indevidos ou configurações incorretas.
        2. Verificação de Segurança do Token de Sessão: Verifique a segurança do token de sessão, incluindo aleatoriedade, singularidade e proteção contra exposição por meio de parâmetros de URL ou cookies inseguros. Garanta que os tokens expirem corretamente,

não sejam reutilizados e sejam tratados corretamente ao fazer logout.

3. Avaliação de Expiração e Tempo de Encerramento da Sessão: Avalie os mecanismos de expiração e tempo de espera para garantir que as sessões sejam adequadamente encerradas após inatividade ou desconectamento.
4. Teste de Vulnerabilidades por Sequestro de Sessão: Teste para vulnerabilidades de sequestro de sessão, como captura de cookies de sessão ou exploração de vulnerabilidades de fixação de sessão.
5. Implementação de Atributos Seguros de Cookie: Garanta que os atributos de cookies seguros estejam ativos, como flags HttpOnly e Secure.

v. Validação de Entrada e Ataques de Injeção:

1. Revisão de Validação de Entrada: Certifique-se de que os campos de entrada do usuário (como nome de usuário, senha, campos de busca, etc.) estejam devidamente validados para evitar vulnerabilidades comuns de aplicação.
2. Ataques de Injeção: Teste a aplicação em busca de vulnerabilidades que possam permitir que um atacante injete código malicioso, SQL, comandos, scripts e injeção LDAP (por exemplo, JavaScript ou cargas úteis maliciosas) dentro da aplicação e suas interações com serviços de backend.
3. Avaliação do Manuseio de Upload de Arquivos: Avalie o tratamento do upload de arquivos para garantir que apenas os tipos permitidos sejam aceitos e processados de forma segura, e que o tamanho e o conteúdo do arquivo sejam validados. Certifique-se de que os uploads de arquivos restrinjam os tipos de arquivos e validem entradas, evitando a execução remota de código.
4. Testes de Validação do Lado do Cliente: Contorne os mecanismos de validação do lado do cliente e avalie se a validação adequada está sendo aplicada no lado do servidor.

vi. Tratamento de Erros e Divulgação de Informações:

1. Avaliação de Sensibilidade a Mensagens de Erro: Avalie se mensagens de erro revelam dados sensíveis sobre o funcionamento interno da aplicação que poderiam ajudar um atacante a planejar novos ataques (por exemplo, rastreamentos de pilha, erros SQL).
2. Identificação de Vazamento de Informação: Identificar casos em que dados sensíveis são expostos inadvertidamente por meio de cabeçalhos do Protocolo de Transporte de Hipertexto (HTTP), mensagens de erro ou outros canais de comunicação.
3. Testes de Manejo de Erros Inesperados: Teste como a aplicação lida com erros inesperados e se dados sensíveis ou detalhes do sistema são expostos durante essas falhas.

vii. Integração e Segurança da API:

1. Avaliação de APIs: Avalie a segurança dos serviços web e APIs usados no GPE, garantindo que eles autentiquem corretamente os usuários, validem as entradas e previnam acessos não autorizados.
2. Testes de Autenticação Baseados em Tokens: Teste a segurança dos tokens OAuth ou de outros mecanismos de autenticação da API, garantindo processos adequados de manuseio e revogação.
3. Avaliação de Limitação de Taxa: Avalie a implementação de mecanismos de limitação de taxa para prevenir ataques e abusos de Negação de Serviço Distribuída (DoS).

viii. Configuração Segura e Fortalecimento:

1. Avaliação de Comunicação Segura: Verifique o uso de HTTPS com padrões modernos de criptografia (TLS 1.2 ou superior) em todos os canais de comunicação entre o cliente e o servidor.
2. Testes de Segurança de Dados em Trânsito: Teste se os dados transmitidos entre a aplicação e os serviços backend estão criptografados usando criptografia forte (TLS 1.2+).
3. Ataque "Homem-No-Meio" (MITM): Teste a vulnerabilidade da aplicação a ataques MITM, garantindo que o tráfego não possa ser interceptado ou modificado por um atacante. Certifique-se de que os certificados sejam validados.
4. Revisão de Exposição Mínima ao Serviço: Confirme que nenhum serviço desnecessário ou porta aberta está rodando no servidor que possa aumentar a superfície de ataque.
5. Avaliação de Fixação de Certificados: Verifique se a aplicação implementa o pin de certificados para evitar o uso de certificados falsificados durante a comunicação com o servidor backend.

ix. Testes de Armazenamento Local de Dados:
    1. Teste de Armazenamento de Dados Inseguros: Teste para dados sensíveis armazenados de forma insegura no dispositivo, incluindo credenciais de autenticação codificadas fixamente, PII, tokens e cookies de sessão armazenados em texto simples ou formatos fracamente criptografados.
    2. Verificação de Permissões de Arquivos e Diretórios: Verifique se as permissões de arquivo estão corretamente definidas, garantindo que apenas usuários autorizados possam acessar arquivos críticos.

x. Gerenciamento de Patches e Testes de Atualização:
    1. Mecanismo de Atualização Segura: Garanta que as atualizações sejam entregues de forma segura e verifique a integridade dos pacotes de atualização.
    2. Aplicação de Patches: Teste se os patches críticos são aplicados prontamente à aplicação e suas dependências.

xi. Lógica de Aplicação e Teste de Fluxo de Trabalho:
    1. Teste de Falhas no Processamento de Transações: Teste para falhas no processamento de transações, como pagamentos insuficientes, pagamentos em excesso ou manipulação dos valores das transações.
    2. Avaliação de Manipulação de Fluxo de Trabalho: Avalie se os fluxos de trabalho podem ser contornados ou manipulados, permitindo que os usuários realizem ações não autorizadas ou pulem etapas críticas.
    3. Teste de Abuso de Funcionalidade: Teste cenários de abuso de funcionalidade em que funções legítimas podem ser usadas indevidamente para ações não intencionais, como reutilizar códigos promocionais ou explorar mecanismos de reembolso.
    4. Validação da Precisão das Apostas e Pagamento: Valide que o processo de inscrição reflita com precisão e segurança os saldos dos patronos, ganhos e histórico de transações.
    5. Segurança da API de Apostas em Eventos: Garanta que as APIs que entregam dados, resultados ou probabilidades de partidas sejam seguras e não possam ser adulteradas.
    6. Teste de Segurança do Saldo do Patrono: Teste a precisão e a segurança dos saldos dos patronos, garantindo que depósitos, saques, apostas e ganhos estejam corretamente refletidos.
    7. Validação de Bônus e Ofertas Promocionais: Valide a implementação de ofertas de bônus e promocionais, garantindo que não possam ser abusadas, contornadas ou manipuladas por falhas lógicas.
    8. Prevenção de Replay de Transações: Certifique-se de que replays ou tentativas de reprodução (como fazer uma nova aposta) não possam levar a transações duplicadas ou ganhos não autorizados.
    9. Avaliação de Detecção de Múltiplas Contas: Avalie a capacidade do aplicativo de detectar e impedir o uso de múltiplas contas para manipular odds, explorar bônus ou envolver conluio.

xii. Componentes e Bibliotecas de Terceiros:
    1. Segurança de Bibliotecas de Terceiros: Revise e avalie a integridade e segurança de quaisquer bibliotecas e dependências de terceiros usadas pelo aplicativo, garantindo que estejam atualizadas e livres de vulnerabilidades conhecidas.
    2. Uso Inseguro de APIs: Teste o uso inadequado de APIs, como implementações inseguras de autenticação biométrica, câmera, microfone e outros recursos do dispositivo.
    3. Gerenciamento de Dependências: Analise as bibliotecas de terceiros usadas na aplicação, verificando quaisquer componentes desatualizados ou vulneráveis que possam comprometer a segurança da aplicação.

c. Para testar aplicações que são executadas a partir de um servidor (aplicações web), a ISF deve realizar as seguintes atividades adicionais de teste:

i. Coleta de Informações Públicas:
    1. Coleta Passiva de Informações: Colete informações sobre o aplicativo usando métodos não intrusivos, como o Google Dorking, para descobrir dados acessíveis publicamente.
    2. Perfil de Tecnologia: Realize buscas WHOIS, enumeração DNS e fingerprinting tecnológico para coletar detalhes sobre a infraestrutura e os serviços da aplicação.

ii. Atendimento entre Sites:
    1. Testes de Scripting Multi-Site (XSS): Teste campos de entrada e parâmetros de URL para ataques XSS e outros relacionados a entradas, garantindo que as entradas estejam devidamente sanitizadas e codificadas. Verifique se os dados apresentados aos usuários estão devidamente higienizados e codificados para mitigar ataques XSS e outros relacionados à saída.
    2. Avaliação de Falsificação de Solicitação Cruzada (CSRF): Avalie a resiliência da aplicação contra ataques CSRF, garantindo o uso adequado de tokens anti-CSRF para proteger contra solicitações não autorizadas.

iii. Uso do Cabeçalho de Segurança:
    1. Implementação do Cabeçalho de Segurança: Garantir a implementação correta de cabeçalhos essenciais de segurança, como Política de Segurança de Conteúdo (CSP) e Segurança de Transporte Estrito (HSTS), para proteger contra vulnerabilidades comuns na web.
    2. Configuração do Cabeçalho de Segurança: Verifique se cabeçalhos de segurança adicionais, como X-Content-Type-Options, estão devidamente configurados para evitar o sniffing do tipo MIME e outros ataques.

d. Para testes de aplicações instaladas no dispositivo do usuário (aplicativos móveis e desktops), o ISF deve realizar as seguintes atividades adicionais de teste:

i. Resistência a Adulterações:
    1. Segurança Binária: Examine os binários da aplicação em busca de fraquezas, garantindo que dados sensíveis não sejam armazenados em formatos inseguros ou incorporados à aplicação.
    2. Técnicas de Ofuscação: Verifique se o código da aplicação está ofuscado para evitar engenharia reversa e manipulação de código por atores maliciosos.
    3. Mecanismos Anti-Adulteração: Teste a presença de mecanismos anti-adulteração que previnam ou detectem alterações não autorizadas nos binários da aplicação ou nos arquivos de configuração.
    4. Autoproteção de Aplicações: Verifique se o aplicativo consegue detectar adulteração ou a presença de depuradores e evitar que agentes maliciosos modifiquem o aplicativo em tempo real.
    5. Proteção contra Reversão: Garanta que o aplicativo evite que atacantes voltem para uma versão vulnerável.

ii. Segurança de Dados Sensíveis e Comunicações:
    1. Cache de Dados e Arquivos Temporários: Certifique-se de que dados sensíveis não sejam armazenados em cache de forma insegura ou deixados em arquivos temporários após o fechamento do aplicativo.
    2. Uso da Área de Transferência: Verifique se dados sensíveis não estão armazenados ou acessíveis involuntariamente via a área de transferência (por exemplo, copiando senhas ou informações de cartão de crédito).
    3. Ataques de Comunicação Interprocessos (IPC): Verifique vulnerabilidades na forma como o aplicativo se comunica com outros processos, garantindo que nenhum dado não autorizado possa ser injetado.

iii. Salvaguardas de Memória:
    1. Vulnerabilidades de Excesso de Buffer: Teste vulnerabilidades de desbordamento de buffer que possam levar à execução remota de código.
    2. Corrupção de Memória: Garanta que proteções de memória, como Prevenção de Execução de Dados (DEP) e Randomização de Layout de Espaço de Endereçamento (ASLR), estejam em vigor.

iv. Proteções de Virtualização e Depuração:
    1. Detecção de Máquinas Virtuais: Garanta que a aplicação possa detectar e evitar ser executada em um ambiente virtualizado, que pode ser usado para manipular ou reverter a engenharia do software.
    2. Anti-Depuração: Teste a presença de técnicas anti-depuração que impeçam o uso de ferramentas de depuração para engenharia reversa da aplicação.

v. Tarefas adicionais de teste de aplicativos móveis:
   1. Análise de Metadados da App Store: Identifique a plataforma do aplicativo (iOS/Android) e revise a listagem da loja de aplicativos, histórico de versões, informações do desenvolvedor e permissões solicitadas pelo aplicativo durante a instalação.
   2. Segurança do Chaveiro/Loja de Chaves: Teste se dados sensíveis estão armazenados de forma segura usando a Keystore do Android ou do iOS, garantindo que os padrões criptográficos adequados sejam seguidos.
   3. Jailbreaking/Detecção de Root: Verifique se o aplicativo pode detectar e responder à execução em um ambiente jailbreak (iOS) ou rooted (Android), limitando o acesso a recursos críticos.

D. Avaliações de Segurança em Nuvem e Contêiner

A Avaliação de Segurança de Nuvem e Contêineres garante a implantação, gestão e operação seguras de ambientes em nuvem e conteinerizados dentro do Ambiente de Produção de Jogos (GPE). A Avaliação de Segurança em Nuvem e Contêineres foca na segurança de componentes baseados em nuvem, aplicações conteinerizadas e nos frameworks de orquestração de suporte para minimizar riscos e melhorar a resiliência de segurança.

D.1. Avaliação de Segurança em Nuvem

O objetivo da Avaliação de Segurança em Nuvem é garantir o gerenciamento seguro dos componentes baseados em nuvem dentro do GPE, garantindo que os controles e configurações GIS específicos da nuvem sejam devidamente implementados e gerenciados. Durante a Avaliação de Segurança em Nuvem, o ISF deve realizar as seguintes atividades-chave:

a. Controles de acesso: Verifique se as políticas de acesso aplicam o princípio do privilégio mínimo e que métodos fortes de autenticação, como autenticação multifator, estão implementados para contas críticas.
b. Gestão de Contas: Avalie os processos de criação, gestão e desativação da conta. Garanta que os papéis e permissões estejam devidamente definidos e que contas inativas ou desnecessárias sejam removidas prontamente.
c. Registro e Monitoramento: Confirme que todas as ações críticas, como acesso a dados sensíveis e alterações de configuração, estão registradas e armazenadas de forma segura. Garanta que mecanismos de monitoramento e alerta estejam em vigor para detectar e responder a potenciais incidentes de segurança.
d. Configuração de Segurança: Revise as configurações da rede e dos recursos para garantir segmentação, isolamento e controle de tráfego adequados. Verifique se os dados sensíveis estão criptografados e se as chaves de criptografia são gerenciadas com segurança.
e. Revisão de Regras e Políticas de Firewall: Garantir que firewalls específicos da nuvem (por exemplo, grupos de segurança, políticas nativas de nuvem) estejam corretamente configurados para restringir o acesso com base no privilégio mínimo.
f. Isolamento de Serviços e Aplicações: Revise a segmentação de serviços e aplicações em nuvem, garantindo que estejam devidamente isolados uns dos outros para minimizar o risco de movimentação lateral por parte de atacantes.

D.2. Avaliação da Segurança dos Contêineres

O objetivo da Avaliação de Segurança de Contêineres é avaliar a postura de segurança dos GPEs que utilizam tecnologia baseada em contêineres (por exemplo, Kubernetes), identificando vulnerabilidades, configurações incorretas e ameaças potenciais para garantir a integridade, confidencialidade e disponibilidade de aplicações e dados. Durante a Avaliação de Segurança do Container, a ISF deve realizar as seguintes atividades-chave:

a. Configuração do Contêiner:
   i. Gerenciamento Seguro de Imagens: Garanta que as imagens dos contêineres sejam de fontes confiáveis, escaneadas regularmente em busca de vulnerabilidades e minimizadas para reduzir superfícies de ataque.
   ii. Endurecimento de Configuração: Verifique se os contêineres estão configurados de acordo com as melhores práticas, com serviços desnecessários desativados e limites de recursos aplicados.

b. Segurança de Orquestração:
   i. Segurança do Cluster: Avalie a segurança da plataforma de orquestração, incluindo configurações do plano de controle, segurança dos nós e isolamento da carga de trabalho.
   ii. Controle de acesso: Revise as configurações do RBAC para garantir a atribuição correta de permissões e o acesso administrativo restrito.
   iii. Políticas de Rede: Avalie a segmentação da rede e o controle de tráfego dentro do ambiente de contêineres para garantir comunicação segura e restrita.
c. Segurança em Tempo de Execução:
   i. Monitoramento e Detecção de Ameaças: Implementar e revisar o monitoramento do comportamento em tempo de execução do contêiner para detectar anomalias e responder a ameaças.
   ii. Gerenciamento de Patches: Garanta que as imagens dos contêineres sejam atualizadas com os patches de segurança mais recentes e que imagens desatualizadas não sejam implantadas.
d. Segurança da Cadeia de Suprimentos:
   i. Gerenciamento de Dependências: Monitore e gerencie bibliotecas e dependências de terceiros para reduzir o risco de ataques à cadeia de suprimentos.
   ii. Segurança do Pipeline: Proteja o pipeline CI/CD para garantir que apenas código verificado e seguro seja implantado.

E. Avaliações e Testes Adicionais

E.1. Avaliação de Segurança de Firewall

O objetivo da Avaliação de Segurança do Firewall é identificar potenciais fraquezas nas configurações do firewall, conjuntos de regras e práticas de gerenciamento. A Avaliação de Segurança do Firewall garante que o firewall seja devidamente configurado e gerenciado para prevenir acessos não autorizados e mitigar ameaças de segurança, em conformidade com as políticas de GIS da Empresa de Jogos e as melhores práticas do setor. Durante a Avaliação de Segurança do Firewall, a ISF deve realizar as seguintes atividades-chave:

a. Análise da Arquitetura de Rede:
   i. Compreendendo o Ambiente: Compreender profundamente a arquitetura de rede do GPE, incluindo os ativos que o firewall deve proteger e as potenciais ameaças a esses ativos.
   ii. Identificação de Falhas de Projeto: Avaliação da posição do firewall dentro da rede para identificar quaisquer falhas ou vulnerabilidades de projeto em sua implantação atual em comparação com as melhores práticas da indústria.
b. Revisão do Conjunto de Regras:
   i. Regra do Privilégio Mínimo: Garantir que as regras sejam configuradas de acordo com o princípio do privilégio mínimo.
   ii. Restrição de Conexão: Confirme que as conexões de entrada e saída estão restritas apenas a serviços necessários.
   iii. Tradução de Endereços de Rede (NAT): Verifique se o NAT está corretamente implementado.
   iv. Bloqueio de Protocolos: Garanta que todos os protocolos desconhecidos ou indefinidos estejam bloqueados.
   v. Presença da Regra de Limpeza: Confirme a presença de uma regra de "limpeza" para lidar com tráfego não especificado.
   vi. Revisão da Documentação das Regras: Revise e confirme se as regras estão devidamente documentadas e que as regras temporárias são desativadas ou removidas quando não forem mais necessárias.
c. Revisão das Configurações de Configuração:
   i. Configuração de Acesso Não Autorizado: Identifique quaisquer configurações de configuração que possam permitir acesso não autorizado ou comprometer a segurança dos sistemas protegidos pelo firewall.
   ii. Conformidade com a Política de Firewall: Verifique se a configuração do firewall está alinhada com as políticas de GIS da Empresa de Jogos e as melhores práticas do setor.
d. Análise do Central Management Console:
   i. Controle de Acesso: Garanta que apenas pessoal autorizado possa acessar o console de gerenciamento do firewall e que os controles de acesso sejam devidamente aplicados.

ii. Proteção do Console: Confirme que o console de gerenciamento está adequadamente protegido contra acessos não autorizados, incluindo o uso de protocolos criptografados para gerenciamento remoto.

e. Registro, Auditoria e Monitoramento:
   i. Configuração de Logs: Certifique-se de que o logging esteja ativado para eventos de segurança (por exemplo, falhas em logins) e que os logs de auditoria estejam configurados para capturar dados relevantes.
   ii. Gestão de Logs: Confirme que os logs de auditoria são escritos em um local central, copiados regularmente e revisados periodicamente para detectar atividades suspeitas.
   iii. Monitoramento e Alerta: Verifique se mecanismos de alerta estão em vigor para fornecer visibilidade em tempo real sobre possíveis incidentes de segurança.

f. Gerenciamento de Patches:
   i. Implementação de Patches: Confirme que existe um sistema para testar patches antes de implantá-los em firewalls de produção, e que todos os patches relacionados à segurança são aplicados prontamente.
   ii. Revisão de Patches: Avalie se o firmware e o software do firewall estão atualizados e alinhados com as melhores práticas de segurança.

g. Segurança de Acesso Remoto:
   i. Segurança de Protocolos: Garanta que protocolos desnecessários para acessar o firewall estejam desativados e que o acesso remoto só seja permitido por protocolos seguros e criptografados.
   ii. Restrições de acesso: Verifique se o acesso remoto ao firewall está restrito a redes confiáveis e endereços IP específicos.
   iii. Filtragem de Tráfego: Confirme que a filtragem de tráfego está adequadamente configurada para controlar o fluxo de dados entre ambientes de nuvem e entre infraestruturas de nuvem e on-premiss.

h. Segurança de Rede Virtual:
   i. Segmentação de Rede: Avalie a segmentação dentro das redes virtuais, garantindo que dados sensíveis e serviços críticos estejam isolados de áreas menos seguras.
   ii. Gestão de Tráfego entre Ambientes: Garantir o gerenciamento seguro do tráfego entre diferentes ambientes de nuvem, bem como entre sistemas em nuvem e on-premises, com foco em criptografia e proteção da integridade dos dados.

i. Integração com Identidade e Gerenciamento de Acesso (IAM):
   i. Políticas de Controle de Acesso: Garanta que as políticas IAM estejam integradas aos firewalls em nuvem para impor controle rigoroso de acesso e acesso baseado em funções.
   ii. Autenticação Multifator (MFA): Verifique se a MFA está sendo aplicada para acessar configurações de firewall em nuvem e consoles de gerenciamento.

j. Automação e Orquestração:
   i. Automação de Configuração: Avalie o uso de ferramentas de automação para gerenciar e aplicar regras e configurações de firewall em ambientes de nuvem, garantindo consistência e reduzindo erros humanos.
   ii. Conformidade de Políticas: Confirme que verificações automatizadas de conformidade estão implementadas para garantir que as configurações do firewall permaneçam alinhadas com as políticas e melhores práticas de GIS.

E.2. Avaliação da Segurança do Banco de Dados

O objetivo da Avaliação de Segurança do Banco de Dados é garantir que os bancos de dados que armazenam dados sensíveis como PII, dados de transações financeiras e dados relacionados a jogos, estejam protegidos contra acessos não autorizados e estejam em conformidade com as melhores práticas e normas regulatórias aplicáveis. A Avaliação de Segurança do Banco de Dados inclui a revisão dos mecanismos de criptografia e da segurança geral do ambiente do banco de dados, incluindo proteções contra dados em repouso e dados em trânsito. A Avaliação de Segurança do Banco de Dados segue as diretrizes do OWASP para Armazenamento Criptográfico e outros padrões do setor, garantindo a segurança e confidencialidade dos dados sensíveis do GPE. Durante a Avaliação de Segurança do Banco de Dados, o ISF deve realizar as seguintes atividades-chave:

a. Revisão de Documentação: A documentação do processo é solicitada da Empresa de Jogos e analisada quanto à completude e alinhamento com as melhores práticas.
   i. Revisão de Configuração:
      1. Linha de Base de Configuração Segura: Verifique a configuração geral do ambiente do banco de dados para garantir que serviços, portas e contas de usuário estejam configurados de forma segura. Procure por serviços desnecessários que possam aumentar a superfície de ataque.
      2. Procedimentos de Backup e Recuperação: Revise como os backups são gerenciados e garanta que eles sejam criptografados e armazenados de forma segura. Os procedimentos de backup e recuperação devem incluir criptografia durante o trânsito e armazenamento.
      3. Configurações de Auditoria e Registro: Verifique se a auditoria está habilitada para ações críticas, como acesso a dados sensíveis, alterações de configuração e tentativas de escalonamento de privilégios. Garanta que os registros de auditoria sejam armazenados de forma segura e revisados regularmente.
      4. Métodos de Criptografia de Dados: Avalie se a criptografia de dados em repouso e dados em trânsito é aplicada corretamente, usando algoritmos de criptografia padrão da indústria (por exemplo, AES-256).
   ii. Controle de Acesso e Autenticação:
      1. Controle de Acesso Baseado em Função (RBAC): Revise as políticas de controle de acesso para garantir que apenas usuários autorizados tenham acesso a bancos de dados sensíveis. Confirme que os papéis de usuário são atribuídos com base no princípio do privilégio mínimo.
      2. Autenticação Multifator (MFA): Garanta que contas críticas de banco de dados, como administradores, estejam protegidas com autenticação multifator.
      3. Gerenciamento de Contas de Usuário: Avalie os processos para criar, gerenciar e desativar contas de usuários do banco de dados, garantindo que contas inativas ou desnecessárias sejam removidas ou desativadas.
   iii. Varredura e Correção de Vulnerabilidades:
      1. Varreduras Regulares de Vulnerabilidades: Certifique-se de que as Varreduras de Vulnerabilidades sejam realizadas regularmente para detectar e corrigir vulnerabilidades de software de banco de dados, patches desatualizados e configurações incorretas.
      2. Gerenciamento de Patches: Verifique se os patches críticos são aplicados rapidamente e que versões desatualizadas do banco de dados estão aposentadas ou devidamente protegidas.
      3. Endurecimento de Banco de Dados: Revise as medidas de reforço de segurança adotadas para prevenir vulnerabilidades comuns em bancos de dados, como ataques de SQL Injection e configurações incorretas.
   iv. Proteção de Dados e Controles de Privacidade:
      1. Máscara de Dados e Tokenização: Garantir que o mascaramento de dados seja aplicado a ambientes não produtivos, especialmente para bancos de dados contendo dados sensíveis.
      2. Monitoramento de Atividade de Banco de Dados (DAM): Garantir que ferramentas de monitoramento de atividade no banco de dados estejam disponíveis para detectar comportamentos anômalos ou tentativas de acesso não autorizadas.
      3. Gerenciamento de Chaves de Criptografia:
      4. Armazenamento de Chaves e Controles de Acesso: Garanta que as chaves de criptografia sejam armazenadas e protegidas com segurança usando um Módulo de Plataforma Confiável (TPM) ou Módulo de Segurança de Hardware (HSM), e que o acesso seja rigorosamente controlado e registrado.
      5. Rotação e Expiração de Chaves: Revise políticas e procedimentos para rotação, expiração e revogação de chaves, garantindo que os ciclos de vida principais sejam gerenciados de forma segura.
   v. Segurança e Isolamento de Rede:
      1. Segmentação de Banco de Dados: Garantir que os bancos de dados estejam devidamente segmentados a partir de segmentos de rede menos seguros. O acesso deve ser restrito com base na lista branca de IP e na zoneamento da rede.

2. Configuração do Firewall: Confirme que os firewalls estão instalados para evitar acessos não autorizados aos servidores de banco de dados e que protocolos seguros são usados para comunicação entre o banco de dados e os servidores de aplicação.
3. Comunicação Criptografada: Verifique se toda a comunicação entre o banco de dados e clientes ou aplicativos está criptografada usando TLS/SSL.

b. Entrevista e Demonstração ao Vivo: Uma entrevista por vídeo é realizada com o Administrador do Banco de Dados (DBA), que demonstra configurações e consultas ao vivo no sistema de banco de dados, permitindo a verificação dos controles GIS em ação.
   i. Verificação de Configuração: Durante a entrevista, verifique visualmente as configurações no banco de dados para garantir que a criptografia e os controles GIS correspondam à documentação.
   ii. Demonstração de Criptografia: Solicite ao DBA que demonstre como os dados criptografados são armazenados e acessados, garantindo que os dados sensíveis sejam criptografados corretamente e estejam em conformidade com os requisitos regulatórios.
   iii. Verificação de Armazenamento de Senhas: Garanta que o DBA execute consultas que mostrem como as senhas são armazenadas (hash e sal) e verifique se os registros antigos também seguem protocolos de criptografia adequados.
   iv. Criptografia de Dados e Controles de Acesso: Revise e confirme a criptografia de PIIs, como nomes legais, números de identificação governamental (números de seguridade social, números de identificação de contribuinte, números de passaporte ou equivalente) e informações financeiras pessoais (números de instrumentos de crédito ou débito, números de conta bancária, etc.), garantindo que todos os campos sensíveis estejam criptografados.

E.3. Avaliação da Segurança da Engenharia Social

O objetivo da Avaliação de Segurança da Engenharia Social é testar o elemento humano da segurança do GPE, identificando vulnerabilidades que poderiam ser exploradas por manipulação em vez de meios técnicos. A Avaliação de Segurança em Engenharia Social ajuda a identificar fraquezas no comportamento humano e na segurança física que podem levar a violações, garantindo uma abordagem mais holística para proteger o GPE. Durante a Avaliação da Segurança em Engenharia Social, a ISF deve realizar as seguintes atividades-chave:

a. Comportamento Humano:
   i. Campanhas de Phishing: Simule ataques de phishing direcionados para avaliar a eficácia do treinamento dos funcionários e a capacidade do GPE de detectar e relatar e-mails suspeitos.
   ii. Vishing e Pretexting: Realize tentativas de engenharia social por telefone para extrair dados sensíveis ou obter acesso não autorizado ao se passar por entidades confiáveis.
   iii. Spear Phishing: Ataques de phishing personalizados direcionados a alvos de alto valor dentro da Empresa de Jogos para testar a robustez das proteções executivas e de acesso privilegiado de contas.

b. Segurança Física:
   i. Tentativas de Intrusão Física: Teste as medidas de segurança física tentando obter acesso não autorizado a áreas restritas dentro do GPE, avaliando a eficácia dos protocolos de segurança.
   ii. Comprometimento de Dispositivos: Tentar instalar dispositivos não autorizados dentro da instalação para interceptar comunicações ou exfiltrar dados, avaliando os controles físicos de GIS existentes.
   iii. Clonagem de Crachás de Acesso: Teste a resiliência dos controles físicos de acesso tentando clonar crachás de acesso dos funcionários e obter acesso a áreas seguras.

E.4. Avaliação de Segurança Sem Fio

O objetivo da Avaliação de Segurança Sem Fio é avaliar a segurança e confiabilidade da infraestrutura sem fio dentro do GPE. A Avaliação de Segurança Sem Fio foca na identificação de vulnerabilidades, configurações incorretas e fraquezas nas redes sem fio que podem levar a acessos não autorizados, interceptação de dados ou outras formas de exploração. Ela garante que as redes sem fio que suportam o GPE sejam seguras, resilientes e devidamente gerenciadas de acordo com as melhores práticas de segurança. A Avaliação de Segurança Sem Fio envolve uma abordagem estruturada, combinando varredura ativa e passiva, revisões de configuração e testes de vulnerabilidades.

a. Os alvos da Avaliação de Segurança Sem Fio são os pontos de acesso sem fio (WAPs), redes sem fio e qualquer infraestrutura sem fio associada dentro do GPE, que incluem:
   i. Redes voltadas ao público usadas por frequentadores, visitantes ou empreiteiros.
   ii. Redes sem fio internas usadas por funcionários para fins administrativos ou operacionais.
   iii. Redes de convidados e acesso sem fio segregado para uso não crítico.
   iv. Dispositivos sem fio usados para operações internas, como terminais portáteis, tablets ou outros dispositivos móveis conectados à infraestrutura sem fio do GPE.

b. Durante a Avaliação de Segurança Sem Fio, a ISF deve realizar as seguintes atividades-chave:
   i. Reconhecimento e Coleta de Informações:
      1. Mapeamento de Pontos de Acesso Sem Fio: Mapeie todos os pontos de acesso na rede GPE para identificar todos os dispositivos transmitindo ou conectando à infraestrutura sem fio.
      2. Levantamento de Rede: Varre-se as redes sem fio para identificar Identificadores de Conjunto de Serviço (SSIDs), dispositivos conectados à rede e pontos de acesso transmitindo dentro do ambiente.
      3. Detecção de Pontos de Acesso Fraudulentos: Identifique pontos de acesso não autorizados ou desonestos que possam ter sido adicionados maliciosamente ou por engano à rede.
   ii. Revisão de Configuração e Segurança:
      1. Criptografia e Controles de Acesso: Certifique-se de que protocolos de criptografia fortes, como WPA3 ou WPA2 com AES, estejam em uso em todas as redes sem fio e que protocolos de criptografia legados (por exemplo, WEP) estejam desativados. Revise os controles de acesso para garantir a segmentação adequada das redes de convidados, públicas e internas.
      2. Gerenciamento de SSIDS: Avalie se SSIDs estão sendo transmitidos desnecessariamente e garanta que SSIDs ocultos estejam configurados para redes críticas.
      3. Autenticação e Autorização: Garantir que os mecanismos de autenticação (por exemplo, 802.1x) sejam corretamente implementados e aplicados, impedindo que dispositivos ou usuários não autorizados acessem redes sensíveis. Verifique o uso correto de portais cativos e chaves pré-compartilhadas, quando aplicável.
      4. Segmentação de Rede: Revise a segmentação entre redes públicas, de convidados e internas para garantir que o acesso a sistemas críticos seja restringido e monitorado.
      5. Identificação de Vulnerabilidades: Identificar vulnerabilidades contra bancos de dados atualizados de vulnerabilidades, incluindo qualquer firmware não atualizado em dispositivos sem fio.
   iii. Detecção e Monitoramento de Intrusão:
      1. Detecção de Pontos de Acesso Fraudulentos: Garanta que os sistemas estejam instalados para detectar e alertar administradores sobre dispositivos sem fio não autorizados ou pontos de acesso não autorizados. Implemente monitoramento contínuo para detectar qualquer atividade incomum nas redes sem fio.
      2. Sistema de Detecção de Intrusão Sem Fio/Sistema de Prevenção de Intrusão (IDS/IPS): Avalie a eficácia de qualquer IDS ou IPS sem fio na identificação e prevenção de ataques como desautenticação, interferência ou ataques MITM.
   iv. Testes Sem Fio Ativos e Passivos:
      1. Testes Passivos: Para ambientes sem fio de alto tráfego, métodos de varredura passiva são utilizados para monitorar e analisar o tráfego sem fio sem interagir com a rede.
      2. Testes Ativos: Em áreas de baixo tráfego ou seguras, métodos de teste ativos (por exemplo, tentativa de conexão, exploração de vulnerabilidades ou captura por aperto de mão) devem ser realizados para avaliar a resiliência da infraestrutura sem fio.
      3. Teste de Sangramento: Avalie o alcance do sinal sem fio para garantir que ele não vaze fora da área de cobertura pretendida, o que poderia expor a rede a atacantes.
   v. Desempenho da Rede Sem Fio e Cobertura de Sinal:
      1. Mapeamento de Cobertura de Sinal: Avalie a posição e a intensidade do sinal dos pontos de acesso sem fio para garantir que o sinal sem fio não ultrapasse o perímetro seguro. Garantir cobertura consistente e confiável nas áreas pretendidas, como as principais zonas operacionais dentro do GPE.

2. Avaliação de Desempenho: Teste a capacidade da rede sem fio de lidar com cargas de tráfego em picos sem degradação em desempenho ou segurança.

vi. Atualizações de firmware: Certifique-se de que todos os pontos de acesso wireless e infraestrutura relacionada estejam rodando firmwares, atualizado para proteger contra vulnerabilidades conhecidas.

vii. Políticas de Rede Sem Fio:

1. Garantir que a rede sem fio esteja em conformidade com as políticas de segurança organizacional, padrões da indústria de jogos e regulamentos relevantes (por exemplo, PCI DSS, GDPR, etc.).
2. Confirme que as redes de convidados e públicas seguem um conjunto separado de políticas para evitar qualquer sobreposição ou acesso não autorizado a redes internas críticas.

viii. Registro e Auditoria: Verifique se os mecanismos de registro estão ativados em todos os pontos de acesso e que os registros de auditoria de acesso são armazenados de forma segura e revisados regularmente para sinais de atividade não autorizada.

ix. Segurança Física: Confirme que os dispositivos da rede sem fio (por exemplo, pontos de acesso e controladores) estão fisicamente protegidos, com acesso restrito apenas a pessoal autorizado.

E.5. Avaliação de Segurança do Código-Fonte

O objetivo da Avaliação de Segurança do Código-Fonte é detectar vulnerabilidades de segurança, incluindo tanto problemas comuns quanto ameaças mais complexas específicas do GPE, tanto por meio de revisão manual quanto do uso de ferramentas automatizadas. Durante a Avaliação de Segurança do Código-Fonte, o ISF deve realizar as seguintes atividades-chave:

a. Varredura Automatizada de Código: Ferramentas automatizadas são usadas para escanear o código-fonte em busca de vulnerabilidades conhecidas e padrões de código que possam indicar falhas de segurança.

b. Revisão Manual de Código: Uma inspeção manual aprofundada é realizada em áreas críticas como tratamento de transações, lógica de jogos e sistemas de autenticação.

c. Autenticação e Autorização: Garantir mecanismos seguros para autenticação do usuário e controle de acesso. Verifique a robustez dos sistemas de autenticação multifator (MFA) e gerenciamento de sessões para evitar acessos não autorizados.

d. Validação de Entrada e Codificação de Saída: Valide todas as entradas do usuário para garantir que estejam devidamente sanitizadas e evitar vulnerabilidades comuns como SQL Injection e Cross-Site Scripting (XSS). Certifique-se de que os dados de saída estejam codificados de forma segura antes de serem devolvidos aos usuários.

e. Tratamento de Dados Sensíveis: Avalie como dados sensíveis, como PII (Informações Pessoais Identificáveis) e informações de pagamento, são tratados, garantindo a criptografia tanto em trânsito quanto em repouso. Avalie o gerenciamento das chaves de criptografia para evitar exposição.

f. Tratamento e Registro de Erros: Revise procedimentos de tratamento de erros para garantir que dados sensíveis, como informações do sistema, não sejam divulgados por meio de mensagens de erro. Os logs de auditoria devem ser devidamente protegidos e evitar registrar dados sensíveis, como credenciais de autenticação.

g. Segurança da Lógica do Jogo: Analise a implementação da lógica central do jogo, incluindo mecanismos do Gerador de Números Aleatórios (RNG), para garantir justiça e integridade. Implementações seguras de RNG são cruciais para evitar manipulação dos resultados do jogo.

h. Bibliotecas e Dependências de Terceiros: Garanta que todas as bibliotecas externas usadas na aplicação estejam atualizadas e livres de vulnerabilidades conhecidas. Audite regularmente dependências como parte do ciclo de vida seguro do desenvolvimento.

E.6. Teste de Simulação Adversarial

O objetivo do Teste de Simulação Adversarial é aprimorar a postura de segurança do GPE simulando cenários sofisticados de ataque do mundo real em todo o espectro de vetores potenciais de ataque, focando tanto nos aspectos digitais quanto físicos da segurança. O Teste de Simulação Adversarial foi projetado para testar a resiliência do GPE contra uma variedade de táticas, técnicas e procedimentos avançados usados por atacantes

do mundo real. O objetivo do Teste de Simulação Adversarial é avaliar a capacidade do GPE de detectar, responder e mitigar técnicas avançadas de ataque que atores ameaçadores determinados possam empregar.

a. Diferente dos Testes de Penetração tradicionais, o Teste de Simulação Adversarial imita um adversário altamente habilidoso e persistente, que busca romper as defesas do GPE por quaisquer meios necessários.
b. Durante o Teste de Simulação Adversarial, a ISF deve realizar as seguintes atividades-chave:
    i. Inteligência de Fonte Aberta (OSINT) e Coleta de Informações:
        1. Informações Publicamente Disponíveis: Colete e analise informações públicas sobre a Empresa de Jogos, sua infraestrutura, funcionários e parceiros.
        2. Registro de Domínios e Informações DNS: Colete dados de registros WHOIS, consultas DNS e detalhes de registro de domínios para identificar possíveis vetores de ataque relacionados ao gerenciamento de domínios.
        3. Perfil de Mídias Sociais: Analise as contas de redes sociais de funcionários-chave para coletar informações que possam ser aproveitadas em ataques de engenharia social.
        4. Documentação Acessível Publicamente: Busque documentos acessíveis publicamente, como PDFs, apresentações e relatórios, que possam conter nomes de funcionários, processos internos ou outros dados sensíveis.
        5. Buscas de Vazamento de Dados e Vazamentos: Investigue se algum dado sensível relacionado à empresa foi exposto em violações anteriores, incluindo credenciais de autenticação e PII.
        6. Pegada Técnica: Identifique infraestrutura, serviços e tecnologias voltados para o exterior utilizados por meio de técnicas de reconhecimento passivo, como banner grabbing, consultas em mecanismos de busca (por exemplo, Google dorking) e bancos de dados de segurança pública.
        7. Relações com Terceiros: Pesquisa parcerias, fornecedores e serviços de terceiros usados pela Empresa de Jogos para identificar potenciais vulnerabilidades na cadeia de suprimentos.
    ii. Ataques Avançados de Rede:
        1. Movimento Lateral: Simule um atacante interno que obteve acesso inicial, testando a capacidade de se mover lateralmente pela rede para acessar Componentes Críticos do Sistema.
        2. Mecanismos de Persistência: Teste as defesas do GPE contra atacantes que tentam estabelecer persistência de longo prazo dentro da rede, garantindo a detecção e remoção de pontos de apoio maliciosos.
        3. Exfiltração de Dados: Simule os métodos que um atacante pode usar para exfiltrar dados sensíveis do GPE, testando a eficácia das medidas de prevenção de perda de dados (DLP).
        4. Reconhecimento Avançado: Realize descobertas e reconhecimento furtivos de redes para mapear a rede interna e identificar ativos e sistemas chave para ataques direcionados.
        5. Testes de Comando e Controle (C2): Estabelecer e manter comunicação com sistemas comprometidos usando várias técnicas C2 para testar as capacidades de detecção da Empresa de Jogos.
        6. Escalonamento de privilégios: Teste a capacidade do GPE de escalar privilégios de acesso de nível inferior para acesso administrativo ou root, aproveitando configurações incorretas ou vulnerabilidades do sistema.
        7. Despejo e Reutilização de Credenciais: Tente extrair e reutilizar credenciais de autenticação de sistemas comprometidos para infiltrar ainda mais a rede ou acessar dados sensíveis.
    iii. Avaliação de Resposta a Incidentes:
        1. Detecção e Alerta: Avalie a eficácia dos sistemas de monitoramento e alerta do GPE na detecção de atividades sofisticadas de ataque, garantindo resposta rápida.
        2. Resposta e Contenção: Avalie a rapidez e eficiência da equipe de resposta a incidentes em conter e mitigar as ameaças simuladas, focando em minimizar o impacto.
        3. Análise Pós-Incidente: Revise a capacidade de realizar análises pós-incidentes detalhadas, implementar lições aprendidas e aprimorar as defesas de segurança para prevenir incidentes futuros.

c. Os resultados do Teste de Simulação Adversarial devem fornecer à Empresa de Jogos uma compreensão detalhada de como suas defesas de segurança funcionam contra cenários de ataque avançados. As conclusões devem informar melhorias estratégicas de segurança e reforçar a importância de uma estratégia de defesa proativa e em camadas, garantindo que o GPE permaneça robusto contra ameaças emergentes.

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.
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.
Ponte	Divide redes para reduzir o tráfego total da rede. Uma ponte permite ou impede que dados passem por ela ao ler o endereço MAC.
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.
Tecnologia de Comunicações	Qualquer método utilizado, e os componentes empregados, para facilitar a transmissão e recepção de informações, incluindo transmissão e recepção por sistemas usando fios, sem fio, cabo, rádio, micro-ondas, luz, fibra óptica, satélite ou redes de dados de computadores, incluindo Internet e intranets.
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

Mandato	Descrições
	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.
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.

Mandato	Descrições
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.
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.
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.
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.

Mandato	Descrições
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.
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.
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.
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.
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.
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.
Placa de Interface de Rede (NIC)	O mecanismo pelo qual terminais e sistemas se conectam à rede. As NICs podem ser placas de expansão adicionais, placas PCMCIA ou interfaces integradas.
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

Mandato	Descrições
	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.
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).
Proxy	Uma aplicação que "quebra" a conexão entre cliente e servidor. O proxy aceita certos tipos de tráfego que entra ou sai de uma rede, processa e encaminha. Isso fecha efetivamente o caminho reto entre as redes internas e externas.
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.
Roteador	Conecta redes entre si. Um roteador usa o endereço de rede configurado por software para tomar decisões de encaminhamento.

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

Mandato	Descrições
	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.
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.
Troca	Conecta dispositivos em uma rede 802.3. Um switch encaminha os dados para seu destino usando o endereço MAC embutido em cada pacote.
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.
Protocolo de Controle de Transmissão/Protocolo de Internet (TCP/IP)	O conjunto de protocolos de comunicação usado para conectar hosts na Internet.
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.
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.
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.
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.