TERMO DE CIÊNCIA E DE AUTORIZAÇÃO

PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610, de 19 de fevereiro de 1998, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano a disponibilizar gratuitamente o documento em formato digital no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

IDENTIFICAÇÃO DA PRODUÇÃO TÉCNICO-CIENTÍFICA

- ☐ Tese (doutorado)
- ☐ Dissertação (mestrado)
- ☐ Monografia (especialização)
- ☑ TCC (graduação)
- ☐ Artigo científico
- ☐ Capítulo de livro
- ☐ Livro
- ☐ Trabalho apresentado em evento
- ☐ Produto técnico e educacional - Tipo:

Nome completo do autor:
Caio Veronez Simões

Matrícula:
2022109202030028

Título do trabalho:
Invasões de Contas e Análise de Segurança de Plataformas Digitais de Vendas de Jogos

RESTRIÇÕES DE ACESSO AO DOCUMENTO

Documento confidencial: ☑ Não ☐ Sim, justifique:

Informe a data que poderá ser disponibilizado no RIIF Goiano: ☐/☐/☐

O documento está sujeito a registro de patente? ☐ Sim ☑ Não

O documento pode vir a ser publicado como livro? ☐ Sim ☑ Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O(a) referido(a) autor(a) declara:

• Que o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;

• Que obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autoria, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;

• Que cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

gov.br Documento assinado digitalmente
CAIO VERONEZ SIMOES
Data: 01/08/2026 14:41:15-0300
Verifique em https://validar.iti.gov.br

Catalão — Local

01/08/2026 — Data

Assinatura do autor e/ou detentor dos direitos autorais

Ciente e de acordo:

gov.br Documento assinado digitalmente
EDUARDO CASTILHO ROSA
Data: 01/08/2026 16:27:11-0300
Verifique em https://validar.iti.gov.br

Assinatura do(a) orientador(a)

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

Ata nº 5/2026 - CCBSI-CAT/GE-CAT/CMPCAT/IFGOIANO

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO CURSO

Aos vinte e dois dias do mês de junho de 2026, às 18 horas, reuniu-se na Sala 212 do IF Goiano Campus Catalão a banca examinadora composta pelos docentes: Eduardo Castilho Rosa (orientador), Luis Felipe Schons Silva (coorientador), Kênia Santos de Oliveira (Membro) e Paulo Rogério de Souza e Silva Filho (Membro), para examinar o Trabalho de Conclusão de Curso (TCC) intitulado "*Invasões de Contas e Análise de Segurança de Plataformas Digitais de Vendas de Jogos*" do estudante Caio Veronez Simões, Matrícula nº 2022109202030028 do Curso de Bacharelado em Sistemas de Informação do IF Goiano – Campus Catalão. A palavra foi concedida ao estudante para a apresentação oral do TCC, onde houve posteriormente a arguição do candidato pelos membros da banca examinadora. Após tal etapa, a banca examinadora decidiu pela **APROVAÇÃO** do estudante, tendo este obtido média 8,27. Ao final da sessão pública de defesa foi lavrada a presente ata que segue assinada pelos membros da Banca Examinadora.

(Assinado Eletronicamente)

Dr. Eduardo Castilho Rosa

Orientador

(Assinado Eletronicamente)

Dr. Luis Felipe Schons Silva

Coorientador

(Assinado Eletronicamente)

Dra Kênia Santos de Oliveira

Membro

(Assinado Eletronicamente)

Ms Paulo Rogério de Souza e Silva Filho

Membro

Documento assinado eletronicamente por:

- **Eduardo Castilho Rosa**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 28/07/2026 22:53:45.
- **Luis Felipe Schons Silva**, **PROF ENS BAS TEC TECNOLOGICO-SUBSTITUTO**, em 28/07/2026 23:04:13.
- **Paulo Rogerio de Souza e Silva Filho**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 29/07/2026 09:41:51.
- **Kenia Santos de Oliveira**, **GERENTE - CD4 - GE-CAT**, em 29/07/2026 10:23:06.

Este documento foi emitido pelo SUAP em 28/07/2026. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 842301
Código de Autenticação: ae4c21f52d

INSTITUTO FEDERAL GOIANO
Campus Catalão
Rua Salustiano Oliveira da Paz, 1621, Bairro Ipanema, CATALAO / GO, CEP 75.705-040
(64)99212-9907

Invasões de Contas e Análise de Segurança de Plataformas Digitais de Vendas de Jogos

Caio Veronez Simões, Luís Felipe Schons Silva, Eduardo Castilho Rosa

[1] Departamento de Sistemas da Informação
Instituto Federal Goiano, Campus Catalão (IF Goiano)

caiovsimoes848@gmail.com, luis.schons@ifgoiano.edu.br,

eduardo.rosa@ifgoiano.edu.br

Abstract. *This study analyzes the security of communications in digital game distribution platforms, considering the growing value associated with user accounts and incidents related to credential compromise. Seven platforms were analyzed: Steam, Epic Games, GOG Galaxy, Ubisoft Connect, EA App, Battle.net, and Xbox. The analysis was conducted through network traffic capture using the Wireshark tool, focusing on TLS protocol parameters such as version, cipher suites, cryptographic algorithms, presence of forward secrecy, and CDN usage. The results indicate that most platforms employ efficient and up-to-date protection mechanisms, with the exception of Battle.net. Additionally, a survey conducted with 112 participants revealed that 61.6% reported experiences with unauthorized access to their accounts, predominantly associated with phishing and the use of malicious software. It was also observed that Steam concentrated the highest number of reported account compromise incidents among the analyzed platforms, despite presenting one of the highest levels of security according to the technical requirements analysis.*
Keywords: *information security; TLS; digital games; networks; cryptography; social engineering; account compromise.*

Resumo. *Este trabalho analisa a segurança das comunicações em plataformas de distribuição digital de jogos, considerando o crescente valor associado às contas de usuários e os incidentes relacionados ao comprometimento de credenciais. Foram analisadas sete plataformas: Steam, Epic Games, GOG Galaxy, Ubisoft Connect, EA App, Battle.net e Xbox. Por meio da captura de tráfego de rede com a ferramenta Wireshark foram analisados parâmetros como o protocolo TLS, como versão, Cipher Suites, algoritmos criptográficos, presença de Forward Secrecy e uso de CDN. Os resultados indicaram que a maioria das plataformas utilizam métodos eficientes e atualizados de proteção, com exceção do Battle.net. Complementarmente, um questionário aplicado a 112 participantes revelou que 61,6% relataram experiências com acessos indevidos a suas contas, predominantemente associadas a phishing e uso de softwares maliciosos. Observou-se também que a Steam concentrou o maior número de relatos de invasão entre as plataformas analisadas, apesar de apresentar um dos níveis mais elevados de segurança segundo a análise dos requisitos técnicos.*
Palavras-chave: *segurança da informação; TLS; jogos digitais; redes; criptografia; engenharia social; furto de contas.*

1. Introdução

A indústria de jogos apresenta crescimento exponencial nos últimos anos, ocupando posição de destaque na indústria de entretenimento [Chattopadhyay et al. 2023]. Plataformas de distribuição digital hospedam milhões de usuários simultaneamente, vinculando cada progresso e investimento a conta do jogador, tornando suas credenciais um ativo digital de alto valor, não apenas financeiro, mas também afetivo. A Steam, por exemplo, registra aproximadamente 42 milhões de usuários *online* em um único momento [SteamDB 2026], evidenciando a escala do ecossistema envolvido.

Nesse contexto, as contas dos usuários deixam de ser simples credenciais de acesso e passam a concentrar um conjunto expressivo de bens digitais, os jogos adquiridos, itens virtuais, moedas digitais e centenas de horas de progressão acumuladas ao longo do tempo. Mesmo em títulos gratuitos, o esforço investido pelos jogadores confere aos seus perfis um valor que transcende o aspecto monetário direto [Lehdonvirta 2008]. Essa mudança de natureza das contas digitais tem consequências diretas para a segurança, ao concentrar patrimônio, as informações de login tornam-se alvos prioritários para atacantes, o que é evidenciado pelo aumento expressivo de incidentes de invasão reportados nas últimas décadas [DaCosta and Seok 2020].

O furto de contas em plataformas de jogos digitais configura-se, em muitos aspectos, como um problema distinto dos ataques corporativos tradicionais. Os vetores mais comuns incluem *phishing*, engenharia social, uso de *softwares* maliciosos e compartilhamento indevido de credenciais [Parizi et al. 2019]. A sofisticação dessas técnicas mantém vulneráveis até mesmo usuários que utilizam autenticação em dois fatores, pois os ataques exploram o comportamento humano, e não falhas técnicas das plataformas [Shen et al. 2016]. As consequências para as vítimas representam não só um prejuízo financeiro, como também a perda do valor sentimental, traduzido em conquistas, vínculos sociais e horas de dedicação [Cheng et al. 2010].

O cenário atual exige uma maior compreensão sobre as melhores práticas de segurança da informação nesse setor. Dentre os mecanismos de proteção das comunições entre cliente e servidor, o protocolo TLS (*Transport Layer Security*) é o principal [Rescorla 2018]. Uma configuração adequada desse protocolo é essencial para garantir a resistência das comunicações a ataques de interceptação e descriptografia retroativa [Lee et al. 2021].

Este trabalho busca analisar os mecanismos de segurança adotados pelas plataformas, com ênfase no uso de protocolos atualizados, na aplicação de boas práticas criptográficas e na relação desses fatores com a ocorrência de ataques a contas de usuários. Nesse contexto, considera-se que, apesar da adoção de tecnologias modernas de proteção, a persistência de incidentes de segurança pode estar associada tanto a lacunas na implementação quanto, principalmente, a fatores relacionados ao comportamento dos usuários. Como diferencial, esta pesquisa integra a análise técnica dos mecanismos de comunicação com a percepção dos usuários, permitindo uma abordagem mais abrangente ao correlacionar aspectos tecnológicos com fatores humanos no contexto da segurança digital.

2. Referencial teórico

O referencial teórico deste trabalho reúne conceitos fundamentais relacionados à segurança em ambientes digitais, abordando tanto os mecanismos técnicos de proteção das comunicações quanto as principais ameaças direcionadas a contas de usuários. Além disso, são discutidos aspectos relacionados ao comportamento dos usuários e à forma como suas práticas influenciam a exposição a incidentes de segurança, bem como a dimensão e os impactos desse problema no contexto das plataformas digitais.

2.1. Invasões de Contas em Ambientes Digitais

O furto de credenciais em plataformas digitais consiste na obtenção não autorizada de credenciais de acesso, permitindo que terceiros assumam o controle sobre os dados, bens e funcionalidades associados ao perfil de um usuário legítimo. Embora esse tipo de incidente não seja exclusivo do contexto de jogos, ele assume características particulares nesse ambiente, onde as contas concentram não apenas informações pessoais, mas também ativos digitais de valor econômico e afetivo acumulados ao longo do tempo [Parizi et al. 2019].

O crescimento da indústria de jogos digitais ampliou significativamente o valor associado a essas contas. Itens virtuais, moedas digitais, progressão em jogos e bibliotecas de títulos adquiridos representam um patrimônio que, em muitos casos, supera o valor de bens físicos comparáveis [Lehdonvirta 2008]. Estudos mais recentes apontam que esse ecossistema digital vem se tornando cada vez mais relevante economicamente, consolidando mercados paralelos e ampliando o interesse de agentes maliciosos [Szatmáry 2024]. Esse cenário torna as credenciais de jogadores alvos cada vez mais atrativos para atacantes, motivados tanto pelo valor de revenda dos itens quanto pela possibilidade de extorsão ou uso indevido de métodos de pagamento cadastrados [DaCosta and Seok 2020].

No contexto brasileiro, o acesso não autorizado a contas digitais pode ser enquadrado como crime de invasão de dispositivo informático, que tipifica a obtenção indevida de dados mediante violação de mecanismos de segurança [Brasil 2012]. Essa legislação estabelece penalidades para indivíduos que acessam, adulteram ou obtêm informações sem autorização do usuário, especialmente quando há prejuízo econômico ou exposição de dados sensíveis.

2.2. Protocolo TCP e TLS

O protocolo TCP (*Transmission Control Protocol*) é um dos pilares da comunicação em rede, sendo responsável por garantir a entrega confiável e ordenada de dados entre dois dispositivos conectados à internet. Esse protocolo estabelece uma sessão antes da transmissão por meio do processo conhecido como *three-way handshake*, no qual cliente e servidor trocam pacotes de sincronização para definir os parâmetros da comunicação. Essa característica torna o TCP fundamental para aplicações que exigem integridade dos dados, como sistemas bancários, serviços de e-mail e plataformas de jogos [Kurose and Ross 2017].

Contudo, esse protocolo por si só não oferece confidencialidade. Para proteger os dados trafegados, utiliza-se o protocolo TLS (*Transport Layer Security*), que atua como uma camada de segurança sobre o TCP. O TLS é responsável pela criptografia dos dados

transmitidos, pela autenticação do servidor e pela garantia da integridade das mensagens [Rescorla 2018]. Sua versão mais recente, o TLS 1.3, publicada em 2018 como RFC 8446, representa um avanço significativo em relação ao TLS 1.2, publicado em 2008 como RFC 5246.

As principais melhorias do TLS 1.3 em relação ao TLS 1.2 incluem a eliminação de algoritmos criptográficos considerados obsoletos e vulneráveis, a redução do número de mensagens trocadas no *handshake*, diminuindo de dois para um RTT*(round-trip-time)*, que é o tempo de ida e volta entre cliente e servidor, também adoção obrigatória de mecanismos que garantem *Forward Secrecy* em todas as conexões [Rescorla 2018]. Do ponto de vista da segurança formal, foi demonstrado que o TLS 1.3 oferece propriedades de segurança superiores ao seu antecessor, sendo resistente a classes de ataques que eram efetivos contra o TLS 1.2 [Bhargavan et al. 2017].

A importância de entender esses fundamentos está no fato de que fazer uma escolha inadequada de versões do protocolo ou de algoritmos criptográficos pode expor as comunicações a vulnerabilidades conhecidas. Em outras literaturas, são demonstrados como servidores que suportam protocolos legados, protocolos e sistemas de segurança mais antigos e desatualizados, podem comprometer a segurança mesmo de conexões modernas [Aviram et al. 2016], evidenciando o risco concreto de manter suporte a versões antigas do protocolo [Dierks and Rescorla 2008].

O processo de estabelecimento da conexão TLS, chamado TLS *Handshake*, envolve a troca de mensagens *Client Hello* e *Server Hello*, cujos pacotes foram capturados e analisados com a ferramenta *Wireshark* [Wireshark Foundation 2024].

2.3. Métodos de Ataque e Comportamento do Usuário

Os principais meios utilizados para o comprometimento de contas em plataformas de jogos incluem *phishing*, engenharia social, uso de *softwares* maliciosos e compartilhamento indevido de credenciais [Parizi et al. 2019]. O *phishing*, em particular, consiste na criação de páginas ou mensagens falsas que simulam comunicações legítimas das plataformas, com o objetivo de induzir o usuário a fornecer voluntariamente suas credenciais de acesso. Já a engenharia social explora aspectos psicológicos e comportamentais para manipular o usuário, frequentemente por meio de ofertas falsas, pedidos de ajuda ou personificação de outros jogadores [Shen et al. 2016].

Um aspecto relevante identificado na literatura é que a adoção de medidas técnicas de proteção, como a autenticação em dois fatores, não elimina completamente o risco de comprometimento quando o vetor de ataque é comportamental. Estudos demonstraram que usuários tendem a subestimar riscos relacionados ao gerenciamento de senhas e ao compartilhamento de credenciais, mesmo quando possuem conhecimento declarado sobre boas práticas de segurança. Esse comportamento é consistente com os dados obtidos neste trabalho, nos quais a maioria das vítimas afirmou utilizar autenticação em dois fatores no momento do incidente [Shen et al. 2016].

O uso de *softwares* piratas e ferramentas não oficiais representa outro vetor recorrente, pois esses programas frequentemente contêm códigos maliciosos capazes de capturar dados de sessão, registrar teclas digitadas ou roubar *cookies* de autenticação armazenados no sistema [DaCosta and Seok 2020]. Esse comportamento é especialmente

prevalente no contexto de jogos, onde modificações não oficiais, ativadores e *hacks* são amplamente difundidos entre parte da base de usuários.

2.4. Impacto e Dimensão do Problema

O comprometimento de contas em plataformas digitais de jogos configura-se como um problema relevante devido à sua alta incidência e às múltiplas consequências associadas, que vão além de perdas financeiras diretas. Do ponto de vista do impacto para as vítimas, a perda de um perfil de jogos não pode ser reduzida apenas à sua dimensão financeira [Lehdonvirta 2008]. O tempo investido em progressão, as conquistas acumuladas e os vínculos sociais formados dentro dos ambientes virtuais constituem perdas que não possuem equivalente direto em moeda, tornando a experiência da perda especialmente traumática para usuários com alto grau de envolvimento com as plataformas. Estudos mais recentes reforçam essa perspectiva ao destacar o papel dos jogos digitais como espaços de interação social e construção de identidade, ampliando o impacto emocional associado à perda de contas [Chattopadhyay et al. 2023].

Destaca-se que, em jogos de multijogador massivo, o furto de credenciais pode comprometer não apenas o usuário diretamente afetado, mas também comunidades inteiras, uma vez que personagens e itens de valor circulam em economias virtuais interdependentes [Suh and Wagner 2007]. Trabalhos recentes indicam que essas economias digitais se tornaram mais complexas e integradas, aumentando o potencial de impacto coletivo decorrente de incidentes de segurança [Szatmáry 2024]. Essa dimensão coletiva do problema reforça a necessidade de abordagens de segurança que considerem tanto os aspectos técnicos das plataformas quanto o comportamento dos usuários que as compõem.

3. Metodologia

O trabalho adotou uma metodologia de pesquisa exploratória, desenvolvida com o objetivo de analisar as configurações de segurança adotadas por plataformas de distribuição digital de jogos, combinando análise técnica de tráfego de rede com coleta de usuários.

A seleção das plataformas analisadas foi orientada por dois critérios principais, a relevância da plataforma no mercado de distribuição digital de jogos e a disponibilidade de uma aplicação instalável para computador, condição necessária para a realização das capturas de tráfego em ambiente controlado. Plataformas que operam exclusivamente via navegador, que não tinham como foco principal a venda de jogos, ou que não disponibilizavam software próprio para computador foram desconsideradas. A partir desses critérios, foram selecionadas sete plataformas, representadas na Tabela 1.

Tabela 1. Tabela das principais plataformas consideradas para o estudo

Plataforma	Utilizada	Motivo
Steam	Sim	Segue os padrões
Epic Games	Sim	Segue os padrões
GOG Galaxy	Sim	Segue os padrões
Ubisoft Connect	Sim	Segue os padrões
EA App	Sim	Segue os padrões
Battle.net	Sim	Segue os padrões
Xbox	Sim	Segue os padrões
Itch.io	Não	Software baseado em navegador (Analise de sites deve ser feita de maneira diferente)
Playstation	Não	Não possui software para computador
Nintendo	Não	Não possui software para computador
Plataformas Mobile	Não	Não possui software para computador
Roblox	Não	O foco da plataforma não é a venda de jogos

A coleta de dados foi realizada por meio da captura de tráfego de rede com a ferramenta *Wireshark*, seguindo um procedimento padronizado aplicado a todas as plataformas para garantir consistência entre as coletas.

Durante a captura, o *Wireshark* [Wireshark Foundation 2024] registra os pacotes trafegados na interface de rede selecionada, organizando-os de forma estruturada e permitindo a aplicação de filtros específicos para análise. Para este trabalho, foram utilizados filtros voltados à identificação de conexões TLS, possibilitando a análise das mensagens de *handshake*, como *Client Hello* e *Server Hello*. A partir dessas mensagens, foram extraídas informações relevantes, como versão do protocolo, *Cipher Suite* e parâmetros criptográficos utilizados, seguindo abordagens semelhantes às utilizadas em estudos de análise de servidores TLS [Lee et al. 2007].

Inicialmente, para a gravação, realizava-se o *logout* do perfil e o encerramento de todas as aplicações abertas. Em seguida, iniciava-se a gravação, a aplicação era aberta, o login realizado e aguardava-se o carregamento completo da tela inicial. Posteriormente, acessava-se a página de um jogo disponível na interface principal, aguardando seu carregamento completo, seguido do retorno à página inicial e do acesso à biblioteca de jogos, onde a aplicação permanecia ativa por um curto período antes da finalização da captura. Todas as capturas foram realizadas entre os dias 5 e 17 de maio de 2026.

A coleta foi conduzida em ambiente controlado, com o objetivo de garantir a consistência dos dados obtidos entre as diferentes plataformas analisadas. Os experimentos foram realizados em um computador com sistema operacional Windows 11 Pro (versão 25H2), equipado com processador AMD Ryzen 3 3200G com Radeon Vega Graphics (3,60 GHz) e 16 GB de memória RAM, em arquitetura de 64 bits. A padronização do processo, permitiu reduzir interferências externas e assegurar que os dados coletados refletissem, de forma comparável, o comportamento das aplicações durante o estabelecimento das conexões.

A partir dos pacotes capturados, foram analisados parâmetros do protocolo TLS relativos à segurança das comunicações estabelecidas entre cliente e servidor, incluindo a

versão do protocolo utilizada, as *Cipher Suites* negociadas, os algoritmos de criptografia e o tipo de chave pública adotados, a presença de *Forward Secrecy*, o uso de CDN (*Content Delivery Network*) e a autoridade certificadora responsável pelo certificado digital. De maneira similar ao estudo de *Lee et al*. (2007), que analisou a força criptográfica de servidores SSL/TLS a partir de capturas de tráfego real, este trabalho adotou a observação direta de *handshakes* TLS como método central para caracterizar o nível de segurança de cada plataforma. Dados complementares, como o número de conexões estabelecidas e o tamanho médio dos pacotes, também foram registrados, embora com caráter auxiliar, dado que sua coleta não foi submetida a controle rigoroso de tempo, o que limita a comparação direta entre plataformas. A coleta de informações nos pacotes capturados utilizou ferramentas de inteligência artificial para auxiliar na identificação de dados, com todos os resultados revisados e validados manualmente pelo autor.

Com o objetivo de contextualizar os resultados técnicos obtidos, foi aplicado um questionário (descrito na Seção 4.1)) via Google Forms a 112 participantes, no período de 18 de março a 2 de abril de 2026. A coleta foi realizada por meio de redes sociais, comunidades voltadas ao público gamer e ambiente acadêmico, incluindo estudantes do Instituto Federal Goiano Campus Catalão nos níveis superior e médio. Após a coleta, as respostas foram verificadas quanto à consistência, onde respostas descartadas foram marcadas em vermelho na planilha e campos sem resposta esperada foram marcados em amarelo.

4. Dados Coletados

4.1. Análise da percepção dos usuários

Como parte da metodologia deste trabalho, foi desenvolvido e aplicado um questionário com o objetivo de coletar dados sobre a percepção dos usuários em relação à segurança de seus perfis em plataformas de distribuição digital de jogos.

A coleta de respostas ocorreu no período de 18 de março a 2 de abril de 2026, totalizando 15 dias. Durante esse período, foram obtidas 112 respostas, provenientes de participantes com diferentes níveis de envolvimento com jogos digitais.

A divulgação do formulário foi realizada por meio de redes sociais, comunidades voltadas ao público *gamer* e ambiente acadêmico, incluindo estudantes do Instituto Federal Goiano - Campus Catalão, possibilitando alcançar um público diversificado. Os dados obtidos por meio do questionário servem como base para a análise da percepção dos usuários, permitindo complementar os resultados da avaliação técnica apresentada anteriormente.

Ele foi estruturado em três seções distintas. A primeira seção teve como finalidade a caracterização dos participantes, contendo perguntas voltadas à identificação do público-alvo, como a verificação se o respondente joga jogos digitais, a frequência com que joga e as plataformas utilizadas. Nessa etapa, foi aplicado um critério de filtragem, no qual participantes que indicaram não jogar foram direcionados automaticamente para o encerramento do formulário, não participando das seções seguintes.

A segunda seção foi destinada à coleta de informações sobre a experiência dos usuários em relação a incidentes de segurança, abordando aspectos como ocorrências de acesso não autorizado a contas e situações envolvendo possíveis comprometimentos de

credenciais. A terceira e última seção teve como foco a percepção dos usuários quanto à segurança das plataformas utilizadas, incluindo questões relacionadas ao uso de mecanismos de proteção, como autenticação em dois fatores, ao nível de confiança nos serviços e à opinião dos participantes sobre casos de perda de credenciais.

Após o encerramento da coleta, foi realizada uma etapa de verificação e tratamento dos dados, na qual respostas inconsistentes foram identificadas e tratadas de forma pontual. Consideraram-se inconsistentes aquelas em que o participante apresentou respostas contraditórias entre perguntas relacionadas, como, por exemplo, indicar que nunca teve uma conta roubada e, ainda assim, responder à questão sobre em qual plataforma ocorreu o incidente.

Nesses casos, as respostas foram desconsideradas apenas nas análises específicas em que a inconsistência impactava diretamente os resultados, sendo mantidas nas demais questões válidas. Ao todo, 16 respostas foram desconsideradas em cinco perguntas distintas. Adicionalmente, foram identificadas duas respostas com ausência de informações obrigatórias em uma questão específica, as quais também foram desconsideradas apenas na análise correspondente.

4.1.1. Perfil dos participantes

A análise do perfil dos participantes tem como objetivo caracterizar o público que respondeu ao questionário, permitindo uma melhor contextualização dos resultados obtidos.

De modo geral, os participantes são usuários ativos de plataformas de distribuição digital de jogos, apresentando diferentes níveis de experiência e frequência de uso. Essa característica contribui para a confiabilidade das respostas, uma vez que os respondentes possuem familiaridade com os serviços analisados.

Ao todo, foram obtidas 112 respostas, das quais 111 correspondem ao público alvo da pesquisa, composto por usuários que jogam jogos digitais. Apenas um respondente indicou não possuir esse hábito, sendo desconsiderado nas análises específicas relacionadas ao uso das plataformas.

4.1.2. Experiências com invasão de contas

A análise das respostas relacionadas a incidentes de segurança permite compreender a frequência e o impacto de invasões de contas entre os participantes.

Foi observado que 69 (62,8%) entrevistados afirmaram já ter sofrido algum tipo de invasão, enquanto 42 (37,8%) relataram nunca ter passado por esse tipo de situação. Esse resultado indica que uma parcela significativa dos usuários já foi afetada por incidentes de segurança, evidenciando que esse tipo de ocorrência é relativamente comum no contexto das plataformas de distribuição digital de jogos.

Em relação às plataformas nas quais ocorreram os incidentes, a Figura 1 apresenta a distribuição dos casos relatados, estando destacado em vermelho o total de ocorrências a cada plataforma. Observa-se que as invasões ocorrem entre diferentes plataformas utilizadas pelos participantes, indicando que o problema não está em um único serviço es-

pecífico.

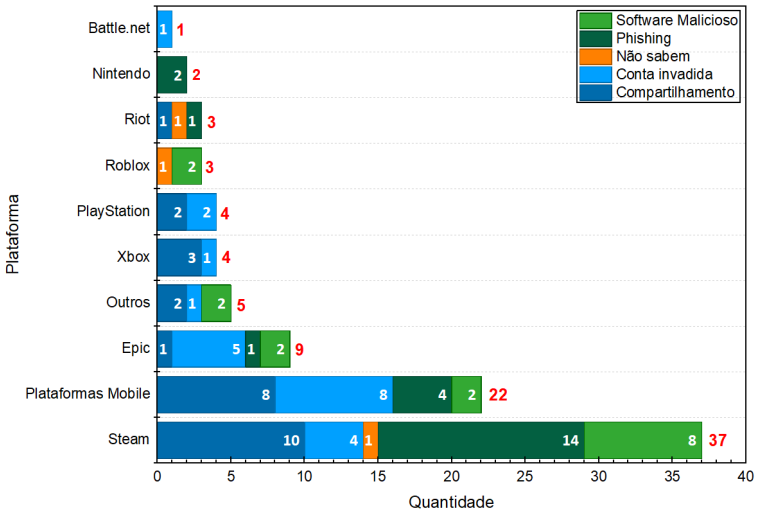


Figura 1. Plataformas onde ocorreram as invasões de conta e quais métodos foram utilizados

No que se refere às formas de ocorrência das invasões, a Figura 1 apresenta os métodos citados pelos participantes, mostrando a distribuição de métodos ocorridos em cada plataforma. Entre os principais relatos, destacam-se o comprometimento de credenciais, acesso indevido de outro dispositivo, compartilhamento de credenciais e ataques de *phishing*.

O compartilhamento de credenciais consiste na prática de fornecer acesso a terceiros, o que aumenta significativamente o risco de uso indevido ou perda de controle da conta. Além disso, o uso de *softwares* piratas também representam um vetor de ataque, uma vez que esses programas podem conter códigos maliciosos capazes de capturar informações sensíveis do usuário, apesar de ser o método com menos ocorrências.

Dessa forma, observa-se que muitos dos incidentes relatados estão associados a práticas de risco por parte dos próprios usuários, reforçando a importância da conscientização e da adoção de medidas básicas de segurança digital.

Complementarmente, observou-se que 36 participantes dos que já tiveram credenciais comprometidas (52,2% dos 69 que sofreram invasão) conseguiram recuperar o acesso às suas contas, enquanto 33 (47,8%) não obtiveram sucesso. Esse resultado evidencia que, embora existam mecanismos de recuperação disponíveis, uma parcela significativa dos usuários ainda enfrenta dificuldades nesse processo, podendo resultar em perdas permanentes.

Além disso, também foram analisadas as estratégias utilizadas pelos usuários para recuperação de suas credenciais. A Figura 2 apresenta os métodos empregados nesse processo, evidenciando as diferentes abordagens adotadas pelos participantes. Destaca-se que o suporte oferecido pelas próprias plataformas se mostrou um dos meios mais eficazes para a recuperação de contas, sendo responsável por grande parte dos casos bem-sucedidos. Esse resultado indica que, apesar das dificuldades relatadas, os sistemas de

atendimento das plataformas desempenham um papel fundamental na resolução desse tipo de problema.

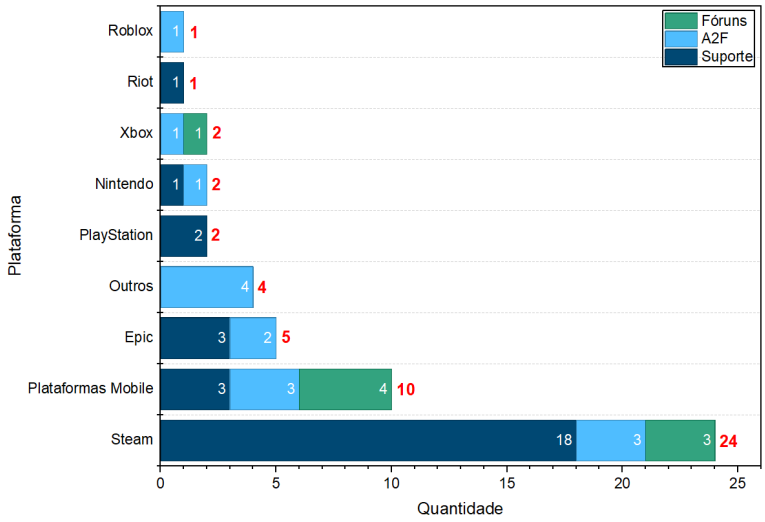


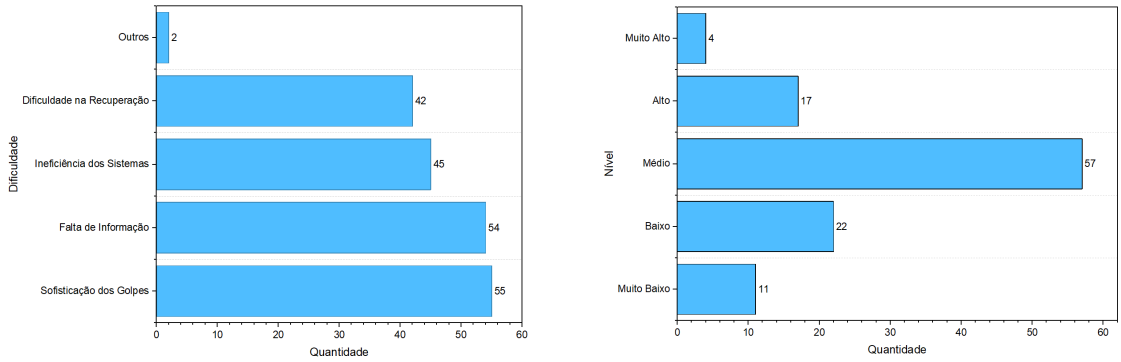
Figura 2. Lista de métodos de recuperação das contas utilizados pelos usuários

Dessa forma, os resultados confirmam que as invasões representam um risco relevante para os usuários, tanto pela frequência com que ocorrem quanto pelas dificuldades associadas à recuperação do acesso, destacando a necessidade de adoção de medidas preventivas mais eficazes, bem como da conscientização dos usuários quanto às boas práticas de segurança digital.

4.1.3. Percepção dos usuários sobre segurança

A análise da percepção dos usuários em relação à segurança digital permite compreender não apenas o nível de conhecimento declarado, mas também como esse conhecimento influencia suas atitudes e comportamentos no uso de plataformas digitais.

Inicialmente, foi solicitado aos participantes que avaliassem seu nível de conhecimento em cibersegurança. A Figura 3b apresenta a distribuição das respostas.



(a) Dificuldades em segurança nas plataformas

(b) Nível de conhecimento em cibersegurança

Figura 3. Percepções dos usuários sobre dificuldades e nível de conhecimento em cibersegurança.

Observa-se que a maioria dos participantes se concentra em níveis intermediários de conhecimento, enquanto uma parcela menor se considera altamente capacitada.

A análise da Figura 3a evidencia que as principais dificuldades percebidas pelos usuários estão relacionadas à sofisticação dos golpes (55 respostas) e à falta de informação (54 respostas), indicando que o fator humano e o desconhecimento ainda são os maiores desafios em termos de segurança. Em seguida, destacam-se a ineficiência dos sistemas (45) e a dificuldade na recuperação de acesso (42), sugerindo que, embora existam mecanismos de proteção, os usuários ainda encontram obstáculos no suporte e na resposta a incidentes. Esses resultados reforçam que a segurança não depende apenas de soluções técnicas, mas também da conscientização dos usuários.

Também foi visto que 91 entrevistados (82,7%) afirmaram adotar algum tipo de medida complementar de segurança, enquanto 19 (17,3%) relataram não utilizar tais recursos. Esse resultado indica uma predominância no uso de mecanismos de proteção, sugerindo um nível relevante de conscientização por parte dos usuários. No entanto, a existência de uma parcela que ainda não adota essas medidas evidencia possíveis lacunas no conhecimento ou na percepção de risco.

Na sequência, foi analisada a percepção dos usuários em relação à segurança das plataformas utilizadas. A Figura 4 apresenta os resultados obtidos.

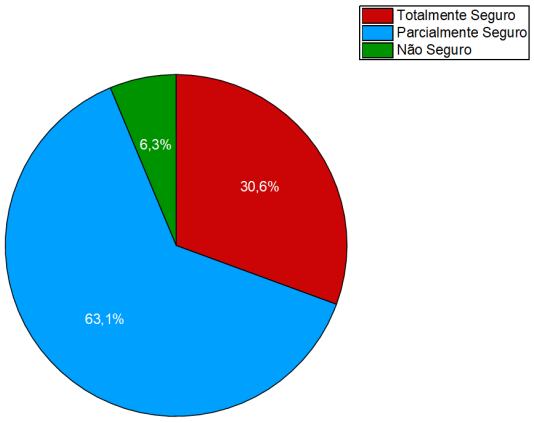


Figura 4. Percepção dos usuários quanto à segurança das plataformas

Observa-se que a maioria dos usuários considera as plataformas parcialmente seguras (63,1%), enquanto 30,6% as avaliam como totalmente seguras e apenas 6,3% as classificam como não seguras. Esses dados indicam uma percepção predominantemente moderada de segurança, sugerindo que, embora exista confiança nas plataformas, ainda há incertezas quanto à efetividade dos mecanismos de proteção.

4.1.4. Discussão dos resultados

De modo geral, observa-se que, apesar de a maioria dos usuários afirmar utilizar medidas de segurança adicionais e declarar possuir um nível intermediário de conhecimento em cibersegurança, as invasões de contas ainda são bastante recorrentes, atingindo 62,8% dos respondentes (assim como foi visto na Seção 4.1.2).

Ao analisar os métodos envolvidos nesses incidentes, verifica-se que uma parcela significativa dos casos está relacionada ao uso inadequado por parte dos próprios usuários, como cair em golpes, compartilhar senhas com terceiros e outras práticas semelhantes (também visto na Seção 4.1.2).

4.2. Coleta e análise dos dados das plataformas

A coleta de dados das plataformas analisadas foi realizada por meio da ferramenta *Wireshark* [Wireshark Foundation 2024]. Essa ferramenta permite uma visualização detalhada dos pacotes transmitidos entre cliente e servidor, o que possibilita a identificação de protocolos, endereços IP, portas utilizadas e informações relacionadas à segurança das comunicações.

A partir dos pacotes capturados, foi possível realizar a análise das características de segurança das comunicações, com foco na configuração do protocolo TLS adotada por cada plataforma. Dessa forma, o uso do *Wireshark* mostrou-se fundamental para a obtenção dos dados técnicos necessários à avaliação comparativa proposta neste estudo.

4.2.1. Endereço de IP

O endereço IP (*Internet Protocol*) é um identificador numérico atribuído aos dispositivos conectados à rede, sendo utilizado para permitir a comunicação entre cliente e servidor por meio do encaminhamento de pacotes de dados.

No *Wireshark*, foi utilizado o filtro "*tls.handshake.extensions_server_name*", que permite identificar pacotes contendo a extensão *Server Name Indication* (SNI) do protocolo TLS. Essa extensão permite ao cliente indicar o nome do servidor durante o processo de *handshake*, que corresponde à etapa inicial da comunicação TLS na qual cliente e servidor estabelecem parâmetros de segurança, como algoritmos criptográficos e chaves de sessão [Rescorla 2018].

A partir da aplicação desse filtro, foram observados todos os pacotes que apresentavam um nome de servidor válido, obtendo diversos resultados, então foi realizada uma análise da frequência dos endereços IP associados a cada plataforma, sendo selecionado o endereço que mais se repetia durante a execução da aplicação. Esse critério foi adotado com o objetivo de identificar o principal servidor responsável pelas comunicações da plataforma naquele contexto de uso, já que uma plataforma tem vários serviços rodando ao mesmo tempo, considerando que uma mesma plataforma pode utilizar diversos serviços simultaneamente, o que resulta em múltiplos endereços IP relacionados.

A identificação da localização geográfica dos endereços IP foi realizada por meio da plataforma Geolocation [Geolocation 2026], que permite mapear, de forma aproximada, a origem geográfica dos servidores a partir dos endereços IP analisados.

Com base nesse procedimento, foi possível estabelecer a relação entre cada plataforma analisada e seu respectivo endereço IP predominante, conforme apresentado na Tabela 2.

Tabela 2. Tabela de IP's analisados referentes a cada plataforma e suas localizações

Plataforma	Endereço IP	Localização
Steam	23.38.154.98	Brasil, São Paulo
Epic Games	104.18.13.225	Estados Unidos, California
GOG Galaxy	151.101.249.55	Brasil, São Paulo
Ubisoft Connect	99.83.188.134	Estados Unidos, Washington
EA App	23.216.191.115	Brasil, São Paulo
Battle.net	137.221.104.171	Países Baixos, Holanda do Norte
Xbox	52.149.193.114	Estados Unidos, Virginia

A identificação do endereço IP predominante de cada plataforma é fundamental para as etapas seguintes da análise, pois permite direcionar a observação do tráfego de rede para os principais servidores envolvidos na comunicação, possibilitando uma avaliação mais precisa dos aspectos de segurança. Destaca-se ainda que a localização dos servidores pode estar associada a diferentes legislações e políticas de cibersegurança, fator relevante para análises mais aprofundadas, embora esse aspecto não seja o foco do presente trabalho.

4.2.2. Domínio do servidor

O domínio do servidor corresponde ao nome dado a um serviço na rede, sendo usado para facilitar a identificação e o acesso aos servidores sem a necessidade de utilizar diretamente endereços IP. Esse mecanismo é essencial para o funcionamento da *Internet*, permitindo a tradução de nomes de domínio em endereços IP por meio do sistema de resolução de nomes.

No contexto deste trabalho, a identificação dos domínios foi utilizada para complementar a análise dos endereços IP, possibilitando associar de forma mais clara as conexões capturadas às plataformas analisadas.

No *Wireshark*, a partir da aplicação do filtro "*ip.addr == IP*", foi inserido o endereço IP previamente identificado para cada plataforma. Esse filtro permite exibir todos os pacotes relacionados a um determinado endereço IP, abrangendo tanto o tráfego de entrada quanto de saída.

Com essa filtragem, foi possível analisar os detalhes dos pacotes capturados, onde o nome de domínio pôde ser observado em campos como o SNI durante o *handshake* TLS. Dessa forma, foi possível identificar o domínio associado às conexões estabelecidas com cada plataforma.

Com base nesse procedimento, foi possível relacionar os domínios de servidor aos respectivos endereços IP analisados, contribuindo para uma compreensão mais detalhada da infraestrutura de comunicação das plataformas estudadas, conforme analisado na Tabela 3.

Tabela 3. Tabela de domínios análisados referentes a cada plataforma

Plataforma	Domínio
Steam	steamcommunity.com
Epic Games	social-overlay.ol.epicgames.com
GOG Galaxy	cfg.gog.com
Ubisoft Connect	public-ubiservices.ubi.com
EA App	desktop-config.juno.ea.com
Battle.net	telemetry-in.battle.net
Xbox	beige.xboxservices.com

Dessa forma, a identificação dos domínios complementou a coleta dos endereços IP, permitindo relacionar as conexões capturadas às plataformas analisadas. No entanto, os domínios, por si só, não permitem conclusões diretas sobre aspectos de segurança. Sua principal utilidade neste trabalho foi servir como base para análises complementares, como a verificação das informações dos certificados digitais utilizados por cada plataforma.

4.2.3. Portas de comunicação utilizadas pelas plataformas

A porta de comunicação é um identificador lógico utilizado pelos protocolos de rede para direcionar os dados ao serviço correto dentro de um dispositivo, cada serviço em execução

em um servidor pode ser associado a uma porta específica, permitindo que múltiplas aplicações utilizem a rede simultaneamente sem que haja congestionamento.

Diferentes portas são associadas a serviços distintos na comunicação em rede, por exemplo, a porta 80 é tradicionalmente utilizada para comunicações HTTP (*Hypertext Transfer Protocol*), um protocolo de aplicação responsável pela troca de informações entre cliente e servidor na *web*, como o carregamento de páginas, envio de formulários e requisição de recursos. No entanto, o HTTP não utiliza mecanismos de criptografia, o que torna os dados transmitidos vulneráveis à interceptação.

Também existe a porta 21, a qual está associada ao protocolo FTP (*File Transfer Protocol*) para transferência de arquivos, enquanto a porta 443 é destinada a conexões seguras que utilizam HTTPS (*Hypertext Transfer Protocol Secure*). O HTTPS consiste na utilização do HTTP em conjunto com mecanismos de criptografia, permitindo garantir a confidencialidade e a integridade dos dados transmitidos entre cliente e servidor.

No *Wireshark*, a porta utilizada foi identificada por meio da análise dos campos de origem e destino presentes no cabeçalho dos protocolos de transporte. A partir dessa análise, foi observado que todas as plataformas analisadas estabeleceram suas comunicações utilizando a porta 443.

De forma complementar, foi realizada uma análise das portas abertas utilizando a ferramenta Zenmap [Lyon 2023], permitindo identificar quais portas estavam disponíveis para conexão nos domínios das plataformas. Diferentemente da porta utilizada na comunicação, as portas abertas representam os pontos de entrada do servidor, ou seja, serviços que estão ativos e aguardando conexões externas, independentemente de terem sido utilizados durante a análise. Os resultados obtidos encontram-se apresentados na Tabela 4.

A partir da comparação entre os dados, observa-se que, embora múltiplas portas estejam abertas em algumas plataformas, como 80 (HTTP), 8080 (porta alternativa para HTTP) e 8443 (porta alternativa para HTTPS), a comunicação efetivamente estabelecida durante a execução das aplicações ocorreu exclusivamente pela porta 443. Portas alternativas correspondem a variações das portas padrão e são geralmente utilizadas em situações específicas, como testes, restrições de rede, balanceamento de serviços ou configurações personalizadas de servidores.

Tabela 4. Tabela de portas utilizadas por cada plataforma

Plataforma	Porta utilizada	Portas abertas
Steam	443	80 e 443
Epic Games	443	80, 443, 8080 e 8443
GOG Galaxy	443	80 e 443
Ubisoft Connect	443	443
EA App	443	80 e 443
Battle.net	443	443
Xbox	443	80 e 443

Esse resultado indica que todas as plataformas analisadas utilizam a porta 443 para a comunicação principal, o que demonstra a adoção de conexões seguras baseadas

em HTTPS. No entanto, ao observar as portas adicionais abertas, é possível identificar diferenças relevantes entre elas. A Steam, por exemplo, mantém abertas as portas 80 e 443, sendo a porta 80 tradicionalmente associada a conexões HTTP não criptografadas, geralmente utilizadas para redirecionamento para HTTPS. Já a Epic Games apresenta um conjunto mais amplo de portas abertas (80, 443, 8080 e 8443), sendo as portas 8080 e 8443 comumente utilizadas como alternativas para serviços *web*.

A presença dessas portas adicionais não implica, por si só, menor segurança, mas pode indicar uma maior complexidade na infraestrutura de rede, o que potencialmente amplia a superfície de exposição caso esses serviços não estejam devidamente configurados e protegidos. Por outro lado, plataformas como Ubisoft Connect e Battle.net, que apresentam apenas a porta 443 aberta, demonstram uma abordagem mais restritiva em termos de serviços expostos.

Dessa forma, não é possível afirmar que a utilização de mais portas torna uma plataforma menos segura de maneira direta. No entanto, uma configuração mais enxuta tende a reduzir possíveis vetores de ataque, desde que atenda adequadamente às necessidades operacionais do serviço. Portanto, a análise das portas deve ser interpretada em conjunto com outros fatores, como configuração de TLS, certificados digitais e práticas gerais de segurança adotadas pelas plataformas.

4.2.4. Protocolo de transporte

O protocolo de transporte é o responsável por garantir a entrega dos dados entre cliente e servidor, ele estabelece regras para controle de fluxo, confiabilidade e integridade da comunicação. No contexto das comunicações analisadas, o principal protocolo observado foi o TCP, amplamente utilizado em aplicações que exigem transmissão confiável de dados.

No *Wireshark* , a identificação do protocolo de transporte pode ser observada diretamente na lista de pacotes capturados, na coluna "*Protocol*", onde os pacotes são classificados como TCP. Além disso, ao selecionar um pacote específico, é possível visualizar na seção de detalhes a camada correspondente ao TCP.

Durante a etapa de coleta de dados, foi possível observar que todas as plataformas analisadas utilizam exclusivamente o protocolo TCP para o transporte de dados. Esse comportamento está diretamente relacionado ao uso de protocolos como o HTTPS, que dependem do TCP para garantir uma comunicação segura e confiável entre cliente e servidor.

4.2.5. Versão do Protocolo TLS

A versão do protocolo TLS utilizada em cada plataforma foi identificada a partir da análise dos pacotes capturados no *Wireshark* durante o processo de *handshake*. No contexto do estabelecimento dessas conexões, as mensagens *Client Hello* e *Server Hello* desempenham papel fundamental. A mensagem *Client Hello* é enviada pelo cliente ao iniciar a comunicação, contendo informações como as versões de TLS suportadas, os conjuntos de cifras (*cipher suites*) disponíveis e extensões adicionais. Em resposta, o servidor envia

a mensagem *Server Hello*, na qual define os parâmetros que serão utilizados na conexão, como a versão do protocolo e o conjunto de cifras selecionado. Dessa forma, boa parte das informações análisadas vem desses pacotes.

Para a análise, foi aplicado no *Wireshark* o filtro "*ip.addr == IP and tls.handshake.type == 2*", com o objetivo de isolar os pacotes do tipo *Server Hello* associados ao endereço IP de cada plataforma analisada. Esse procedimento permitiu focar diretamente nas respostas do servidor durante o *handshake*, onde são definidos os parâmetros da conexão segura.

Ao selecionar os pacotes filtrados, a confirmação da versão do TLS foi realizada na seção de detalhes do protocolo. No caso do TLS 1.3, essa identificação exige uma análise mais minuciosa, pois podem aparecer informações relacionadas a versões anteriores em diferentes partes do pacote. Especificamente, o campo "*Version*" presente no cabeçalho do *Server Hello* pode indicar TLS 1.2 por motivos de compatibilidade, enquanto a versão efetivamente negociada é apresentada na extensão "*Supported Versions*", onde é possível confirmar o uso do TLS 1.3.

Dessa forma, a análise considerou como critério principal o valor presente na extensão "*Supported Versions*", garantindo a identificação correta da versão do protocolo utilizada por cada plataforma. A partir dos dados obtidos, foi realizada uma análise comparativa entre as versões TLS 1.2 e TLS 1.3, cujos resultados são apresentados na Tabela 5, evidenciando a adoção predominante de versões mais recentes do protocolo. Esse comportamento indica a adoção de versões consideradas seguras do protocolo, como o uso do TLS 1.3, que incorpora melhorias mais recentes em termos de segurança e desempenho, enquanto o TLS 1.2 ainda permanece amplamente utilizado e considerado seguro, embora não represente o estado mais atual do protocolo [Rescorla 2018].

Tabela 5. Tabela de versões TLS referêntes a cada plataforma

Plataforma	Versão TLS
Steam	TLS 1.3
Epic Games	TLS 1.3
GOG Galaxy	TLS 1.3
Ubisoft Connect	TLS 1.2
EA App	TLS 1.3
Battle.net	TLS 1.2
Xbox	TLS 1.3

Assim, verifica-se a predominância do uso do TLS 1.3 entre as plataformas analisadas, refletindo a adoção de padrões mais modernos de segurança, embora ainda haja suporte ao TLS 1.2.

4.2.6. Cipher Suites

Uma *cipher suite* é um conjunto de algoritmos criptográficos utilizado durante o estabelecimento de uma conexão segura, ela é responsável por definir como serão realizados os processos de proteção dos dados transmitidos entre cliente e servidor. De forma ge-

ral, uma *cipher suite* é composta por diferentes elementos, cada um com uma função específica dentro da comunicação segura.

A estrutura das *cipher suites* pode variar de acordo com a versão do protocolo TLS utilizada. No TLS 1.2, a *cipher suite* define explicitamente todos os algoritmos envolvidos na comunicação, incluindo o método de troca de chaves, o mecanismo de autenticação, o algoritmo de criptografia e a função de integridade, já no TLS 1.3 houve uma simplificação dessa estrutura, na qual a *cipher suite* passa a especificar apenas os algoritmos de criptografia e integridade, enquanto os mecanismos de troca de chaves são negociados separadamente durante o processo de *handshake*. Essa mudança contribui para maior segurança e eficiência no estabelecimento da conexão.

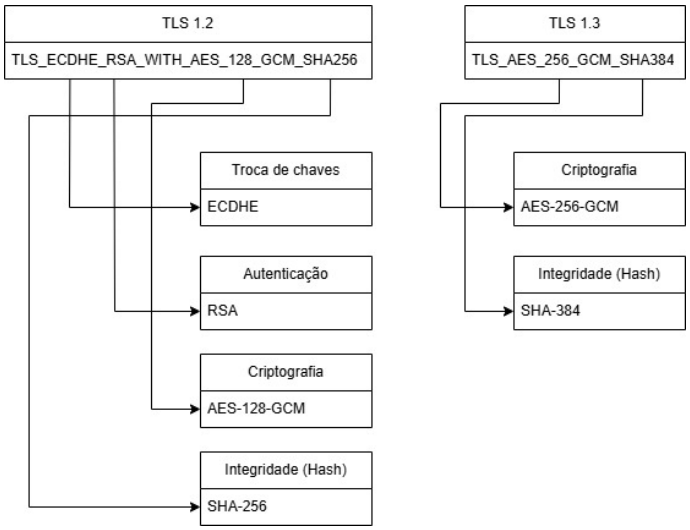


Figura 5. Diagrama referente à estrutura das *cipher suites* nos protocolos TLS 1.2 e TLS 1.3

Esses elementos atuam de forma complementar, onde o algoritmo de troca de chaves consiste no processo pelo qual cliente e servidor estabelecem de forma segura um segredo compartilhado, utilizado posteriormente na criptografia da comunicação. A autenticação está relacionada à verificação da identidade do servidor (e, em alguns casos, do cliente), garantindo que a conexão está sendo estabelecida com a entidade correta. A criptografia, por sua vez, é responsável por proteger os dados transmitidos, impedindo que terceiros consigam interpretá-los mesmo que tenham acesso aos pacotes. Por fim, o mecanismo de integridade, geralmente baseado em funções de *hash*, tem como objetivo assegurar que as informações não foram alteradas durante o tráfego na rede, permitindo a detecção de qualquer modificação indevida nos dados.

Para este trabalho, a identificação da *cipher suite* teve como objetivo analisar os padrões criptográficos que são adotados pelas plataformas estudadas, permitindo avaliar o nível de segurança utilizado nas conexões estabelecidas. A adoção de algoritmos mais modernos e robustos está diretamente relacionada à proteção contra ataques e à garantia da confidencialidade das informações transmitidas.

A coleta dessas informações foi realizada observando pacotes do tipo *Server Hello*, nas quais o servidor informa a *cipher suite* selecionada para a sessão. Essa

informação pode ser visualizada na seção de detalhes do protocolo TLS, no campo correspondente à *cipher suite*, presente na estrutura do pacote.

Além da *cipher suite* selecionada, que é destacada no pacote *Server Hello*, também é possível observar uma lista de *cipher suites* suportadas pelo cliente, enviada no pacote *Client Hello*. Essa lista representa o conjunto de algoritmos que o cliente é capaz de utilizar na comunicação segura, sua existência está relacionada ao processo de negociação do protocolo TLS, no qual o servidor escolhe, dentre as opções fornecidas pelo cliente, a *cipher suite* mais adequada que também esteja presente em sua própria configuração. Esse mecanismo garante compatibilidade entre diferentes implementações e permite que a conexão utilize o nível mais alto de segurança suportado por ambas as partes.

A partir da identificação desses dados, foi possível determinar os algoritmos utilizados por cada uma das plataformas analisadas. Os resultados obtidos são apresentados nas Tabelas 6 e 7.

Tabela 6. Componentes das *cipher suites* TLS 1.3

Plataforma	Criptografia	Integridade
Steam	AES-256-GCM	SHA-384
Epic Games	AES-128-GCM	SHA-256
GOG Galaxy	AES-128-GCM	SHA-256
EA App	AES-256-GCM	SHA-384
Xbox	AES-256-GCM	SHA-384

A Tabela 6 apresenta os algoritmos utilizados nas *cipher suites* associadas ao TLS 1.3. Observa-se que, nesse protocolo, a estrutura das *cipher suites* é simplificada, sendo composta essencialmente pelos algoritmos de criptografia e de integridade. Nota-se a predominância do uso de modos GCM associados ao algoritmo AES, com chaves de 128 e 256 bits, além do uso de funções de *hash* como SHA-256 e SHA-384.

Tabela 7. Componentes das *cipher suites* TLS 1.2

Plataforma	Troca de Chaves	Autenticação	Criptografia	Integridade
Ubisoft Connect	ECDHE	RSA	AES-128-GCM	SHA-256
Battle.net	RSA	RSA	AES-128-GCM	SHA-256

Já a Tabela 7 apresenta os componentes das *cipher suites* para conexões que utilizam TLS 1.2. Diferentemente do TLS 1.3, observa-se uma estrutura mais detalhada, na qual são explicitamente definidos os algoritmos de troca de chaves, autenticação, criptografia e integridade. No caso analisado, destaca-se o uso do ECDHE para troca de chaves, proporcionando sigilo direto *forward secrecy*, bem como o uso de RSA para autenticação, que não utiliza desta tecnologia. Além disso, assim como no TLS 1.3, são utilizados algoritmos AES em modo GCM e funções de hash SHA-256.

Com base nos dados coletados, observa-se que as plataformas que utilizam TLS 1.3 apresentam configurações mais seguras, principalmente pelo uso de *cipher suites* com AES-256-GCM e SHA-384, que oferecem maior robustez criptográfica. Por outro lado, plataformas como Epic Games e GOG Galaxy, embora também utilizem TLS 1.3, adotam

AES-128-GCM e SHA-256, que, apesar de seguras, possuem menor nível de resistência em comparação às anteriores. Já no caso do TLS 1.2, observa-se que a utilização de ECDHE na Ubisoft Connect garante propriedades importantes como *forward secrecy*, tornando-a mais segura em relação ao uso exclusivo de RSA na Battle.net, que não oferece essa característica. Dessa forma, verifica-se que, de maneira geral, as configurações mais modernas e seguras estão associadas ao uso do TLS 1.3 e de algoritmos mais robustos.

4.2.7. Algoritmo de criptografia

Um algoritmo de criptografia é o componente responsável por garantir a confidencialidade dos dados transmitidos durante uma conexão segura, impedindo que terceiros consigam interpretar as informações mesmo que tenham acesso ao tráfego de rede. No protocolo TLS, a criptografia utilizada é do tipo simétrica, ou seja, cliente e servidor utilizam a mesma chave secreta, previamente estabelecida durante o processo de *handshake*.

Assim como nas *cipher suites*, os algoritmos de criptografia utilizados podem variar de acordo com a versão do protocolo TLS. No TLS 1.2, diferentes algoritmos podiam ser empregados, incluindo modos de operação mais antigos, como CBC (*Cipher Block Chaining*), que apresentavam algumas limitações de segurança. Já no TLS 1.3, houve uma padronização para o uso de algoritmos mais modernos e seguros, com destaque para o AES no modo GCM (*Galois/Counter Mode*), que oferece simultaneamente confidencialidade e integridade dos dados [Rescorla 2018].

Neste trabalho, foram identificados principalmente os algoritmos AES_128_GCM e AES_256_GCM, ambos amplamente utilizados em implementações modernas do protocolo TLS. O AES (*Advanced Encryption Standard*) é um algoritmo de criptografia simétrica reconhecido por sua eficiência e alto nível de segurança, sendo adotado como padrão em diversas aplicações de segurança da informação.

A principal diferença entre AES_128 e AES_256 está no tamanho da chave criptográfica utilizada. No caso do AES_128, a chave possui 128 bits, enquanto no AES_256 possui 256 bits. Em termos de segurança, o AES_256 oferece uma maior resistência contra ataques de força bruta devido ao maior número de combinações possíveis. Por outro lado, o AES_128 apresenta melhor desempenho computacional, exigindo menos processamento, o que pode ser vantajoso em cenários que demandam maior eficiência. Ainda assim, ambos são considerados seguros quando utilizados com modos de operação modernos, como o GCM.

No contexto da análise realizada, a identificação do algoritmo de criptografia teve como objetivo verificar se as plataformas analisadas utilizam padrões atualizados e seguros. A adoção de algoritmos como AES em modo GCM indica conformidade com boas práticas de segurança, contribuindo para a proteção dos dados transmitidos.

A coleta dessas informações foi realizada a partir da análise das *cipher suites* presentes nos pacotes TLS capturados no *Wireshark*. A partir da identificação da *cipher suite* selecionada, foi possível extrair diretamente o algoritmo de criptografia utilizado na sessão, conforme apresentado na Tabela 8.

Tabela 8. Tabela de algoritmos de criptografia adotados por cada plataforma

Plataforma	Algoritmo de Criptografia
Steam	AES_256_GCM
Epic Games	AES_128_GCM
GOG Galaxy	AES_128_GCM
Ubisoft Connect	AES_128_GCM
EA App	AES_256_GCM
Battle.net	AES_128_GCM
Xbox	AES_256_GCM

Em ambientes que exigem alta performance, como plataformas de distribuição digital de jogos, a escolha por algoritmos mais eficientes pode contribuir para a redução de latência e melhor experiência do usuário. É importante considerar que essas plataformas frequentemente operam em conjunto com os próprios jogos, compartilhando recursos do sistema durante a execução. Dessa forma, a adoção do AES_128 pode estar relacionada à busca por maior eficiência computacional, reduzindo o impacto no desempenho geral da aplicação. Ainda assim, a presença do AES_256 demonstra que algumas plataformas optam por um nível adicional de robustez criptográfica, priorizando maior resistência teórica a ataques de força bruta. Ambos os algoritmos são considerados seguros e estão em conformidade com recomendações atuais, sendo o AES_128 geralmente preferido por sua eficiência, enquanto o AES_256 é adotado em cenários que demandam maior margem de segurança.

4.2.8. Tamanho da Chave Pública

O tamanho da chave pública é um dos parâmetros fundamentais nos mecanismos criptográficos utilizados durante o estabelecimento de conexões seguras, estando diretamente relacionado ao nível de segurança oferecido pelos algoritmos assimétricos. No protocolo TLS, a criptografia assimétrica é empregada principalmente nas etapas iniciais do *handshake*, sendo utilizada para autenticação e, em determinadas configurações, para o estabelecimento do segredo compartilhado [Rescorla 2018].

O segredo compartilhado é um valor criptográfico gerado de forma conjunta entre cliente e servidor durante o processo de *handshake*, sem que esse valor seja transmitido diretamente pela rede. Esse mecanismo é viabilizado por algoritmos de troca de chaves, como o *Diffie-Hellman* e suas variações, que permitem que ambas as partes obtenham o mesmo valor a partir de informações trocadas publicamente. A partir desse segredo, são derivadas as chaves simétricas utilizadas na criptografia da sessão, garantindo a confidencialidade das informações e contribuindo para a segurança da comunicação [Rescorla 2018].

De forma geral, o tamanho da chave pública refere-se à quantidade de bits utilizados na geração da chave criptográfica, influenciando diretamente a complexidade necessária para comprometer o algoritmo por meio de ataques de força bruta ou métodos matemáticos avançados. Chaves maiores tendem a oferecer maior segurança, porém implicam em maior custo computacional, tornando as operações criptográficas mais lentas

[Kurose and Ross 2017].

No TLS 1.2, é comum a utilização de algoritmos como o RSA (*Rivest–Shamir–Adleman*), um sistema de criptografia assimétrica baseado na dificuldade computacional de fatorar números inteiros grandes. Nesse contexto, o tamanho da chave pública, como 2048 ou 4096 bits, é um fator determinante para a segurança da comunicação, pois define o nível de resistência do algoritmo frente a ataques criptográficos [Dierks and Rescorla 2008].

Já no TLS 1.3, observa-se uma maior adoção de algoritmos baseados em curvas elípticas, como o ECDHE (*Elliptic Curve Diffie-Hellman Ephemeral*), que utilizam propriedades matemáticas dessas curvas para realizar operações criptográficas de forma mais eficiente, essas propriedades baseiam-se na dificuldade de resolver problemas matemáticos envolvendo pontos em curvas elípticas (ECC), considerados computacionalmente inviáveis de serem quebrados. Esses algoritmos oferecem níveis de segurança equivalentes aos métodos tradicionais com tamanhos de chave significativamente menores, como 256 bits, além de proporcionarem melhor desempenho [Bhargavan et al. 2017].

Para este trabalho, a análise do tamanho da chave pública teve como objetivo identificar os padrões adotados pelas plataformas estudadas, permitindo avaliar o nível de robustez dos mecanismos de autenticação e troca de chaves utilizados. A utilização de chaves adequadas está diretamente relacionada à resistência contra ataques criptográficos e à conformidade com boas práticas de segurança.

A coleta dessas informações foi realizada de maneiras distintas, conforme a versão do protocolo TLS utilizada pela plataforma. Nos casos em que foi identificado o uso do TLS 1.2, aplicou-se o filtro "*ip.addr == IP and tls.handshake.type == 11*" no *Wireshark*, permitindo isolar as mensagens de certificado (*Certificate*) durante o *handshake*. A partir da análise dos detalhes desses pacotes, foi possível identificar o tamanho da chave pública no campo "RSA Public-Key".

Já nas plataformas que utilizam TLS 1.3, devido às mudanças no processo de *handshake* e ao aumento da proteção das mensagens, não foi possível aplicar o mesmo método. Nesses casos, a coleta foi realizada por meio do acesso ao domínio da plataforma em um navegador web e da inspeção do certificado digital da conexão segura. A partir dessa análise, foi possível identificar o tipo e o tamanho da chave pública em campos como "Algoritmo de chave pública do assunto" e "Chave pública da entidade".

O resultado final da análise do tamanho das chaves ficou da seguinte forma:

Tabela 9. Tabela de tamanho da chave publica utilizados por cada plataforma

Plataforma	Tamanho da Chave
Steam	256 bits - ECC
Epic Games	256 bits - ECC
GOG Galaxy	256 bits - ECC
Ubisoft Connect	256 bits - ECC
EA App	256 bits - ECC
Battle.net	2048 bits - RSA
Xbox	2048 bits - RSA

Os resultados apresentados evidenciam uma predominância do uso de algoritmos baseados em curvas elípticas com chaves de 256 bits. Esse padrão está alinhado com as práticas modernas adotadas no TLS 1.3, que priorizam maior eficiência e desempenho sem comprometer a segurança [Bhargavan et al. 2017]. Por outro lado, observa-se que algumas plataformas ainda utilizam chaves RSA de 2048 bits, possivelmente devido à necessidade de compatibilidade com versões anteriores do protocolo ou a requisitos específicos de infraestrutura. De modo geral, os dados indicam uma tendência de migração gradual para algoritmos mais eficientes, mantendo níveis elevados de segurança.

No entanto, estudos indicam que essa evolução ainda está em curso e que mudanças no cenário tecnológico podem levar à reavaliação de algoritmos tradicionais, incluindo o próprio RSA, não necessariamente como solução predominante, mas como parte de um contexto mais amplo de adaptação às limitações práticas e aos avanços da computação quântica [Campos et al. 2024].

4.2.9. Autoridade certificadora

A Autoridade Certificadora (AC) é uma entidade responsável por emitir e validar certificados digitais utilizados em conexões seguras na Internet. No contexto do protocolo TLS, as ACs são fundamentais para o processo de autenticação, pois garantem que a identidade do servidor acessado pelo cliente é legítima e confiável [Rescorla 2018].

Os certificados digitais seguem o padrão X.509 e contêm informações como o nome do domínio, a chave pública do servidor e a assinatura digital da autoridade certificadora responsável por sua emissão. Essa assinatura permite que o cliente verifique a autenticidade do certificado, assegurando que ele não foi alterado e que foi emitido por uma entidade confiável.

Durante o estabelecimento de uma conexão segura, o cliente valida o certificado apresentado pelo servidor com base em uma lista de autoridades certificadoras confiáveis previamente armazenadas no sistema ou navegador. Caso o certificado não seja válido ou não seja reconhecido, o cliente pode alertar o usuário sobre possíveis riscos de segurança.

A coleta das informações referentes às autoridades certificadoras foi realizada por meio do acesso ao domínio das plataformas em um navegador web e da inspeção do certificado digital da conexão segura. A partir dessa análise, foi possível identificar a autoridade emissora nos campos correspondentes ao “Issuer” do certificado, permitindo identificar a autoridade certificadora associada a cada plataforma, conforme mostrado na Tabela 10.

Tabela 10. Tabela de autoridades certificadoras utilizadas por cada plataforma

Plataforma	AC
Steam	DigiCert
Epic Games	Let's Encrypt
GOG Galaxy	DigiCert
Ubisoft Connect	DigiCert
EA App	DigiCert
Battle.net	DigiCert
Xbox	Microsoft Azure

Os resultados apresentados evidenciam a predominância da autoridade certificadora DigiCert, responsável pela emissão da maioria dos certificados observados. Esse resultado indica uma forte preferência por soluções mais presentes no mercado, amplamente reconhecidas por sua confiabilidade e adoção em ambientes corporativos de grande escala.

Ainda que em menor número, também foram identificadas autoridades certificadoras como a Let's Encrypt e a Microsoft, que, apesar de não predominarem na amostra analisada, são amplamente reconhecidas e confiáveis no contexto da segurança digital. Destaca-se que a Let's Encrypt é uma autoridade certificadora gratuita e automatizada, amplamente utilizada para facilitar a adoção de HTTPS, especialmente em aplicações *web*. A presença dessas entidades demonstra que diferentes abordagens podem ser adotadas pelas plataformas, sem comprometer os padrões de segurança exigidos para comunicações seguras.

4.2.10. Forward Secrecy

A propriedade de *Forward Secrecy*, também conhecida como *Perfect Forward Secrecy* (PFS), refere-se à capacidade de um protocolo criptográfico de garantir que o comprometimento de chaves privadas de longo prazo não comprometa a confidencialidade de sessões passadas. No contexto do TLS, essa propriedade é alcançada por meio do uso de algoritmos de troca de chaves efêmeras, como o *Ephemeral Diffie-Hellman* (DHE) e sua variante baseada em curvas elípticas (ECDHE) [Rescorla 2018].

A utilização de *Forward Secrecy* assegura que, mesmo que um atacante obtenha acesso à chave privada do servidor, ele não será capaz de descriptografar comunicações previamente interceptadas, uma vez que cada sessão utiliza chaves temporárias independentes. Por conta disso, essa característica é considerada uma das principais melhorias de segurança adotadas nas versões mais recentes do protocolo TLS.

A verificação da presença de *Forward Secrecy* foi realizada com base na versão do protocolo TLS e na análise de *cipher suites* utilizadas por cada plataforma. Para conexões que utilizam TLS 1.3, a presença de *Forward Secrecy* foi considerada garantida, uma vez que essa versão do protocolo adota exclusivamente mecanismos de troca de chaves efêmeras [Rescorla 2018].

Para as plataformas que utilizam TLS 1.2, foi necessária uma análise adicional da

cipher suite. Nesses casos, a presença de algoritmos de troca de chaves efêmeras, como ECDHE, foi utilizada como critério para identificar o suporte à *Forward Secrecy*.

A partir dessa análise, verificou-se que a plataforma Ubisoft Connect, embora utilize TLS 1.2, possui ECDHE em sua *cipher suite*, indicando a presença de *Forward Secrecy*. Por outro lado, a plataforma Battle.net, que também utiliza TLS 1.2, não apresenta mecanismos de troca de chaves efêmeras, o que indica a ausência dessa propriedade de segurança, cujos resultados são apresentados na Tabela 11.

Tabela 11. Presença de *Forward Secrecy* nas plataformas analisadas

Plataforma	Possui FS
Steam	Sim
Epic Games	Sim
GOG Galaxy	Sim
Ubisoft Connect	Sim
EA App	Sim
Battle.net	Não
Xbox	Sim

Os resultados apresentados indicam que a maioria das plataformas analisadas adota o uso de *Forward Secrecy*, refletindo a utilização de práticas modernas de segurança, especialmente com a adoção do TLS 1.3 e de algoritmos efêmeros em TLS 1.2. No entanto, observa-se que a plataforma Battle.net não apresenta suporte a essa propriedade, o que representa uma limitação significativa do ponto de vista da segurança. A ausência de *Forward Secrecy* implica que, em caso de comprometimento da chave privada do servidor, comunicações passadas podem ser potencialmente descriptografadas, diferentemente das plataformas que utilizam essa proteção. Dessa forma, evidencia-se que a adoção dessa propriedade é um fator importante na garantia da confidencialidade a longo prazo das comunicações.

4.3. Número de conexões e tamanho médio dos pacotes

O número de conexões estabelecidas por uma aplicação durante sua execução representa a quantidade de comunicações realizadas com servidores, estando diretamente relacionado à arquitetura da aplicação. Esse comportamento pode envolver múltiplos serviços, como autenticação, distribuição de conteúdo, telemetria e atualizações. De forma complementar, o tamanho médio dos pacotes transmitidos caracteriza como ocorre a troca de dados, indicando o volume de informação transportado em cada unidade de comunicação.

A análise conjunta de ambos permite uma compreensão mais ampla do comportamento das plataformas em rede. Enquanto o número de conexões evidencia o grau de distribuição e complexidade das interações, o tamanho dos pacotes reflete as estratégias adotadas para transmissão de dados, podendo indicar comunicações mais fragmentadas ou mais concentradas.

A coleta dessas informações foi realizada por meio das estatísticas do Wireshark, utilizando a opção “Statistics” e, em seguida, “Conversations”. Foram analisadas as conversas TCP estabelecidas entre pares de endereços IP e portas. Para cada endereço IP

remoto, foi contabilizado o número de conexões distintas, bem como o volume total de dados trafegado e a quantidade de pacotes, permitindo estimar o tamanho médio por meio da razão entre bytes e número de pacotes.

Os resultados obtidos são apresentados na Tabela 12, possibilitando a comparação entre as plataformas analisadas.

Tabela 12. Número de conexões e tamanho médio dos pacotes por plataforma

Plataforma	Número de conexões	Tamanho médio dos pacotes
Steam	7	10 kB
Epic Games	30	1 kB
Ubisoft Connect	10	70 kB
GOG Galaxy	7	1 kB
EA App	19	54 kB
Battle.net	32	11 kB
Xbox	8	1 kB

Os resultados mostram variações significativas entre as plataformas analisadas. Em relação ao número de conexões, observa-se que plataformas como Epic Games e Battle.net apresentam valores mais elevados, sugerindo arquiteturas mais distribuídas, enquanto outras, como Steam e GOG Galaxy, apresentam menor quantidade de conexões, indicando maior centralização dos serviços.

Quanto ao tamanho médio dos pacotes, verifica-se que Epic Games, GOG Galaxy e Xbox utilizam pacotes menores, sugerindo uma comunicação mais fragmentada. Em contraste, Ubisoft Connect e EA App apresentam pacotes significativamente maiores, indicando maior concentração de dados por transmissão. Steam e Battle.net apresentam valores intermediários, caracterizando um comportamento mais equilibrado.

É importante ressaltar que neste estudo, essas métricas não foram utilizadas como critério direto de avaliação de segurança, mas sim como apoio à caracterização do comportamento das plataformas e à identificação dos endereços IP mais relevantes para as análises detalhadas de tráfego.

4.3.1. Uso de CDN's

O uso de redes de distribuição de conteúdo (CDNs) é um aspecto relevante na análise de aplicações que dependem de comunicação em rede, pois essas infraestruturas são responsáveis por otimizar a entrega de dados ao usuário final. As CDNs permitem a distribuição de conteúdo por meio de servidores geograficamente distribuídos, reduzindo a latência, melhorando o desempenho e aumentando a disponibilidade dos serviços.

A presença de CDNs pode indicar uma arquitetura mais escalável e preparada para lidar com grandes volumes de acesso, sendo amplamente utilizada por plataformas que realizam distribuição de conteúdo digital, como jogos, atualizações e mídias.

A identificação do uso de CDN foi realizada a partir dos endereços IP observados durante a captura de tráfego de rede. Esses endereços foram analisados por meio da

consulta no serviço *WHOIS* [ARIN 2026]. A partir dessas consultas, foi possível identificar a organização responsável por cada bloco de IP, permitindo verificar se os endereços estavam associados a provedores de CDN ou a infraestruturas próprias das plataformas.

Os resultados obtidos são apresentados na Tabela 13, possibilitando identificar quais plataformas fazem uso de redes de distribuição de conteúdo em sua comunicação.

Tabela 13. Uso de CDNs por cada plataforma

Plataforma	Usa CDN	CDN utilizada
Steam	Sim	Akamai
Epic Games	Sim	Cloudflare CDN
GOG Galaxy	Sim	Fastly CDN
Ubisoft Connect	Sim	Amazon Web Services
EA App	Sim	Akamai
Battle.net	Não	–
Xbox	Sim	Microsoft

Os resultados apresentados indicam que a maioria das plataformas analisadas utiliza redes de distribuição de conteúdo, evidenciando a adoção de infraestruturas voltadas à melhoria de desempenho, escalabilidade e disponibilidade dos serviços. Observa-se a utilização de provedores amplamente reconhecidos, como Akamai, Cloudflare e Fastly, além de soluções baseadas em grandes provedores de nuvem, como Amazon Web Services e Microsoft. Por outro lado, a plataforma Battle.net não apresentou indícios do uso de CDN pública, o que pode indicar a utilização de uma infraestrutura própria ou uma abordagem distinta na distribuição de conteúdo.

4.4. Análise dos dados

A partir dos dados coletados e analisados, foi possível identificar padrões relevantes no comportamento das plataformas de distribuição digital em relação aos mecanismos de segurança adotados. Os resultados obtidos permitem não apenas caracterizar tecnicamente cada plataforma, mas também estabelecer uma comparação entre elas com base em critérios objetivos, evidenciando diferentes níveis de aderência às práticas modernas de segurança da informação.

4.4.1. Critérios de avaliação

Para fazer uma comparação de segurança entre as plataformas analisadas, foi definido um conjunto de critérios técnicos baseados em práticas reconhecidas de segurança em comunicações digitais [Rescorla 2018]. Esses critérios foram selecionados por representarem mecanismos fundamentais para garantir a confidencialidade e a integridade dos dados transmitidos entre cliente e servidor.

A avaliação foi conduzida de forma qualitativa, sendo os resultados representados por símbolos na Tabela 14. O símbolo "•" indica que a plataforma atende plenamente ao critério avaliado, refletindo a adoção de tecnologias consideradas mais atuais e alinhadas

com a segurança da informação. Já o símbolo "○" representa atendimento parcial, indicando que a plataforma utiliza mecanismos funcionais, porém menos modernos ou com menor nível de robustez em comparação às alternativas mais recentes.

Os critérios considerados incluem a versão do protocolo TLS empregada, o suporte ao *Forward Secrecy*, o uso de CDN's e a análise de possíveis vetores de ataque relacionados à implementação. De forma geral, foram consideradas como práticas mais seguras o uso do TLS 1.3, suporte a *Forward Secrecy* e a utilização de CDN, enquanto a análise dos vetores de ataque busca identificar potenciais fragilidades associadas à implementação dos mecanismos criptográficos adotados.

Essa abordagem permite uma análise comparativa clara e objetiva entre as plataformas, mantendo fundamentação técnica nos critérios adotados.

4.4.2. Comparação entre plataformas

A partir dos dados obtidos, foi possível realizar uma comparação direta entre as plataformas analisadas, conforme apresentado na Tabela 14. Observa-se que as plataformas apresentam elevado nível de aderência aos critérios definidos, ainda que nenhuma atenda integralmente a todos eles, demonstrando a adoção consistente de práticas modernas de segurança. Esses resultados técnicos se comunicam com os dados obtidos no questionário, indicando que, apesar do nível de segurança identificado, ainda há uma percepção significativa de vulnerabilidade por parte dos usuários.

É importante ressaltar que a presença do símbolo "○"não implica necessariamente que a plataforma seja insegura, mas sim que utiliza tecnologias consideradas menos atuais em relação ao estado da arte em segurança da informação.

De modo geral, os resultados indicam que a maioria das plataformas analisadas apresenta um alto nível de adoção de mecanismos de segurança, atendendo a maior parte dos critérios estabelecidos e demonstrando alinhamento com práticas atuais da área de segurança. As diferenças observadas entre elas são pontuais e não comprometem significativamente o nível geral de proteção. Destaca-se, no entanto, a plataforma Battle.net, que apresentou menor aderência aos critérios avaliados, configurando-se como uma exceção em relação às demais.

Tabela 14. Tabela de comparação de segurança de plataformas

Plataforma	TLS	FS	CDN	Vetores de ataque de implementação
Steam	●	●	●	○
Epic Games	●	●	●	○
GOG Galaxy	●	●	●	○
Ubisoft Connect	○	●	●	○
EA App	●	●	●	○
Battle.net	○	○	○	●
Xbox	●	●	●	●

Os critérios utilizados na Tabela 14 consideram diferentes aspectos relacionados à segurança das comunicações. Na coluna referente ao protocolo TLS, plataformas que

utilizam versões mais recentes, como TLS 1.3, foram classificadas com o símbolo ”•”, enquanto aquelas que utilizam TLS 1.2 receberam ”○”. Em relação à propriedade de *Forward Secrecy*, foi atribuído ”•”às plataformas que implementam esse mecanismo e ”○”àquelas que não o apresentam. De forma similar, o uso de CDN's foi indicado por ”•”, sendo ”○”utilizado para plataformas que não fazem uso desse recurso. Esses critérios permitem uma comparação objetiva entre os diferentes níveis de adoção de práticas de segurança nas plataformas analisadas.

No que se refere aos vetores de ataque relacionados à implementação, observa-se que a maioria das plataformas utiliza mecanismos baseados em criptografia de curva elíptica, especialmente em protocolos modernos como TLS. Embora esses mecanismos ofereçam alto nível de segurança, estudos indicam que implementações baseadas em ECC podem ser mais suscetíveis a falhas decorrentes de erros de implementação, particularmente em algoritmos como ECDSA. Tais vulnerabilidades não estão necessariamente associadas a robustez teórica dos algoritmos, mas sim a forma como são implementados na prática [Nyangaresi et al. 2023]. Dessa forma, todas as plataformas analisadas estão potencialmente sujeitas a esse tipo de vetor, justificando a classificação adotada.

A análise comparativa indica que a maioria das plataformas apresenta alto nível de conformidade com práticas modernas de segurança, embora nenhuma atenda integralmente a todos os critérios. Plataformas como Steam, Epic Games, GOG Galaxy e EA App demonstram elevada aderência, enquanto a Battle.net apresenta menor conformidade. No geral, observam-se variações pontuais que refletem diferentes níveis de maturidade, sem comprometer significativamente a segurança das plataformas.

4.5. Relação entre análise e formulário

A partir dos resultados obtidos nas análises técnica e empírica, foi possível estabelecer uma relação direta entre os mecanismos de segurança implementados pelas plataformas e a ocorrência de incidentes reportados pelos usuários. De modo geral, a análise técnica evidenciou que as plataformas avaliadas apresentam um elevado nível de segurança, com a adoção de protocolos modernos, como o TLS 1.3, uso de *Forward Secrecy*, algoritmos criptográficos robustos e certificação por autoridades confiáveis. Esses elementos indicam que, do ponto de vista estrutural, as plataformas estão alinhadas com as boas práticas atuais de segurança da informação.

No entanto, os dados obtidos por meio do formulário revelaram um cenário aparentemente contraditório, no qual plataformas tecnicamente mais seguras, como a Steam, foram também as mais associadas a casos de contas invadidas. Esse resultado, à primeira vista, pode sugerir uma inconsistência entre a eficácia dos mecanismos de proteção e a segurança percebida pelos usuários. Por outro lado, os problemas de segurança da Steam podem não necessariamente estar relacionados a aspectos técnicos, mas sim associados a mecanismos de engenharia social que não puderam ser analisados neste estudo.

Contudo, essa aparente contradição pode ser explicada por fatores externos à infraestrutura técnica das plataformas. Um dos principais aspectos a ser considerado é o tamanho da base de usuários. Plataformas como a Steam possuem uma quantidade significativamente maior de usuários quando comparadas às demais analisadas, o que naturalmente aumenta a exposição a incidentes de segurança em termos absolutos. Dessa forma, um maior número de ocorrências não implica, necessariamente, menor nível de

segurança, mas pode refletir simplesmente a maior escala de utilização da plataforma.

Além disso, os resultados indicam que o fator humano desempenha um papel central na ocorrência de invasões de contas. Mesmo com a disponibilidade de mecanismos de segurança avançados, como autenticação em dois fatores e conexões criptografadas, práticas inadequadas por parte dos usuários, como uso de softwares ilícitos e suscetibilidade a ataques de engenharia social, continuam sendo vetores relevantes de comprometimento. Esse comportamento reforça a ideia de que a segurança não depende exclusivamente das tecnologias implementadas, mas também da forma como são utilizadas.

Dessa forma, a relação entre as análises evidencia que, embora as plataformas apresentem um alto nível de segurança técnica, a efetividade dessas medidas está diretamente condicionada ao comportamento dos usuários. Assim, os resultados apontam que os principais fatores associados às invasões de contas não estão relacionados a falhas estruturais das plataformas, mas sim à forma como os usuários interagem com os mecanismos de segurança disponíveis.

5. Conclusão e Trabalhos Futuros

O presente trabalho teve como objetivo analisar a segurança em plataformas digitais de venda de jogos, relacionando aspectos técnicos com a percepção dos usuários a partir de dados coletados por meio de formulário.

Os resultados obtidos indicam que, embora a maioria dos usuários declare possuir um nível intermediário de conhecimento em cibersegurança e utilize medidas adicionais de proteção, as invasões de contas ainda são recorrentes, atingindo uma parcela significativa dos respondentes. Esse cenário evidencia que o conhecimento declarado nem sempre se traduz em práticas seguras no uso cotidiano das plataformas.

A análise técnica demonstrou que, de modo geral, as plataformas avaliadas apresentam um bom nível de segurança, com adoção de protocolos modernos, mecanismos de criptografia robustos e práticas alinhadas ao estado da arte. Ainda assim, observou-se um aparente conflito entre a avaliação técnica e os dados empíricos, uma vez que a plataforma Steam, que apresentou os mecanismos de segurança mais completos entre as analisadas, foi também a mais citada em casos de contas invadidas.

Além disso, observou-se que uma parcela considerável dos usuários conseguiu recuperar suas contas, demonstrando a eficácia dos mecanismos de suporte e recuperação disponibilizados pelas plataformas. Ainda assim, a ocorrência frequente de invasões reforça a necessidade de maior conscientização por parte dos usuários quanto às boas práticas de segurança.

De acordo com os resultados, conclui-se que, apesar da evolução dos mecanismos técnicos de proteção, o fator humano continua sendo um dos principais elementos de vulnerabilidade. Dessa forma, ações voltadas à educação em cibersegurança e ao uso adequado das ferramentas de proteção são fundamentais para a redução dos riscos e para o fortalecimento da segurança nas plataformas digitais.

Como continuidade deste trabalho, destaca-se a possibilidade de ampliação da amostra utilizada no formulário, de modo a obter um conjunto de dados mais representativo. Um maior número de respostas poderia permitir análises mais aprofundadas e a identificação de padrões que não foram evidenciados neste estudo.

Além disso, algumas variáveis coletadas poderiam ser exploradas de forma mais detalhada. A questão relacionada ao ano em que ocorreu o incidente, por exemplo, não apresentou um padrão claro, possivelmente devido à quantidade limitada de respostas. Com uma base de dados mais ampla, seria possível investigar esse aspecto de forma mais consistente.

No que se refere à análise técnica, um ponto a ser aprimorado diz respeito à coleta de dados de rede. Durante a etapa de captura de pacotes utilizando o *Wireshark*, não houve uma padronização rigorosa no tempo de coleta para cada aplicação, o que pode ter influenciado métricas como o tamanho médio dos pacotes. Dessa forma, estudos futuros podem adotar um controle mais preciso desse processo, garantindo maior confiabilidade e comparabilidade entre os dados obtidos.

Por fim, ressalta-se que a metodologia aplicada neste trabalho não se limita ao contexto de plataformas digitais de venda de jogos. A abordagem utilizada pode ser adaptada e replicada em outros tipos de plataformas digitais, possibilitando a análise de segurança e comportamento do usuário em diferentes cenários, o que amplia o potencial de aplicação desta pesquisa.

6. Repositório de Dados

Os arquivos utilizados ao longo do desenvolvimento deste trabalho, incluindo capturas de rede obtidas com o *Wireshark* e a base de dados gerada a partir do formulário aplicado, foram organizados e disponibilizados em um repositório *online*. O acesso pode ser realizado por meio do seguinte link: `https://github.com/caiovsimoes/Arquivos-TCC.git`.

Referências

ARIN (2026). Whois/rdap search tool. American Registry for Internet Numbers. Acesso em: 16 março 2026.

Aviram, N., Schinzel, S., Somorovsky, J., Heninger, N., Dankel, M., Steube, J., Valenta, L., Adrian, D., Halderman, J. A., Dukhovni, V., et al. (2016). {DROWN}: breaking {TLS} using {SSLv2}. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 689–706.

Bhargavan, K., Langley, A., et al. (2017). The security of tls 1.3. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 325–340. IEEE.

Brasil (2012). Lei nº 12.737, de 30 de novembro de 2012. `https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm`. Dispõe sobre a tipificação criminal de delitos informáticos.

Campos, B. et al. (2024). A evolução da computação quântica: Impacto na criptografia rsa e a segurança nacional.

Chattopadhyay, S., Tiwari, M., Tiwari, T., Kapila, D., et al. (2023). Role of cyber security in gaming technology. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pages 446–451. IEEE.

Cheng, Y. et al. (2010). Security and privacy in massively multiplayer online games and virtual worlds. *University of Twente Research*.

DaCosta, B. and Seok, S. (2020). Cybercrime in online gaming. In *Encyclopedia of Criminal Activities and the Deep Web*, pages 881–892. IGI Global.

Dierks, T. and Rescorla, E. (2008). The transport layer security (tls) protocol version 1.2. Technical Report RFC 5246, IETF.

Geolocation (2026). Ip geolocation lookup. Acesso em: 15 maio 2026.

Kurose, J. F. and Ross, K. W. (2017). *Computer Networking: A Top-Down Approach*. Addison Wesley, 7 edition.

Lee, H., Kim, D., and Kwon, Y. (2021). Tls 1.3 in practice: How tls 1.3 contributes to the internet. In *Proceedings of the Web Conference 2021*, pages 70–79.

Lee, H. K., Malkin, T., and Nahum, E. (2007). Cryptographic strength of ssl/tls servers: Current and recent practices. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pages 83–92.

Lehdonvirta, V. (2008). *Real-money trade of virtual assets: new strategies for virtual world operators*. Icfai University Press.

Lyon, G. (2023). Nmap network scanning. Acesso em: 2026.

Nyangaresi, V. O., Jasim, H. M., Mutlaq, K. A.-A., Abduljabbar, Z. A., Ma, J., Abduljaleel, I. Q., and Honi, D. G. (2023). A symmetric key and elliptic curve cryptography-based protocol for message encryption in unmanned aerial vehicles. *Electronics*, 12(17):3688.

Parizi, R. M., Dehghantanha, A., Choo, K.-K. R., Hammoudeh, M., and Epiphaniou, G. (2019). Security in online games: Current implementations and challenges. In *Handbook of big data and IoT security*, pages 367–384. Springer.

Rescorla, E. (2018). The transport layer security (tls) protocol version 1.3. Technical Report RFC 8446, IETF.

Shen, C., Yu, T., Xu, H., Yang, G., and Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security*, 61:130–141.

SteamDB (2026). Steam & game stats. Acesso em: 29 de mai. 2026.

Suh, S. and Wagner, D. (2007). Security and privacy in online games. *IEEE Security & Privacy*, 5(4):11–15.

Szatmáry, K. S. (2024). Cybersecurity of the gaming industry. In *2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, pages 000441–000446. IEEE.

Wireshark Foundation (2024). Wireshark: Go deep. Acesso em: 5 março 2026.