UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS VII - PATOS
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

EMERSON RODRIGUES DOS SANTOS

LEVANTAMENTO SOBRE O NÍVEL DE CONHECIMENTO QUE ESTUDANTES DE COMPUTAÇÃO DA UEPB – CAMPUS VII TÊM SOBRE CIBERSEGURANÇA

PATOS - PB
2025

EMERSON RODRIGUES DOS SANTOS

LEVANTAMENTO SOBRE O NÍVEL DE CONHECIMENTO QUE ESTUDANTES DE COMPUTAÇÃO DA UEPB – CAMPUS VII TÊM SOBRE CIBERSEGURANÇA

Trabalho de Conclusão de Curso II apresentado ao curso de Bacharelado em Ciência da Computação do Centro de Ciências Exatas e Aplicadas da Universidade Estadual da Paraíba, como requisito para à obtenção do título de bacharel em Ciência da Computação.

Orientador: Vinicius Angustus Alves Gomes

PATOS - PB
2025

S237l Santos, Emerson Rodrigues dos.
Levantamento sobre o nível de conhecimento que estudantes de computação da UEPB – Campus VII têm sobre cibersegurança [manuscrito] / Emerson Rodrigues dos Santos. - 2025.
51 f. : il. color.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Ciência da computação) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas, 2025.

"Orientação : Prof. Grad. Vinícius Augustus Alves Gomes, Coordenação do Curso de Computação - CCEA".

1. Segurança da informação. 2. Cibersegurança. 3. Engenharia social. 4. Malware. I. Título

21. ed. CDD 005.8

Elaborada por Kaliane Eveny Martins de Oliveira - CRB - 15/986 BSC7

EMERSON RODRIGUES DOS SANTOS

LEVANTAMENTO SOBRE O NÍVEL DE CONHECIMENTO QUE ESTUDANTES DE COMPUTAÇÃO DA UEPB – CAMPUS VII TÊM SOBRE CIBERSEGURANÇA

Trabalho de Conclusão de Curso apresentado à Coordenação do Curso de Ciência da Computação da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Ciência da Computação

Aprovada em: 05/06/2025.

BANCA EXAMINADORA

Documento assinado eletronicamente por:

- **Rosangela de Araujo Medeiros** (***.723.558-**), em **14/06/2025 11:16:56** com chave **3a80e874492a11f0ac8b1a7cc27eb1f9**.
- **Vinícius Augustus Alves Gomes** (***.754.334-**), em **13/06/2025 16:32:22** com chave **2072aaa0488d11f0be7306adb0a3afce**.
- **Harllem Alves do Nascimento** (***.796.924-**), em **13/06/2025 19:31:00** com chave **14ee9d9248a611f0850206adb0a3afce**.

Documento emitido pelo SUAP. Para comprovar sua autenticidade, faça a leitura do QrCode ao lado ou acesse https://suap.uepb.edu.br/comum/autenticar_documento/ e informe os dados a seguir.
Tipo de Documento: Folha de Aprovação do Projeto Final
Data da Emissão: 16/06/2025
Código de Autenticação: 7b4737

Dedico este trabalho à minha família, em especial aos meus pais e irmãos, aos amigos que conquistei ao longo desta jornada, a todos os meus professores e a todos que me apoiaram de alguma forma. Este trabalho só foi possível graças ao apoio, incentivo e presença de cada um de vocês.

AGRADECIMENTOS

Aos meus pais, Solineide Rodrigues e Francisco Tito, agradeço pela dedicação incansável, amor incondicional e apoio constante em todos os momentos da minha vida. Vocês são minha base, mesmo diante dos maiores desafios. Tudo o que conquistei até aqui é, em grande parte, reflexo do que aprendi com vocês.

Ao meu orientador, professor Vinicius Augustus, sou profundamente grato pelo conhecimento transmitido com tanto zelo, paciência e entusiasmo ao longo da minha formação. Em especial, agradeço pela orientação dedicada durante a realização deste trabalho, que foi essencial para meu crescimento acadêmico e profissional. Cada conselho, sugestão e incentivo foi fundamental nesta trajetória — e sua paciência, especialmente, merece todo o meu reconhecimento.

A todos os professores que fizeram parte da minha formação, meu muito obrigado. Cada um contribuiu de forma significativa para minha trajetória acadêmica e pessoal, compartilhando conhecimento, incentivando a curiosidade e despertando em mim o desejo constante de aprender.De maneira especial, agradeço à professora Rosângela Medeiros. pela sua contribuição fundamental na minha vida academica.

Aos meus irmãos, Elezângela, Emanuel, Elaine e Edson, que sempre estiveram ao meu lado, oferecendo apoio, compreensão e palavras de incentivo nos momentos em que mais precisei, deixo meu carinho e gratidão.

E a todos que compartilharam comigo momentos de aprendizado, risos, conversas, dificuldades e superações ao longo desta jornada — em especial Harllem, Daniel, Elanio e Dayane — meu sincero agradecimento. Cada um de vocês fez parte desta caminhada de forma única e especial, contribuindo para que eu chegasse até aqui.

“Se é uma boa ideia, vá em frente e faça
porque é mais fácil pedir desculpas do que conseguir permissão"
Grace Hopper

RESUMO

O aumento de ataques cibernéticos, fraudes digitais, roubo de dados e exposição de informações sensíveis evidencia a necessidade de que profissionais da área de tecnologia da informação estejam preparados para lidar com esses riscos. Nesse contexto, este trabalho tem como objetivo investigar o nível de conhecimento dos alunos do curso de Ciência da Computação do Campus VII da Universidade Estadual da Paraíba (UEPB), localizado em Patos, sobre temas fundamentais relacionados à segurança da informação, como credenciais de acesso, práticas seguras na internet, engenharia social, malwares e medidas preventivas. A proposta se justifica pela importância de avaliar a formação desses futuros profissionais que estarão diretamente envolvidos no processo. Avaliar o conhecimento atual desses discentes permite identificar lacunas que podem comprometer a segurança das soluções que desenvolverão no futuro, além de subsidiar melhorias curriculares. A metodologia adotada para o desenvolvimento da pesquisa foi de caráter exploratório, com abordagem quali-quantitativa. A coleta de dados foi realizada por meio da aplicação de um questionário elaborado com perguntas objetivas e disponibilizado via Google Forms, permitindo maior alcance e participação dos alunos. Os dados coletados permitem identificar comportamentos e conhecimentos relacionados à segurança da informação. Os resultados demonstraram que, de modo geral, os alunos possuem conhecimento sobre os temas abordados. No entanto, observou-se uma deficiência no reconhecimento da engenharia social e também lacunas no conhecimento técnico relacionado ao funcionamento, identificação e remoção de malwares, bem como na utilização de ferramentas como firewalls. Conclui-se que, embora os estudantes demonstrem um bom nível de consciência em diversos aspectos da segurança da informação, ainda existem pontos que precisam ser reforçados, principalmente no que diz respeito à identificação de ameaças menos técnicas e mais comportamentais, como a engenharia social.

Palavras-chave: Segurança da informação; Cibersegurança; Engenharia social; Malware.

ABSTRACT

The rise in cyberattacks, digital fraud, data theft, and exposure of sensitive information highlights the need for Information Technology professionals to be prepared to deal with these risks. In this context, this work aims to investigate the level of knowledge among students of the Computer Science program at Campus VII of the State University of Paraíba (UEPB), located in Patos, regarding fundamental topics related to information security, such as access credentials, safe internet practices, social engineering, malware, and preventive measures. The proposal is justified by the importance of assessing the education of these future professionals who will be directly involved in the process. Evaluating the current knowledge of these students makes it possible to identify gaps that may compromise the security of the solutions they will develop in the future, in addition to supporting curricular improvements. The methodology adopted for the development of the research was exploratory in nature, with a qualitative and quantitative approach. Data collection was carried out through a questionnaire with objective questions, made available via Google Forms, allowing for broader reach and student participation. The collected data made it possible to identify behaviors and knowledge related to information security. The results showed that, in general, students have knowledge about the topics addressed. However, a deficiency was observed in the recognition of social engineering, as well as gaps in technical knowledge related to the functioning, identification, and removal of malware, and in the use of tools such as firewalls. It is concluded that although students demonstrate a good level of awareness in several aspects of information security, there are still areas that need to be strengthened, especially regarding the identification of less technical and more behavioral threats, such as social engineering.
Keywords: Information security; Cybersecurity; Social engineering; Malware; collected data.

LISTA DE GRÁFICOS

Gráfico 1 – Períodos letivos do respondentes 27
Gráfico 2 – Resposta às questões sobre gestão de senhas 28
Gráfico 3 – Resposas às questões sobre engenharia social 29
Gráfico 4 – Respostas às questões sobre conexões seguras 31
Gráfico 5 – Respostas às questões sobre malware 33
Gráfico 6 – Respostas às questões sobre boas práticas de segurança da informação . . . 35

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
DoS	Denial of Service (Negação de Serviço)
DDoS	Distributed Denial of Service (Negação de Serviço Distribuída)
TI	Tecnologia da Informação
UEPB	Universidade Estadual da Paraíba
VPN	Virtual Private Network

SUMÁRIO

Agradecimentos **4**

1 INTRODUÇÃO **12**
1.1 Contextualização do problema **12**
1.2 Objetivo **13**
1.2.1 Objetivo Geral ***13***
1.2.2 Objetivos Específicos ***13***
1.3 Questões de Pesquisa **14**
1.4 Estrutura do Trabalho **14**
1.5 Justificativa **14**

2 REFERENCIAL TEÓRICO **16**
2.1 Segurança da informação **16**
2.1.1 Proteção de informações ***17***
2.1.2 Segurança da informação ***17***
2.2 Ameaças **18**
2.2.1 Vírus ***19***
2.2.1.1 Ataques *20*
2.3 Riscos **20**
2.4 Vulnerabilidade **21**
2.4.1 Tipos de vulnerabilidade ***21***
2.5 Engenharia Social **21**
2.5.1 Táticas utilizadas ***22***
2.5.2 Características das vítimas ***23***
2.6 Mitigação **23**

3 METODOLOGIA **25**
3.1 A coleta de dados **25**
3.2 Tipologia da Pesquisa **25**
3.3 Coleta de Dados **25**
3.4 Universo Investigado **26**
3.5 Instrumento de coleta **26**
3.6 Análise de dados **26**

4 RESULTADOS E DISCUSSÕES **27**
4.1 Gestão de senhas **27**
4.2 Engenharia social **29**
4.3 Conexões **30**

4.4 Malware 32
4.5 Boas práticas 34

5 CONSIDERAÇÕES FINAIS 38

REFERÊNCIAS 40

Apêndice A – Instrumento de Pesquisa 43

1 INTRODUÇÃO

Nesta seção, apresenta-se uma visão geral desta pesquisa, de modo a descrever a contextualização do problema, objetivos e questões de pesquisas.

1.1 Contextualização do problema

A população brasileira tem enfrentado problemas com ameaças digitais. Portais de notícia divulgaram que, só no primeiro semestre de 2024, o número de ciberataques cresceu em 38, a exemplo do olhar digital (2024); nesse cenário é possível demonstrar a crescente preocupação com as ameaças à rede no país, pois a falta de conhecimento da população pode gerar problemas no âmbito pessoal e institucional.

Em adição, o relatório de revisão do *Cybersecurity Capacity Maturity Model for Nations Brazil* (Brasil, 2023) chama a atenção para a ausência de dados precisos sobre a conscientização dos usuários de internet, o que limita a criação de políticas públicas eficazes. Para avaliar o nível de maturidade em segurança digital, o relatório propõe cinco níveis, que vão desde o inicial até o dinâmico, sendo eles: inicial, formativo, estabelecido, estratégico e dinâmico. O conhecimento dos usuários foi definido como formativo, um nível baixo de conhecimento sobre ameaças.

Pode-se considerar uma ameaça qualquer evento que possa comprometer a confiabilidade, a integridade ou a disponibilidade de uma rede. ABNT (2001) Aborda a importância desses pilares. Pegando como exemplo um empresário dono de uma plataforma de entrega, que precisa garantir que seus clientes, sempre que necessitarem, tenham acesso à plataforma (disponibilidade); que as encomendas enviadas cheguem ao comprador final sem avarias e no prazo correto (confiabilidade) e; que os pacotes enviados não sejam abertos e tenham seu conteúdo inalterado (integridade). Nesse contexto, a rede pode ser considerada os caminhos utilizados para levar os pacotes ao seu destino.

Sendo assim, é preciso considerar que não apenas as redes, mas também os usuários estão expostos a diversos tipos de ameaças, como *phishing*, *vishing* e ancoragem, além de ataques que utilizam engenharia social. Essas táticas visam enganar as vítimas para que revelem informações pessoais ou financeiras.(Lobo, 2016) explicita que os atacantes evocam autoridade que não possuem para convencer as vítimas, por meio de *sites*, e-mails, mensagens e chamadas telefônicas.

Bem como as ameaças já citadas, os *malwares*, combinação das palavras em inglês "*malicious software*"e que significam códigos maliciosos, são mais um perigo ao usuário da internet Prado *et al* (2016)ressalta que esses programas subvertem o sistema operacional em benefício do atacante, entre eles programas como ransomware, *hijacker* e *keylogger* exploram as fragilidades dos sistemas para roubar, alterar ou apagar dados. Além disso, *malwares* como cavalo de Troia, *rootkit* e *backdoor* podem até mesmo criar novas vulnerabilidades. Por fim, os *hoaxes*, ou boatos digitais, disseminados por e-mail e redes sociais, visam gerar pânico e desinformação.resumo do E-book Cisco Networking Academy (2021)

Golpes bem-sucedidos podem resultar em perdas financeiras, pois os dados roubados permitem acesso a contas bancárias e cartões de crédito, possibilitando saques. Além disso, criminosos podem extorquir vítimas, ameaçando divulgar informações sensíveis ou bloqueando o acesso a dados, como no caso do *ransomware WannaCry* em 2017, que criptografou dados em escala global e exigiu pagamento para liberá-los como demostrado pela materia do olhar digital(2022).

Estudo divulgado pela eCampus News (2024) revelou que 64% das universidades sofreram ataques de ransomware em 2022, frente a 44% no ano anterior. A mesma pesquisa aponta que a combinação de *phishing*[1], ataques de negação de serviço (DDoS), malware e acesso não autorizado representa uma ameaça constante às operações acadêmicas.Nesse contexto, a Universidade Estadual da Paraíba (UEPB), como qualquer outra instituição de ensino superior que opera em ambiente digital, também está exposta a riscos significativos à segurança da informação. Ameaças como ataques de negação de serviço, interceptação de dados, disseminação de malware e vazamento de informações confidenciais — incluindo dados acadêmicos e pessoais de alunos e servidores — representam desafios reais. A crescente sofisticação dessas ameaças e a relevância dos dados para as atividades acadêmicas e administrativas tornam a segurança da informação uma preocupação central para a instituição.

1.2 Objetivo

Diante desse cenário, este estudo tem como objetivo avaliar o nível de conhecimento dos alunos da UEPB sobre segurança da informação. A pesquisa busca identificar as principais lacunas nesse conhecimento. Ao analisar o conhecimento dos alunos, este trabalho pretende contribuir para o desenvolvimento de estratégias mais eficazes de conscientização e treinamento em segurança da informação na UEPB.

1.2.1 Objetivo Geral

O objetivo principal desta pesquisa é investigar a relação entre o conhecimento dos alunos do curso de Ciência da Computação, localizado no Campus VII da Universidade Estadual da Paraíba, sobre segurança cibernética e os hábitos de segurança que eles adotam.

1.2.2 Objetivos Específicos

Para alcançar o objetivo principal deste trabalho, será necessário passar pelos seguintes objetivos específicos:

- Elaborar um questionário sobre os temas pesquisados, visando coletar dados sobre os conhecimentos e hábitos de segurança digital.

[1] Temas como *phishing* e *vishing* serão abordados e explicados com maior detalhamento na seção de Referencial Teórico.

- Desenvolvimento e montagem de um panorama contemplando as informações concebidas sobre os dados recolhidos.

1.3 Questões de Pesquisa

Para complementar a análise deste trabalho, foram levantadas as seguintes questões de pesquisa.

- **QP1**. Os alunos estão cientes e tomam os devidos cuidados com suas informações credenciais para acesso de serviços na rede?
- **QP2**. Os estudantes possuem conhecimento suficiente para identificar e se proteger de ataques de engenharia social?
- **QP3**. Os alunos adotam boas práticas ao se conectarem à redes e serviços digitais?
- **QP4**. Os estudantes sabem se proteger, reconhecer e lidar com problemas provindos de malwares?
- **QP5**. Os discentes sabem identificar as medidas preventivas de segurança para caso de uso indevido de seus dispositivos por terceiros?

1.4 Estrutura do Trabalho

Este trabalho apresenta seis seções e está organizado da seguinte maneira: na Seção 1, apresenta-se uma visão geral desta investigação com relação a contextualização do problema, objetivos e questões de pesquisa; na Seção 2, apresenta-se os temas e trabalhos relacionados à pesquisa; na Seção 3, apresenta-se a metodologia desta pesquisa; na Seção 4, analisa-se e discuti-se os resultados; na Seção 5, apresenta-se as considerações finais e sugestões para trabalhos futuros; e ao final, encontra-se as referências e os apêndices utilizados do decorrer desta pesquisa.

1.5 Justificativa

De acordo com matéria divulgada pelo portal Olhar Digital(2024), um estudo realizado pela *Check Point Research* apontou que os ataques cibernéticos aumentaram em 70% em 2024 no Brasil. No contexto geral da américa latina setor de Educação e Pesquisa tem se destacado como um dos principais alvos, devido à grande quantidade de informações sensíveis armazenadas e à fragilidade dos mecanismos de proteção utilizados por muitas instituições. Diante desse panorama, torna-se justificável compreender o nível de conscientização e os hábitos de segurança digital dos alunos do curso de Ciência da Computação campus VII, visto que esses estudantes são os futuros profissionais responsáveis por atuar em áreas onde possivelmente terão que enfrentar e prevenir essas ameaças em suas respectivas profissões. Santos e Sott (2016), Silva (2003), Freitas (2017) e Gabbay (2006). Quando listam as principais ameaças

a um sistema de informação apontam fatores como má gestão de senhas, desinformação, uso indevido da internet e, à engenharia social ,técnica que explora o comportamento humano para obter acesso a dados sensíveis. Nesse sentido, Lobo (2016) define a engenharia social como o uso estratégico do conhecimento sobre o comportamento humano para induzir uma pessoa a agir conforme a intenção do atacante. Portanto, esta pesquisa se justifica pela importância em identificar como os estudantes de Computação compreendem e aplicam conceitos básicos de cibersegurança, contribuindo para o fortalecimento de práticas mais seguras no ambiente acadêmico e, futuramente, no mercado de trabalho.

2 REFERENCIAL TEÓRICO

Nesta seção, será apresentado o referencial teórico da pesquisa. Os autores e estudos selecionados serviram como embasamento para a análise dos dados obtidos. Além disso, contribuíram para contextualizar o tema da cibersegurança, permitindo compreender os principais conceitos, ameaças e desafios relacionados ao comportamento digital dos estudantes

2.1 Segurança da informação

A informação, antes contida em livros e documentos, hoje tornou-se algo comum em nossas vidas digitais e analógicas. Seja em um simples post nas redes sociais ou em grandes bases de dados corporativas. Neste tópico, será explorada a natureza da informação e segurança de informação.

Por informação, entende-se como um conjunto de dados articulados entre si, que depois de organizados ou processados, produzem sentido ou significado sobre um assunto Santos e Sott(2016). Por tanto, um conjunto de dados por si só não configura informação, é preciso que eles estejam organizadas de formas lógicas para produzir sentido.

Em seus estudos, Laureano e Moraes (2005), explicam que nem todas as informações são cruciais ou essenciais a ponto de serem merecedoras de cuidados especiais. Já a importância de certas informações é tão grande que qualquer custo para garantir sua integridade será menor do que o prejuízo causado por sua perda.

Ainda sobre o estudo de Laureano e Moraes (2005), os autores classificam as informações em quatro tipos. A primeira é a pública, que são, por exemplo, informações gerais sobre a empresa, produtos e serviços que podem ser acessadas por qualquer pessoa, como informações de contato, horários de funcionamento e comunicados gerais.

Assim como a Interna, que são dados internos da empresa, como relatórios de desempenho, projetos em desenvolvimento, políticas internas e informações financeiras não estratégicas. A divulgação dessas informações pode prejudicar a competitividade da empresa.

Há também as informações confidenciais, que se referem a dados estratégicos, como planos de negócios, informações sobre clientes, fornecedores e parceiros, dados financeiros detalhados e informações sobre propriedade intelectual. O vazamento dessas informações pode causar prejuízos financeiros, perda de clientes e danos à reputação da empresa.

Por fim as informações secretas, são altamente confidenciais, como fórmulas de produtos, algoritmos, processos de fabricação e informações sobre segurança da informação. A divulgação dessas informações pode levar à perda de vantagem competitiva, sabotagem e danos irreparáveis à empresa.

2.1.1 Proteção de informações

Em um cenário globalizado e altamente competitivo, a informação é considerada por muitos o ativo mais valioso das empresas (Gabbay, 2006). Pelo grau de importância da informação é preciso protegê-la dos riscos a que está submetida. Segundo Machado *et al.* (2022), as empresas são vulneráveis a diversos tipos de incidentes de segurança da informação, que podem ocorrer por falhas internas, como ações de colaboradores ou políticas inadequadas, ou por ataques externos.

Outrossim Takeuchi (2023) explica que atitudes e comportamentos inadequados dos usuários podem aumentar significativamente o risco de incidentes de segurança, expondo sistemas e dados a ameaças externas. Usuários de informações desconhecem seu valor e podem colocar a si ou uma instituição numa condição vulnerável, principalmente, quando diante de um engenheiro social. (Lobo, 2016).

2.1.2 Segurança da informação

Segurança de informação pode ser compreendida como um conjunto de protocolos, práticas e estudos que visam garantir a proteção da informação no âmbito físico e digital. Segundo Santos e Sott (2016), a segurança da informação garante que todos os dados importantes estejam protegidos contra ameaças, tanto físicas quanto digitais.

Por sua vez a ABNT (2001) fala que a segurança da informação é construída sobre uma base sólida de controles, que incluem políticas de segurança, práticas operacionais, procedimentos de segurança, estruturas organizacionais e mecanismos de *software* todos trabalhando em conjunto para proteger os dados.

Sendo assim, Santos e Sott (2016) dividem a segurança da informação em dois tipos, segurança física e segurança lógica. A segurança física consiste em proteger os ativos físicos da organização, como equipamentos de armazenamento e infraestrutura, contra ameaças externas e internas, garantindo a confidencialidade e a integridade dos dados. Alguns exemplos: crachás, senhas, cartões magnéticos e trancas.Já a segurança lógica, tem como objetivo preservar a integridade e confidencialidade das informações, evitando alterações, divulgações não autorizadas e perdas.

Para Santos e Sott (2016, a segurança da informação visa proteger todos os dados contra qualquer tipo de ameaça. As ameaças não estão restritas ao espectro digital, mas também ao físico. A meta da segurança da informação é prevenir ou minimizar danos a *hardwares, softwares* e dados, provenientes de ações acidentais ou intencionais, desastres naturais e outras ameaças. (Gabbay, 2006).

A ABNT (2001) explica que a segurança da informação precisa preservar esses três critérios:

- Confidencialidade: Acesso restrito a informações sensíveis, apenas para pessoas autorizadas.

- Integridade: Manutenção da precisão e completude dos dados.
- Disponibilidade: Garantia de acesso contínuo aos dados por usuários autorizados.

Então, Laureano e Moraes (2005) explicam que para garantir que a informação seja segura o sistema administrativo precisa seguir critérios como o não repúdio que comunica que ao enviar uma mensagem o emissor ou o receptor pode dizer que não enviou ou que não recebeu tal mensagem. O mesmo ocorre com quem faz uma negociação e depois nega ter feito.

Ainda, a legalidade afirma que um sistema deve assegurar que a informação foi criada e utilizada de acordo com as leis e regulamentos aplicáveis. Já a autenticidade, consiste em garantir que a informação não foi alterada desde sua origem até o destino final.

Por sua vez privacidade, é o direito de um indivíduo controlar o acesso às suas informações pessoais, garantindo que somente ele possa visualizá-las, modificá-las e compartilhá-las. Para finalizar, a auditoria é o processo de rastrear todas as etapas de um processo ou negócio, identificando quem, onde e quando cada ação ocorreu.

2.2 Ameaças

Uma ameaça representa qualquer fator que possa causar danos, perda ou violação de seus dados e informações (Santos; Sott, 2016). Para sintetizar, uma ameaça é qualquer evento ou causa potencial que possa ter um impacto negativo em um sistema de informação. (Gabbay, 2006) , as ameaças são eventos ou condições que têm o potencial de violar a segurança dos sistemas, resultando em incidentes que podem causar danos significativos ao negócio

Santos e Sott (2016), Silva (2003), Freitas (2017) e Gabbay (2006) em seus estudos dividem as ameaças em dois tipos, internas e externas. Nesse primeiro grupo enquadram-se:

- **Vírus de computador**: Dispositivos de armazenamento portátil infectados podem comprometer o funcionamento dos computadores.
- **Incêndios**: A ocorrência de incêndios pode levar à perda de dados e danos à infraestrutura.
- **Erros humanos**: Funcionários mal treinados podem danificar equipamentos e causar perda de informações.
- **Fraca gestão de senhas**: Anotar senhas em papeis ou arquivos expõe as informações a riscos de vazamento
- **Descarte inadecuado de documentos**: O descarte incorrecto de documentos com informações confidenciais pode levar a vazamentos de dado
- **O uso indevido da internet por funcionários**: Como o acesso a sites pessoais e redes sociais, expõe a empresa a riscos de segurança e diminui a produtividade.

Quanto às ameaças externas, é preciso que haja vetores para ela acontecerem, logo fala-se sobre atacantes. Iniciando este tópico, então, é necessário diferenciar hacker e cracker, isso para definir que o cracker é a ameaça e não o hacker. (Almeida *et al*, 2011). Hackers não utilizam ferramentas contra a sociedade, pois seguem um código de ética. Crackers, por outro lado, são especialistas em informática que usam seus conhecimentos para fins maliciosos.

Em 2003, Silva listou os principais atacantes:

Cyberpunks Possuem mais experiência, são motivados por desafios e diversão, explorando sistemas e protocolos em busca de vulnerabilidades. Costumam ser os primeiros a identificar falhas em *softwares* e serviços.

Insiders Funcionários insatisfeitos que detêm acesso privilegiado aos sistemas de uma organização, tornando-se uma ameaça interna significativa, especialmente em termos de perdas financeiras.

Coders Desenvolvem ou divulgam técnicas de invasão, seja em palestras ou outros meios, contribuindo para a comunidade *hacker*, tanto para fins legítimos quanto maliciosos.

Script Kiddies São iniciantes que utilizam ferramentas prontas encontradas na internet para realizar ataques, sem necessariamente compreender o funcionamento técnico. Seus atos, embora inexperientes, contribuíram para a conscientização sobre a necessidade de políticas de segurança robustas nas organizações.

White hats Profissionais da segurança cibernética contratados por empresas para identificar e corrigir vulnerabilidades em seus sistemas.

Black hats Utilizam suas habilidades para fins maliciosos, como invadir sistemas, roubar dados confidenciais e causar danos.

Gray hats Situam-se entre os dois extremos. Podem explorar vulnerabilidades com a intenção de alertar os responsáveis ou, em outros casos, buscar ganhos financeiros não autorizados.

2.2.1 Vírus

Um vírus de computador se trata de um programa malicioso, ou seja, um *software* criado para causar danos a dados, informações e a sistemas computacionais (Santos; Sott, 2016). Vírus são programas maliciosos capazes de infectar sistemas e alterar arquivos, causando diversos danos.

Pontes (2014) lista os principais tipos de vírus, iniciando pelo Cavalo de Tróia (Trojan) que é um programa malicioso disfarçado que, ao ser executado, realiza ações prejudiciais ao sistema ou aos dados do usuário, como abrir portas para invasores, roubar informações ou instalar outros malwares.

Em seguida, o texto relata sobre *ransomware*, que se trata de um tipo de *malware* que criptografa os arquivos de um usuário, exigindo o pagamento de um resgate para a sua recuperação. Além de criptografar os dados, o *ransomware* pode bloquear o acesso ao sistema operacional. Adicionalmente, *spyware* categoriza um software malicioso que monitora as atividades de um usuário, coletando informações pessoais sem o seu consentimento. Essas informações podem ser utilizadas para fins como fraude, espionagem ou venda ilícita dessas informações.

Por fim, *worms* são vírus que se espalham sozinhos pela rede, infectando outros computadores. Essa ameaça não necessita ser executada para infectar um computador, sendo independente em sua ativação.

2.2.1.1 Ataques

Ataques cibernéticos são ações maliciosas que visam causar danos a sistemas e dados, e utilizam diversas técnicas para enganar e explorar seus alvos. Santos e Sott (2016) listam os mais comuns, iniciando pelo *phishing*, uma técnica que induz as vítimas a fornecer informações confidenciais através de e-mails ou sites falsos. Outras técnicas incluem o *sniffing*, que intercepta dados em movimento na rede, e o ataque do meio, que manipula a comunicação entre duas partes.

Ataques de negação de serviço (DoS e DDoS) sobrecarregam sistemas para torná-los indisponíveis, enquanto *backdoors* permitem o acesso secreto a sistemas e *botnets* controlam redes de computadores infectados para realizar ataques em larga escala. O *spoofing*, que consiste em se passar por alguém ou algo confiável, é uma técnica fundamental em muitos desses ataques.

2.3 Riscos

Risco, em segurança da informação, é a combinação da probabilidade de uma ameaça explorar uma vulnerabilidade e causar um impacto negativo em um ativo de informação. Segundo a ABNT (2005), risco é a combinação da probabilidade de um evento e de suas consequências.

Gusmão (2017) classifica risco em três tipos: risco inerente, risco de controle; e risco de detecção.Este primeiro fala sobre a probabilidade de erros ou irregularidades nas demonstrações financeiras, independentemente dos controles internos, por exemplo: Uma empresa de tecnologia que desenvolve *software* está sujeita a um alto risco inerente devido à natureza imaterial de seus produtos. Definir o valor de mercado de um software é complexa e sujeita a diversas incertezas, como mudanças tecnológicas, concorrência e obsolescência.

Já Risco de Controle é a probabilidade de que os controles internos falhem em prevenir ou detectar erros significativos.Para facilitar a compreensão, uma loja virtual que não possui um sistema de segurança robusto para proteger os dados dos clientes está sujeita a um alto risco de controle. A falta de controles adequados pode levar a vazamentos de informações confidenciais, como números de cartão de crédito, causando danos à reputação da empresa e prejuízos financeiros.Por último, Risco de Detecção se trata da probabilidade de que os

procedimentos de auditoria não identifiquem erros relevantes.

2.4 Vulnerabilidade

Uma vulnerabilidade trata-se de uma fraqueza ou falha em um sistema, aplicação, processo ou outro ativo que pode ser explorada por uma ameaça, resultando em um incidente de segurança ABNT(2005)

2.4.1 Tipos de vulnerabilidade

Lobo (2016) lista os tipos de vulnerabilidade, iniciando pela a vulnerabilidade mais básica, que reside no ambiente físico onde o servidor está localizado. Por exemplo, um servidor situado em um porão sem vigilância adequada, o equipamento fica exposto a riscos como incêndios e acesso não autorizado, colocando em perigo a integridade dos dados.

Avançando para a infraestrutura do servidor, percebe-se que o *hardware* utilizado também apresenta fragilidades. Discos rígidos antigos e uma fonte de alimentação desprotegida tornam o sistema vulnerável a falhas e danos causados por eventos externos.

Além do *hardware*, o *software* utilizado no servidor também apresenta lacunas de segurança. A ausência de atualizações e a configuração inadequada do banco de dados expõem o sistema a ataques e exploração de vulnerabilidades conhecidas.

Complementando as vulnerabilidades anteriores, a forma como os dados são armazenados e protegidos também merece atenção. O uso de fitas magnéticas para *backup*, aliado à falta de um plano de recuperação de desastres, aumenta o risco de perda permanente dos dados em caso de incidentes.

A comunicação de dados também é um ponto crítico. A rede Wi-Fi desprotegida e o uso de senhas fracas expõem a empresa a interceptações e acessos não autorizados.Por fim, o fator humano representa uma das maiores ameaças à segurança da informação.

A possibilidade de um funcionário insatisfeito vazar dados confidenciais demonstra a importância de implementar políticas de segurança e programas de conscientização para os colaboradores.

2.5 Engenharia Social

Engenharia social consiste em utilizar o conhecimento sobre o comportamento humano para induzir as pessoas a agir de determinada forma. Lobo (2016) define a engenharia social como a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo.

Segundo Pereira *et al.* (2021), baseados nos estudos de Lafrance (2004), os motivos que levam indivíduos a praticar engenharia social são diversos e complexos. A motivação financeira, como o desejo de obter lucros ilícitos através de fraudes ou venda de informações confidenciais, é a mais comum. No entanto, outros fatores também podem influenciar os atacantes, como a

curiosidade e o desafio de superar obstáculos técnicos, a busca por vantagens competitivas em um ambiente corporativo, a pressão social por reconhecimento e a adesão a ideologias políticas ou sociais.

Em casos mais raros, a motivação pode ser altruísta, com o objetivo de ajudar organizações a identificar e corrigir vulnerabilidades em seus sistemas. Embora menos frequente, essa motivação demonstra que a engenharia social pode ser utilizada tanto para fins maliciosos quanto para fins benéficos.

Sendo assim, Pereira *et al* (2021) lista os tipos de engenheiros em seu trabalho. O engenheiro casual é o indivíduo motivado pela curiosidade e pelo desafio de invadir sistemas, sem necessariamente possuir um alto nível de conhecimento técnico. Quanto ao político, costuma ser um ativista digital que utiliza suas habilidades técnicas para promover uma causa política.

Adicionalmente, o engenheiro criminoso gera ataques cibernéticos sofisticados, executados e organizados com o objetivo de obter ganhos financeiros. Por fim, o interno, que são funcionários ou terceiros autorizados, que exploram seu conhecimento dos sistemas da organização para cometer atos maliciosos.

2.5.1 Táticas utilizadas

Lobo (2016) discorre sobre as táticas utilizadas na engenharia social. Ela é usada por cibercriminosos para manipular pessoas e obter acesso a informações confidenciais. Uma das técnicas mais comuns é o *phishing*, onde o atacante envia e-mails ou mensagens falsas, se passando por entidades confiáveis, para induzir a vítima a clicar em *links* maliciosos ou fornecer dados pessoais.

Além do *phishing*, os atacantes também podem utilizar a técnica do disfarce, se passando por colegas de trabalho ou representantes de empresas conhecidas para obter informações confidenciais. Outra forma de obter informações é através da coleta de dados descartados de forma inadequada, como documentos ou dispositivos de armazenamento, que podem conter informações sensíveis.

A manipulação emocional também é uma ferramenta poderosa nas mãos dos cibercriminosos. Através do apelo sentimental, como a criação de um senso de urgência ou medo, os atacantes podem persuadir as vítimas a tomar decisões precipitadas e fornecer informações confidenciais.

Para aumentar a eficácia de suas ações, os atacantes podem utilizar técnicas de programação neurolinguística, que visam influenciar o comportamento e a percepção das pessoas, facilitando a manipulação. A engenharia social também se manifesta na internet, através da criação de sites e páginas falsas que imitam sites legítimos, com o objetivo de coletar dados pessoais e credenciais de acesso. Essa técnica, conhecida como engenharia social na internet, é uma das mais utilizadas por cibercriminosos.

2.5.2 Características das vítimas

Segundo Torres (2012) e Lobo (2016), as vítimas de ataques de engenharia social geralmente apresentam algumas características em comum:A vaidade e o ego podem tornar as pessoas mais suscetíveis a elogios e informações que as favoreçam, diminuindo sua capacidade de identificar manipulações. A autoconfiança excessiva pode levar à subestimação dos riscos e à exposição de informações confidenciais. A valorização da formação profissional pode fazer com que indivíduos busquem por informações e oportunidades de aprendizado, mesmo que isso as coloque em situações de vulnerabilidade.

O altruísmo e o desejo de ajudar são frequentemente explorados por atacantes, que se passam por pessoas necessitadas ou em situação de dificuldade para obter informações confidenciais. A busca por aprovação social pode levar as pessoas a confiar em estranhos e a compartilhar informações pessoais. A tendência de diluir a responsabilidade e atribuir a culpa a outros pode levar a decisões arriscadas, como clicar em links suspeitos ou fornecer informações confidenciais.

Por fim, a vulnerabilidade à persuasão é uma característica comum em muitas vítimas. Técnicas de persuasão, como o uso de linguagem emocional e a criação de um senso de urgência, podem ser utilizadas para manipular as pessoas e induzi-las a tomar ações que beneficiem o atacante.

2.6 Mitigação

Este tópico apresenta uma compilação das principais recomendações de segurança digital presentes nas cartilhas do Comitê Gestor da Internet no Brasil (Brasil, 2012) e da Companhia de Águas e Esgotos do Rio Grande do Norte (CODERN, 2021).

Inicialmente é necessário falar sobre *softwares* de Segurança, como, por exemplo, os antivírus que realizam varreduras regularmente para detectar e remover vírus, *malwares* e outras ameaças. Bem como firewall que monitora e controla o tráfego de dados, impedindo que *hackers* acessem seu dispositivo. Adicionalmente, existem outros *softwares* como *anti-spywares* e *anti-rootkits*, para uma proteção mais completa.

Para manter a segurança, bons hábitos podem ser seguidos pelo usuário, como o gerenciamento de contas, priorizando o uso de contas de usuário com privilégios limitados para tarefas diárias e reservando a conta de administrador apenas para operações que exigem permissões elevadas.

Quanto a manutenção de atualizações regulares no sistema operacional, nos aplicativos e nos drivers é fundamental para corrigir vulnerabilidades que poderiam ser exploradas. Além disso, a personalização das configurações de segurança do navegador, como o bloqueio de pop-ups e a desativação da execução automática de arquivos, contribui para a redução de riscos de infecções.

A navegação segura na internet envolve cuidados como a atenção a e-mails e mensagens,

evitando interagir com links ou anexos de remetentes desconhecidos e verificando o endereço de e-mail do remetente, com o apoio de filtros de *spam*.

Também é recomendado evitar acessar informações sensíveis em redes públicas de Wi-Fi. Bem como a proteção de senhas é igualmente importante, com a criação de combinações fortes e únicas para cada conta, o uso de gerenciadores de senhas para armazenamento seguro e a ativação da autenticação de dois fatores para reforçar a segurança.

3 METODOLOGIA

Esta seção descreve os procedimentos metodológicos adotados para a realização da pesquisa. São apresentados o tipo de abordagem utilizada, a definição dos instrumentos de coleta de dados e a caracterização da amostra.

3.1 A coleta de dados

A coleta de dados desta pesquisa foi realizada por meio da aplicação de questionários online, desenvolvidos com base nos objetivos do estudo e nas variáveis previamente definidas. A escolha deste instrumento está alinhada à natureza descritiva da investigação, permitindo a coleta sistemática e objetiva de informações relevantes ao tema Wazlawick (2021)

3.2 Tipologia da Pesquisa

Conforme proposto por Wazlawick (2021), esta investigação pode ser especificada como um estudo primário de caráter descritivo, pois procura registrar de maneira objetiva percepções e dados obtidos diretamente do contexto analisado. A coleta de dados visa retratar experiências e comportamentos relevantes à problemática abordada. Para melhor caracterizar Yin (2010), o método de estudo de caso é apropriado quando se deseja compreender um fenômeno em seu ambiente real, especialmente quando se deseja analisar relações complexas e múltiplas variáveis. Nesta pesquisa, o estudo de caso único foi adotado como técnica de investigação, permitindo observar em específico o campus VII da UEPB. Essa abordagem qualitativa permite uma compreensão mais contextualizada do problema investigado.

Organizada com base em um referencial teórico estruturado, a metodologia orienta todas as etapas de coleta e análise de dados. Além de fundamentar o presente trabalho, também serve como base para pesquisas futuras que pretendam explorar o tema da cibersegurança no ambiente acadêmico, especialmente no contexto de instituições públicas de ensino superior. Assim, a pesquisa segue os princípios dos métodos qualitativos destacados por Yin (2010), alinhando observação sistemática, descrição detalhada e análise interpretativa

3.3 Coleta de Dados

A coleta de dados desta pesquisa foi realizada por meio da aplicação de questionários online, desenvolvidos com base nos objetivos do estudo e nas variáveis previamente definidas. A escolha deste instrumento está alinhada à natureza descritiva da investigação, permitindo a coleta sistemática e objetiva de informações relevantes ao tema Wazlawick (2021).

3.4 Universo Investigado

A pesquisa foi direcionada aos alunos regularmente matriculados no curso de Ciência da Computação da Universidade Estadual da Paraíba (UEPB), Campus VII, a partir do segundo período letivo. A escolha desse recorte considerou que esses discentes, a partir desse ponto do curso, já tiveram contato prévio com conceitos de segurança da informação, especialmente por meio da disciplina de Introdução à Computação UEPB (2024), ofertada no primeiro período. Por esse motivo, considerou-se que esses estudantes estariam mais preparados e capacitados para compreender o conteúdo abordado no questionário e fornecer respostas mais alinhadas com os objetivos da pesquisa.

3.5 Instrumento de coleta

O instrumento de coleta deste trabalho foi um questionário, que foi disponibilizado na plataforma *Google Forms*, permanecendo aberto para respostas durante um período de duas semanas, com o objetivo foi facilitar o acesso remoto e ampliar o alcance da pesquisa entre os estudantes. O *link* para o formulário foi amplamente divulgado por diferentes canais, como grupos de representantes de turma, grupos institucionais da coordenação do curso de Ciência da Computação e também por meio de abordagens diretas aos discentes.

O instrumento foi composto por 26 perguntas objetivas, distribuídas em cinco áreas temáticas: gestão de senhas, conexão segura, *malwares*, engenharia social e boas práticas de segurança da informação. utilizando da escala Likert de cinco pontos, organizadas com a intenção de coletar dados qualitativos relacionados ao conhecimento e às práticas de cibersegurança por parte dos alunos. Esse processo de coleta visou construir um panorama realista sobre o comportamento e o nível de conscientização dos estudantes quanto à segurança da informação no contexto acadêmico.

A fins de consulta, o apêndice 5 apresenta o instrumento de pesquisa e suas questões.

3.6 Análise de dados

A partir da análise estatística dos dados coletados, buscou-se identificar o nível de conhecimento dos alunos do curso de Ciência da Computação sobre conceitos básicos de segurança da informação. Também procurou avaliar a percepção dos discentes em relação aos riscos cibernéticos e seus hábitos de segurança online. Ao relacionar esses dados, foi possível inferir as principais lacunas de conhecimento dos participantes, bem como os fatores que influenciam a adoção de práticas seguras. Com base nos resultados obtidos, espera-se contribuir para a melhoria da segurança cibernética no contexto institucional.

4 RESULTADOS E DISCUSSÕES

Nesta seção serão apresentados os resultados obtidos através da aplicação do questionário elaborado. Com base nestes resultados, serão inferidas as discussões que eles levantam quanto às práticas de segurança dos avaliados.

A primeira pergunta da pesquisa buscava saber de qual período os participantes estavam cursando. Dito isso, a maioria dos 101 respondentes estavam participando do 7º período, representando 34,7% do total, seguido do 2º período, com 12,9%. Contudo houve participação relevante de todos os períodos, incluído alunos que já passaram do número de períodos estimado para a duração do curso. Vide o gráfico a seguir (Gráfico 1).

Gráfico 1 – Períodos letivos do respondentes

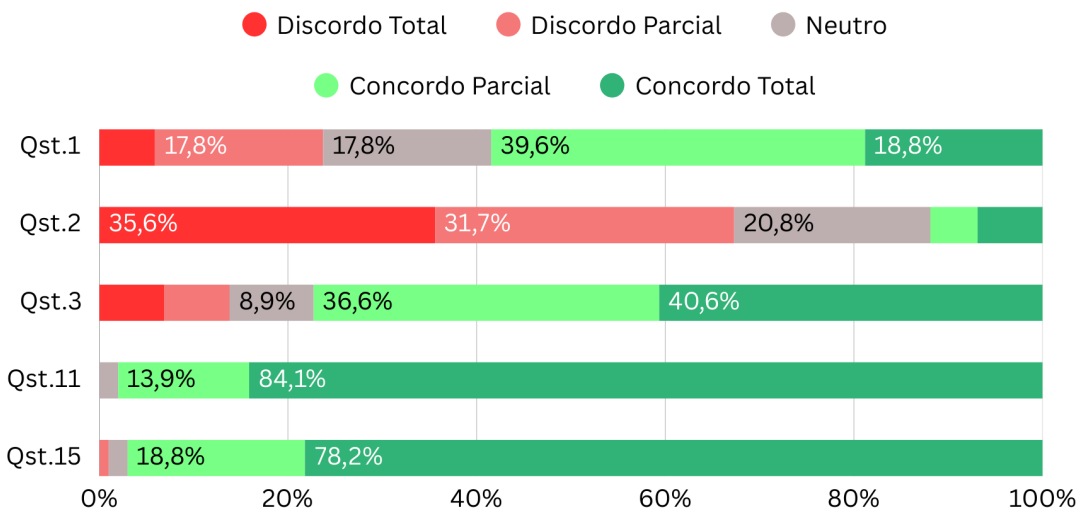
Fonte: Elaborado pelo autor (2025).

Observando o conteúdo visado em cada questão, foram divididas 5 subseções que abordam temas em comum. Vide a seguir.

4.1 Gestão de senhas

Inicialmente foram observados os comportamentos dos alunos quanto a sua gestão e segurança de senhas. O gráfico abaixo mostra as questões e resultados que abordam este tema.

Gráfico 2 – Resposta às questões sobre gestão de senhas



Fonte: Elaborado pelo autor (2025).

Na primeira questão sobre o tema 58,4% dos participantes concordaram total ou parcialmente sobre a importância de sempre utilizar senhas fortes e únicas para cada uma de suas contas em serviços online. Contudo na segunda questão, que perguntava se os participantes alteravam as senhas regularmente mesmo quando não solicitados, 67,4% discordavam total ou parcialmente com essa afirmação. Isto indica que apesar de saberem a importância de aplicarem senhas fortes, não consideram importante alterá-las periodicamente.

Adicionalmente, foi perguntado para os participantes se estes entendem os riscos do uso de senhas fracas e repetidas. 98,1% concordaram com a afirmação. Quanto ao serem questionados sobre a utilização da autenticação em dois fatores (2FA), 77,2% relataram concordar total ou parcialmente, denotando alta adesão à prática. Isso mostra que aliado ao conhecimento da fragilidade de senhas, os respondentes também fazem uso ou tem conhecimento da funcionalidade de segurança de 2FA, quando disponível, aumentando a resiliência de suas credenciais.

Por fim, a última pergunta deste tema, questiona se os discentes entendem os perigos do compartilhamento de dispositivos ou credenciais de acesso com outras pessoas. Obteve-se que 97% dos respondentes concordam que entendem os riscos deste compartilhamento.

Com o que foi observado, percebe-se que a maioria dos participantes entendem os riscos associados à má gestão de senhas. Porém, mesmo com este conhecimento, ainda há espaço para aplicação deste conhecimento, tornando-o prática. Pode ser somado a isso que, de acordo com o (2012) as senhas são amplamente utilizadas como mecanismo de autenticação por sua simplicidade, sendo fundamentais para garantir que o acesso a um recurso digital seja feito por um usuário autorizado.Uma má gestão de senha pode permitir que usuários não autorizados acessem dados ou programas, permitindo que causem vazamento de dados sensíveis ou ataques

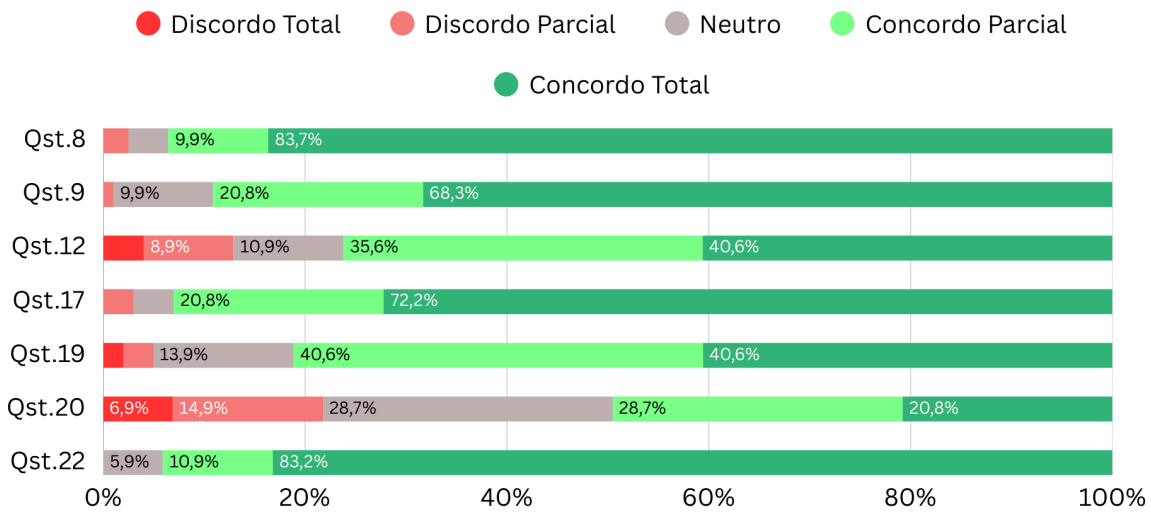
a pessoas e organizações.

Segundo (Santos; Sott, 2016), uma ameaça pode ser entendida como qualquer fator capaz de causar danos, perdas ou violação de dados e informações. Nesse sentido,Lobo (2016), ao listar os principais riscos no contexto empresarial, destaca que o uso de redes Wi-Fi desprotegidas e de senhas fracas expõe os sistemas a interceptações e acessos não autorizados. Embora seu enfoque seja o ambiente corporativo, esses riscos são igualmente relevantes no âmbito pessoal, visto que os mesmos comportamentos inseguros podem comprometer a privacidade e a segurança.

4.2 Engenharia social

A segunda subseção da pesquisa teve como foco o tema engenharia social. As questões abordaram tanto o nível de conhecimento dos participantes sobre o tema, quanto o seu comportamento no dia a dia. O gráfico a seguir apresenta as perguntas aplicadas e os resultados obtidos.

Gráfico 3 – Resposas às questões sobre engenharia social



Fonte: Elaborado pelo autor (2025).

A questão 8 ocupou-se em saber se os respondentes possuíam o hábito de evitar compartilhar informações pessoais em redes sociais. Dos participantes, 87,1% concordam, indicando não disporem do costume de compartilhar essas informações. Já a questão 9 investigou o nível de desconfiança dos participantes quanto ao recebimento de *links* ou anexos por e-mail, mesmo quando aparentam ser legítimos. Nesse caso, 89,1% dos participantes demonstraram cautela no uso do correio eletrônico.

A questão 12 investigou se os respondentes possuíam conhecimento para identificar possíveis tentativas de *phishing* em e-mails ou mensagens. Os resultados foram: 76,2% concordaram

total ou parcialmente, enquanto 10,9% permaneceram neutros. Um indicativo que a maioria acredita ter conhecimento para evitar prováveis atividade fraudulentas. Por sua vez, a questão 17 avaliou o grau de consciência dos estudantes quanto aos riscos de vazamento de dados em serviços *online*. A grande maioria, 93,1% dos discentes, demonstrou ter conhecimento sobre o tema.

A questão 19 teve como objetivo questionar se os estudantes são capazes de identificar e evitar sites falsos (*fake websites*). Os resultados mostraram que 81,2% dos participantes concordaram total ou parcialmente, enquanto 13,9% ficaram neutros. Isso demonstra que apesar da grande maioria afirmar sentir segurança sobre o tema, uma parte importante apresenta dúvidas sobre a temática. Em seguida, a questão 22 verificou se os alunos buscavam evitar clicar em *pop-ups* ou anúncios suspeitos durante a navegação na internet. Nesse caso, 94,1% dos respondentes afirmaram possuir esse hábito.

Por fim, a questão 20 buscou saber se os estudantes estão cientes dos riscos associados à engenharia social e sabem como se proteger contra esse tipo de ameaça. Os resultados revelaram uma divisão entre os respondentes: 49,5% concordaram total ou parcialmente, 28,7% ficaram neutros, e 21% discordaram total ou parcialmente. Apesar de a maioria demonstrar conhecimento sobre o tema, os resultados também evidenciam que uma parcela relevante dos estudantes apresentam insegurança ou acreditam possuir pouca ou nenhuma informação quanto aos riscos e formas de prevenção relacionados à engenharia social.

Conclui-se, então, que, nas questões não explicitamente relacionadas à engenharia social, a maioria dos discentes demonstraram ter conhecimento sobre práticas de segurança, como: evitar o compartilhamento de informações pessoais em redes sociais; desconfiar de e-mails com *links* ou anexos; além de identificar sites falsos e *pop-ups*. Contudo, na questão 20, foi percebido uma divisão significativa entre os participantes quanto ao entendimento sobre os riscos da engenharia social e sobre como se proteger contra essas ameaças. Esse contraste sugere que, embora os alunos tenham conhecimento sobre comportamentos de segurança de forma isolada, muitos deles não associam essas ações e conhecimentos à engenharia social, indicando um lapso na compreensão geral do tema.

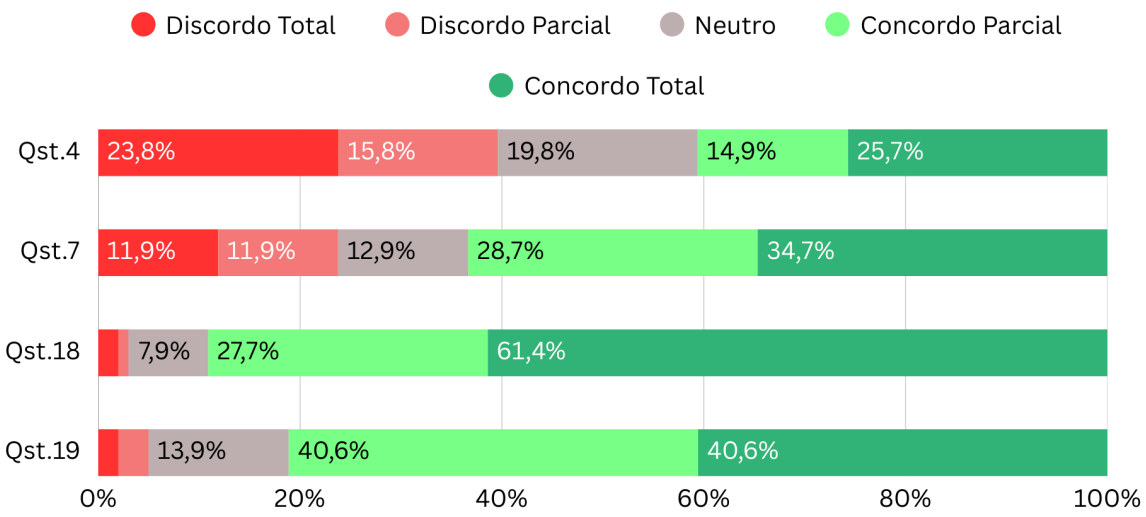
A existência desse lapso pode representar um risco. De acordo com Santos (2016), todos os níveis hierárquicos dentro de uma organização podem ser alvos de ataques de engenharia social, desde recepcionistas e funcionários operacionais até cargos de gerência e diretoria, uma vez que qualquer colaborador pode ser induzido a agir, ainda que de forma não intencional, em benefício do atacante. Fazendo um paralelo com a pesquisa, uma pessoa que não possui conhecimento sólido sobre engenharia social, pode ser um alvo fácil de manipulação, podendo fornecer informações pessoais ou empresariais.

4.3 Conexões

A terceira subseção abordou o tema conexões, englobando temas relacionados ao uso de redes *Wi-Fi* e acesso a *sites*. O gráfico a seguir apresenta as questões aplicadas e os resultados

obtidos.

Gráfico 4 – Respostas às questões sobre conexões seguras



Fonte: Elaborado pelo autor (2025).

A questão 4 verificou se os estudantes evitam se conectar a redes *Wi-Fi* públicas sem o uso de um VPN e os resultados obtidos foram: 40,6% concordaram total ou parcialmente; enquanto 19,8% ficaram neutros; e 39,5% discordaram total ou parcialmente. Esses dados demonstram uma divisão entre os respondentes, um indício que uma parte expressiva dos estudantes ainda não adota essas medidas de proteção ao utilizar redes públicas.

Ainda no tema, a questão 7 analisou se os estudantes verificam se os sites acessados por eles possuem conexão segura (HTTPS). Nesse item, 63,4% concordaram com a afirmação, 12,9% permaneceram neutros e 23,8% discordaram. Assim como na questão anterior, foi percebido uma divisão, o que pode indicar que nem todos os estudantes observam se os sites que os mesmo utilizam, atendem a esse critério de segurança durante a navegação na internet.

Por sua vez, a questão 18 apurou se os discentes entendem os riscos de usar dispositivos USB desconhecidos ou não confiáveis. Destes, 89,1% afirmaram positivamente, demonstrando que tomam tal cuidado. Finalizando as questões desse tema a questão 19, que indagou se os respondentes sabiam como identificar e evitar sites falsos (*fake websites*). Um total de 81,2% concordaram e 13,9% ficaram neutros. Os resultados sugerem que a maioria acredita ter capacidade de reconhecer *sites*fraudulentos, embora ainda exista uma pequena parcela de insegurança.

Ao analisar os resultados, observa-se que a grande maioria dos participantes demonstra compreender os riscos associados ao uso de dispositivos USB sem as devidas precauções. Ao mesmo tempo, quando o tema aborda conexão com *sites*, mesmo que a maioria dos respondentes

afirme ter conhecimento para identificar sites falsos, nota-se uma divisão em relação a práticas como verificar se a conexão é segura (HTTPS) e utilização de VPN. Essa falta de atenção a detalhes técnicos pode indicar que, apesar da confiança demonstrada pelos participantes, eles podem expor seus dispositivos a riscos, uma vez que não adotam as medidas de segurança recomendadas para a navegação e conexão segura na internet.

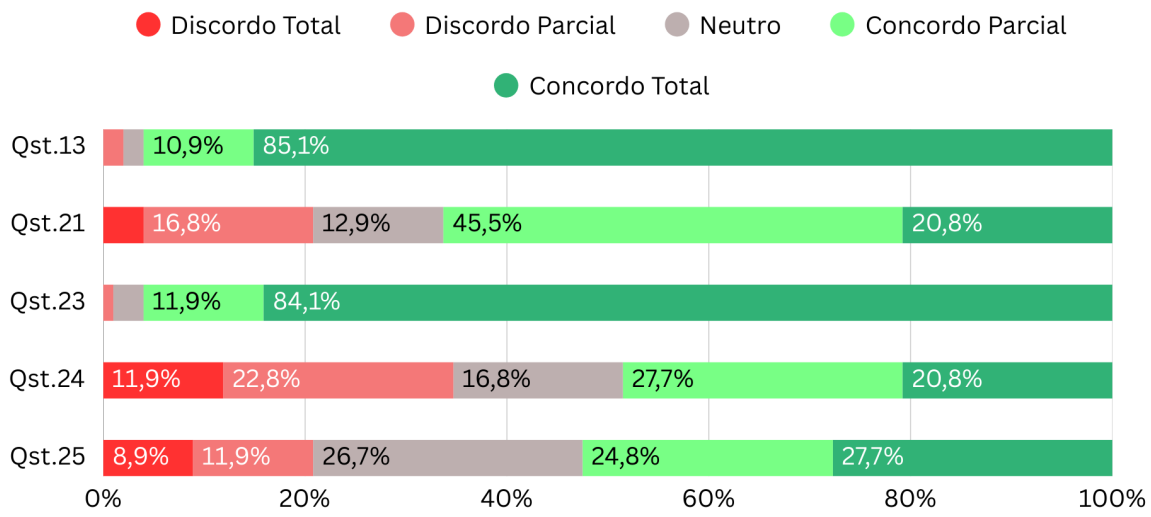
Sendo assim, não adotar cuidados básicos, como verificar se a conexão utiliza o protocolo HTTPS, pode facilitar a interceptação de dados, resultando no roubo de senhas e outras informações sensíveis. O CERT.br(2012) explica que o protocolo HTTP não oferece criptografia, tampouco garante a proteção dos dados contra interceptações, modificações ou retransmissões indevidas. Além disso, não assegura a identidade do *site* acessado, o que o torna inadequado para transmissões que envolvam informações sigilosas, como senhas, dados bancários e números de cartão de crédito. Nesses casos, é recomendado o uso do protocolo HTTPS, que proporciona conexões seguras.

Quando os autores Santos e Sott (2016), Silva (2003), Freitas (2017) e Gabbay (2006) dividem as ameaças em dois tipos — internas e externas —, eles destacam, entre as ameaças internas, exemplos como vírus de computador, disseminados por meio de dispositivos de armazenamento portátil, e o uso indevido da internet por funcionários, como o acesso a sites e redes sociais que expõem a empresa a riscos de segurança. Apesar de os autores focarem em um ambiente empresarial, esse cenário é facilmente aplicável ao âmbito pessoal. Para exemplificar as ameaças, Pontes (2014) cita os principais tipos de vírus em seu estudo. Entre eles, destaca-se um que merece atenção especial neste tópico: os worms, que são vírus capazes de se espalhar sozinhos pela rede, infectando outros computadores sem a necessidade de serem executados pelo usuário. Essa ameaça atua de forma independente, tornando-se altamente perigosa. Ainda é possível destacar que Santos e Sott (2016) listam os ataques mais comuns, iniciando pelo phishing, técnica que induz as vítimas a fornecer informações confidenciais por meio de e-mails ou sites falsos, sendo uma das ameaças mais frequentes no ambiente digital atual.

4.4 Malware

A quarta subseção dos resultados aborda o tema *malware*, com o objetivo de verificar se os participantes têm consciência dos riscos associados, são capazes de identificar possíveis sinais de infecção e adotam medidas preventivas. O gráfico a seguir apresenta as questões aplicadas e os resultados obtidos.

Gráfico 5 – Respostas às questões sobre malware



Fonte: Elaborado pelo autor(2025).

A questão 13 investigou se os participantes tinham conhecimento sobre os riscos de instalar *softwares* provenientes de fontes não confiáveis. A maioria, 96% dos respondentes, concordaram, indicando que a maioria está ciente dos perigos associados a essa prática. Desta feita, a questão 21 apurou se os participantes sabiam identificar sinais de infecção por *malware* em seus dispositivos. Os resultados mostraram uma divisão: 20,8% concordaram totalmente, mas dá-se destaque para o número de respostas "concordo parcialmente", com 45,5% das respostas. Além disso, 12,9% neutros e 20,8% discordando da afirmação. Essa segmentação sugere um nível de insegurança por parte dos participantes quanto ao reconhecimento de possíveis sinais de infecção.

Na questão 23, buscou-se apurar se os respondentes compreendem a importância de não executar arquivos desconhecidos baixados da internet. Um total de 96,1% apoiou a afirmação, ratificando a adoção desse comportamento. Em seguida, a questão 24 investigou se os discentes sabiam como remover *malware* de um dispositivo infectado. Os resultados foram os seguintes: 48,5% concordaram total ou parcialmente com a afirmativa; 16,8% permaneceram neutros; e 24,8% discordaram total ou parcialmente. Neste tópico, novamente, a opção "concordo totalmente" teve menor adesão que o "concordo parcialmente", o que identifica insegurança ou falta de conhecimento por parte dos participantes sobre as *formas* de remover infecções causadas por programas maliciosos.

Por fim, a questão 25 inquiriu se os respondentes utilizavam firewalls como forma de proteção em redes domésticas ou corporativas. Os resultados mostraram que 52,5% concordaram com a afirmativa, 26,7% permaneceram neutros, e 20,8% discordaram. Essa segmentação sugere que, em sua maioria, essa prática não está consolidada ou não há conhecimento aprofundado

sobre o uso e configuração de *firewalls* por parte dos participantes.

As informações apresentadas neste tópico demonstram que a maioria dos respondentes possui conhecimento sobre os riscos associados a malwares e reconhece a importância de não executar arquivos provenientes de fontes inseguras. No entanto, observa-se um declínio progressivo na confiança ou no conhecimento dos discentes à medida que os temas foram se tornando mais técnicos, como a identificação de possíveis infecções, a remoção de *malwares* e a utilização de *firewalls*. Esses resultados evidenciam uma lacuna no conhecimento, especialmente no que diz respeito às ações a serem tomadas após a infecção dos dispositivos.

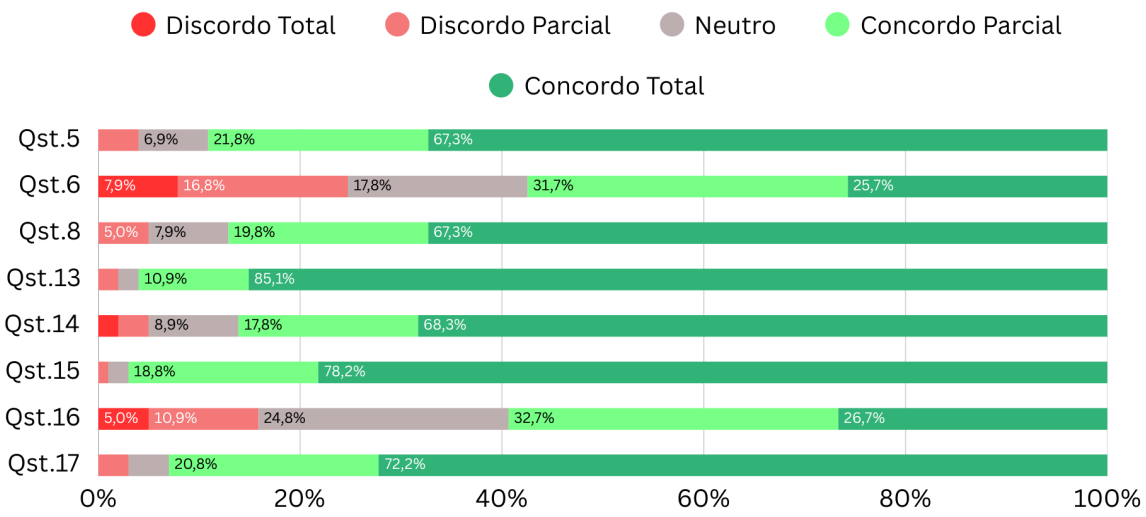
Consequentemente, não identificar ou remover *malwares* permite que o dispositivo seja invadido por programas como o cavalo de troia (*Trojan*). Um *trojan*, segundo o CERT.br 2023b, é um programa que, além de executar as funções aparentes para as quais foi criado, também realiza atividades maliciosas sem o conhecimento do usuário, podendo comprometer a segurança do sistema. Quando presente em um computador, o *trojan* pode abrir espaço para outros tipos de ameaças. Um exemplo é o *backdoor*, que, conforme explica o CERT.br2012, é um tipo de programa que permite o retorno de um invasor a um computador já comprometido, geralmente por meio da modificação ou criação de serviços específicos para manter o acesso ao sistema.

Pontes (2014) cita diversos tipos de vírus e os problemas causados por eles. Entre os que merecem destaque, está o spyware, um software malicioso que monitora as atividades do usuário e coleta informações pessoais sem seu consentimento. Outro exemplo relevante é o ransomware, que consiste em um tipo de malware capaz de criptografar os arquivos do usuário, exigindo o pagamento de um resgate para sua liberação. Quando Santos e Sott (2016) tratam dos ataques virtuais, mencionam que alguns deles utilizam máquinas previamente infectadas para realizar ações em massa. Um exemplo são os ataques de negação de serviço (DoS e DDoS), que visam sobrecarregar sistemas e torná-los indisponíveis. Além disso, destacam os backdoors, que permitem acessos secretos e não autorizados aos sistemas, e as botnets, que consistem em redes de computadores infectados e controlados remotamente para executar ataques em larga escala.

4.5 Boas práticas

A quinta e última subseção trata dos cuidados relacionados à segurança digital, abrangendo desde a atualização de sistemas operacionais e o compartilhamento de dados pessoais em redes sociais, até os cuidados em casos de perda ou roubo de dispositivos. O gráfico a seguir apresenta as questões aplicadas e os resultados obtidos nesta categoria.

Gráfico 6 – Respostas às questões sobre boas práticas de segurança da informação



Fonte: Elaborado pelo autor (2025).

A questão 5, averiguou se os participantes mantêm seus sistemas operacionais e aplicativos sempre atualizados. O resultado foi que 89,1% dos respondentes concordaram, indicando que essa prática está consolidada entre os alunos. Em adição, a questão 6 abordou o tema *backup*, questionando se os respondentes têm o hábito de realizar uma cópia de segurança de seus arquivos regularmente. Os dados mostram que 57,4% concordaram, 17,8% permaneceram neutros e 24,7% discordaram. Apesar da maioria concordar com a prática, ainda é possível observar um percentual de respondentes que discordam ou se mostram indiferentes, o que sugere que a realização de *backups* não é amplamente adotada.

Dando continuidade, a questão 8 inquiriu se os discentes evitaram o compartilhamento de dados pessoais em redes sociais. Os resultados mostraram que 83,1% confirmaram essa prática, demonstrando que esse cuidado é comum entre os participantes. Na sequência, a questão 13 examinou se os respondentes estão cientes dos riscos associados à instalação de *softwares* provenientes de fontes não confiáveis. O resultado foi que 96% concordaram com a afirmativa, evidenciando que esse conhecimento está bem difundido entre os alunos.

Ainda dentro do tema, a questão 14 analisou se os participantes reconhecem a importância de *criptografar* dados sensíveis. O resultado mostrou que 86,1% responderam positivamente, atestando que, em sua maioria, os alunos compreendem a relevância dessa prática de segurança. Em seguida, a questão 15 pesquisou se os respondentes entendem os perigos de compartilhar dispositivos ou credenciais de acesso com outras pessoas. Observou-se que 97% concordaram com a afirmativa, um claro indicativo de que os discentes possuem bom nível de consciência sobre os riscos envolvidos.

Por fim, a questão 16 debruçou se sobre o tema perda e roubo de dispositivos, questio-

nando se os universitários sabiam como se proteger nessas situações. Dos respondentes, 59,4% concordaram total ou parcialmente, 24,8% permaneceram neutros, e 15,9% discordaram total ou parcialmente. Esses dados evidenciam que, embora a maioria tenha algum conhecimento sobre o tema, ainda há espaço para que esse conhecimento se torne mais amplo. Logo em seguida, a questão 17 investigou se os participantes têm conhecimento sobre possíveis vazamentos de dados em serviços *on-line*. O resultado foi o seguinte: 93,1% afirmaram estar cientes, o que permite concluir que esse tipo de conhecimento está bem estabelecido entre os respondentes.

Nesta subseção, foi possível observar que a maioria dos respondentes demonstrou ter conhecimento amplo em diversos aspectos relacionados à segurança digital, como a manutenção de sistemas operacionais atualizados, o não compartilhamento de dados pessoais em redes sociais, a evitação da instalação de *softwares* de fontes não confiáveis, a importância da criptografia de dados sensíveis, os riscos do compartilhamento de dispositivos e credenciais de acesso e o conhecimento sobre possíveis vazamentos de dados em serviços on-line. Em todas essas questões, a maioria expressiva dos participantes confirmou estar ciente dos cuidados necessários e de colocá-los em prática .

No entanto, nas questões 6 e 16, que abordaram, respectivamente, a realização de *backups* e os cuidados frente à perda ou roubo de dispositivos, apesar de a maioria também ter indicado conhecimento, essa maioria não foi absoluta, o que aponta para uma lacuna a ser trabalhada no que diz respeito à adoção e consolidação dessas práticas específicas.

Sobre a utilização de backup, o CERT.br(2023b) explicita que a perda de dados pode ocorrer por diversos motivos, como acidentes, falhas no sistema, furtos, atualizações mal sucedidas ou defeitos físicos no dispositivo. Manter cópias de segurança é essencial para minimizar os impactos e facilitar a recuperação dessas informações. A perda desses dados pode acarretar prejuízos pessoais, financeiros e empresariais, sendo, portanto, fundamental tanto o conhecimento quanto a prática regular da realização de **backups**.

Quanto ao tema roubo ou perda de dispositivos, outro fascículo do CERT.br (2023a) apresenta diversas recomendações importantes, como manter o aparelho sempre atualizado para evitar a exploração de vulnerabilidades por criminosos, bloquear aplicativos sensíveis, e desabilitar funções que permanecem ativas mesmo com a tela bloqueada, como responder mensagens. Esses cuidados podem prevenir o roubo de dados ou o acesso indevido a contas bancárias e redes sociais, o que pode resultar em extorsões, invasões de contas, chantagens, golpes contra familiares e amigos, entre outros prejuízos.

A pesquisa apresentou uma lista de ameaças descritas por autores como Santos e Sott (2016), Silva (2003), Freitas (2017) e Gabbay (2006). No entanto, mais do que conhecer essas ameaças, é fundamental que os usuários desenvolvam consciência sobre a importância de se proteger no ambiente digital. Como destaca Lobo (2016), muitas vezes os próprios usuários desconhecem o valor das informações que manipulam, o que os torna vulneráveis — especialmente diante de técnicas de engenharia social, que exploram comportamentos humanos para obter acesso indevido a dados sensíveis. Segundo Santos e Sott (2016), a segurança da informação tem

como objetivo garantir que todos os dados relevantes estejam protegidos contra ameaças físicas e digitais. Por isso, adotar medidas de precaução — como o uso de senhas fortes, cuidados com e-mails suspeitos e a adoção de boas práticas no uso de redes — é essencial para prevenir riscos e minimizar impactos. A conscientização e a adoção de comportamentos seguros são passos fundamentais para enfrentar os diferentes tipos de ameaças no contexto atual.

5 CONSIDERAÇÕES FINAIS

Em um contexto ao qual ataques virtuais, golpes digitais e novas ameaças surgem constantemente, a segurança da informação torna-se um tema crucial. Este trabalho buscou investigar o nível de conhecimento dos estudantes de Ciência da Computação sobre práticas básicas de proteção digital, considerando seu papel futuro como profissionais de tecnologia da informação. Para isso, este trabalho abordou os conceitos de informação e seu valor, definiu o que é segurança da informação, analisou diferentes tipos de ameaças, como *vírus* e engenharia social, e discutiu temas como riscos, vulnerabilidades e os cuidados que devem ser adotados para a proteção dos dados, culminando na realização pesquisa e análise dos resultado.

Em relação à **QP1**, essa pesquisa buscou compreender se os estudantes estarão cientes e tomarão os devidos cuidados com suas informações credenciais para acesso de serviços na rede. A análise dos dados revelou que, embora a maioria dos estudantes demonstra estar ciente das medidas de segurança necessárias, nem todos colocam esses conhecimentos em prática, o que pode representar um ponto de vulnerabilidade.

Quanto à **QP2**, que investigou se os respondentes possuem conhecimento para identificar e se defender de ataques de engenharia social, os resultados indicam que a maioria demonstra compreender os cuidados necessários. No entanto, é importante destacar que esse entendimento parece ser superficial. Quando os cuidados foram abordados sem mencionar diretamente o termo "engenharia social", o índice de acerto foi alto; por outro lado, ao serem questionados explicitamente sobre o conhecimento desse tipo de ataque, pouco mais de 50% afirmaram conhecê-lo. Isso sugere que muitos estudantes ainda não possuem um domínio aprofundado sobre o tema.

A **QP3** buscou investigar se os estudantes adotam boas práticas ao se conectarem a redes e serviços digitais. Os dados indicaram que, embora a maioria adote estas práticas, essa não é uma maioria absoluta. Isso revela que ainda existe uma parcela significativa de alunos que não seguem medidas básicas de segurança.

Em relação à **QP4** (que buscou verificar se os estudantes sabem se proteger, reconhecer e lidar com problemas causados por (*malwares*), a análise dos dados revelou que a maioria dos respondentes afirmou adotar cuidados preventivos, como evitar a execução de arquivos provenientes de fontes desconhecidas. No entanto, houve uma queda nas respostas positivas quando os alunos foram questionados sobre a capacidade de identificar sinais de infecção, remover *malwares* ou utilizar ferramentas como o *firewall*. Isso indica que, apesar de possuírem conhecimentos básicos sobre prevenção, ainda há lacunas no que diz respeito ao enfrentamento de situações em que o dispositivo já foi comprometido.

Por fim, a **QP5** abordou se os discentes sabem identificar medidas preventivas de segurança em casos de uso indevido de seus dispositivos por terceiros. Os dados indicam que, em sua maioria, os estudantes possuiam esse conhecimento; no entanto, essa maioria não é absoluta. Esse resultado aponta para a existência de uma lacuna que ainda precisa ser preenchida,

evidenciando a necessidade de maior aprofundamento nesse aspecto da segurança da informação.

Para finalizar este trabalho, aqui são notadas sugestões para investigações futuras. A partir dos resultados obtidos, observou-se a necessidade de uma investigação mais aprofundada sobre o tema da engenharia social. Apesar de muitos respondentes adotarem práticas seguras, poucos associaram essas ações diretamente ao conceito de engenharia social, o que evidencia uma lacuna conceitual relevante. Em segundo lugar, recomenda-se explorar mais detalhadamente o conhecimento dos alunos sobre os diferentes tipos de malwares, seus impactos e as medidas que devem ser tomadas ao identificar uma infecção. Por fim, seria pertinente investigar quais práticas de segurança da informação os discentes realmente aplicam em seu cotidiano, considerando que, em diversos momentos da pesquisa, embora demonstrasse conhecimento teórico, não necessariamente o colocavam em prática.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Códigos de prática para a gestão da segurança da informação**. 2001. Norma Brasileira. Citado 2 vezes nas páginas 12 e 17.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Códigos de prática para a gestão da segurança da informação**. 2005. Norma Brasileira. Citado 2 vezes nas páginas 20 e 21.

BRASIL, B. C. G. da Internet no. **Cartilha de segurança para internet**. 4. ed. São Paulo: CGI.br, 2012. Acesso em: 1 nov. 2024. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Citado 3 vezes nas páginas 23, 28 e 32.

BRASIL, G. **Relatório de Revisão do Cybersecurity Capacity Maturity Model for Nations (CMM) Brasil**. Brasília, 2023. Acesso em 15 out. 2024. Disponível em: https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/cmm-report-brazil-2023_final_pt.pdf. Citado na página 12.

CISCO NETWORKING ACADEMY. **Cyber Academy – Módulo 1: Fundamentos da Segurança Cibernética**. 2021. https://pt.scribd.com/document/770673594/E-book-Cyber-Academy-Modulo-1-Fundamentos-Da-Seguranca-Cibernetica-1. E-book. Acesso em: 08 jun. 2025. Citado na página 12.

CODERN. **Cartilha Codern: dicas de segurança**. Natal, 2021. Acesso em: 1 nov. 2024. Disponível em: https://codern.com.br/wp-content/uploads/2021/06/Cartilha-Codern-DICAS-DE-SEGURANCA-v1.pdf. Citado na página 23.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de segurança para internet**. 4. ed. São Paulo: CGI.br, 2012. Acesso em: 6 maio 2025. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Citado na página 34.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Furto de celular**. São Paulo: NIC.br, 2023. Acesso em: 7 maio 2025. Disponível em: https://cartilha.cert.br/fasciculos/furto-de-celular/fasciculo-furto-de-celular.pdf. Citado na página 36.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Proteção de dados**. São Paulo: NIC.br, 2023. Acesso em: 7 maio 2025. Disponível em: https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf. Citado 2 vezes nas páginas 34 e 36.

ECAMPUS NEWS. **Cyber attacks on colleges and universities: How businesses help safeguard higher education from cyber threats**. 2024. Acesso em: 08 jun. 2025. Disponível em: https://www.ecampusnews.com/newsline/2024/04/12/cyber-attacks-on-colleges-and-universities-how-businesses-help-safeguard-higher-education-from-cyber-thr Citado na página 13.

FREITAS, D. T. **Insegurança em smartphones: Uma pesquisa de campo no contexto do campus VII da UEPB**. Dissertação (Mestrado) — Universidade Estadual da Paraíba (UEPB), 2017. Acesso em: 15 de novembro de 2023. Disponível em: http://dspace.bc.uepb.edu.br/jspui/handle/123456789/18928. Citado 4 vezes nas páginas 14, 18, 32 e 36.

GABBAY, M. S. **Fatores influenciadores da implementação de ações de gestão de segurança da informação: um estudo com executivos e gerentes de tecnologia da informação das empresas do Rio Grande do Norte**. Dissertação (Mestrado) — Universidade Federal do Rio Grande do Norte, 2006. Disponível em: https://bdtd.ibict.br/vufind/Record/UFRN_c4df3a0366e2f14b5f362cc6f494c32e. Citado 5 vezes nas páginas 14, 17, 18, 32 e 36.

GUSMÃO, J. A. do P. Auditoria dos sistemas de informação com foco nos controles de riscos. **QUALIA-A ciência em movimento**, v. 3, n. 1, p. 75–93, 2017. Citado na página 20.

LAFRANCE, Y. **Psychology: A Precious Security Tool**. [S.l.], 2004. 27 p. Citado na página 21.

LAUREANO, M. A. P.; MORAES, P. E. S. Segurança como estratégia de gestão da informação. **Revista Economia & Tecnologia**, v. 8, n. 3, p. 38–44, 2005. Citado 2 vezes nas páginas 16 e 18.

LOBO, J. T. C. **Engenharia social e a segurança da informação no ambiente corporativo**. Dissertação (Mestrado) — Nome da Universidade, 2016. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/407. Citado 8 vezes nas páginas 12, 15, 17, 21, 22, 23, 29 e 36.

LORENZO, A. D. **Ataques cibernéticos crescem quase 70% no Brasil em um ano**. 2024. Acesso em: 08 jun. 2025. Disponível em: https://olhardigital.com.br/2024/07/19/seguranca/ataques-ciberneticos-crescem-quase-70-no-brasil-em-um-ano/. Citado na página 14.

MACHADO, J. dos S. *et al.* As principais ameaças digitais e suas formas de mitigação no contexto da segurança da propriedade intelectual. **Conjecturas**, v. 22, n. 8, p. 147–162, 2022. Disponível em: https://repositorio.ifs.edu.br/biblioteca/handle/123456789/1759. Citado na página 17.

OLHAR DIGITAL. **WannaCry: o ciberataque que parou o mundo**. 2022. Acesso em: 08 jun. 2025. Disponível em: https://olhardigital.com.br/especial/wannacry/. Citado na página 13.

OLHAR DIGITAL. **Ciberataques no Brasil aumentam 38% no primeiro trimestre de 2024**. 2024. Acesso em: 08 jun. 2025. Disponível em: https://olhardigital.com.br/2024/04/22/seguranca/ciberataques-no-brasil-aumentam-38-no-primeiro-trimestre-de-2024/. Citado na página 12.

PEREIRA, L. A. d. S.; VICENTINE, A. L.; RIZO, A. C. O impacto da engenharia social na segurança da informação: uma abordagem orientada à gestão corporativa. **AtoZ: novas práticas em informação e conhecimento**, Curitiba, v. 12, n. 3, p. 45–62, 2021. Acesso em: 19 out. 2024. Disponível em: https://revistas.ufpr.br/atoz/article/view/64640. Citado 2 vezes nas páginas 21 e 22.

PONTES, M. V. F. Política de segurança da informação: uma contribuição para o campus iv. Universidade Federal da Paraíba, 2014. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/17031. Citado 3 vezes nas páginas 19, 32 e 34.

PRADO, T. A. S.; NASCIMENTO, I. P.; RIBEIRO, A. A. M. Cibersegurança: ameaças e vulnerabilidades em ambientes computacionais. *In*: **Anais do XVI Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)**. Recife: SBC, 2016. p. 79–86. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/19298/19127. Citado na página 12.

SANTOS, D. P. d. A engenharia social no brasil e seus riscos. 2016. Acesso em: 21 maio 2025. Disponível em: http://repositorio.utfpr.edu.br/jspui/handle/1/19455. Citado na página 30.

SANTOS, R. L. C. d.; SOTT, M. R. W. Aspectos da segurança da informação: Sua importância para as organizações. 2016. Acesso em: 21 maio 2025. Disponível em: https://ri.unipac.br/repositorio/wp-content/uploads/2019/08/Ronan.pdf. Citado 10 vezes nas páginas 14, 16, 17, 18, 19, 20, 29, 32, 34 e 36.

SILVA, P. M. **Políticas de segurança da informação nas organizações**. Tese (Doutorado) — Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós . . . , 2003. Disponível em: https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/84739/198174.pdf?sequence=1&isAllowed=y. Citado 5 vezes nas páginas 14, 18, 19, 32 e 36.

TAKEUCHI, E. C. Fatores humanos em cibersegurança uma revisão sistemática da literatura. Universidade Federal de Uberlândia, 2023. Disponível em: https://repositorio.ufu.br/bitstream/123456789/36792/1/FatoresHumanosCiberseguranÃğa.pdf. Citado na página 17.

TORRES, P. **Engenharia social**. 2012. http://www.dgti.ufla.br/site/?p=631. Acesso em: 8 nov. 2015. Citado na página 23.

UNIVERSIDADE ESTADUAL DA PARAÍBA (UEPB). **Relatório PPC – Curso de Ciência da Computação**. 2024. Relatório institucional interno. Disponível via sistema da UEPB (RelatórioPPC?id=21&rl=RelatorioPPC). Acesso em: 08 jun. 2025. Citado na página 26.

WAZLAWICK, R. S. **Metodologia de pesquisa para ciência da computação**. 3. ed. Rio de Janeiro: LTC, 2021. Citado na página 25.

YIN, R. K. **Estudo de caso: planejamento e métodos**. 4. ed. Porto Alegre: Bookman, 2010. Citado na página 25.

APENDICE A – INSTRUMENTO DE PESQUISA

Questionário sobre segurança da informação

O presente questionário faz parte do meu trabalho de conclusão de curso, TCC. Ele tem o intuito de levanta informações sobre como está o conhecimento geral dos discentes do curso de ciências da computação sobre segurança da informação.
obs: O email coletado não será usado para associar as resposta a ou usuário. Ele apenas evitara que algum participante responda mais de uma vez.

* Indica uma pergunta obrigatória

1. Qual período do curso de Ciência da Computação você está cursando? *

Marcar apenas uma oval.

- 2º
- 3º
- 4º
- 5º
- 6º
- 7º
- 8º
- 9º
- 10º
- Eu já ultrapassei a quantidade regular de semestres

2. 1. Eu sempre utilizo senhas fortes e únicas para cada conta online. *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente.

3. 2. Eu altero minhas senhas regularmente, mesmo que não seja solicitado *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

4. 3. Eu utilizo autenticação de dois fatores (2FA) sempre que disponível *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

5. 4. Eu evito conectar-me a redes Wi-Fi públicas sem utilizar uma VPN. *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

6. 5. Eu mantenho meus sistemas operacionais e aplicativos sempre atualizados. *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

7. 6. Eu faço backup regularmente dos meus dados importantes. *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

8. 7. Eu verifico se os sites que visito possuem conexão segura (HTTPS). *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

9. 8. Eu evito compartilhar informações pessoais em redes sociais *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

10. 9. Eu desconfio de links ou anexos recebidos por e-mail, mesmo que pareçam legítimos. *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

11. 10. Eu utilizo software antivírus em todos os meus dispositivos. *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

12. *

11. Eu entendo os riscos associados ao uso de senhas fracas ou repetidas.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

13. *

12. Eu sei identificar possíveis tentativas de phishing em e-mails ou mensagens.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

14. *

13. Eu estou ciente dos riscos de instalar software de fontes não confiáveis.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

15. *

14. Eu reconheço a importância de criptografar dados sensíveis.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

16. *

15. Eu entendo os perigos de compartilhar dispositivos ou credenciais de acesso com outras pessoas.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

17. *

16. Eu sei como proteger meus dispositivos contra roubo ou perda física.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

18. 17. Eu estou ciente dos riscos de vazamento de dados em serviços online. *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

19. 18. Eu entendo os riscos de usar dispositivos USB desconhecidos ou não confiáveis. *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

20. 19. Eu sei como identificar e evitar sites falsos (fake websites). *

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

21. *

20. Eu estou ciente dos riscos de engenharia social e como me proteger contra ela.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

22. *

21. Eu sei como identificar sinais de infecção por malware em meus dispositivos.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

23. *

22. Eu evito clicar em pop-ups ou anúncios suspeitos enquanto navego na internet.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

24. *

23. Eu entendo a importância de não executar arquivos desconhecidos baixados da internet.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

25. *

24. Eu sei como remover malware de um dispositivo infectado.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente

26. *

25. Eu utilizo firewalls para proteger minha rede doméstica ou corporativa.

Marcar apenas uma oval.

- Eu concordo totalmente.
- Concordo parcialmente.
- Não concordo nem discordo
- Discordo parcialmente.
- Discordo totalmente