INSTITUTO FEDERAL
Pernambuco

# O IMPACTO DO SUPORTE METODOLÓGICO E FERRAMENTAL ORIENTADO A SEGURANÇA DA INFORMAÇÃO NO ENSINO PRÁTICO DE CURSOS DE DESENVOLVIMENTO DE SOFTWARE

THE IMPACT OF METHODOLOGICAL AND TOOL SUPPORT ORIENTED TO INFORMATION SECURITY IN PRACTICAL TEACHING OF SOFTWARE DEVELOPMENT COURSES

**Poliana Santos de Queiroz**
psq@discente.ifpe.edu.br
**Guilherme José de Carvalho Cavalcanti**
guilherme. cavalcanti@belojardim.ifpe.edu.br

---

**Resumo:**
Este Trabalho de Conclusão de Curso (TCC) explora a necessidade crítica de atualizar e aprimorar os currículos dos cursos de formação para desenvolvedores de software, com ênfase especial na segurança da informação. Este estudo argumenta que as experiências práticas obtidas por meio de laboratórios, simulações e competições de hacking são vitais para que os estudantes não apenas consolidem seus conhecimentos teóricos, mas também desenvolvam habilidades essenciais para resolver problemas complexos na área. O foco principal do estudo foi entender como a educação em segurança da informação pode ser melhorada para atender às rápidas mudanças tecnológicas e às demandas do mercado de trabalho atual. Adotamos uma metodologia que combinou entrevistas estruturadas com profissionais ativos no setor de tecnologia e análises qualitativas e quantitativas. Discutimos a importância das certificações profissionais como meio de validar as habilidades técnicas dos profissionais de TI, além de enfatizar a necessidade de desenvolver habilidades comportamentais como curiosidade, persistência e comprometimento, fundamentais para o sucesso no campo. O estudo também criticou a abordagem comum de recrutamento das empresas para posições em segurança da informação, muitas vezes terceirizada, que pode não capturar adequadamente as competências essenciais requeridas para enfrentar desafios específicos da área. Propôs-se, então, uma maior sinergia entre as instituições de ensino e o setor empresarial, visando garantir que a educação oferecida esteja em plena sintonia com as necessidades práticas e atuais, preparando profissionais mais qualificados para proteger infraestruturas tecnológicas e para contribuir efetivamente com a segurança cibernética. Os resultados desta investigação ressaltam a urgência de aprimorar a entrega de conteúdo educacional em segurança da informação,

assegurando que este esteja alinhado com as evoluções e exigências contemporâneas do campo, contribuindo assim para a formação de uma base sólida e responsiva de profissionais de TI.

**Palavras-chave:** Segurança da informação, Experiência prática, Engajamento profissional, Currículo em tecnologia, Desenvolvimento de habilidade.

**Abstract:**
This term paper explores the critical need to update and improve the curricula of training courses for software developers, with a special emphasis on information security. This study argues that practical experiences gained through labs, simulations and hacking competitions are vital for students not only to consolidate their theoretical knowledge, but also to develop essential skills to solve complex problems in the field. The main focus of the study was to understand how information security education can be improved to meet the rapid technological changes and demands of the current job market. We adopted a methodology that combined structured interviews with professionals active in the technology sector and qualitative and quantitative analyses. We discussed the importance of professional certifications as a means of validating the technical skills of IT professionals, in addition to emphasizing the need to develop soft skills such as curiosity, persistence and commitment, fundamental for success in the field. The study also criticized the common approach of companies to recruit for information security positions, often outsourced, which may not adequately capture the essential competencies required to address specific challenges in the field. Greater synergy between educational institutions and the business sector was therefore proposed, with the aim of ensuring that the education offered is fully aligned with current practical needs, preparing professionals who are better qualified to protect technological infrastructures and to effectively contribute to cybersecurity. The results of this investigation highlight the urgency of improving the delivery of educational content in information security, ensuring that it is aligned with the contemporary developments and demands of the field, thus contributing to the formation of a solid and responsive base of IT professionals.
**Keywords:** Information security, Practical experience, Professional engagement, Technology CV, Skill development.

## 1 INTRODUÇÃO

Nos últimos anos, a tecnologia tem avançado a passos largos, transformando a maneira como realizamos nossas atividades cotidianas. Graças à internet, podemos fazer compras online, utilizar serviços bancários digitais, solicitar entregas expressas, entre muitos outros serviços. Este avanço também trouxe à tona questões importantes como a engenharia social. Kevin Mitnick (2002), um famoso hacker e especialista em segurança, define engenharia social como “a prática de obter informações confidenciais através da manipulação de usuários legítimos. Um engenheiro social frequentemente usa truques psicológicos para enganar os indivíduos a fim de obter acesso a sistemas ou dados.”

Além disso, a tecnologia permite que as pessoas trabalhem de qualquer lugar do mundo, desde que tenham acesso à internet. Dispositivos móveis, como smartphones e tablets, também aceleram os processos, possibilitando o acesso à internet, envio de mensagens, realização de ligações e acesso a informações em qualquer lugar.

Com essa evolução, a informação ganhou uma nova importância. A troca constante de dados valiosos por meio de dispositivos conectados à rede desperta o interesse de pessoas mal-intencionadas. Notícias de invasões em redes de bancos ou roubos de informações de grandes empresas são cada vez mais comuns. Portanto, é crucial que as organizações contem com profissionais especializados e dedicados à proteção dessas informações.

Diante deste cenário, torna-se imperativo que as instituições educacionais, especialmente focadas no desenvolvimento de software, incorporem práticas robustas de segurança da informação em seus currículos. A proteção eficaz das informações não apenas resguarda os dados que circulam nas redes internas das empresas, mas também prepara os futuros profissionais para enfrentar e mitigar ameaças cibernéticas, como ataques de malware, phishing e roubo de dados. Portanto, este trabalho visa explorar o impacto de um suporte metodológico e ferramental e orientado à segurança da informação no ensino prático de cursos de desenvolvimento de software, identificando como essa abordagem pode fortalecer as competências dos discentes na proteção eficaz das informações no ambiente digital. A proteção das informações é essencial, pois protege as informações que circulam na rede, tornando-as menos vulneráveis a ataques cibernéticos, como o roubo de dados, malware, phishing, etc. Para Schneier (2011):

> “As ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados." O crime no ciberespaço inclui tudo o que se pode esperar do mundo físico: roubo, extorsão, vandalismo, voyeurismo, exploração, jogos de trapaças, fraude, etc.”

As fragilidades que levam a problemas de segurança podem ser evitadas, ou, pelo menos, minimizadas. Sendo assim, instituições de ensino na área da tecnologia da informação (TI) necessitam se adequar aos novos tipos de saberes adivinhos da cultura digital. Segundo Hargreaves (1998), as regras do mundo estão mudando, logo está na hora das regras de ensino

e do trabalho docente também mudarem. Assim, de acordo com Queiroz, Braga e Leick (2008, p. 5):

> "Os educadores estão sendo desafiados a mudar e a inovar com o intuito de atender as expectativas da atual sociedade. Mudar para adquirir novas técnicas metodológicas capazes de transformarem o espaço-escola do aprendiz em algo dinâmico, significativo e participativo, aproximando a teoria da prática com uma postura interdisciplinar, permitindo assim a criação de destrezas para com a vida."(Queiroz, Braga e Leick (2008, p. 5)

Nos currículos das instituições de ensino superior para área de tecnologia da informação, observa-se uma falta de especificidade nas diretrizes para a educação em Segurança da Informação. Geralmente, os programas não especificam os detalhes ou a sequência didática recomendada para as disciplinas dessa subárea.

> "Embora a segurança da informação seja reconhecida como uma área crítica dentro da tecnologia da informação, muitos currículos de ensino superior ainda não apresentam diretrizes claras e específicas para o ensino desta subárea. A falta de uma sequência didática bem definida e detalhada impede que os alunos adquiram uma compreensão profunda e abrangente dos conceitos e práticas essenciais para a proteção eficaz de informações." (SANDHU, 2013).

Como resultado, há uma variedade de modelos curriculares adotados por diferentes instituições, tanto no Brasil quanto no exterior. Diante dessa diversidade, torna-se crucial avaliar a percepção de ex-alunos formados em cursos de TI sobre o ensino de Segurança da Informação. Essa análise é fundamental para entender a importância atribuída à disciplina e para identificar oportunidades de melhorias ou adaptações nos currículos. O intuito é garantir que os estudantes de graduação e pós-graduação, futuros profissionais da área, desenvolvam as competências necessárias exigidas pelo mercado de trabalho ao concluir os estudos.

Nesse contexto, o objetivo principal deste trabalho de conclusão de curso caracteriza-se em avaliar o nível de preparação e formação em Segurança da Informação que estudantes receberam ao decorrer do seu curso relacionado a área de tecnologia e desenvolvimento de software. Além de determinar o impacto da formação em Segurança da Informação na empregabilidade dos alunos e na sua capacidade de lidar com questões de segurança em suas carreiras. Como objetivos específicos, pretende-se (1) avaliar a eficácia das grades curriculares, determinando se atualmente os currículos preparam os estudantes com conhecimento necessário em Segurança da Informação, essencial no desenvolvimento de software; (2) medir a integração de Segurança no desenvolvimento de software,

verificando até que ponto a Segurança da Informação está integrada as práticas de ensino; (3) analisar recursos educacionais disponibilizado aos alunos; (4) verificar se os estudantes têm oportunidades suficientes em práticas ou projetos reais; (5) verificar se houve colaborações e palestras de profissionais da área como uma ferramenta de ensino e inspiração para os alunos. Os resultados discutidos neste estudo foram obtidos por meio de um questionário no Google Forms, distribuído entre indivíduos que concluíram cursos na área de Tecnologia da Informação

## 2 FUNDAMENTAÇÃO TEÓRICA

Para uma compreensão mais aprofundada dos temas abordados nesta pesquisa, esta seção detalha os conceitos fundamentais relacionados à Segurança da Informação nos cursos de tecnologia.

### 2.1 Currículo e Ensino

A inovação tecnológica trouxe mudanças significativas e permanentes ao processo educativo, exigindo que as Instituições de Ensino se adaptem aos novos conhecimentos provenientes da cultura digital. Essas instituições são frequentadas por jovens que cresceram em meio a constantes transformações e avanços tecnológicos. O progresso tecnológico redefine o propósito das instituições de ensino, que passa a ser o de formar cidadãos preparados para uma sociedade tecnologicamente avançada.

Assim, de acordo com Queiroz, Braga e Leick (2008, p. 5):

> “Os educadores estão sendo desafiados a mudar e a inovar com o intuito de atender as expectativas da atual sociedade. Mudar para adquirir novas técnicas metodológicas capazes de transformarem o espaço-escola do aprendiz em algo dinâmico, significativo e participativo, aproximando a teoria da prática com uma postura interdisciplinar, permitindo assim a criação de destrezas para com a vida.”( Queiroz, Braga e Leick (2008, p. 5).

No início da década de 1990, nosso país alcançou um marco significativo com a aprovação da Lei de Diretrizes e Bases (LDB), que estabeleceu as bases para uma educação de maior qualidade, acessível a todos os grupos da sociedade. Conforme a LDB 9394/96, o sistema educacional brasileiro é organizado em dois níveis principais: educação básica e ensino superior. Além disso, a lei destaca dois aspectos cruciais:

1) Educação Profissional e Tecnológica – Visa preparar os estudantes para o mercado de trabalho, promovendo a atualização e o aprimoramento de conhecimentos tecnológicos e científicos.

2) Financiamento e Formação de Educadores – A LDB 9394/96 também trata da alocação de recursos financeiros e das diretrizes para a formação dos profissionais da educação, essenciais para a implementação de uma educação eficaz e de qualidade.

Segundo a Lei de Diretrizes e Bases (LDB, 1996), que é a legislação mais significativa do Brasil em relação à educação. Promulgada em dezembro de 1996 sob o número 9394/96, a lei foi instituída com o propósito de assegurar o direito de acesso à educação gratuita e de qualidade para toda a população, valorizar os profissionais da educação e definir as responsabilidades da União, dos estados e dos municípios no que se refere à oferta de educação pública.

## 2.2 Importância da Segurança da Informação

Atualmente as informações são extremamente valiosas, pois fundamentam tomadas de decisão e o surgimento de novas ideias de negócio. Com os avanços tecnológicos, acessar informações tornou-se mais fácil, sendo possível recebê-las diretamente em smartphones, mediante aplicativos de mensagens ou por e-mail. No entanto, essa facilidade de acesso também levou a uma disseminação massiva de informações. Diante desse cenário, surge o desafio significativo de proteger esses dados. Segundo Sêmola (2014, p. 43), ele conceitua que a informação é “conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas”.

É correto dizer que as informações trocadas podem variar desde mensagens comuns de caráter comunicativo até dados de alta relevância para a organização, destacando assim a necessidade de protegê-los. A relevância de uma informação muitas vezes depende de quem a possui. Por exemplo, uma informação que pode parecer trivial para uma telefonista pode ser crucial para alguém que compreende todo o contexto. Como Mitnick e Simon apontam (2003, p. 21), “Assim como as peças de um quebra-cabeça, cada informação pode parecer irrelevante sozinha.”

No entanto, ao juntar as peças, uma imagem clara se forma. Nesse cenário, torna-se evidente que a informação é um ativo valioso dentro dos negócios de uma organização. Aprender a protegê-la é essencial para o sucesso empresarial, seja essa informação uma troca de dados entre máquinas ou entre profissionais. No contexto adequado, a informação revela sua verdadeira importância, portanto, é fundamental que seu acesso seja restrito apenas a indivíduos autorizados.

Diante disso, a segurança surge como o principal desafio no manejo da informação. Proteger um ativo tão valioso não é uma tarefa simples, evidenciando a importância de uma gestão eficaz da segurança da informação em ambientes corporativos. A segurança da informação envolve a preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações cruciais para uma organização ou indivíduo. Esta preservação abrange o ambiente físico, tecnológico e a gestão de pessoas, tornando-se um campo de interesse vital para qualquer organização que valorize a qualidade e a continuidade de seus negócios. Segundo Sêmola (2014, p. 41), a segurança da informação pode ser vista como uma área de conhecimento dedicada à proteção dos ativos informacionais contra acessos não autorizados, alterações indevidas e problemas de indisponibilidade.

Essa definição sublinha a necessidade de profissionais com conhecimentos especializados capazes de assegurar que as informações permaneçam inalteradas e protegidas de acessos inapropriados, enquanto garantem sua disponibilidade para usuários autorizados. Um dos principais desafios da segurança da informação é sensibilizar os colaboradores sobre sua importância. Como destacam Ferreira e Araújo (2014, p. 89), é fundamental que os colaboradores tratem suas senhas como informações confidenciais, sem as compartilhar ou acessando sistemas de outros sem permissão explícita. Por essas razões, estabelecer uma gestão eficaz de segurança da informação é uma tarefa complexa, mas com a aplicação de conhecimentos adequados e a eficiência em cada etapa do processo, é possível criar um ambiente corporativo seguro. Assim, garante-se a confidencialidade, integridade, disponibilidade e autenticidade das informações da organização

## 2.3 Impacto da Formação em Segurança da Informação na Carreira Profissional

Segundo Laudon e Laudon (1999, p. 4) profissionais de Tecnologia da Informação (TI) devem saber identificar problemas e oportunidades e utilizar sistemas de informação para aumentar a capacidade de reação das organizações. Sendo essa uma habilidade fundamental para definir um profissional qualificado em TI. Eles também destacam a importância de investimentos contínuos em sistemas e profissionais, alertando que a ausência desses investimentos pode expor as empresas a sérios riscos.

Takahashi (2000, p. 49) critica os currículos de graduação por estarem frequentemente obsoletos e desalinhados com as revoluções tecnológicas, sugerindo que um reposicionamento dos Parâmetros Curriculares Nacionais (PCNs) deve ser considerado. Os Parâmetros Curriculares Nacionais (PCNs) são diretrizes elaboradas pelo Ministério da Educação (MEC) do Brasil para orientar a elaboração dos currículos escolares. Os PCNs não são um currículo em si, mas sim um conjunto de orientações que ajudam os educadores a planejar e implementar o ensino. Takahashi (2000, p 49) Também observa a importância para países em desenvolvimento de absorver e aplicar novas tecnologias, não apenas as gerar.

Quanto ao ingresso dos estudantes no mercado de trabalho, Cabral e Caprino (2015, p. 15) também discutem a seleção de profissionais de segurança em TI, criticando empresas por muitas vezes delegarem essa tarefa a agências de recrutamento externas, o que pode levar a uma ênfase excessiva em habilidades técnicas em detrimento de características comportamentais como curiosidade, persistência e comprometimento, que eles consideram essenciais para um bom analista de segurança.

Oliveira (2009, p. 75) complementa argumentando que certificações profissionais podem permitir que as organizações concentrem seus esforços de seleção nos aspectos comportamentais dos candidatos, uma vez que o conhecimento técnico é assegurado pela certificação.

Em conclusão, a preparação adequada de profissionais em segurança da informação é crucial não apenas para a proteção das infraestruturas tecnológicas, mas também para a capacidade de inovação e competitividade no mercado global. As discussões levantadas por

Laudon e Laudon, Cabral e Caprino, e outros estudiosos destacam a necessidade urgente de atualização contínua dos currículos de TI e de métodos de ensino que acompanhem o ritmo acelerado das mudanças tecnológicas. Além disso, a implementação de certificações reconhecidas e o desenvolvimento de habilidades comportamentais são essenciais para formar profissionais que não apenas dominem as técnicas de segurança, mas que também estejam preparados para enfrentar desafios complexos e dinâmicos. As instituições de ensino e as empresas devem, portanto, trabalhar juntas para garantir que a formação em segurança da informação seja robusta, atualizada e alinhada com as exigências contemporâneas, transformando os desafios em oportunidades para a criação de um ambiente digital mais seguro e confiável.

## 2.4 Engenharia Social e Educação em Segurança da Informação

Qualquer tentativa de acessar informações de forma não autorizada é considerada um ataque. O agente que busca se apropriar indevidamente de informações no âmbito tecnológico é conhecido como hacker. Conforme Mitnick e Simon (2003, p. 6) afirmam, “a mente do hacker busca constantemente maneiras de contornar as robustas defesas da tecnologia de segurança”, demonstrando que hackers ou pessoas mal intecionadas utilizam seu conhecimento avançado para explorar vulnerabilidades e executar ataques. Uma das técnicas frequentemente empregadas é a engenharia social, que envolve a manipulação de usuários legítimos para obter informações confidenciais. Kevin Mitnick, um renomado especialista em segurança, define engenharia social como “a prática de obter informações confidenciais através da manipulação de usuários legítimos” (MITNICK, 2002), evidenciando a importância de conscientizar e treinar usuários para identificar e resistir a tais tentativas de manipulação. Para além da Engenharia social exitem outros tipos de ataques, bem conhecidos e bastantes consolidados, são esses:

- Vírus: Programas pequenos projetados para causar danos, que se propagam infectando outros softwares.
- Trojan: Softwares que se disfarçam como aplicativos legítimos ou documentos para abrir brechas de segurança no sistema.
- Worm: Diferente do vírus, não requer um programa hospedeiro para se espalhar, sendo capaz de se replicar automaticamente e causar danos extensivos ao sistema infectado.
- Sniffers: Programas que capturam e analisam dados trafegando em uma rede.

- Exploit: Utiliza vulnerabilidades específicas para ganhar controle sobre sistemas.
- Spoofing: Técnica que falsifica dados para enganar sistemas e usuários, fazendo-os acreditar que estão interagindo com fontes confiáveis, como em casos de IP ou e-mail spoofing.
- Scanners de portas: ferramentas que examinam um sistema em busca de pontos vulneráveis.
- DoS (Denial of Service): Ataque que visa incapacitar um sistema por sobrecarga, frequentemente utilizando múltiplos sistemas comprometidos, conhecido como ataque DDoS (Distributed Denial of Service).
- Engenharia Social: Conforme descrito por Mitnick e Simon (2003, p.VII), essa técnica utiliza persuasão para enganar pessoas, fazendo-as acreditar que o atacante é alguém que ele não é.

Em síntese, um ataque é o método pelo qual um hacker ou qualquer pessoa mal intencionada obtém acesso não autorizado a um sistema. Uma vez dentro, o invasor pode copiar, deletar ou modificar informações, e eventualmente tentar ocultar seus rastros para dificultar a detecção e resposta por parte dos profissionais de segurança da informação.

## 2.5 LGPD

De acordo com Marcondes (2021, p. 57), a Lei Geral de Proteção de Dados (LGPD) é uma das legislações mais significativas no Brasil em termos de proteção de dados pessoais. Aprovada em 2018 e em vigor desde 2020, a LGPD já impactou profundamente as empresas que operam online. Para estar conforme os novos requisitos legais, as empresas foram forçadas a adaptar suas políticas de privacidade e segurança de dados. A LGPD introduziu mudanças substanciais nos procedimentos relativos a dados pessoais e estabeleceu novos direitos para os titulares dos dados.

Saffi (2019, p. 24) ressalta que a LGPD é crucial para proteger os direitos de privacidade dos cidadãos brasileiros. A lei exige que as empresas que coletam informações de usuários da internet adotem práticas específicas para assegurar a proteção dos dados pessoais. O consentimento do usuário, um dos principais aspectos da LGPD, exige que as empresas informem claramente aos usuários quais dados estão sendo coletados e como serão utilizados.

Oliveira (2020, p. 12) enfatiza que o consentimento deve ser explícito para a coleta e armazenamento de dados.

Além disso, a LGPD assegura que os titulares dos dados possuam direitos específicos, como acesso, correção e exclusão de seus dados pessoais. Pereira (2021, p. 74) afirma que os indivíduos devem poder acessar todas as informações pessoais coletadas por empresas e solicitar sua eliminação.

Contudo, como aponta Saffi (2019, p. 31), a implementação da LGPD ainda é um desafio para muitas empresas, que podem enfrentar sanções significativas pelo não cumprimento. Dado que a LGPD é uma lei relativamente recente no Brasil, sua interpretação ainda pode evoluir, o que gera incertezas para as empresas.

Marcondes (2021, p. 62) argumenta que a LGPD desempenha um papel crucial ao conscientizar as empresas sobre a importância da proteção de dados pessoais. Apesar dos desafios para implementar todas as disposições da lei, a conscientização sobre a privacidade dos dados é uma tendência global. As empresas que adotam boas práticas de proteção de dados se beneficiam da confiança e satisfação dos clientes.

Oliveira (2020, p. 17) vê a LGPD como uma oportunidade para as empresas aprimorarem seus processos de privacidade e proteção de dados pessoais. A lei obriga as empresas a revisarem suas práticas de coleta e tratamento de dados, o que pode resultar em uma melhor proteção dos dados dos usuários e na eficiência dos processos internos.

Conclusivamente, a LGPD é uma legislação fundamental para a proteção de dados pessoais na internet. Embora sua implementação represente um desafio, também oferece uma oportunidade para o aprimoramento nas práticas de privacidade e proteção de dados pessoais.

## 3 METODOLOGIA

Esse trabalho de conclusão de curso explora a necessidade crítica de atualizar e aprimorar os currículos dos cursos de formação para desenvolvedores de software, com ênfase especial na segurança da informação. E se configura como uma pesquisa empírica qualitativa-quantitativa e de propósito exploratório, descritivo e pesquisa de melhoria. Segundo Bhattacharya (2008), uma pesquisa empírica tem como objetivo principal observar

um fenômeno no mundo social e então gerar conhecimento sobre este fenômeno. A abordagem de pesquisa quali-quantitativa conforme apresenta Knechtel (2014, p. 106), “[...] interpreta as informações quantitativas por meio de símbolos numéricos e os dados qualitativos mediante a observação, a interação participativa e a interpretação do discurso dos sujeitos (semântica)”. A pesquisa qualitativa tem como intuito investigar o que indivíduos fazem, sabem, pensam, e sentem mediante observação, entrevistas, e análise de documentos (PATTON, 2002). Isto posto, Minayo (2009) assegura que há uma relação fértil e frutuosa entre abordagens quantitativas e qualitativas, e devem ser vistas em oposição complementar. Em educação especificamente, a pesquisa quali-quantitativa possibilita descrever os fenômenos observados pelo pesquisador assim como fundamentar essas visões por meio de evidências.

É importante ressaltar que embora metodologicamente as pesquisas tenham definições diferentes, as pesquisas quantitativas e qualitativas possuem a mesma validação científica. Flick (2004) salienta que as convergências destas abordagens, oportunizam credibilidade aos resultados, uma vez que além de vasto embasamento teórico descritivo, os dados estatísticos irão validar as observações, ao mesmo tempo, em que fundamentará as informações adquiridas.

Nesse sentido, o fenômeno investigado foi a eficácia e a abrangência do ensino de Segurança da Informação em cursos de tecnologia, focando especificamente em como esse ensino prepara os estudantes para aplicar práticas de segurança em ambientes de desenvolvimento de software. O fenômeno central é a integração da Segurança da Informação na educação tecnológica e seu impacto na preparação profissional dos estudantes para enfrentar desafios relacionados à Segurança no mercado de trabalho.

Diferentes métodos de pesquisa servem para diferentes propósitos. Um tipo de método pode não atender a todos os propósitos. Assim, Runeson e Host (2008) destacam quatro tipos de propósitos de uma pesquisa:

- Exploratório: descobrir o que está acontecendo, buscar novos conhecimentos e gerar ideias e hipóteses para novas pesquisas;
- Descritivo: retratar uma situação ou fenômeno;
- Explicativo: buscar uma explicação de uma situação ou um problema, principalmente, mas não necessariamente sob a forma de uma relação causal;
- Pesquisa de melhoria: tentar melhorar um determinado aspecto do fenômeno

estudado.

De acordo com esses propósitos, esta pesquisa irá se classificar como exploratória, descritiva e pesquisa de melhoria, pois tem como características principais descobrir e descrever o impacto, contextualização, engajamento, intencionalidade, interdisciplinaridade, inter-relacionamentos e inclusão da disciplina de Segurança da Informação em cursos de instituições de ensino superior voltados para a área de Tecnologia.

Conforme Marconi e Lakatos (2010), os métodos de procedimentos são etapas mais concretas de uma pesquisa com uma finalidade mais restrita de explicação geral dos fenômenos e menos abstrata. Diante dos objetivos específicos descritos neste projeto, serão utilizados os seguintes procedimentos: pesquisa bibliográfica e questionário.

A pesquisa bibliográfica foi realizada com o intuito de investigar material já elaborado em livros de referência e nos principais periódicos e conferências que possuem objetivos semelhantes ao que esta pesquisa se propõe. A principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente (GIL, 2008).

Posteriormente, realizou- se um questionário voltado para pessoas que fizeram cursos na área de tecnologia, para observar como o fenômeno investigado se comporta em um contexto real. O questionário, segundo Gil (1999, p.128), pode ser definido “como a técnica de investigação composta por um número mais ou menos elevado de questões apresentadas por escrito às pessoas, tendo por objetivo o conhecimento de opiniões, crenças, sentimentos, interesses, expectativas, situações vivenciadas etc.”.

Diante do tipo de pesquisa, natureza e propósito e procedimentos utilizados ao longo deste

| **Quadro Metodológico da Pesquisa** | |
|---|---|
| **Tipo da Pesquisa** | Empírica |
| **Natureza da Pesquisa** | Qualitativa/Quantitativa |
| **Quanto ao Propósito** | Exploratório, Descritivo e Pesquisa de melhoria |
| **Quanto aos Procedimentos** | Bibliografia e Questionário |

trabalho, o Quadro 1 apresenta um resumo do quadro metodológico deste trabalho de conclusão de curso:

**Quadro 1. Quadro Metodológico da Pesquisa**

## 4. RESULTADOS E DISCUSSÕES

Nesta seção, apresentamos as estatísticas geradas a partir dos dados coletados. A amostra do estudo consistiu em 124 respostas, com a restrição de que os participantes fossem desenvolvedores formados na área de tecnologia e atualmente atuando no mercado de trabalho. O questionário foi aplicado por meio do Google Forms e distribuído via mensagens diretas no Twitter, Instagram e LinkedIn. Os participantes foram selecionados com base na descrição de seus perfis nas redes sociais, indicando que já eram graduados e atuavam na área de TI.

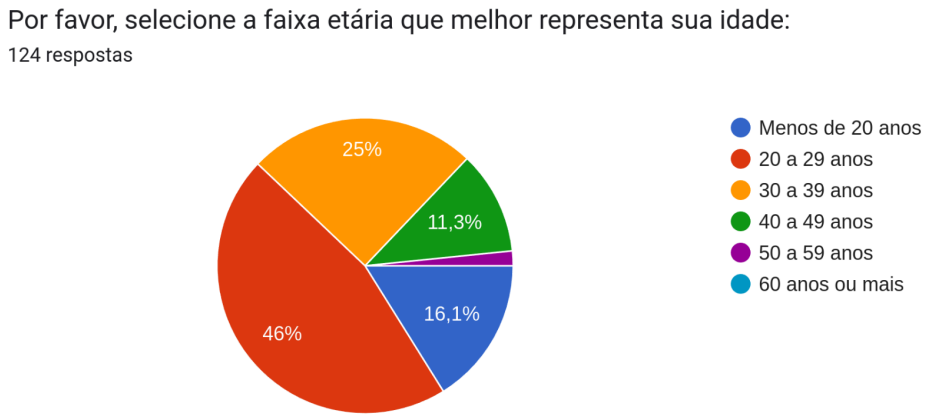


**Figura 2 - Faixa etária de idade dos participantes**

A análise do gráfico de distribuição etária revela que a maioria dos participantes do estudo se enquadra na faixa etária de 20 a 29 anos, representando 46% do total. Observa-se uma menor participação nas faixas etárias extremas, com 1,6% dos participantes entre 50 a 59 anos. As faixas de 30 a 39 anos, 40 a 49 anos e menos de 20 anos apresentam uma distribuição relativamente equilibrada.

Este perfil etário sugere que a amostra é predominantemente jovem, o que pode refletir as tendências de engajamento com o tema de estudo. A menor representatividade de participantes mais velhos pode indicar uma área de potencial expansão para pesquisas futuras, visando uma compreensão mais abrangente das diferentes perspectivas geracionais sobre o tema abordado neste trabalho.

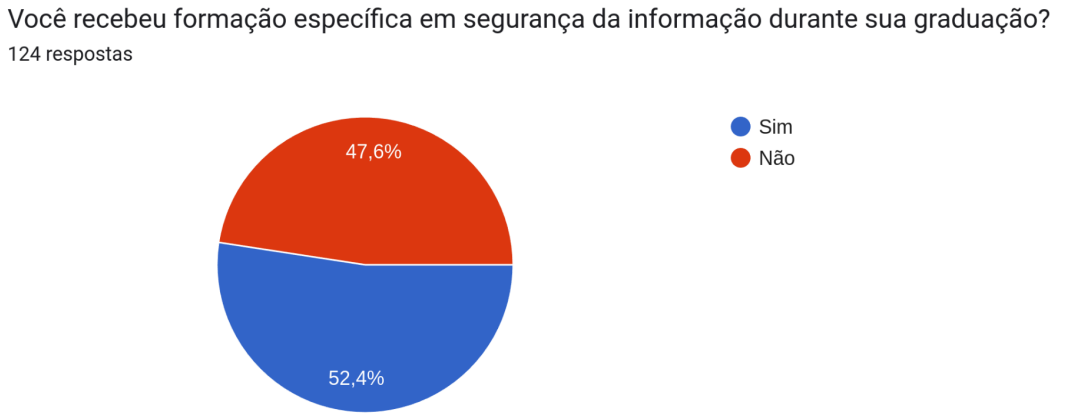


**Figura 3 - Formação em Segurança da Informação Durante Graduação**

O gráfico ilustra as respostas dos participantes à pergunta "Você recebeu formação específica em segurança da informação durante sua graduação?". Conforme os dados coletados, 52,4% dos entrevistados afirmaram ter recebido formação específica em segurança da informação durante seus estudos universitários, enquanto 47,6% indicaram que não receberam tal formação.

Essa distribuição quase equilibrada destaca uma lacuna significativa na inclusão da segurança da informação como parte essencial do currículo em cursos de graduação. A presença de uma maioria que não recebeu formação específica sugere a necessidade de revisões curriculares que incorporem mais profundamente aspectos de segurança da informação, considerando sua importância crescente no cenário tecnológico atual.

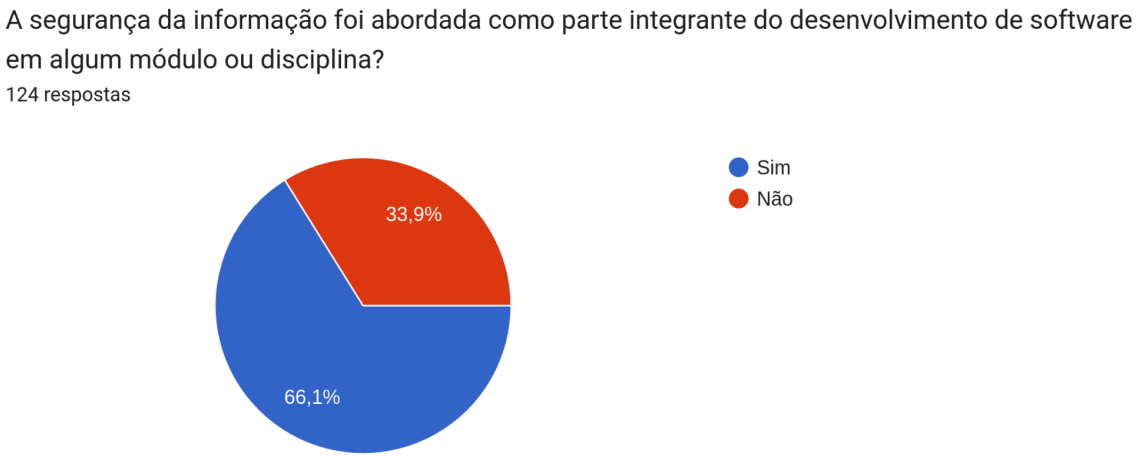


**Figura 4 - Integração da Segurança da Informação No Desenvolvimento de Software**

O gráfico apresenta as respostas à questão “A segurança da informação foi abordada como parte integrante do desenvolvimento de software em algum módulo ou disciplina?”. Nota-se que uma maioria de 66,1% dos participantes afirmou que sim, a segurança da informação foi incorporada como parte integrante do desenvolvimento de software durante sua formação. Em contraste, 33,9% dos entrevistados indicaram que não houve tal integração.

Este resultado reflete uma tendência positiva na educação de TI, onde dois terços dos respondentes reconhecem a inclusão da segurança da informação no processo de desenvolvimento de software. No entanto, a proporção significativa de 33,9% que não percebeu essa integração, destacando a necessidade de uma abordagem mais consistente e abrangente na educação em segurança da informação, assegurando que todos os futuros profissionais de software estejam equipados para enfrentar desafios de segurança no ambiente digital.

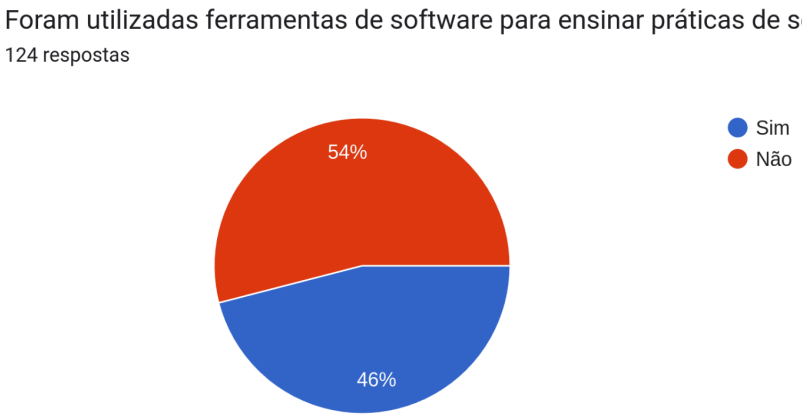


**Figura 5 - Uso de Ferramentas de Software no Ensino de Práticas de Segurança da Informação**

A pergunta investiga se foram utilizadas ferramentas de software para ensinar práticas de segurança da informação durante a graduação, e revela uma divisão quase igual entre as respostas. Aproximadamente 54% dos participantes indicaram que não houve utilização de ferramentas de software específicas para o ensino de segurança da informação, enquanto 46% afirmaram que tais ferramentas foram empregadas.

Essa distribuição mostra uma considerável falta de uniformidade no emprego de ferramentas tecnológicas dedicadas à educação em segurança da informação. A utilização de tais ferramentas é fundamental para uma aprendizagem prática e eficaz, indicando que, para quase metade dos respondentes, pode haver uma oportunidade perdida de engajamento mais concreto e aplicado das práticas de segurança. O fato de que mais da metade dos participantes não experienciou o uso de ferramentas software específicas ressalta a necessidade de uma integração mais robusta de recursos tecnológicos no currículo de TI, visando fortalecer a preparação dos estudantes para enfrentar desafios de segurança no ambiente profissional.

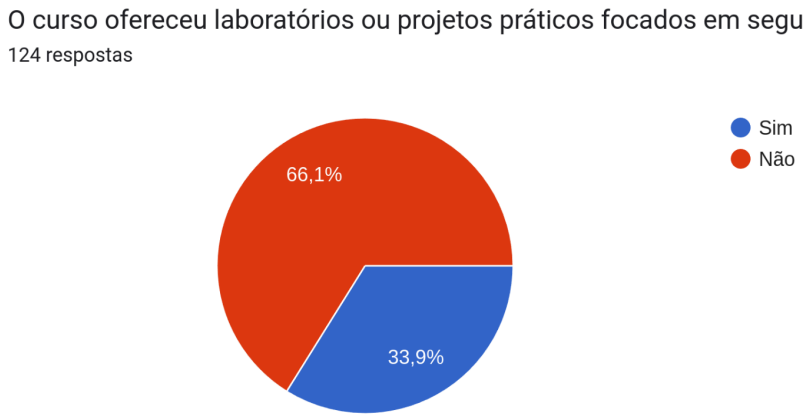


**Figura 6 - Oferta de Laboratórios ou Projetos Práticos em Segurança da Informação**

A pergunta analisa se os cursos ofereceram laboratórios ou projetos práticos focados em segurança da informação. Os resultados mostram que 66,1% dos participantes indicaram que seus cursos não ofereceram tais recursos práticos, enquanto 33,9% confirmaram a presença de laboratórios ou projetos práticos voltados para a segurança da informação.

As porcentagens destacam uma falta de equilíbrio precário na incorporação de práticas aplicadas em segurança da informação nos currículos acadêmicos. A presença de laboratórios e projetos práticos é crucial para uma compreensão profunda e aplicada do campo, sugerindo que uma proporção significativa de alunos pode estar saindo dos cursos sem a experiência prática necessária para enfrentar desafios reais na área de segurança da informação. Este resultado sublinha a importância de aumentar a oferta de atividades práticas nos cursos de TI, garantindo que todos os graduandos tenham a oportunidade de desenvolver habilidades críticas e práticas essenciais para sua futura carreira profissional.

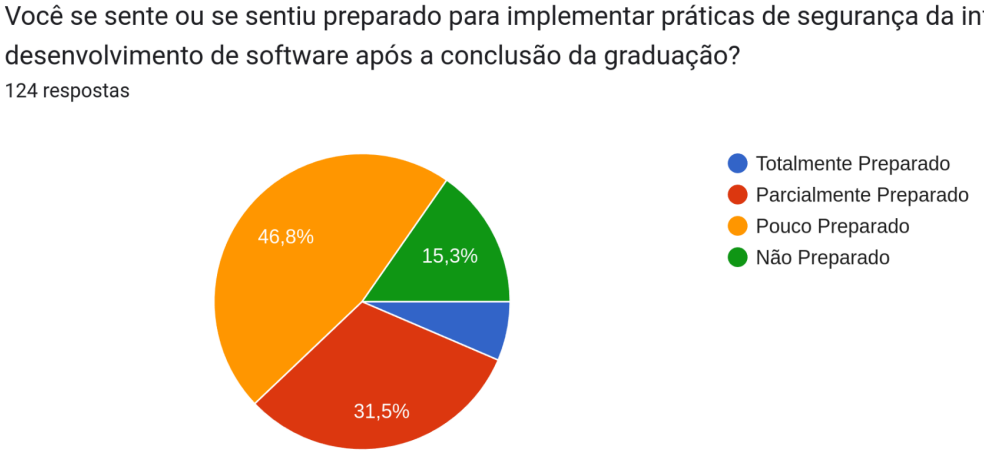


**Figura 7 - Preparação para Implementar Práticas de Segurança da Informação**

A pergunta examina a percepção dos participantes sobre sua preparação para implementar práticas de segurança da informação no desenvolvimento de software após a graduação. Os dados revelam uma distribuição preocupante: 46,8% dos entrevistados sentiram-se apenas "pouco preparados", 31,5% se consideraram "parcialmente preparados", e 15,3% afirmaram estar "não preparados". Apenas 6,5% dos participantes se sentiram "totalmente preparados".

Esta distribuição sugere que a maioria dos graduados não se sente adequadamente equipada para enfrentar os desafios da segurança da informação no contexto do desenvolvimento de software. Apenas uma pequena fração dos respondentes indicou sentir-se completamente preparada, o que levanta questões significativas sobre a eficácia dos currículos de TI em abordar as competências necessárias para a prática efetiva de segurança da informação. A falta de preparo apontada pela maioria dos participantes destaca a necessidade urgente de reformulações nos programas de estudo, com um foco maior em treinamento prático e teórico em segurança da informação, para melhor equipar os futuros profissionais para os desafios contemporâneos do setor.

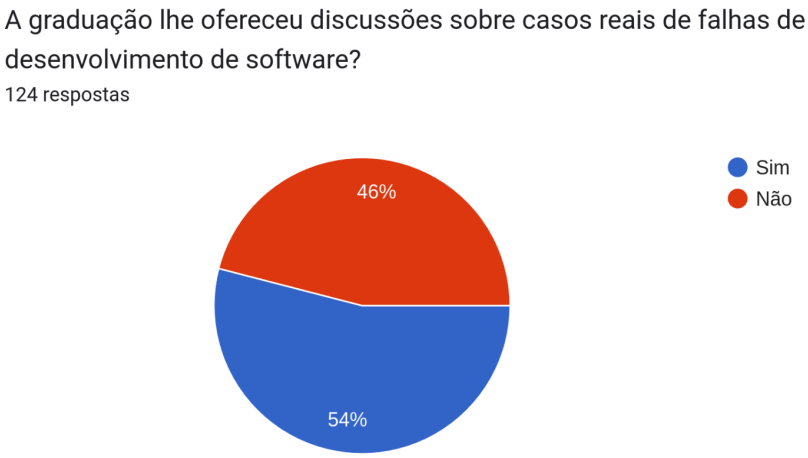


**Figura 8 - Discussões sobre Casos Reais de Falhas de Segurança no Desenvolvimento de Software**

O gráfico apresenta as respostas dos participantes à pergunta: "A graduação lhe ofereceu discussões sobre casos reais de falhas de segurança no desenvolvimento de software?" Segundo Schneier (2000, p. 45), "Examinar casos reais de falhas na segurança da informação é essencial porque nos permite entender como os sistemas falham e como os atacantes exploram as fraquezas, possibilitando o desenvolvimento de defesas melhores." Analisando o gráfico, uma ligeira maioria de 54% dos candidatos afirmou que sim, suas graduações incluíram discussões sobre casos reais de falhas de segurança, enquanto 46% dos participantes relataram que não tiveram essa oportunidade.

Este resultado indica que, embora mais da metade dos participantes tenha tido acesso a discussões enriquecedoras sobre falhas reais, ainda existe uma parcela significativa de alunos que concluiu o curso sem essa experiência vital. A análise de casos reais é essencial para compreender as complexidades e as implicações práticas da segurança da informação no desenvolvimento de software. A falta dessa exposição para quase metade dos respondentes sugere uma área de melhoria para os currículos de TI, visando fornecer uma formação mais completa e aplicada que prepare os estudantes de forma eficaz para os desafios reais do campo.


**Figura 9 - Colaboração com Profissionais de Segurança da Informação Durante a Graduação**

O gráfico aborda a questão: “Houve colaboração ou palestras de profissionais da área de segurança da informação durante a graduação?”. Uma maioria de 58,9% dos participantes relatou que não houve colaborações ou palestras de especialistas em segurança da informação em seus cursos, enquanto 41,1% confirmaram a presença de tais atividades.

Essa distribuição indica uma oportunidade perdida para a maioria dos alunos que não tiveram a chance de interagir com profissionais atuantes na área. A integração de especialistas como palestrantes ou colaboradores em programas acadêmicos é fundamental para oferecer insights práticos e atualizados sobre as tendências e desafios da segurança da informação. O fato de que uma parcela significativa de alunos não teve acesso a essas experiências destaca a necessidade de as instituições de ensino fortalecerem suas parcerias com o setor e enriquecerem seus currículos com mais interações práticas e profissionais, melhorando assim a preparação dos estudantes para os desafios do mercado de trabalho.

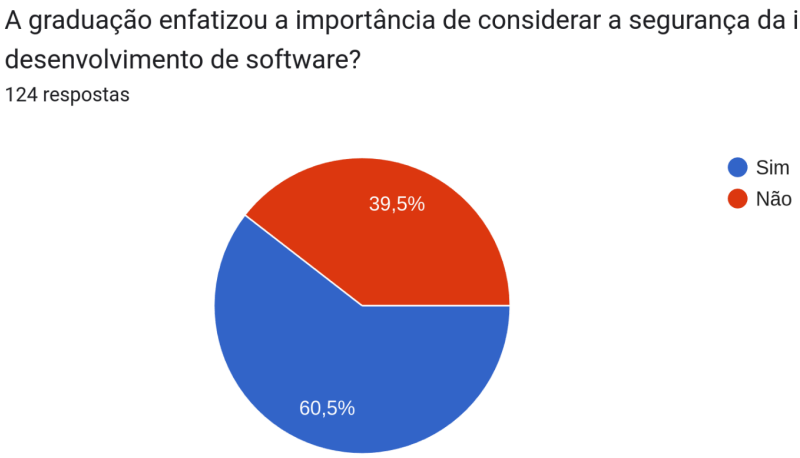


**Figura 10 - Enfatizando a Segurança da Informação desde o Início do Desenvolvimento de Software**

O gráfico mostra as respostas à pergunta "A graduação enfatizou a importância de considerar a segurança da informação desde o início do desenvolvimento de software?". Dos participantes, 60,5% afirmaram que sim, sua graduação destacou a necessidade de integrar práticas de segurança da informação desde as fases iniciais do desenvolvimento de software, enquanto 39,5% responderam que não.

Esses resultados indicam que, embora a maioria dos alunos tenha recebido algum nível de orientação sobre a importância da segurança desde o início do desenvolvimento de software, ainda há uma parcela considerável de graduandos que não percebeu essa ênfase durante sua formação. Este gap sugere uma área de melhoria para os cursos de TI, ressaltando a necessidade de fortalecer a integração da segurança da informação como um componente fundamental e não opcional do currículo. Tal ênfase é crucial para preparar profissionais capazes de desenvolver software que não apenas atenda às necessidades funcionais, mas que também seja resiliente contra ameaças de segurança.

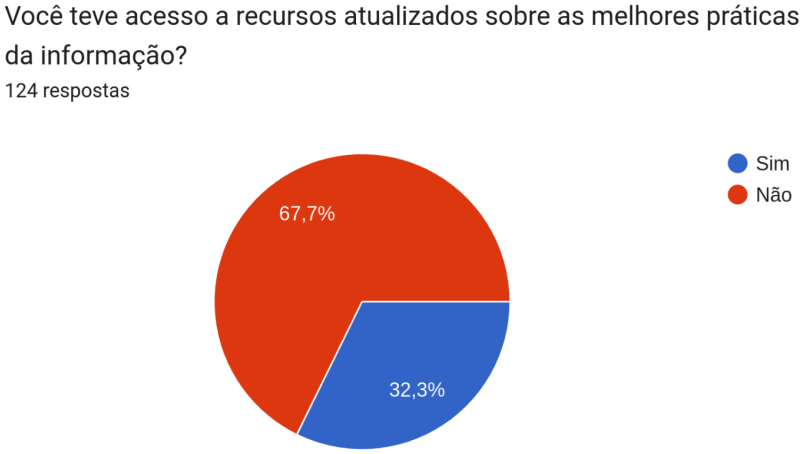


**Figura 11 - Acesso a Recursos Atualizados em Segurança da Informação**

O gráfico detalha as respostas dos participantes à pergunta: "Você teve acesso a recursos atualizados sobre as melhores práticas e ferramentas de segurança da informação durante sua graduação?" Uma significativa maioria de 67,7% dos respondentes relatou que não teve acesso a tais recursos, enquanto apenas 32,3% afirmaram que sim.

Essa predominância de respostas negativas revela uma lacuna preocupante na educação em segurança da informação dentro dos cursos de graduação em TI em desenvolvimento de software. O acesso a recursos atualizados é fundamental para a formação de profissionais que possam enfrentar eficazmente os desafios emergentes e as ameaças contínuas no campo da segurança cibernética. A falta de exposição a materiais recentes e relevantes pode comprometer significativamente a capacidade dos graduados de aplicar as melhores práticas e utilizar as ferramentas mais eficientes no mercado. Este resultado sublinha a necessidade urgente de as instituições de ensino revisarem e atualizarem seus currículos para incorporar e enfatizar recursos e ferramentas contemporâneos em segurança da informação, garantindo que os alunos estejam bem preparados para suas carreiras profissionais.

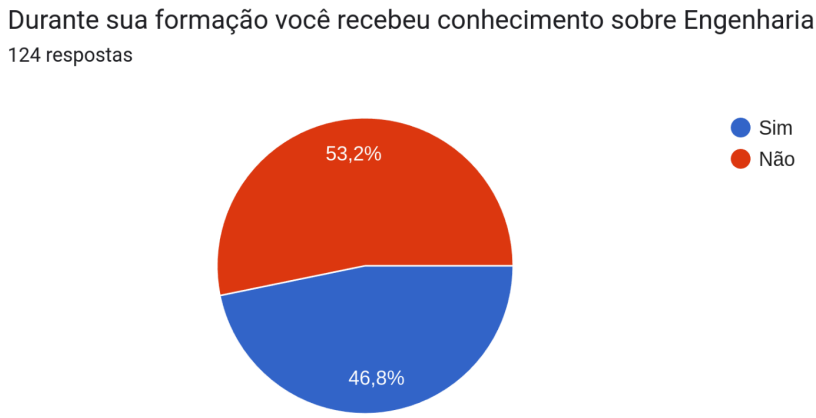


**Figura 12 - Educação sobre Engenharia Social na Formação Acadêmica**

O gráfico expõe as respostas dos participantes à pergunta: "Durante sua formação, você recebeu conhecimento sobre Engenharia Social?" Os resultados mostram que 46,8% dos entrevistados afirmaram ter recebido conhecimento sobre Engenharia Social, enquanto 53,2% responderam que não.

A predominância de respostas negativas aponta para uma lacuna significativa na educação de segurança da informação nas instituições de ensino. A engenharia social, sendo uma das técnicas mais prevalentes e insidiosas usadas em ataques cibernéticos, é fundamental para o currículo de qualquer curso focado em TI e segurança da informação. O fato de uma maioria dos formandos não ter sido adequadamente exposta a essas estratégias destaca a necessidade urgente de integrar mais profundamente o ensino de técnicas de manipulação psicológica e social nos programas de segurança da informação, preparando melhor os alunos para reconhecer e combater tais ameaças no ambiente profissional.

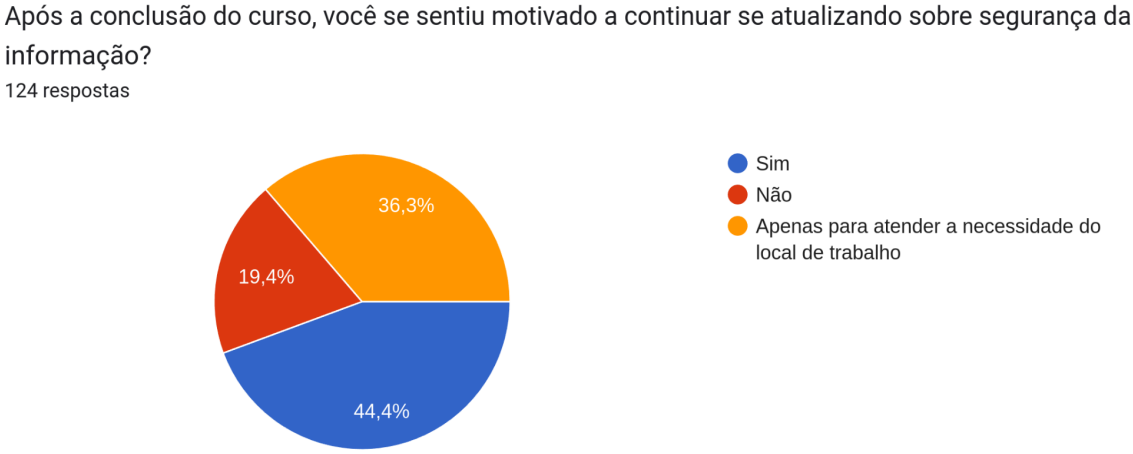


**Figura 13 - Motivação para Atualização Contínua em Segurança da Informação Pós-Graduação**

A pergunta questiona se os participantes se sentiram motivados a continuar se atualizando sobre segurança da informação após a conclusão de seus cursos. De acordo com os resultados, 44,4% dos entrevistados indicaram que sim, se sentiram motivados a manter-se atualizados independentemente de exigências externas. Por outro lado, 19,4% dos participantes responderam que não se sentiram motivados a seguir atualizando seus conhecimentos na área. Além disso, 36,3% dos respondentes mencionaram que se mantêm atualizados apenas para atender às necessidades de seus locais de trabalho.

Essa distribuição de respostas sugere que, embora uma parcela significativa dos graduados reconheça a importância de se manter atualizado em segurança da informação, uma grande parte dessa atualização é impulsionada principalmente por exigências profissionais, em vez de um interesse pessoal contínuo no campo. Isso ressalta a necessidade de programas de graduação não apenas equipar os alunos com habilidades técnicas, mas também inspirar um compromisso duradouro com o aprendizado e a adaptação contínuos na área de segurança da informação, vital para enfrentar o cenário de ameaças que evolui rapidamente.

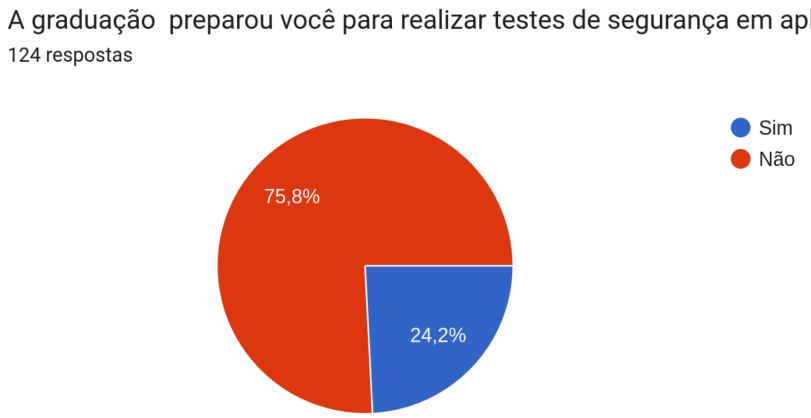


**Figura 14 - Preparação para Realizar Testes de Segurança em Aplicações de Software**

A pergunta analisa as respostas à pergunta "A graduação preparou você para realizar testes de segurança em aplicações de software?". A maioria dos participantes, representando 75,8%, afirmou que não se sentiram preparados para executar testes de segurança após a conclusão de seus cursos. Em contraste, apenas 24,2% dos entrevistados sentiram-se adequadamente preparados para essa tarefa crucial.

Este resultado destaca uma deficiência significativa nos currículos de formação em Tecnologia da Informação e Segurança da Informação. Testes de segurança são essenciais para identificar e mitigar vulnerabilidades em software antes que sejam exploradas por atores mal-intencionados. A falta de preparo adequado para realizar tais testes sugere que muitos programas de graduação podem não estar totalmente alinhados com as necessidades práticas e exigências do mercado de trabalho em segurança cibernética. Este achado reforça a necessidade de revisar e enriquecer os currículos universitários para incluir treinamento intensivo em técnicas de teste de segurança, garantindo que os futuros profissionais estejam mais bem equipados para proteger aplicações de software contra ameaças.

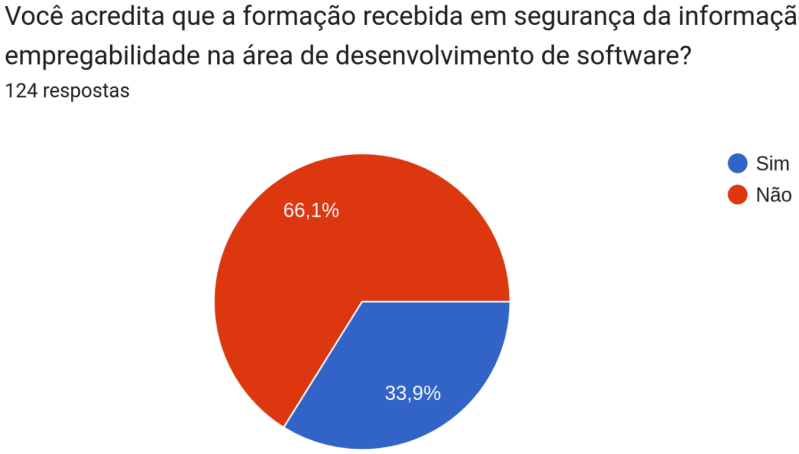


**Figura 15 - Contribuição da Formação em Segurança da Informação para a Empregabilidade em Desenvolvimento de Software**

O gráfico apresenta as respostas à pergunta: "Você acredita que a formação recebida em segurança da informação contribuiu para sua empregabilidade na área de desenvolvimento de software?". Os dados revelam que 66,1% dos participantes sentem que sua formação em segurança da informação não contribuiu significativamente para sua empregabilidade no campo do desenvolvimento de software, enquanto 33,9% acreditam que sim, houve uma contribuição positiva.

Essa maioria indica uma possível desconexão entre o conteúdo dos cursos de segurança da informação e as exigências do mercado de trabalho em desenvolvimento de software. A percepção de que a formação em segurança da informação não está alinhada com as necessidades práticas dos empregadores sugere a necessidade de uma revisão curricular que melhor integre conhecimentos de segurança da informação com habilidades práticas demandadas na indústria de software. Este ajuste curricular poderia potencialmente aumentar a relevância e a aplicabilidade das competências aprendidas, melhorando assim as perspectivas de emprego dos formandos.

## 5 CONSIDERAÇÕES FINAIS

Este estudo procurou explorar a eficácia da formação em segurança da informação nos cursos de desenvolvimento de software, revelando lacunas significativas entre a educação

oferecida e as necessidades práticas e contemporâneas do mercado de trabalho. A análise dos dados coletados indica que uma porcentagem considerável de graduados sente-se insuficientemente preparada para enfrentar os desafios da segurança da informação no ambiente profissional. Além disso, uma porcentagem grande das pessoas que responderam o questionário relatou uma falta de recursos educacionais atualizados, pouca exposição a casos reais de falhas de segurança, e uma insuficiente integração de práticas e teóricas em seus currículos.

A experiência prática permite aos profissionais de segurança da informação testar e refinar suas habilidades em ambientes controlados e reais. Isto inclui participar de simulações de ataque, gerenciar incidentes de segurança em tempo real e implementar soluções que protejam contra vulnerabilidades específicas. Esta aplicação prática ajuda a solidificar o entendimento teórico e a desenvolver uma intuição para identificar e responder a ameaças emergentes. Métodos de Obtenção de Experiência Prática como:

- Laboratórios e Simulações: Laboratórios de segurança cibernética onde os alunos possam praticar técnicas de hacking ético, análise forense, e outras metodologias de segurança em um ambiente seguro e controlado.
- Estágios e Colaborações com a Indústria: Estágios em empresas e organizações onde os estudantes possam trabalhar em projetos de segurança da informação reais, oferecendo uma experiência valiosa que não pode ser replicada em um ambiente de sala de aula.
- Competições de Hacking (CTFs): Competições de Capture The Flag (CTF) e outras competições de habilidades de segurança que ofereçam aos participantes desafios práticos que requer aplicação de conhecimentos para resolver problemas complexos de segurança.
- O engajamento com profissionais do setor e a análise de casos reais são componentes vitais na formação em segurança da informação. Estas interações enriquecem o aprendizado, fornecem insights valiosos e prepara os estudantes para enfrentar desafios reais no ambiente profissional.
- Mentoria e Orientação: Profissionais experientes servem como mentores, oferecendo orientação, compartilhando suas trajetórias de carreira e aconselhando sobre as melhores práticas e estratégias no campo da segurança da informação.

- Atualização sobre Tendências da Indústria: O contato com profissionais ajuda estudantes a se manterem atualizados sobre as últimas tendências, tecnologias e ameaças, o que pode vir a garantir que o aprendizado esteja alinhado com as necessidades atuais do mercado.
- Networking: Interagir com profissionais e estabelece conexões valiosas que possam abrir portas para oportunidades de estágio, emprego e futuras colaborações.

O Aprendizado Através de Casos Reais como:

- Aplicação Prática do Conhecimento: Estudar casos reais permite que os alunos vejam como as teorias e técnicas de segurança são aplicadas em situações reais, ajudando a solidificar o entendimento e a desenvolver habilidades práticas.
- Análise de Falhas e Sucessos: Os casos reais oferecem a oportunidade de analisar tanto as falhas quanto os sucessos, proporcionando conhecimento sobre o que funciona ou não em termos de medidas de segurança.
- Desenvolvimento de Pensamento Crítico: A resolução de problemas complexos apresentados em estudos de caso ajuda a desenvolver o pensamento crítico e a capacidade de tomada de decisão rápida e eficaz.

Alguns Métodos de Engajamento:

- Palestras e Workshops: Convidar profissionais para palestrar sobre temas específicos ou conduzir workshops práticos é uma forma de proporcionar a estudantes uma visão das operações de segurança da informação.
- Visitas Técnicas: Organizar visitas técnicas a empresas e centros de operações de segurança que permitam que os estudantes observem profissionais em ação e entendam o funcionamento interno de estratégias de segurança eficazes.
- Parcerias com Empresas: Estabelecer parcerias formais com empresas para projetos de pesquisa, desenvolvimento e treinamento prático para enriquecer significativamente o currículo e oferecendo experiências relevantes aos alunos.

Uma melhor Integração Curricular com (1) Cursos Interativos: Integrar o engajamento com profissionais e o estudo de casos reais como parte do currículo regular para garantir que todos os alunos tenham acesso a  experiências enriquecedoras;(2) Projetos Capstone: Incentivar

projetos finais envolvendo casos reais ou simulações próximas da realidade, orientados por profissionais do setor, para que os estudantes possam demonstrar a aplicação de seus aprendizados de maneira concreta e mensurável.

Os resultados deste trabalho sugerem que é de grande importância para as instituições de ensino revisarem e atualizarem seus programas de estudo para incluir uma formação mais robusta e alinhada com as dinâmicas do campo de segurança da informação. Isso inclui o desenvolvimento de currículos que não apenas abordem teorias de segurança da informação, mas que também integrem aplicações práticas através de laboratórios, projetos, e a colaboração com profissionais da área.

Ademais, a empregabilidade dos graduados, conforme indicado pelas respostas ao questionário, poderiam ser significativamente melhoradas pela incorporação de conhecimentos e habilidades em segurança da informação que são diretamente relevantes para os desafios do desenvolvimento de software moderno. Isso não apenas prepararia melhor os alunos para o mercado de trabalho, mas também contribuiria para a criação de softwares mais seguros e confiáveis.

Em conclusão, este estudo destaca a necessidade de uma mudança paradigmática na forma como a segurança da informação é ensinada dentro dos cursos de desenvolvimento de software. Há uma necessidade clara para que as instituições de ensino superior ampliem seu foco para além das habilidades técnicas básicas, adotando uma abordagem mais holística que prepare os estudantes para os desafios multifacetados do mundo real. Tal mudança não apenas beneficiará os futuros profissionais da área, mas também fortalecerá a infraestrutura tecnológica e a segurança da informação de forma global.

**REFERÊNCIAS**

BHATTACHARYA, H. Empirical Research. *In*: GIVEN, L. M. **The SAGE Encyclopedia of Qualitative Research Methods**. 1. ed. California: Sage Publications, v. 1 e 2, 2008. Cap. Entrada E, p. 253-255.

BRASIL. **Lei n.º 9.394, de 20 de dezembro de 1996.** Estabelece as diretrizes e bases da educação nacional. Diário Oficial da União, Brasília, DF, 23 dez. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9394.htm. Acesso em: 29 mar. 2024.

CABRAL, Carlos; CAPRINO, William. **Trilhas em Segurança da Informação:** Caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015.

FERREIRA, F. N. F.; ARAÚJO, M. T. D. **Políticas de Segurança da Informação:** Guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2008.

FLICK, U. **Uma introdução à pesquisa qualitativa**. Porto Alegre: Bookman, 2004.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 5. ed. São Paulo: Atlas, 1999.

HARGREAVES, A. **Os professores em tempos de mudança**. Lisboa: McGraw-Hill, 1998.

KNECHTEL, M. R. **Metodologia da pesquisa em educação:** uma abordagem teórico-prática dialogada. Curitiba: Intersaberes, 2014.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação com Internet**. Rio de Janeiro: LTC, 1999.

MARCONDES, F. R. S. **A nova Lei Geral de Proteção de Dados Pessoais:** Comentários à Lei n. 13.709/18. São Paulo: Thomson Reuters Brasil, 2021.

BRASIL. **Medida Provisória n° 954, de 2020.** Disponível em: http://planalto.gov.br/ccivil_03/_Ato2019-2022/2020Mpv/mpv954.htm. Acesso em: 29 mar. 2024.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

MINAYO, M. C. **O desafio da pesquisa social.** *In*: MINAYO, M. C. (Org.). Pesquisa social: teoria, método e criatividade. Rio de Janeiro: Vozes, 2009.

MITNICK, K. D.; SIMON, W. L. **The Art of Deception:** Controlling the Human Element of Security. Indianapolis: Wiley Publishing, Inc., 2002.

MITNICK, K. D.; SIMON, W. L. **A arte de enganar**. São Paulo: Pearson Education, 2003.

OLIVEIRA, Fátima Bayma de. **Tecnologia da informação e comunicação:** articulando processos, métodos e aplicações. Rio de Janeiro: E-papers, 2020.

OLIVEIRA, T. L. S. **A proteção de dados pessoais na Internet:** uma análise à luz da Lei Geral de Proteção de Dados Pessoais. São Paulo: Saraiva Educação, 2020.

PATTON, M. Q. **Qualitative Evaluation and Research Methods**. Newbury Park: Sage Publications, 2002.

PEREIRA, L. S. **A Lei Geral de Proteção de Dados (LGPD):** seus aspectos fundamentais. São Paulo: Novo Século Editora, 2019.

SAFFI, P. C. **Proteção de dados pessoais na era digital:** Lei Geral de Proteção de Dados Pessoais - LGPD. Rio de Janeiro: Forense, 2019.

SANDHU, R. S. **Educating the Next Generation of Information Security Professionals**. Information Security Journal: A Global Perspective, v. 22, n. 2, p. 61-66, 2013.

SÊMOLA, M. **Gestão da segurança da informação:** uma visão executiva. 2. ed. São Paulo: Elsevier, 2014.

SCHNEIER, Bruce. **Secrets and Lies:** Digital Security in a Networked World. New York: John Wiley & Sons, 2000.

SCHNEIER, Bruce. **Segurança.com:** segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001.

TAKAHASHI, Tadao. **Sociedade da informação no Brasil:** livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

QUEIROZ, Tânia D.; BRAGA, Márcia M. V.; LEICK, Elaine Penha. **Pedagogia de projetos interdisciplinares**. São Paulo: Rideel, 2008.

RUNESON, P.; HÖST, M. Guidelines for Conducting and Reporting Case Study Research in Software Engineering. **Empirical Software Engineering**, v. 14, n. 2, p. 131-164, 2008.

**Apêndice**

## Pesquisa de TCC em Segurança da Informação

### Consentimento para Participação em Pesquisa

Prezado(a) participante,

Você está sendo convidado(a) a participar de um estudo que visa investigar o suporte metodológico e ferramental orientado à segurança da informação no ensino prático de cursos de desenvolvimento de software. Este estudo busca compreender a experiência de ex-alunos e avaliar como a formação em segurança da informação impacta a prática profissional no desenvolvimento de software.

Sua participação envolverá:

- Responder a um questionário composto por perguntas fechadas. A estimativa de tempo para a conclusão é de 3 minutos.

Confidencialidade:

- As informações coletadas neste questionário serão utilizadas exclusivamente para fins acadêmicos relacionados a este estudo. Suas respostas serão tratadas com a máxima confidencialidade, e qualquer publicação resultante deste estudo não incluirá informações que possam identificar individualmente os participantes.

Consentimento:

- Ao prosseguir com o preenchimento do questionário, você concorda que suas respostas sejam utilizadas como parte deste estudo. Por favor, esteja ciente de que sua participação é voluntária, e você pode optar por retirar-se a qualquer momento.

Confirmação de Consentimento:

Eu li e entendi as informações acima. Estou ciente dos objetivos do estudo, da minha participação e dos usos das informações coletadas. Por meio desta, dou meu consentimento informado para que minhas respostas sejam utilizadas para fins deste estudo.

Aceite:

- ☐ Concordo
- ☐ Não Concordo

Por favor, selecione a faixa etária que melhor representa sua idade:

- ☐ Menos de 20 anos
- ☐ 20 a 29 anos
- ☐ 30 a 39 anos
- ☐ 40 a 49 anos
- ☐ 50 a 59 anos
- ☐ 60 anos ou mais

Você recebeu formação específica em segurança da informação durante seu curso?

- ☐ Sim
- ☐ Não

A segurança da informação foi abordada como parte integrante do desenvolvimento de software em algum módulo ou disciplina?

- ☐ Sim
- ☐ Não

Foram utilizadas ferramentas de software para ensinar práticas de segurança da informação?

- ☐ Sim
- ☐ Não

O curso ofereceu laboratórios ou projetos práticos focados em segurança da informação?

- ☐ Sim
- ☐ Não

Você se sente preparado para implementar práticas de segurança da informação no desenvolvimento de software após a conclusão do curso?

- ☐ Totalmente preparado
- ☐ Parcialmente preparado
- ☐ Pouco preparado
- ☐ Não preparado

O curso ofereceu discussões sobre casos reais de falhas de segurança no desenvolvimento de software?

- ☐ Sim
- ☐ Não

Houve colaboração ou palestras de profissionais da área de segurança da informação durante o curso?

- ☐ Sim
- ☐ Não

O curso enfatizou a importância de considerar a segurança da informação desde o início do desenvolvimento de software?

- ☐ Sim
- ☐ Não

Você teve acesso a recursos atualizados sobre as melhores práticas e ferramentas de segurança da informação?

- ☐ Sim
- ☐ Não

Durante sua formação você recebeu conhecimento sobre Engenharia social?

- ☐ Sim
- ☐ Não

Após a conclusão do curso, você se sentiu motivado a continuar se atualizando sobre segurança da informação?

- ☐ Sim

☐ Não

O curso preparou você para realizar testes de segurança em aplicações de software?

☐ Sim
☐ Não

Você acredita que a formação recebida em segurança da informação contribuiu para sua empregabilidade na área de desenvolvimento de software?

☐ Sim
☐ Não

Agradecemos sinceramente sua contribuição para este estudo. Sua experiência e percepções são valiosas para nós e para o avanço do conhecimento na área de desenvolvimento de software.

Atenciosamente,

Poliana Santos de queiroz
(87)999022492
Instituto Federal de Pernambuco - IFPE