Conhecimento, percepção e lacunas na formação prática em segurança da informação: um estudo com discentes universitários de tecnologia da UFC Campus Russas

Isis Nascimento de Lavor[1], Valéria Maria da Silva Pinheiro[1], Fernanda Ferreira do Nascimento[1], José Maria da Silva Monteiro Filho[1], Javam de Castro Machado[1]

[1]Universidade Federal do Ceará (UFC)
Caixa Postal 6001 – 60020-181 – Fortaleza – CE – Brazil

{isislavor, fernanda.nascimento}@alu.ufc.br, valeria.pinheiro@ufc.br,

{jose.monteiro, Javam.Machado}@lsbd.ufc.br

Abstract. *This study investigates the relationship between technical knowledge, risk perception, and information security behaviors among undergraduate Computer Science and Software Engineering students at brazilian Federal University. It starts from the premise that technical knowledge, while necessary, is not sufficient on its own to guarantee the consistent adoption of secure practices in digital environments. The research employed a mixed-methods approach, utilizing a structured questionnaire based on the HAIS-Q and SeBIS models. The results indicate that factors such as convenience, urgency, normalization of risk, and institutional limitations influence the adoption of insecure digital behaviors, even among students who are aware of the risks involved. It is concluded that strengthening the information security culture in higher technological education requires the implementation of continuous educational strategies with an emphasis on the human factor.*

Resumo. *Este estudo investiga a relação entre conhecimento técnico, percepção de risco e comportamentos de segurança da informação entre estudantes de graduação em Ciência da Computação e Engenharia de Software de uma Universidade Federal brasileira. Parte-se da premissa de que o conhecimento técnico, embora necessário, não é, por si só, suficiente para garantir a adoção consistente de práticas seguras em ambientes digitais. A pesquisa abordou métodos mistos, com aplicação de questionário estruturado baseado nos modelos HAIS-Q e SeBIS. Os resultados indicam que fatores como comodidade, pressa, normalização do risco e limitações institucionais influenciam a adoção de comportamentos digitais inseguros, mesmo entre estudantes que possuem conhecimento acerca dos riscos envolvidos. Conclui-se que o fortalecimento da cultura de segurança da informação no ensino superior tecnológico requer a implementação de estratégias educacionais contínuas, com ênfase no fator humano.*

1. Introdução

De acordo com Hoepers (2024), o ser humano deve ser reconhecido como o elo principal, e não meramente o mais fraco, na cadeia da cibersegurança. Sob essa ótica, os fatores humanos exercem influência direta na eficácia das estratégias de proteção digital, tornando fundamental a compreensão do comportamento dos usuários. No ambiente universitário, especialmente em cursos de tecnologia, presume-se que a imersão em infraestruturas especializadas e o domínio técnico sobre redes e sistemas garantam a adoção de práticas seguras. No entanto, observa-se frequentemente um distanciamento entre o saber teórico e a prática cotidiana, manifestado em comportamentos inseguros como o uso de senhas fracas ou a exposição em redes públicas.

A relevância dessa análise é acentuada pela crescente vulnerabilidade do setor educacional. Em 2024, o setor de Educação e Pesquisa foi o mais visado por cibercriminosos, com um aumento de 75% nos ataques em relação ao ano anterior [1]. Além disso, 79% das instituições de ensino superior foram alvo de *ransomware* em 2022 (Sophos, 2023). Apesar desse cenário crítico, pesquisas que investigam o comportamento de estudantes brasileiros diante de riscos digitais ainda são limitadas. Como destacam Ali et al. (2021), compreender o fator humano é essencial para o desenvolvimento de intervenções educacionais adaptadas às realidades locais.

Diante do exposto, este estudo busca compreender como estudantes de cursos de tecnologia de uma universidade pública lidam com os aspectos comportamentais da segurança da informação (SI). Para tanto, a pesquisa visa identificar o nível de conhecimento técnico dos discentes, analisar a percepção de vulnerabilidade e investigar a relação entre fatores individuais e a adoção de práticas seguras. O restante deste artigo está organizado como segue: a Seção 2 discute os trabalhos relacionados; a Seção 3 descreve os procedimentos metodológicos; a Seção 4 analisa os resultados e a Seção 5 encerra o trabalho com as conclusões.

2. Trabalhos relacionados

Estudos anteriores têm destacado que o conhecimento técnico, isoladamente, não assegura a adoção consistente de práticas seguras. Freire et al. (2020), em estudo realizado com profissionais de TI ($n = 13$) e usuários finais ($n = 52$) de uma instituição federal de ensino, identificaram diferenças entre as ameaças priorizadas pelos especialistas e os comportamentos cotidianos associados à ocorrência de incidentes. Os resultados ressaltam a influência do descuido e da ausência de treinamento, reforçando a necessidade de ações educativas contínuas voltadas ao fator humano.

Sob a perspectiva das características individuais, Henklain et al. (2024) investigaram as relações entre traços de personalidade, conhecimentos e práticas de cibersegurança. O estudo empregou instrumentos destinados à avaliação da personalidade, da desejabilidade social, do conhecimento técnico e de comportamentos autorrelatados. Os achados evidenciam a importância de considerar conjuntamente variáveis individuais e conhecimentos sobre temas como *phishing* e privacidade para compreender as práticas preventivas adotadas pelos usuários.

[1] Security Report 2025. Disponível em: `https://www.checkpoint.com/security-report/`. Acesso em: 18 jun. 2025.

Em contexto mais próximo ao desta pesquisa, Ferreira et al. (2025) analisaram a conscientização em cibersegurança de 199 estudantes brasileiros da área de Computação, considerando diferentes níveis de exposição educacional ao tema. Os autores observaram associação entre maior contato com conteúdos de cibersegurança e melhor desempenho, embora tenham identificado lacunas mesmo entre estudantes com múltiplas fontes de formação. Também verificaram um desalinhamento entre percepção e desempenho real, uma vez que parte dos participantes tendia a subestimar o próprio desempenho.

Embora os estudos apresentados abordem o fator humano sob as óticas da gestão, da personalidade e do desempenho técnico, persiste uma lacuna quanto à influência direta da percepção de risco e das barreiras comportamentais cotidianas na conversão do conhecimento em hábito. A presente pesquisa diferencia-se ao investigar como a subestimação do risco e a busca por comodidade neutralizam o domínio técnico, oferecendo uma análise qualitativa das justificativas dos estudantes que complementa as métricas quantitativas de conscientização até então exploradas na literatura nacional.

3. Metodologia

Esta pesquisa tem como objetivo analisar a relação entre conhecimento técnico, percepção de risco e comportamentos de segurança digital entre estudantes universitários dos cursos de Ciência da Computação e Engenharia de Software. Adotou-se uma abordagem quali-quantitativa, possibilitando uma compreensão mais ampla das práticas, percepções e dificuldades relatadas pelos participantes. Do ponto de vista metodológico, trata-se de uma pesquisa descritiva, desenvolvida por meio de *survey*, com coleta de dados realizada a partir da aplicação de um questionário estruturado.

A abordagem adotada segue o método hipotético-dedutivo, no qual, a partir de fundamentos teóricos sobre segurança da informação e comportamento humano diante de riscos cibernéticos, formulam-se hipóteses que são posteriormente confrontadas com os dados empíricos coletados.A revisão da literatura foi feita com buscas conduzidas prioritariamente no Portal de Periódicos da CAPES, de mecanismos de inteligência artificial e na Biblioteca Digital da Sociedade Brasileira de Computação (SOL/SBC). Foram considerados estudos nacionais e internacionais relevantes, publicados majoritariamente nos últimos dez anos, com exceção de obras clássicas amplamente consolidadas na literatura.

3.1. Definição das questões de pesquisa e do modelo teórico

Este estudo analisa a relação entre as variáveis: comportamento digital inseguro (variável dependente), conhecimento técnico (independente), percepção de risco (moderadora), conscientização (auxiliar) e perfil (controle). Enquanto a hipótese nula (H_0) prevê a ausência de correlação entre as variáveis, as hipóteses alternativas sugerem que a vulnerabilidade digital decorre do baixo conhecimento técnico (H_1) e da reduzida percepção de risco (H_2), além de apontarem a falta de conscientização (H_3) como fator determinante para atitudes inseguras, mesmo entre indivíduos com domínio técnico.

Para analisar as associações entre os índices (conhecimento, percepção de risco, conscientização e comportamento), utilizou-se o coeficiente de correlação de *Spearman* (ρ). A escolha deste método não paramétrico justifica-se pela natureza ordinal das escalas *Likert*, pela assimetria das distribuições e pelo tamanho reduzido da amostra, condições que inviabilizariam o uso da correlação de *Pearson*. A interpretação dos resultados

baseou-se na magnitude de ρ: valores próximos a 0,1 indicam associação fraca; 0,3, moderada; e 0,5 ou superiores, forte. O nível de significância adotado foi de 5% ($p < 0,05$).

3.2. Instrumento, coleta e análise de dados

O questionário foi desenvolvido na plataforma *Google Forms*[2] e construído a partir da adaptação de dois instrumentos consolidados na literatura de segurança da informação: o *Human Aspects of Information Security Questionnaire* (HAIS-Q) e a *Security Behavior Intentions Scale* (SeBIS). O HAIS-Q foi utilizado para fundamentar as dimensões de conhecimento teórico e prático, enquanto o SeBIS orientou a elaboração dos itens voltados à percepção de risco e às intenções comportamentais no cotidiano digital. A escolha e adaptação desses instrumentos justificam-se pela necessidade de avaliar não apenas o saber teórico dos estudantes, mas também a sua sensibilidade ao risco e a efetiva aplicação de hábitos seguros no ambiente acadêmico. A estrutura geral do instrumento, suas seções, métricas e temas abordados estão sintetizados na Tabela 1.

Tabela 1. Estrutura e detalhamento do questionário de pesquisa.

Seção/Dimensão	Instrumento base	Escala/Formato	Resumo dos temas e questões
1. Perfil demográfico e acadêmico	Elaboração própria	Múltipla escolha e campo aberto	Idade, gênero, curso (CC/ES), período, uso de laboratórios/Wi-Fi, contato prévio com segurança e histórico de incidentes (Q1 a Q19).
2. Conhecimento técnico	Adaptado do HAIS-Q	Objetiva (resposta única) e Likert (1 a 5)	Conhecimento sobre senhas fortes, *phishing*, atualização de software, uso de VPN/HTTPS, 2FA, identificação de links suspeitos e permissões (Q20 a Q30).
3. Percepção de risco	Adaptado do SeBIS	Likert (1=Discordo Totalmente a 5=Concordo Totalmente)	Vulnerabilidade percebida a golpes, riscos no Wi-Fi público da universidade, receio em computadores coletivos e medo de vazamento de dados (Q31 a Q36).
4. Conscientização em segurança	Adaptado do HAIS-Q e SeBIS	Frequência (1=Nunca a 5=Sempre)	Ações preventivas: atualização periódica, não salvar senhas em PCs públicos, uso de senhas distintas, bloqueio de tela e *logout* (Q37 a Q43).
5. Comportamentos digitais inseguros	Adaptado do SeBIS	Frequência (1=Nunca a 5=Sempre)	Hábitos de risco: reuso de senhas entre sistemas (SIGAA/Moodle), compartilhamento de credenciais, telas desbloqueadas e cliques em links suspeitos (Q44 a Q50).
6. Percepções qualitativas	Elaboração própria	Discursiva aberta	Motivações para práticas inseguras, papel da universidade na formação em segurança e recursos desejados pelos estudantes (Q51 a Q55).

A coleta de dados da pesquisa seguiu os princípios éticos que regem os estudos com seres humanos, conforme a Resolução nº 510/2016 do Conselho Nacional de Saúde.

[2]O formulário e as imagens complementares de resultados deste trabalho estão disponíveis em: `https://github.com/isislavor/tcc-ciberseguranca.git`

Todos os participantes foram convidados a participar de forma voluntária, anônima e consciente, mediante a aceitação do Termo de Consentimento Livre e Esclarecido (TCLE), apresentado no início do questionário online. A amostra foi não probabilística por conveniência, formada por participantes que responderam voluntariamente ao questionário *online*, divulgado e-mail institucional, redes sociais e grupos acadêmicos. A análise foi conduzida de forma mista: a etapa quantitativa utilizou *scripts* em *Python* para estatística descritiva, análises de grupos e correlações de *Spearman*, com suporte da biblioteca *Matplotlib* para visualização dos dados. Já a etapa qualitativa adotou uma abordagem indutiva e exploratória, organizando os relatos em categorias temáticas baseadas em padrões recorrentes de sentido. Essa integração permitiu confrontar métricas estatísticas com as percepções subjetivas dos participantes. A pesquisa reconhece limitações de generalização devido ao recorte específico e ao uso de amostragem por conveniência, que favorece o viés de autosseleção e a exclusão digital. Apesar dessas barreiras, o estudo destaca-se pela transparência e por oferecer uma base sólida para futuras investigações que busquem ampliar o escopo e integrar novas metodologias no campo da segurança da informação.

4. Resultados

4.1. Caracterização da amostra

A amostra foi composta por 31 estudantes, destes 67,7% (n = 21) dos participantes pertencem ao curso de Ciência da Computação, enquanto 32,2% (n = 10) estão matriculados em Engenharia de Software. Essa distribuição permite uma análise comparativa entre formações com estruturas curriculares semelhantes, porém com enfoques distintos. Em relação à faixa etária, 61,3% (n = 19) dos participantes encontra-se concentrada entre 21 e 24 anos, refletindo o perfil predominante de estudantes de graduação em cursos de tecnologia.

A presença majoritária de jovens adultos é relevante para a análise do comportamento digital, considerando que esse grupo apresenta elevado nível de exposição a ambientes digitais e uso intensivo de tecnologias no cotidiano acadêmico e pessoal.Quanto ao tempo de uso da internet por dia, os resultados indicam que 54,8% (n = 17) dos respondentes utiliza a internet por cerca de 6 a 8 horas diariamente. Esse dado sugere que os participantes possuem ampla familiaridade com o uso da internet, o que reforça a pertinência de investigar não apenas o conhecimento técnico formal, mas também os hábitos e comportamentos desenvolvidos ao longo do tempo. No que diz respeito ao contato prévio com conteúdos relacionados à segurança da informação, 51,6% (n = 16) dos participantes afirmaram já ter tido algum tipo de exposição ao tema, seja por meio de disciplinas acadêmicas, atividades complementares, eventos, cursos ou materiais informativos.

Ainda assim, uma parcela de 35,5% (n = 11) dos respondentes declarou não possuir contato prévio significativo e 12,9% (n = 4) declarou não se recordar de experiências formativas nessa área, indicando heterogeneidade no nível de formação específica em segurança da informação entre os estudantes. Por fim, ao serem questionados sobre experiências prévias com incidentes digitais, cerca de 41,9% (n = 13) dos participantes relatou já ter vivenciado, enquanto 58,1% (n = 18) afirmou nunca ter enfrentado esse tipo de ocorrência ou ter presenciado ocorrer apenas com terceiros. Esse resultado evidencia diferentes níveis de vivência prática com riscos cibernéticos, o que pode influenciar diretamente a percepção de risco e a adoção de comportamentos de segurança.

4.2. Resultados descritivos

A análise descritiva contemplou cinco dimensões: conhecimento técnico objetivo, conhecimento declarado, percepção de risco, conscientização em segurança da informação e comportamentos digitais inseguros. A Tabela 2 apresenta uma síntese das médias, medianas e desvios padrão observados em cada índice, permitindo uma visão geral dos resultados antes de sua análise individual.

Tabela 2. Resumo estatístico dos índices analisados

Dimensão	Média	Mediana	D. Padrão	Interpretação
Conhecimento técnico objetivo	4,23	5,00	1,09	Elevado
Conhecimento declarado	3,92	3,83	0,79	Moderado a elevado
Percepção de risco	4,05	4,17	0,74	Elevada
Conscientização em SI	4,35	4,43	0,54	Elevada
Comportamento digital inseguro	2,20	2,14	0,72	Baixo a moderado

Fonte: Dados da pesquisa (2025).

4.2.1. Conhecimento técnico em SI

O conhecimento técnico objetivo foi avaliado por meio de questões de múltipla escolha, nas quais os participantes deveriam identificar práticas corretas e incorretas relacionadas à segurança da informação, abrangendo temas como uso de senhas, autenticação, proteção de dados e reconhecimento de ameaças comuns. A análise do índice de conhecimento objetivo indica uma média de 4.23, com desvio padrão de 1.09, em uma escala de 1 a 5 (acertos por questão). Esse resultado evidencia um nível elevado de conhecimento técnico entre os estudantes participantes. A mediana igual a 5 reforça a concentração das respostas nos níveis mais altos da escala. Apesar do bom desempenho geral, observou-se dispersão moderada nos dados, com valores mínimos mais baixos. Esse resultado aponta para uma heterogeneidade no nível de conhecimento técnico, mesmo em uma amostra composta exclusivamente por estudantes da área de tecnologia da informação. De forma geral, os dados sugerem que os estudantes demonstram maior domínio sobre conceitos e práticas de segurança mais difundidos, enquanto lacunas podem persistir em aspectos que exigem maior aprofundamento técnico ou contextual.

Além do desempenho objetivo, os participantes foram convidados a avaliar o próprio nível de conhecimento em segurança da informação por meio de afirmações em escala *Likert* de cinco pontos, variando de discordo totalmente (1) a concordo totalmente (5). Os resultados indicam que a autoavaliação do conhecimento apresentou média de 3.92, com desvio padrão de 0.79, sugerindo uma percepção moderada a elevada do próprio domínio em segurança da informação. A distribuição das respostas concentrou-se nos níveis intermediários e superiores da escala, indicando que a maioria dos participantes considera possuir conhecimento satisfatório sobre o tema. Entretanto, ao comparar os resultados da autoavaliação com o desempenho nas questões objetivas, observa-se um desalinhamento parcial entre o conhecimento percebido e o conhecimento efetivamente demonstrado. Enquanto o índice de conhecimento objetivo apresentou média superior, a autoavaliação foi ligeiramente inferior, sugerindo que parte dos estudantes tende a subestimar ou não reconhecer plenamente seu próprio nível de conhecimento técnico.

4.2.2. Percepção de risco

A percepção de risco cibernético foi avaliada por meio de afirmações em escala *Likert* de cinco pontos, variando de discordo totalmente (1) a concordo totalmente (5). Os resultados indicam que o índice médio de percepção de risco foi de 4.05, com desvio padrão de 0.74. A mediana observada foi de 4.17, evidenciando concentração das respostas nos níveis superiores da escala. Esses valores apontam para uma percepção de risco elevada entre os estudantes participantes, sugerindo que, de modo geral, eles reconhecem a existência de ameaças relevantes no ambiente digital.

A dispersão relativamente baixa dos dados indica uma percepção de risco relativamente homogênea no grupo analisado, com poucos participantes apresentando valores muito distantes da média. Ainda assim, a presença de respostas em níveis intermediários revela que nem todos os estudantes se percebem igualmente vulneráveis, o que pode estar associado a diferenças individuais de experiência prévia, formação específica ou exposição a incidentes digitais. De forma geral, os resultados sugerem que os estudantes possuem consciência sobre os riscos associados ao uso de tecnologias digitais, reconhecendo a possibilidade de ocorrência de incidentes de segurança da informação.

4.2.3. Conscientização em segurança da informação

Os resultados indicam que o índice médio de conscientização foi de 4.35, com desvio padrão de 0.54. A mediana observada foi de 4.43, evidenciando forte concentração das respostas nos níveis mais altos da escala. Esses valores apontam para um elevado nível de conscientização em segurança da informação entre os estudantes participantes, sugerindo que, de modo geral, eles reconhecem a relevância do tema e demonstram atenção às questões relacionadas à proteção de dados e à segurança digital. A baixa dispersão dos dados indica um padrão relativamente homogêneo de respostas, com pouca variação entre os participantes. Esse resultado sugere que a conscientização em segurança da informação é amplamente compartilhada no grupo analisado, independentemente de diferenças individuais de curso, período acadêmico ou experiências prévias.

Entretanto, embora os elevados índices de conscientização indiquem reconhecimento da importância da segurança da informação, esse resultado não implica, necessariamente, a adoção consistente de comportamentos digitais seguros. Como apontado pela literatura, a conscientização representa uma condição necessária, mas não suficiente, para a mudança efetiva de comportamento. Assim, torna-se fundamental analisar, nas seções subsequentes, como esse elevado nível de conscientização se relaciona com a percepção de risco e, principalmente, com os comportamentos digitais efetivamente adotados pelos estudantes.

4.2.4. Comportamentos digitais inseguros

A análise descritiva indica que o índice médio de comportamento digital inseguro foi de 2.20, com desvio padrão de 0.72. A mediana observada foi de 2.14, sugerindo que, em média, os participantes relataram adotar práticas inseguras com frequência baixa a moderada. Esses valores indicam que, embora os comportamentos inseguros não sejam pre-

dominantes, eles estão presentes de forma recorrente no cotidiano digital dos estudantes. A dispersão moderada dos dados evidencia variações individuais relevantes, com alguns participantes apresentando níveis mais elevados de comportamento inseguro, enquanto outros relataram adoção mais consistente de práticas seguras. Esse resultado sugere que fatores individuais e contextuais exercem influência significativa sobre a forma como os estudantes lidam com a segurança da informação no uso diário das tecnologias.

Quando analisados em conjunto com os resultados das seções anteriores, observa-se um cenário caracterizado por uma aparente contradição: apesar dos elevados níveis médios de conhecimento técnico, percepção de risco e conscientização em segurança da informação, os estudantes ainda relatam a adoção de comportamentos digitais inseguros em determinadas situações. Esse achado reforça a premissa central desta pesquisa de que o conhecimento, por si só, não é suficiente para garantir práticas seguras de forma consistente. De forma sintética, os dados descritivos evidenciam que os participantes apresentam níveis elevados de conhecimento técnico, percepção de risco e conscientização em segurança da informação. Ainda assim, observa-se a presença de comportamentos digitais inseguros com frequência baixa a moderada, indicando um desalinhamento entre saber, perceber e agir. Esse resultado reforça a necessidade de análises relacionais mais aprofundadas, apresentadas na seção subsequente, a fim de investigar como essas dimensões se articulam entre si.

4.3. Análise de correlação entre os índices comportamentais

O índice de comportamentos digitais inseguros foi adotado como variável de referência nos cruzamentos, por representar o desfecho principal do estudo, isto é, a frequência com que os estudantes adotam práticas que podem expor informações, sistemas ou dados pessoais a riscos cibernéticos. A correlação entre o índice de conhecimento técnico objetivo e o índice de comportamentos digitais inseguros foi negativa e fraca ($\rho = -0,257$), não apresentando significância estatística ($\rho > 0,05$). Esse resultado indica que, embora haja uma tendência de redução de comportamentos inseguros à medida que o conhecimento técnico objetivo aumenta, não foi possível identificar uma associação consistente entre essas variáveis na amostra analisada.Em contraste, o índice de conhecimento técnico declarado apresentou uma correlação negativa moderada e estatisticamente significativa com o índice de comportamentos inseguros ($\rho = -0,448$; $\rho < 0,05$). Esse resultado sugere que estudantes que se percebem como mais conhecedores em segurança da informação tendem a relatar menor frequência de práticas digitais inseguras.

A percepção de risco também apresentou associação negativa moderada e estatisticamente significativa com os comportamentos inseguros ($\rho = -0,412; \rho < 0,05$). Esse achado indica que estudantes que se percebem mais vulneráveis a ameaças digitais tendem a adotar menos comportamentos de risco, reforçando a importância da percepção subjetiva na adoção de práticas seguras. Destaca-se a forte correlação negativa observada entre o índice de conscientização em segurança da informação e o índice de comportamentos digitais inseguros ($\rho = -0,675; p < 0,001$). Esse resultado, além de estatisticamente significativo, apresenta elevada magnitude, indicando que níveis mais altos de conscientização estão fortemente associados à redução da frequência de práticas inseguras entre os participantes.

4.4. Análises por grupos

- **Área de interesse:** A Figura 1 apresenta as médias dos índices por área de interesse profissional. Observa-se que os participantes interessados em Infraestrutura/Redes/DevOps e Segurança apresentaram, em geral, maiores níveis de conscientização e conhecimento, além de menores índices de comportamento digital inseguro. Em contrapartida, o grupo de UI/UX & Design apresentou a maior média de comportamento inseguro. De modo geral, a percepção de risco permaneceu elevada em todas as áreas analisadas.

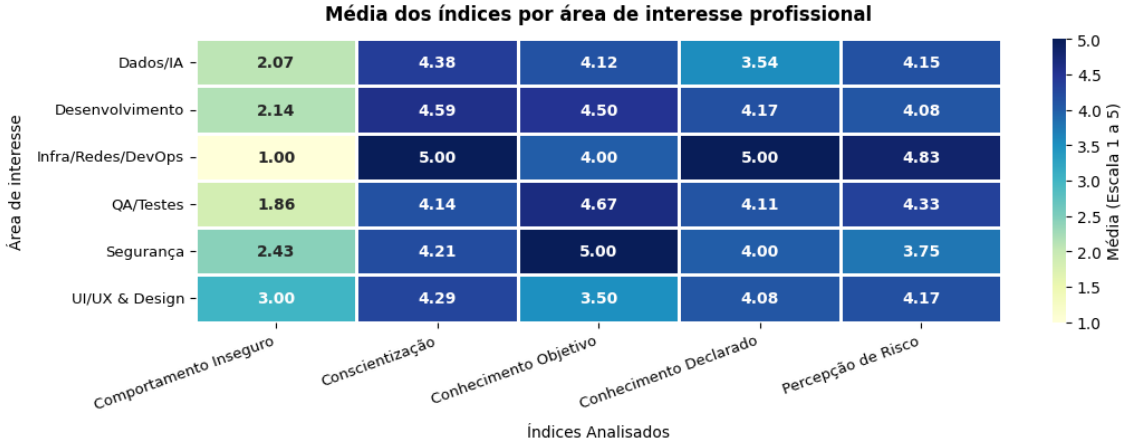

Figura 1. Mapa de calor das médias dos índices analisados segundo a área de interesse profissional.

- **Curso:** No recorte por curso, os resultados indicam médias bastante próximas entre estudantes de Ciência da Computação e Engenharia de Software em todos os índices analisados. Ambos os grupos apresentaram níveis elevados de conscientização e de percepção de risco, bem como médias semelhantes de comportamento inseguro, sugerindo que as diferenças curriculares não se refletiram nos comportamentos dos alunos.

- **Contato prévio com SI:** Os participantes que declararam ter cursado disciplinas ou participado de atividades formativas na área (n = 11) apresentaram média ligeiramente superior no índice de conhecimento técnico objetivo (-x = 4,55; dp = 0,82) quando comparados aos estudantes que não tiveram contato prévio (n = 16; $\bar{x}$ = 4,13; dp = 1,20) e àqueles que não se lembravam (n = 4; $\bar{x}$ = 3,75; dp = 1,26). Entretanto, as médias do índice de comportamento digital inseguro mostraram-se semelhantes entre os grupos: 2,22 (dp = 0,83) para os participantes com contato prévio, 2,20 (dp = 0,58) para os que não tiveram contato e 2,14 (dp = 1,08) para os que não se lembravam. Padrão semelhante foi observado no índice de conscientização em segurança da informação.

4.5. Resultados qualitativos

A análise qualitativa permitiu organizar as percepções dos estudantes em quatro categorias centrais: Comodidade e Praticidade, que destaca como a pressa e a busca por agilidade levam à reutilização de senhas e à rejeição de protocolos como o 2FA; Subestimação do Risco, onde a ausência de incidentes prévios gera um excesso de confiança e uma falsa sensação de invulnerabilidade; Formação Insuficiente, que aponta lacunas curriculares e

um ensino de segurança fragmentado ou superficial; e Dificuldade de Habitação, que revela a barreira entre o saber técnico e a prática cotidiana devido a barreiras operacionais, ao esforço cognitivo e unindo esses pontos, os resultados indicam que o comportamento inseguro é multicausal, envolvendo fatores comportamentais e contextuais, e geram uma expectativa por maior intervenção institucional da universidade por meio de disciplinas e campanhas educativas. Por fim, exemplos dessas percepções estão detalhados na Tabela 3, enquanto o conjunto completo de respostas, dados tratados e os *scripts* de análise encontram-se preservados e disponíveis para consulta no repositório público da pesquisa.

Tabela 3. Exemplos de respostas abertas por categoria temática

Categoria	**Excerto da resposta (anonimizado)**
Comodidade e praticidade	"Por comodidade, às vezes a gente prefere usar a mesma senha ou deixar a conta logada para não perder tempo."
Subestimação do risco	"Muitos acreditam que nada vai acontecer, porque nunca tiveram problemas antes."
Formação insuficiente	"Nunca tive disciplina específica sobre segurança da informação, só palestras bem superficiais."
Dificuldade de manter hábitos	"Sei que usar senhas diferentes é o certo, mas é difícil lembrar de todas."

Fonte: Dados da pesquisa (2025).

5. Conclusão

Os resultados indicam que o conhecimento técnico objetivo não apresentou associação estatisticamente significativa com a frequência de comportamentos digitais inseguros. Esse achado sugere que o simples domínio conceitual sobre SI não é suficiente para garantir a adoção consistente de práticas seguras no cotidiano digital, mesmo entre estudantes da área de tecnologia. Dessa forma, H_1 não foi confirmada pelos dados empíricos. Em contraste, observou-se que a percepção de risco cibernético e, principalmente, a conscientização em segurança da informação apresentaram associações negativas e estatisticamente significativas com os comportamentos inseguros. Tais achados sugerem a confirmação de H_2 e H_3, destacando-se a forte correlação entre conscientização e comportamento digital. Isso evidencia que estudantes mais conscientes e sensíveis ao risco tendem a adotar menos práticas inseguras, reiterando que a falta de conscientização é o fator determinante para atitudes vulneráveis, mesmo entre indivíduos com domínio técnico.

A análise qualitativa reforçou esses achados ao revelar que a adoção de práticas inseguras está frequentemente associada à comodidade, à pressa, à subestimação dos riscos e à dificuldade de manter hábitos seguros no dia a dia. Além disso, os participantes apontaram lacunas na formação acadêmica, caracterizada por abordagens pontuais e pouco integradas ao currículo, bem como expressaram a expectativa de maior atuação institucional por meio de disciplinas, oficinas, palestras e ações contínuas de conscientização. Como contribuição, este estudo amplia a compreensão sobre o chamado *gap* entre conhecimento e comportamento em segurança da informação no contexto universitário, evidenciando que saber o que é seguro não implica, necessariamente, agir de forma segura. Ao focar em um público em formação técnica, a pesquisa fornece subsídios relevantes para reflexões sobre práticas pedagógicas, políticas institucionais e estratégias educativas voltadas à promoção de uma cultura de segurança da informação mais efetiva.

6. Agradecimentos

A autora agradece à Lenovo pelo apoio à Residência do Projeto Connor, realizada por meio de investimentos da Lei de Informática, no âmbito do MCTI. Parte deste trabalho foi desenvolvido durante o período de formação da autora no referido projeto.

7. Declaração sobre uso de Inteligência Artificial

Os autores declaram que utilizaram ferramentas de Inteligência Artificial generativa como apoio à revisão textual, correção gramatical e aprimoramento da redação acadêmica do manuscrito. O uso dessas ferramentas não substituiu a análise crítica, interpretação dos resultados, elaboração metodológica ou produção intelectual dos autores, que permanecem integralmente responsáveis pelo conteúdo, originalidade e conclusões apresentadas neste trabalho.

Referências

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2):179–211. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/074959789190020T. Acesso em: 26 jun. 2025.

Alam, S. (2022). Cybersecurity: Past, present and future. arXiv preprint arXiv:2207.01227v3. Disponível em: https://arxiv.org/abs/2207.01227. Acesso em: 18 jun. 2025.

Alexandre Júnior, J. C. (2019). Cibercrime: um estudo acerca do conceito de crimes informáticos. *Revista Eletrônica da Faculdade de Direito de Franca*, 14(1):341–351. Disponível em: https://revistas.unifacef.com.br/index.php/REFAFI/article/view/602. Acesso em: 24 jun. 2025.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., and Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, 11(8). Disponível em: https://www.mdpi.com/2076-3417/11/8/3383. Acesso em: 18 jun. 2025.

Alves, R. N., Alves, J. M. H., Vasconcelos, I. O., and Cruz, C. A. B. d. (2024). Fator humano na segurança da informação: um mapeamento dos comportamentos de risco no ambiente digital. *Texto Livre*, 17:e51184. Disponível em: https://periodicos.ufmg.br/index.php/textolivre/article/view/51184. Acesso em: 18 jun. 2025.

Bardin, L. (2015). *Análise de conteúdo*. Edições 70, Lisboa, 1 edition.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br) (2024). *Cartilha de Segurança para Internet*. NIC.br – Núcleo de Informação e Coordenação do Ponto BR, São Paulo, 14 edition. Disponível em: https://cartilha.cert.br/. Acesso em: 18 jun. 2025.

CHECK POINT SOFTWARE TECHNOLOGIES (2025). Security report 2025. Disponível em: https://www.checkpoint.com/security-report/. Acesso em: 18 jun. 2025.

COMPUTAÇÃO BRASIL (2024). Computação Brasil – número 52. Disponível em: https://journals-sol.sbc.org.br/index.php/comp-br/issue/view/326. Acesso em: 18 jun. 2025.

CONSELHO NACIONAL DE JUSTIÇA (CNJ) (2023). *Cartilha de Segurança da Informação*. CNJ, Brasília. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2023/06/cartilha-seguranca-da-informacao-2023.pdf. Acesso em: 18 jun. 2025.

Egelman, S., Harbach, M., and Peer, E. (2016). Behavior ever follows intention? a validation of the security behavior intentions scale (sebis). In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '16, pages 5257–5261, New York, NY, USA. Association for Computing Machinery. Disponível em: https://doi.org/10.1145/2858036.2858265. Acesso em: 18 jun. 2025.

Ferreira, V., OliveiraJr, E., Zarpelão, B., and Zorzo, A. (2025). Characterizing cybersecurity awareness among brazilian computer science higher education students. In *Anais do XXXIII Workshop sobre Educação em Computação*, pages 63–74, Porto Alegre, RS, Brasil. SBC. Disponível em: https://sol.sbc.org.br/index.php/wei/article/view/36155. Acesso em: 18 jun. 2025.

FORTINET (2023). Resumo da pesquisa global sobre conscientização e treinamento em segurança de 2023. Disponível em: https://brasiline.com.br/wp-content/uploads/2023/06/brasiline-relatorio-fortinet-conscientizacao-e-treinamento-em-2023.pdf. Acesso em: 18 jun. 2025.

Freire, R. F. P., Silva, H. C. C., Queiroz, R. G., and Batista, A. A. M. (2020). O fator humano como uma vulnerabilidade em segurança da informação. *Revista Brasileira de Administração Científica*, 11(3):147–164. Disponível em: https://sustenere.inf.br/rbadm/article/download/3902/2190. Acesso em: 18 jun. 2025.

Henklain, M., Lobo, F., Feitosa, E., Cavalcante, L., Alencar, J., Bríglia, V., Araújo, G., and Alves, G. (2024). Caracterização de conhecimentos e comportamentos de cibersegurança: Estudo exploratório com dados predominantes do extremo norte brasileiro. In *Anais do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*, pages 76–91, Porto Alegre, RS, Brasil. Sociedade Brasileira de Computação. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/30018. Acesso em: 18 jun. 2025.

Hintzbergen, J., Hintzbergen, K., Smulders, A., and Baars, H. (2018). *Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002*. Brasport, Rio de Janeiro, 1 edition. Disponível em: https://www.amazon.com.br/dp/8574528609. Acesso em: 18 jun. 2025.

Hoepers, C. (2024). A importância dos fatores humanos para a cibersegurança. *Computação Brasil*, (52):61–66. Disponível em: https://journals sol.sbc.org.br/index.php/comp-br/article/view/4604. Acesso em: 17 jun. 2025.

KASPERSKY (2025). What is cybersecurity? definition, types, threats and tips. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-cybersecurity. Acesso em: 27 jun. 2025.

MIT TECHNOLOGY REVIEW BRASIL (2025). Mit technology review brasil – maior plataforma de tecnologia e inovação no brasil. Disponível em: https://mittechreview.com.br/. Acesso em: 27 jun. 2025.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T. (2017). The human aspects of information security questionnaire (haisq): Two further validation studies. *Computers & Security*, 66:40–51. Disponível em: https://www.sciencedirect.com/science/article/pii/S0167404817300081. Acesso em: 18 jun. 2025.

Silva, L. G. L. d. (2024). Segurança cibernética no brasil: uma análise dos fatores institucionais que precedem a política de segurança cibernética entre 2008–2020. Disponível em: https://dspace.unila.edu.br/handle/123456789/8528. Acesso em: 18 jun. 2025.

Slovic, P. (2016). The perception of risk. In Sternberg, R. J., Fiske, S. T., and Foss, D. J., editors, *Scientists Making a Difference: One Hundred Eminent Behavioral and Brain Scientists Talk About Their Most Important Contributions*, pages 179–182. Cambridge University Press, Cambridge. Disponível em: https://www.cambridge.org/core/books/scientists-making-a-difference/perception-of-risk/C1A877478096CC44F59E923C41775E02. Acesso em: 26 jun. 2025.

SOPHOS (2023). The state of ransomware in education 2023. Disponível em: https://www.sophos.com/pt-br/press/press-releases/2023/07/the-state-of-ransomware-in-education. Acesso em: 18 jun. 2025.

Takeuchi, E. C. (2023). Fatores humanos em cibersegurança: uma revisão sistemática da literatura. Disponível em: https://repositorio.ufu.br/handle/123456789/36792. Acesso em: 27 jun. 2025.

Tolah, A., Furnell, S. M., and Papadaki, M. (2019). A comprehensive framework for understanding security culture in organizations. In Drevin, L. and Theocharidou, M., editors, *Information Security Education – WISE 12: 12th IFIP WG 11.8 World Conference*, volume 562 of *IFIP Advances in Information and Communication Technology*, pages 143–156, Cham. Springer. Disponível em: https://ro.ecu.edu.au/ecuworkspost2013/6513/. Acesso em: 26 jun. 2025.

Vance, A., Siponen, M., and Pahnila, S. (2012). Motivating is security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3-4):190–198. Disponível em: https://psycnet.apa.org/record/2012-12998-008. Acesso em: 16 jun. 2025.