Caracterização de conhecimentos e comportamentos de cibersegurança: Estudo exploratório com dados predominantes do extremo norte brasileiro

Marcelo H. Oliveira Henklain[1], Felipe Leite Lobo[1], Eduardo Luzeiro Feitosa[2], Luiz G. Dallagnol Cavalcante[1], José V. Rocha de Alencar[1], Vitor J. Carneiro Bríglia[1], Guilherme Miranda de Araújo[1] e Guilherme da Silva Alves[1]

[1]Departamento de Ciência da Computação – Universidade Federal de Roraima – Boa Vista – Roraima – Brasil

[2]Instituto de Ciência da Computação – Universidade Federal do Amazonas – Manaus – Amazonas – Brasil

{marcelo.henklain, felipe.lobo}@ufrr.br, efeitosa@icomp.ufam.edu.br, {gugadcavalcante, victorbvbr, vitorjordao8762, guimiranda2003, lirioberto}@gmail.com

Abstract. *Despite the importance of the human factor in cybersecurity, research in this direction is scarce. Therefore, our objective was to characterize cybersecurity knowledge and behaviors, assessing their relationship with the Big Five personality factors. A total of 232 Brazilians, mostly from the northern region, participated. We observed higher scores in agreeableness and openness, and lower neuroticism. The knowledge level ranged from "moderate to good" and the frequency of cybersecurity behaviors was low. We found evidence of an association between personality traits and cybersecurity knowledge and behavior. Future studies are needed to include a more diverse sample.*

Resumo. *Embora o fator humano seja crucial na cibersegurança, as pesquisas nessa direção são escassas. Por isso, o nosso objetivo foi caracterizar conhecimentos e comportamentos de cibersegurança, avaliando a sua relação com os cinco grandes fatores de personalidade. Participaram 232 brasileiros, majoritariamente, da região norte. Observamos escores mais elevados de amabilidade e abertura, e baixo neuroticismo. O conhecimento foi de "moderado a bom" e a frequência de comportamento de cibersegurança foi baixa. Encontramos evidências de associação entre traços de personalidade e conhecimento e comportamento de cibersegurança. Estudos futuros devem contemplar uma amostra mais diversa.*

1. Introdução

O fator humano precisa ser considerado nos estudos sobre cibersegurança porque a tecnologia é produzida por e para pessoas [Guilherme et al., 2021; Hoepers, 2024]. É crucial entender como elas se comportam diante dos sistemas e das políticas de segurança e por qual motivo agem assim [Parsons et al., 2017; Aljohani et al., 2020; Alanazi et al., 2022]. Esse conhecimento pode contribuir para o desenvolvimento de sistemas mais robustos e com políticas de segurança mais efetivas [Hartwig and Reuter, 2021].

Historicamente, a literatura de cibersegurança tem considerado o usuário como o elo frágil da segurança por ele não agir conforme as expectativas do desenvolvedor

[Švábenský et al., 2020; Guilherme et al., 2021]. Os dados mostram que as pessoas, tipicamente, não adotam boas práticas de criação e uso de senhas [Aljohani et al., 2020], tendem a ser enganadas por ataques de *phishing* [Syafitri et al., 2022] e, dificilmente, têm consciência do quanto sua conduta na Internet pode ser monitorada por técnicas como *cookies* e *fingerprinting* [Li et al., 2023]. Precisamos, portanto, investigar como sistemas e políticas podem ajudar usuários a criar e utilizar senhas fortes, evitar *phishing* e proteger a privacidade [Ruoslahti et al., 2021].

Apesar da urgência, poucos estudos caracterizam ou buscam entender os fatores humanos na cibersegurança [Rahman et al., 2021], especialmente, no Brasil [Soares et al., 2020]. Especificamente, a literatura sobre a relação entre personalidade e comportamentos de cibersegurança é escassa. Isso ocorre mesmo diante de seu potencial para a customização de intervenções educacionais e de campanhas sobre boas práticas de segurança, identificação de perfis de personalidade com maior probabilidade de exibir comportamentos inseguros e recomendação de ações de proteção baseada na personalidade do usuário [Kennison and Chan-Tin, 2020]. Por esse motivo, o nosso objetivo foi caracterizar conhecimentos e comportamentos de cibersegurança, avaliando a sua relação com a personalidade. Para tanto, conduzimos estudo exploratório do tipo *survey* com brasileiros maiores de 18 anos. Nosso estudo inova por meio da criação preliminar de instrumentos para pesquisas em cibersegurança e pelas análises propostas, envolvendo a Teoria dos Cinco Grandes Fatores de personalidade.

2. Fundamentação teórica

2.1. Cibersegurança e o Fator humano

A Cibersegurança é uma subárea da Ciência da Computação que busca proteger um computador ou sistema contra acessos não-autorizados ou tentativas de desvirtuar a sua finalidade precípua [Rahman et al., 2021]. Em última instância, busca proteger o usuário de computador ou sistema.

Mais do que soluções técnicas no âmbito da computação, essa área precisa considerar como o usuário usa o computador e em que medida age conforme recomendado, para garantir o seu adequado funcionamento. Precisa, então, promover o comportamento de cibersegurança, que consiste em evitar ou atenuar ameaças virtuais [Alanazi et al., 2022]. Nesse cenário, o conhecimento sobre personalidade pode ser útil.

2.2. Personalidade humana

Genericamente, a personalidade pode ser entendida como conjuntos de comportamentos apresentados com certa regularidade e que distinguem as pessoas entre si. Para explicar esses comportamentos, é importante considerar a história evolutiva da espécie, a história individual de cada pessoa e a história cultural [Banaco et al., 2012]. De modo específico, a Psicologia possui diversas abordagens para o estudo da personalidade. A Teoria dos Cinco Fatores (TCF) é uma delas e, segundo Mansur-Alves e Saldanha-Silva (2019), consiste em uma das contribuições mais promissoras porque conta com 30 anos de pesquisas empíricas e evidências de sua validade obtidas em mais de 50 países. Por isso adotamos essa teoria como referência para orientar o nosso estudo.

A TCF propõe que humanos possuem cinco tendências básicas de personalidade, cuja origem está na história evolutiva da espécie e que podem ser detalhadas em termos de facetas (características mais específicas). Essas tendências contemplam predisposições

e sensibilidades a estímulos que podem favorecer ou dificultar aprendizagens ao longo da vida, impactando na formação da personalidade. As cinco tendências são: Neuroticismo: grau de instabilidade emocional e suscetibilidade a eventos aversivos; Extroversão: tendência a exploração do ambiente e interação com pessoas; Amabilidade: busca por relacionamentos interpessoais profundos; Conscienciosidade: controle comportamental para realizar tarefas; e Abertura a novas experiências: busca por novas experiências e apreço pela novidade. Para a TFC, a interação entre 'tendências básicas e aprendizagens' com 'condições do corpo e do ambiente em determinado momento', ajuda a entender comportamentos e, portanto, a personalidade. Mensurar essas tendências básicas é útil para compreendermos mais sobre as probabilidades de emissão de comportamentos.

3. Trabalhos relacionados

Apresentamos nesta seção estudos que caracterizam o comportamento de cibersegurança ou buscam compreendê-lo. Eles explicitam lacunas no conhecimento que justificam o problema de pesquisa que selecionamos. Cain et al. (2018), por exemplo, investigaram o conhecimento e comportamento de cibersegurança de 268 participantes (92% dos EUA). Foi observado que os usuários utilizam antivírus atualizados, mas não realizam escaneamentos regulares. A maioria compartilha dados pessoais sensíveis em redes sociais digitais e não verificam as configurações de privacidade. Usuários mais velhos são mais prudentes que os jovens, e homens têm mais conhecimento sobre cibersegurança do que mulheres, embora não exista diferença de gênero em termos de conduta segura. Concluiu-se que, tipicamente, usuários não adotam comportamentos de cibersegurança.

Em um dos poucos estudos brasileiros nessa linha, Guilherme et al. (2021) avaliaram 207 internautas, tipicamente, jovens e sem treinamento em cibersegurança, com mais de 12h diárias na Internet. Verificou-se que a pandemia por Covid-19 intensificou o uso da Internet e que mais de 70% dos internautas já fizeram *download* de programas suspeitos, mais de 55% compartilharam celular ou computador, mais de 41% compartilharam conta pessoal, mais de 29% compartilharam dados de cartão crédito em *app* de mensagem, mais de 40% sempre utilizam a mesma senha, mais de 20% já clicaram em *links* contidos em e-mail suspeito e mais de 19% já acessaram conta bancária em Wi-Fi público. Esses percentuais inspiram preocupação e confirmam achados anteriores no Brasil de Soares et al. (2020). Todavia, dados indicaram que treinamento em cibersegurança ajuda a promover condutas seguras.

O estudo de Kennison e Chan-Tin (2020), por sua vez, ilustra uma linha de pesquisas que busca explicar o comportamento de cibersegurança. Eles avaliaram se personalidade, tendência a exibir condutas de risco, busca por sensações e conhecimento sobre senhas favorecem comportamentos de cibersegurança. Participaram 292 pessoas, tipicamente, mulheres jovens, dos cursos de psicologia e comunicação social. Foi observado que: (1) mais conhecimento sobre senhas está associado a menos condutas inseguras; (2) mulheres, mas não homens, que buscam por sensações (ex.: apreço por aventura e novidade) apresentam mais condutas de risco; (3) para mulheres (e não para homens), conscienciosidade prediz conduta de risco em uma relação inversamente proporcional; (4) maior instabilidade emocional prediz maior grau de conduta de risco.

Nessa mesma direção, Alanazi et al. (2022) avaliaram se consciência sobre ameaças virtuais, intenção de agir de forma segura e o controle comportamental percebido favorecem comportamentos de cibersegurança. Participaram 1581 estudantes de vários

cursos, sendo mais de 98% saudita, entre 18 e 30 anos. Foi observado que a conduta segura está mais relacionada a saber como implementá-la do que ao entendimento sobre ameaças virtuais. Por isso, treinamentos práticos seriam preferíveis àqueles que visem apenas comunicar informações. Verificou-se também que normas sociais e consciência dos riscos aumentam a probabilidade de adoção de comportamentos de cibersegurança.

Por fim, Rahman et al. (2021) investigaram a produção científica em cibersegurança relacionada a fatores humanos, cuja fonte de dados foram eventos dessa área. Entre 2015 e 2020, foram encontrados 27 estudos, que indicaram a existência de três principais linhas de pesquisa: características e comportamentos de usuários, sistemas de cibersegurança e medida de usabilidade dos sistemas. Sobre os usuários, predominaram os universitários de computação dos EUA e da Europa. No quesito de metodologia, destacaram-se os estudos qualitativos. Verificou-se, ainda, que são escassas pesquisas sobre desenvolvimento de instrumentos para o campo da cibersegurança.

Com base nos estudos examinados, observamos que nem sempre vieses de resposta são controlados, que instrumentos para avaliação de conhecimento, por vezes, pedem que o participante se autoavalie, sem efetivamente testar o seu conhecimento em tarefas com gabarito e que os brasileiros têm sido pouco estudados. Também não identificamos pesquisas que avaliem a relação entre personalidade e conhecimentos e comportamentos de cibersegurança. Por isso, definimos como objetivo deste estudo caracterizar conhecimentos e comportamentos de cibersegurança, avaliando a sua relação com a personalidade. As nossas perguntas de pesquisa em relação a amostra investigada de brasileiros foram: **PP01.** Quais são as características de personalidade da amostra? **PP02.** Quais são as características do conhecimento sobre cibersegurança? **PP03.** Quais são as características do comportamento de cibersegurança? **PP04.** Em que medida traços de personalidade se associam com conhecimento e comportamentos de cibersegurança?

4. Método

4.1. Participantes

Participaram 234 pessoas, mas duas precisaram ser excluídas. Os dados de caracterização dos 232 participantes remanescentes, cuja média de idade foi de 27,34 anos (*DP* = 10,20), variando de 18 a 66, são exibidos na Tabela 1. Essa amostra está balanceada em termos de gênero, das identidades branca e parda, nas faixas de renda de ‘até 2’ a ‘mais de 10 a 15’ salários-mínimos e nas graduações de Computação e Psicologia. Nas demais variáveis, predominaram pessoas sem deficiência (87,93%), na faixa etária de 18 a 23 (52,59%), solteiras (79,31%), sem filhos (82,33%), com ensino superior em andamento (61,64%), residentes em Roraima (76,29%) e da área de informática (32,29%, sendo 57 homens, 14 mulheres e 1 pessoa que se classificou na categoria outros).

4.2. Instrumentos

Descrevemos a seguir os instrumentos aplicados neste estudo. Eles podem ser acessados junto com a base de dados anonimizada: http://dx.doi.org/10.13140/RG.2.2.23397.41449

Questionário de Caracterização do Participante (QCP). Avaliava: (1) idade; (2) gênero; (3) identidade étnico-racial; (4) presença de deficiência; (5) renda familiar; (6) estado civil; (7) existência de filhos ou dependentes; (8) escolaridade; (9) área de ensino técnico para quem interrompeu, cursa ou completou; (10) curso de nível superior,

para quem interrompeu, está estudando ou concluiu; (11) estado no qual reside, com opção para indicar se mora fora do Brasil; (12) se realizou curso sobre cibersegurança.

Inventário dos Cinco Grandes Fatores de Personalidade (ICGFP-5, adaptado por Andrade, 2008). Possui 32 itens que avaliam por autorrelato os cinco grandes fatores de personalidade, sendo 9 sobre Abertura, 6 sobre Conscienciosade, 8 sobre Extroversão, 3 sobre Amabilidade e 6 sobre Neuroticismo. A resposta é fornecida em uma escala Likert de concordância, "1 = Discordo Totalmente" a "5 = Concordo Totalmente". Nos estudos psicométricos, foram coletados dados em todo o Brasil e as evidências foram favoráveis. Neste estudo, o Lambda de Guttman (G6) foi 0,86, indicando confiabilidade adequada.

Escala de Desejabilidade Social Marlowe-Crowne – Versão reduzida com 20 itens (EDSMC20, adaptada por Gouveia et al., 2009). Mensura a tendência de uma pessoa a se comportar em função do que ela percebe como socialmente desejável. Trata-se de instrumento de autorrelato, cuja resposta é dada em escala dicotômica de 'verdadeiro' ou 'falso'. No estudo de adaptação para o Brasil, apresentou evidências psicométricas adequadas. Neste estudo, o índice de Kuder-Richardson 20 (KR-20), técnica apropriada para escalas dicotômicas, foi 0,67, indicando confiabilidade adequada.

Inventário de Conhecimentos sobre Cibersegurança – Versão para Não-especialistas (I2C). Desenvolvido para este estudo, sendo composto por 36 itens, dos quais 14 avaliam conhecimentos sobre senhas, 12 sobre *phishing* e 10 sobre privacidade. Essa medida independe da percepção da pessoa, mas a medida de segurança nas próprias respostas que podemos derivar, depende de como o avaliado se percebe. O I2C é respondido em uma escala tipo Likert de quatro níveis, "1 = Totalmente seguro de que a afirmação é falsa", "2 = Parcialmente seguro de que a afirmação é falsa", "3 = Parcialmente seguro de que a afirmação é verdadeira" e "4 = Totalmente seguro de que a afirmação é verdadeira". Na correção, os níveis 1 e 2 são codificados como 'falso' e os níveis 3 e 4 como 'verdadeiro'. É realizada a contagem de respostas 1 e 4 como medida do nível de segurança. O instrumento foi elaborado de modo que metade dos itens têm gabarito verdadeiro e a outra metade é falsa. Essa regra se aplica a cada uma das suas três dimensões (senhas, *phishing* e privacidade). O G6 foi 0,64, sendo aceitável. Antes do I2C, incluímos três itens abertos para avaliar em que medida os participantes criam senhas fortes, pensando em proteger uma rede social, uma conta de e-mail e uma conta de banco.

Escala de Autoavaliação sobre Comportamentos de Cibersegurança (EACC). Desenvolvido para esta pesquisa, com 13 itens, sendo 3 sobre senhas (2 itens indicadores positivos, de adoção de comportamentos seguros, e 1 negativo, de comportamento inseguro), 2 sobre *phishing* (1 positivo e 1 negativo), 5 sobre privacidade (3 positivos e 2 negativos) e 3 sobre *malware* (1 positivo e 2 negativos). Esse instrumento é respondido em escala tipo Likert de quatro níveis, "1 = Raramente" a "4 = Frequentemente". O G6 foi 0,69, sendo aceitável. Associado a esse instrumento, mas sem compor o seu escore, perguntamos se o participante sabia o que é: (1) *fingerprinting* e se utiliza *software* para bloqueá-lo; (2) *cookie* e se utiliza *software* para bloqueá-lo; (3) *malware* e se utiliza *software* antivírus; (4) se utiliza *software* para proteção de privacidade; (5) *phishing* e se utiliza *software* para proteção contra esse tipo de ataque.

4.3. Procedimento de coleta e análise de dados

Esta pesquisa foi aprovada por Comitê de Ética, CAAE n. 77411823.6.0000.5302. No formulário do Google que criamos, o participante precisava manifestar concordância com

o Termo de Consentimento Livre e Esclarecido, antes de iniciar a sua participação. O *link* para o formulário foi divulgado nas redes sociais dos pesquisadores por 1 mês.

Incluímos ao longo do formulário cinco itens para examinar se os participantes estavam respondendo com atenção, o qual requeria a seleção de uma opção específica de resposta. Qualquer erro, implicava na exclusão do participante. Também examinamos se as mesmas respostas foram fornecidas em todos os itens do ICGFP-5 e da EDSMC. Caso isso ocorresse, também implicaria em exclusão. Examinamos, ainda, se o participante forneceu resposta impossível ou incoerente com os requisitos de participação no estudo. Ao examinar os dados, notamos que 1 participante forneceu as mesmas respostas nos 20 itens da EDSMC e outro reportou ter 11 anos de idade. Logo, ambos foram excluídos.

Tabela 1. Caracterização sociodemográfica da amostra (*n* = 232).

Variável	Frequência	%	Variável	Frequência	%
Gênero			**Estado civil**		
Masculino	116	50,00	Solteiro(a)	184	79,31
Feminino	113	48,71	Casado(a)	38	16,38
Outro	3	1,29	Divorciado(a)	9	3,88
Faixa etária (anos)			Viúvo(a)	1	0,43
18 – 23	122	52,59	**Filhos**		
24 - 29	46	19,83	Sim	41	17,67
30 - 35	29	12,50	Não	191	82,33
36 - 41	11	4,74	**Região de residência**		
42 - 47	10	4,31	Norte	183	79,00
48 - 53	4	1,72	Nordeste	12	5,00
54 - 59	2	0,86	Centro-oeste	6	3,00
60 - 65	7	3,02	Sudeste	21	9,00
66 - 71	1	0,43	Sul	10	4,00
Identidade étnico-racial			**Estado de residência**		
Branca	105	45,26	Roraima	177	76,29
Parda	104	44,83	Outros	55	23,71
Preta	19	8,19	**Escolaridade**		
Amarela	2	0,86	EMC	8	3,45
Indígena	2	0,86	ETC	1	0,43
Renda familiar (salário-mínimo)			ESI	2	0,86
≤ 02	35	15,09	ESA	2	0,86
> 02 a ≤ 03	34	14.66	ESC	29	12,50
> 03 a ≤ 05	49	21.12	PGI	1	0,43
> 05 a ≤ 06	33	14.22	PGA	9	3,88
> 06 a ≤ 08	16	6.90	PGC	39	16,81
> 08 a ≤ 10	26	11.21	**Curso de graduação (*n* = 223)**		
> 10 a ≤ 15	21	9.05	Computação	63	28,25
> 15 a ≤ 20	10	4.31	Psicologia	47	21,08
> 20 a ≤ 30	4	1.72	Medicina	32	14,35
> 30	4	1.72	Outros	81	36,32
Deficiência			**Área do ensino superior (*n* = 223)**		
Sim	28	12,07	Informática	72	32,29
Não	204	87,93	Outra	151	67,71

Nota. EMC: Médio Completo; ETC: Técnico Completo; ESI: Sup. Interrompido; ESA: Sup. em Andamento; ESC: Sup. Completo; PGI: Pós Interrompida; PGA: Pós em Andamento; PGC: Pós Completa.

Calculamos estatísticas descritivas para caracterização de personalidade, conhecimento, segurança sobre conhecimento e comportamentos de cibersegurança. Conduzimos análises estatísticas inferenciais paramétricas, teste t e ANOVA ($\alpha = 5\%$), pois as variáveis que examinamos tipicamente tenderam à normalidade, quando

analisados os seus gráficos Q-Q e resultados no teste de Shapiro-Wilk. Ademais, conduzimos todos os testes com estatísticas não-paramétricas e os achados não mudaram. Com relação aos dados de gênero, apenas para as análises estatísticas inferenciais, classificamos as três respostas "Outros" como feminino, considerando os nomes informados pelas participantes. Procedemos assim, pois a análise inferencial de um grupo com apenas três pessoas não seria adequada.

5. Resultados e Discussão

4.1. PP01 - Quais são as características de personalidade da amostra?

A Figura 1A exibe os achados sobre os traços de personalidade e a Figura 1B os dados sobre desejabilidade social. Os asteriscos representam a média aritmética.

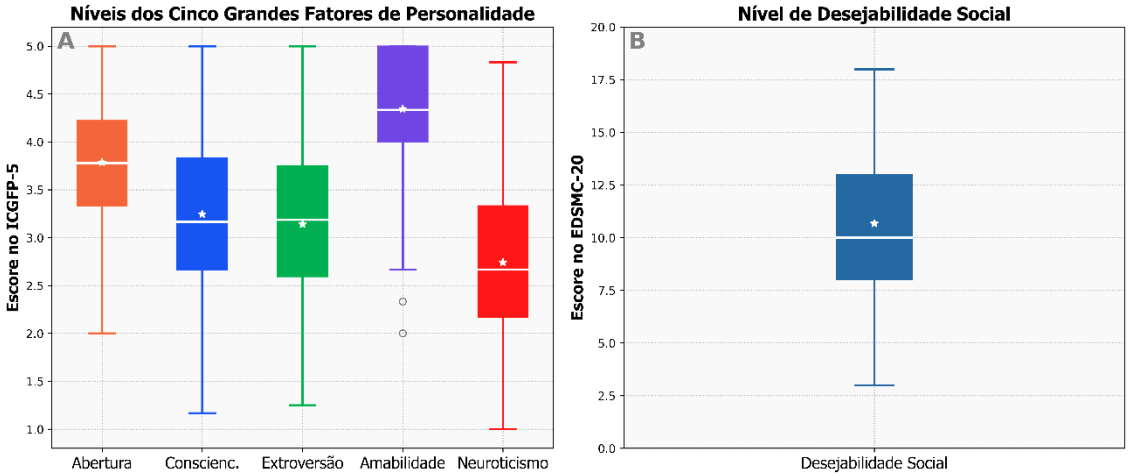

Figura 1. Resultados no ICGFP-5 (Figura 1A) e Resultados no EDSMC-20 (Figura 1B).

Conforme Figura 1A, na presente amostra, destacaram-se os traços de amabilidade (*Média* = 4,34; *DP* = 0,61) e abertura (*Média* = 3,79; *DP* = 0,62), sendo que neuroticismo (*Média* = 2,74; *DP* = 0,83) obteve maior concentração de escores nos menores graus da escala. Esses dados sugerem que para os nossos participantes são importantes os relacionamentos profundos (amabilidade) e o contato com novas experiências (abertura), e que sabem lidar de modo equilibrado com eventos negativos da vida (neuroticismo baixo). A exceção de abertura, encontramos uma diferença de escores estatisticamente significativa entre homens e mulheres, sempre com as mulheres apresentando maiores médias, em relação a conscienciosidade ($t_{(230)}$ = -2,755; p = 0,006; d = -0,362), extroversão ($t_{(230)}$ = -2,298; p = 0,022; d = -0,302), amabilidade ($t_{(230)}$ = -3,199; p = 0,002; d = -0,420) e neuroticismo ($t_{(230)}$ = -2,386; p = 0,018; d = -0,313). Essa diferença confirma achados de Kennison e Chan-Tin (2020). Consideraremos esse resultado em nosso exame da relação entre ICGFP-5, I2C e EACC.

Na Figura 1B, notamos que 50% dos dados então entre as pontuações 8 e 13, sugerindo que a presente amostra exibiu grau moderado de desejabilidade social. Encontramos diferença entre homens (*Média* = 10,94; *DP* = 3,22) e mulheres (*Média* = 10,48; *DP* = 3,43), mas ela não foi estatisticamente significativa ($t_{(230)}$ = 1,224; p = 0,222). Avaliaremos adiante o grau de correlação entre pontuação de desejabilidade e as demais medidas deste estudo, para examinar se existem achados que não estejam representando a verdadeira opinião dos participantes. Com relação à personalidade, não houve

associação estatisticamente significativa entre o escore na EDSMC20 e abertura (r = -0,092; p = 0,164) e extroversão (r = -0,034; p = 0,606). Mas, a encontramos com amabilidade (r = 0,183; p < 0,01), conscienciosidade (r = 0,233; p < 0,001) e neuroticismo (r = -0,424; p < 0,001). As associações positivas foram fracas, mas sugerem que pessoas com maior amabilidade e conscienciosidade também se comportam mais em função de desejabilidade social. A maior correlação indicou que quanto mais comportamentos de instabilidade emocional, menos a pessoa age em função de desejabilidade social. Tal resultado faz sentido, pois os comportamentos indicadores de neuroticismo são pouco desejáveis socialmente. Em conjunto, esses resultados sugerem que as respostas à ICGFP-5 foram coerentes com o que de fato os participantes percebem sobre si.

4.2. PP02 - Quais são as características do conhecimento sobre cibersegurança?

A Figura 2 exibe os achados em relação ao conhecimento dos participantes sobre cibersegurança. Na Figura 2A vemos que esta amostra apresentou conhecimento de "moderado a bom" em cibersegurança, visto que a média de acertos foi de 66,42% (*DP* = 8,84). A média dos 72 participantes da área de informática foi de 69,44% (*DP* = 9,38), enquanto dos demais 160 foi de 65,05% (*DP* = 8,26). Essa diferença foi estatisticamente significativa, mas com baixo tamanho do efeito ($t_{(230)}$ = -3,589; p < 0,001; d = 0,145). Esse pequeno d sugere que os itens do I2C podiam ser corretamente respondidos por qualquer pessoa, não só as da área de informática. Isso é positivo, pois buscamos caracterizar o comportamento de usuários de um modo geral. Também encontramos diferença estatisticamente significativa com pequeno tamanho do efeito ($t_{(230)}$ = -3,205; p < 0,002; d = 0,166) entre o conhecimento de quem reportou ter feito curso sobre cibersegurança (n = 47; *Média* = 70,04; *DP* = 8,23) e quem não fez nenhum (n = 185; *Média* = 65,50; *DP* = 8,77). Nossos dados indicam que o investimento em capacitação sobre informática de modo geral e cibersegurança em particular, favorece o conhecimento sobre cibersegurança, embora seja incerto se ele se traduz em práticas no cotidiano [Kennison and Chan-Tin, 2020; Rahman et al., 2021].

Com relação à segurança nas respostas, conforme Figura 2B, a variabilidade nos dados foi maior. A amplitude das respostas foi de 97,22 contra 50 nos dados de conhecimento. Esse resultado sugere que muitos participantes sentiram insegurança sobre suas respostas no I2C. A média de segurança foi de 50% (*DP* = 20,55). Participantes da área de informática (n = 72; *Média* = 55,52; *DP* = 18,16) ou que fizeram cursos de cibersegurança (n = 72; *Média* = 55,52; *DP* = 18,16), apresentaram maior segurança do que aqueles de outras áreas (n = 160; *Média* = 48,04; *DP* = 21,18) ou sem curso sobre cibersegurança (n = 72; *Média* = 55,52; *DP* = 18,16). Essas diferenças foram estatisticamente significativas, mas com tamanho do efeito pequeno (participantes da área *versus* de outras: $t_{(230)}$ = -2,597; p = 0,01; d = 0,143; com *versus* sem curso de cibersegurança: $t_{(230)}$ = -4,157; p < 0,001; d = 0,167). Essa vantagem de quem é da área de informática ou já fez cursos sobre cibersegurança, em relação a acertos e segurança, sugere que o instrumento refletiu adequadamente a diferença entre grupos que era esperada. Por fim, para o conhecimento não houve diferença estatisticamente significativa em função do gênero ($t_{(230)}$ = -0,309; p = 0,758), mas as mulheres sentiram-se menos seguras (*Média* = 45,12; *DP* = 19,69) do que os homens (*Média* = 55,60; *DP* = 20,12; $t_{(230)}$ = 4,013; p < 0,001; d = 0,136), corroborando achados sobre dificuldades experimentadas por mulheres para inserção na computação [Teles et al., 2023].

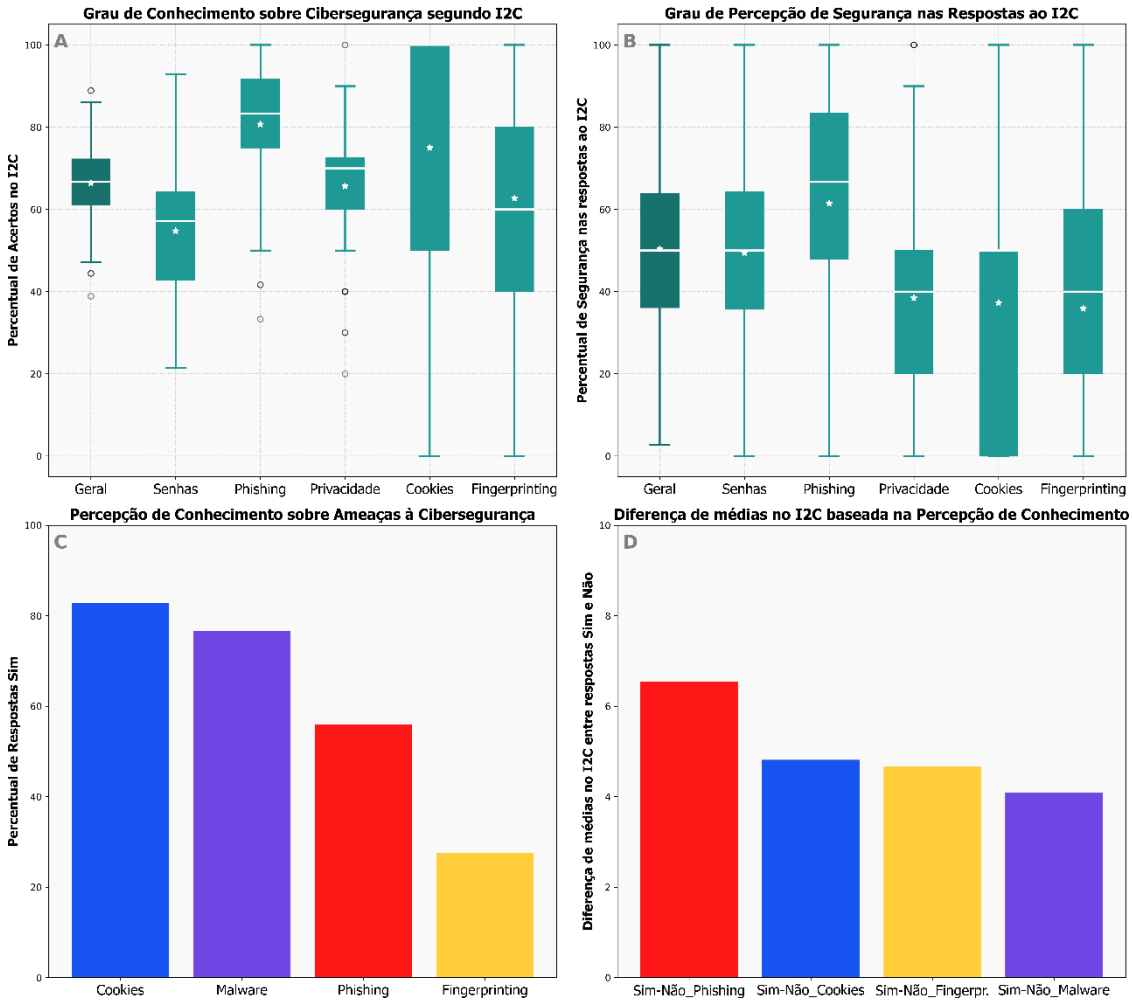

Figura 2. Resultados de acertos no I2C (Figura 2A), Resultados de segurança nas respostas ao I2C (Figura 2B), Respostas 'sim' às questões sobre conhecimento de ameaças à cibersegurança (Figura 2C) e Diferença de médias no I2C em função do conhecimento (Figura 2D).

Na Figura 2C verificamos que a maioria afirma saber o que são *cookies* (82,76%) e *malwares* (76,72%). Por outro lado, poucas pessoas, a despeito de ser um ataque comum, sabem o que é *phishing* (56,03%) e menos ainda conhecem o que é *fingerprinting* (27,59%). Na Figura 2D, quando calculamos a média de notas no I2C para quem respondeu 'sim' e 'não' para cada um desses quatro conceitos e subtraímos uma média da outra, verificamos que o participante que domina esses conceitos acerta mais no I2C. Quando executamos esse procedimento, calculando as médias só para os itens do I2C relativos a 'senhas', '*phishing*', 'privacidade', '*cookies*' e '*fingerprinting*', o padrão se mantém. Mesmo quando calculamos testes t, comparando as médias dos grupos 'sim' e 'não', os resultados em sua maioria foram estatisticamente significativos, ainda que com pequenos tamanhos do efeito. Esse dado sugere que o relato do participante sobre conceitos que ele conhece, parece ser informativo sobre o seu real conhecimento, tendo especial valor a informação sobre o conhecimento do conceito de '*phishing*'.

Ainda no âmbito do conhecimento sobre cibersegurança, avaliamos em que medida os participantes criaram senhas fortes, pensando em proteger contas de rede social, e-mail e banco. A Tabela 2 exibe os resultados gerais de entropia das senhas criadas, bem como uma descrição dos tipos de caracteres adotados. Vemos que a entropia

foi similar para rede social e e-mail e, surpreendentemente, menor para banco. A nossa hipótese para esse achado é a de que, apesar da instrução de que não havia restrições de extensão ou caracteres, os participantes consideraram que senhas de banco possuem apenas números. Os dados de ausências de caracteres apoiam essa ideia, pois nas senhas de banco houve mais ausências de letras maiúsculas, minúsculas e de caracteres especiais.

Tabela 2. Entropia e caracterização das senhas criadas (*n* = 232).

Senha	**Entropia**				
	Média	**DP**	**Mediana**	**Mínimo**	**Máximo**
Rede	78.01	41.17	72.10	19.93	471.93
Email	76.86	39.65	72.10	19.93	471.93
Banco	57.80	45.94	51.70	13.29	471.93
Senha	**Média de ocorrência de caracteres**				
	Maiúscula	**Minúscula**	**Número**	**Especial**	**Extensão**
Rede	1.52	5.57	4.02	1.49	12.60
Email	1.52	5.59	3.81	1.51	12.43
Banco	1.13	3.09	5.18	1.13	10.53
Senha	**Contagem de ausência de caracteres**				
	Maiúscula	**Minúscula**	**Número**	**Especial**	**Total**
Rede	51	19	14	0	84
Email	53	19	16	63	151
Banco	122	107	12	115	356

Em termos de entropia, é forte a senha que possui, no mínimo, 60 bits [Glory et al., 2019]. Em média, as senhas criadas atenderam a esse requisito. Contudo, encontramos senhas com entropias muito baixas, variando de 13,29 a 19,93. Até o 1º quartil, nenhuma das senhas atendeu ao critério de 60 bits, variando de 21,59 (banco) até 58,99 (rede social). Observamos que mesmo em condição de pesquisa, na qual solicitou-se a criação de apenas três senhas, os participantes repetiram em 7,76% dos casos a mesma senha para rede social, e-mail e banco. Os percentuais de repetição entre 'rede social e banco', 'e-mail e banco' e 'rede social e e-mail' foram, respectivamente, 8,19%, 9,91% e 15,95%. Esses dados confirmam a tendência histórica de criação de senhas frágeis e de repeti-la em múltiplas contas [Ji et al., 2017; Bošnjak et al., 2018]. Com relação às características das senhas, observamos boa extensão, acima de 10 caracteres em média, mas pouco uso de letras maiúsculas e caracteres especiais. Com a inclusão desses elementos, as senhas ficariam mais fortes, sem grande esforço adicional. Esse é um exemplo de *insight* que estudos como este podem gerar e que auxiliam na elaboração de capacitações.

Finalmente, observamos que os dados de acertos no I2C (r = -0,029; p = 0,665), grau de segurança (r = 0,070; p = 0,285) e afirmações acerca do conhecimento sobre *cookies* (r = -0,048; p = 0,463), *malware* (r = 0,062; p = 0,344), *phishing* (r = -0,085; p = 0,196) e *fingerprinting* (r = 0,043; p = 0,510), assim como a entropia das senhas criadas pelos participantes (Senha 1: r = -0,078; p = 0,238; Senha 2: r = 0,012; p = 0,860; Senha 3: r = -0,030; p = 0,648), não apresentaram associação com a EDSMC20. Temos, então, uma evidência de que tais dados não se associam a um responder por desejabilidade social. A exceção da segurança e das afirmações sobre conhecimento, isso era esperado porque as demais variáveis supracitadas não envolvem opinião ou relato do participante.

4.3. PP03 - Quais são as características do comportamento de cibersegurança?

A Figura 3A exibe os achados sobre comportamentos de cibersegurança apresentados pelos usuários com base em sua percepção (Figura 3A), englobando (1) criação e uso de

senhas, (2) manejo de ataques de *phishing* e *malware*, e (3) cuidado com a privacidade, envolvendo proteção contra técnicas de *tracking* (*cookies*, *supercookies* e *fingerprinting*), conhecimento sobre LGPD e cuidados no uso da Internet. A Figura 3B exibe as respostas de 'sim' e 'não' em relação ao uso de *softwares* para proteção digital.

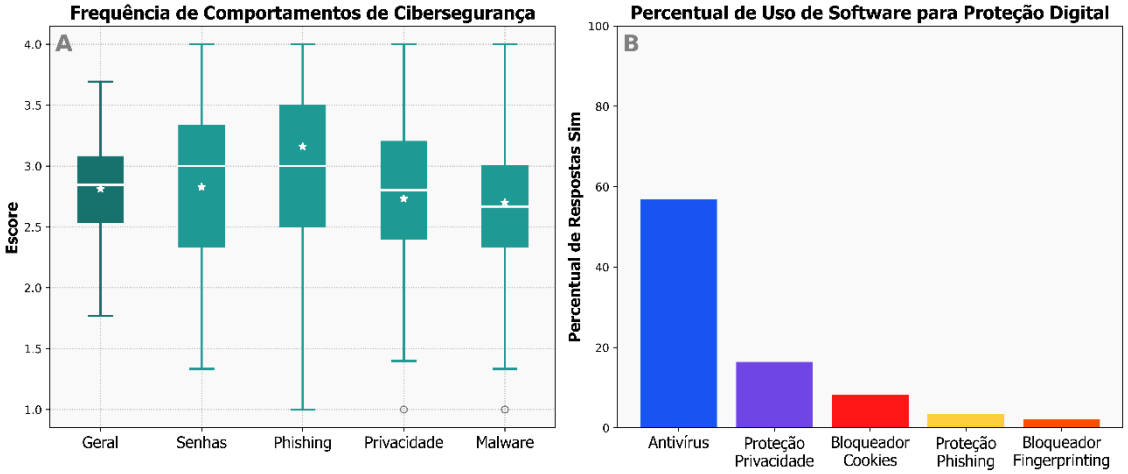

Figura 3. Resultados na EACC (Figura 3A) e Respostas 'sim' sobre uso de *software* (Figura 3B).

Conforme Figura 3A, mais de 50% dos participantes apresentaram escores acima de 2 na EACC. Nos casos do escore geral e dos itens de *phishing*, observamos que mais de 50% dos participantes pontuaram acima de 2,5. Contudo, média e mediana, geralmente, ficaram abaixo de 3, sugerindo que comportamentos de cibersegurança são infrequentes. Sobre uso de senhas e proteção contra *phishing*, a mediana foi igual a 3, existindo 25% dos participantes com pontuação entre 3 e 3,5. Isso sugere que esses comportamentos ocorrem de modo raro a frequente, existindo a necessidade de aperfeiçoamento dessas condutas. Além disso, na Figura 3B notamos que o *software* mais usual é o antivírus e, mesmo nesse caso, apenas 56,90% dos participantes reportaram utilizá-lo. A adoção de outros *softwares* é infrequente. Esses resultados replicam aqueles encontrados por Cain et al. (2018) e Guilherme et al. (2021).

Tal como fizemos em relação ao exame do conhecimento, conduzimos alguns testes t comparando grupos. Observamos que as diferenças de médias obtidas em relação a adoção de comportamentos de cibersegurança foram estatisticamente significativas ($t_{(230)}$ = -3,154; p < 0,002; d = 0,144) para participantes da área de informática (*Média* = 2,94; *DP* = 0,36) em relação aos que são de outras áreas (*Média* = 2,76; *DP* = 0,43). É importante ressaltar que, apesar de a média das pessoas da área de informática ser superior à dos demais e próxima ao escore 3, indicador de comportamento frequente, a pontuação média não foi tão alta como deveria para quem é da área, corroborando os resultados de Cain et al. (2018) em relação às comparações entre especialistas e não-especialistas. Quando agrupamos apenas os itens relacionados aos comportamentos específicos, que avaliaram adoção de senhas seguras, proteção contra *phishing*, proteção da privacidade e proteção contra *malware*, e calculamos o seu escore (conforme Figura 3A), notamos que o grupo de participantes da área de informática sempre supera aqueles de áreas diversas e os testes t são significativos, a exceção do escore relativo aos itens de *phishing*. Observamos exatamente o mesmo padrão quando comparamos escores em função de o participante já ter ou não realizado curso na área de cibersegurança.

Com relação ao gênero, notamos uma diferença pequena e estatisticamente significativa ($t_{(230)} = 5{,}377$; $p < 0{,}001$; $d = 0{,}139$) entre homens (*Média* = 2,95; *DP* = 0,37) e mulheres (*Média* = 2,67; *DP* = 0,41). A nossa hipótese para essas diferenças de gênero que temos encontrado é a de que condições culturais que distanciam mulheres da tecnologia [Teles et al., 2023; Lopes et al., 2023], acabam por reduzir as chances de que aprendam a se proteger no ciberespaço, o que alerta para a importância de capacitações específicas em cibersegurança para essa população. Também avaliamos se houve associação entre esses dados e a EDSMC20. Identificamos associação estatisticamente significativa e de baixa magnitude com a EACC ($r = 0{,}198$; $p = 0{,}002$), o que era esperado. Consideramos que o grau da correlação foi pequeno. Logo, as respostas à EACC não são um reflexo de desejabilidade social. Nas perguntas sobre uso de antivírus ($r = 0{,}098$; $p = 0{,}135$), proteção da privacidade ($r = -0{,}024$; $p = 0{,}717$), bloqueador de *cookies* ($r = -0{,}046$; $p = 0{,}489$), proteção contra *phishing* ($r = 0{,}056$; $p = 0{,}399$) e bloqueador de *fingerprinting* ($r = -0{,}053$; $p = 0{,}424$), não encontramos associação com a EDSMC20.

4.4. PP04 - Em que medida traços de personalidade se associam com conhecimento e comportamentos de cibersegurança?

Passamos, por fim, ao exame das possíveis relações entre personalidade, conhecimento sobre cibersegurança e comportamentos de cibersegurança. Para tanto, apresentamos na Tabela 3 uma matriz de correlação envolvendo essas variáveis, sendo que calculamos as correlações específicas para mulheres (abaixo da diagonal) e para homens (acima da diagonal). Não incluímos nesta matriz as correlações da base de dados completa (homens mais mulheres) por economia de espaço, mas também as analisaremos.

Tabela 3. Matriz de correlações.

Variável	1	2	3	4	5	6	7	8
1. Abertura	—	0.15	0.31***	0.19*	0.04	-0.12	0.12	0.10
2. Conscienciosidade	0.15	—	0.12	0.19*	-0.23*	0.16	0.09	0.23*
3. Extroversão	0.25**	-0.04	—	0.26**	-0.05	-0.12	0.13	0.07
4. Amabilidade	0.07	0.24**	0.19*	—	-0.25**	0.04	0.10	0.26**
5. Neuroticismo	-0.03	-0.33***	-0.16	-0.19*	—	-0.14	-0.29*	-0.06
6. Conhecimento	-0.01	-0.22*	-0.20*	-0.20*	0.11	—	0.24*	0.26**
7. Segurança	0.05	-0.00	0.08	0.20*	-0.18	0.16	—	0.30**
8. Comportamento	0.23*	0.19	-0.09	-0.01	-0.18	0.22*	0.30**	—

Nota. * p < .05, ** p < .01, *** p < .001. Abaixo da diagonal = Mulheres; Acima = Homens.

Encontramos correlações pequenas e esperadas entre as variáveis de personalidade, sugerindo que também nesta amostra, além de outros estudos, o ICGFP-5 mediu corretamente os cinco grandes fatores. Também identificamos correlação entre grau de conhecimento e grau de segurança, o que era esperado. No caso de conhecimento e comportamentos de cibersegurança, era esperada correlação, mas não de grande magnitude, pois é sabido que, mesmo reconhecendo a conduta correta, muitos usuários, por motivos como custo de resposta, podem não exibir comportamento de cibersegurança. Cain et al. (2018) notaram, por exemplo, que mesmo o fato de ter sofrido ataques ou ter recebido treinamento em segurança, não garantem a adoção de boas práticas.

Consideramos interessante o achado de uma associação moderada entre grau de segurança no próprio conhecimento e comportamento de cibersegurança (Geral: $r = 0{,}35$; $p < 0{,}001$; Mulheres ou Homens: $r = 0{,}30$; $p < 0{,}01$). Uma hipótese para explicar esse resultado é a de que, além da exposição ao treinamento sobre segurança, é preciso avaliar

o quanto ele foi efetivo em fazer as pessoas considerarem que dominam o assunto e que sabem, na prática, como lidar com ameaças virtuais. Nesse sentido, Alanazi et al. (2022) observaram que o comportamento seguro está mais relacionado à capacidade prática de implementá-lo (ex.: saber como atualizar um *software*) do que ao entendimento sobre segurança ou uma noção genérica de que somos vulneráveis a ameaças.

Com relação a associação entre personalidade e conhecimento, considerando os dados gerais, encontramos apenas uma correlação estatisticamente significativa, que foi negativa, entre extroversão e conhecimento, sugerindo que os mais extrovertidos conhecem menos sobre cibersegurança e vice-versa. Tal resultado pode ser explicado pelo fato de que, nesta amostra, quem mais conhecia sobre cibersegurança era da área de computação e foram os que exibiram menor extroversão (Correlação entre ter ou não graduação em computação e extroversão: r = -0,293; p < 0,001). No caso da segurança no próprio conhecimento, encontramos apenas uma correlação, fraca e negativa, com neuroticismo (r = -0,228; p < 0,001), sugerindo que pessoas mais instáveis emocionalmente sentem-se menos seguras em relação ao próprio conhecimento. Pela lógica do que o neuroticismo mensura, é esperado que os mais instáveis se sintam menos seguros no geral. Verificamos também que pessoas mais instáveis emocionalmente adotam menos comportamentos de cibersegurança (r = -0,167; p < 0,011). Uma vez que a segurança no próprio conhecimento aumenta as chances de emissão desses comportamentos, é compreensível que pessoas que confiem menos nas próprias ações, se engajem menos em práticas de segurança. Por outro lado, observamos correlação entre abertura e comportamento de cibersegurança (r = 0,157; p < 0,05), sugerindo que a disposição para ter contato com novos estímulos pode estar diretamente vinculada com a adoção de condutas seguras. É possível que isso tenha relação com o fato de que comportamentos de cibersegurança requerem exploração de informações, que mudam ao longo do tempo, sobre como se proteger e sobre como as tecnologias funcionam.

Com relação aos dados das mulheres, observamos na Tabela 3 que conscienciosidade, extroversão e amabilidade se relacionaram positivamente entre si e, cada uma, com o grau de conhecimento sobre cibersegurança. O resultado de conscienciosidade nos surpreendeu, mas uma hipótese é a de que a maior parte das mulheres do estudo (44,83% de 116 mulheres) era dos cursos de medicina e psicologia. Apesar de possuírem alta conscienciosidade, que é importante para o desempenho acadêmico, elas possivelmente conhecem menos sobre informática, seja por fatores culturais, como pelo conjunto típico de disciplinas das suas graduações. Observamos também que se sentiram mais seguras em relação às próprias respostas, as mulheres com maior nível de amabilidade. Pode ser que a maior confiança que essas mulheres depositam nos outros, seja aplicada a elas próprias. Por fim, notamos que mulheres mais abertas a novas experiências apresentaram mais comportamentos de cibersegurança, contrariando achados da literatura. Kennison e Chan-Tin (2020) encontraram associação positiva entre busca por sensações, que se relaciona com abertura, e comportamento de risco. Além disso, para as mulheres, maior conscienciosade e menor neuroticismo estavam associados a menor grau de comportamento de risco, o que não verificamos em nossos dados.

No caso dos homens, não encontramos associações entre personalidade e conhecimento, mas apenas com segurança e comportamento de cibersegurança. O grau de segurança foi maior, quanto menor o grau de instabilidade emocional. A emissão de comportamentos de cibersegurança, se associou positivamente com conscienciosidade e amabilidade. Ambas confirmam achados de Alanazi et al. (2022) de que normas sociais

e consciência dos riscos aumentam a probabilidade de comportamentos de cibersegurança. Normas sociais se vinculam à faceta de dever do fator conscienciosidade, mas também à faceta de complacência do fator amabilidade. A consciência do risco, tem relação direta com a conscienciosidade em geral. Segundo Egelman e Peer (2015), comportamentos de cibersegurança estão relacionados com pensamento de longo prazo, o que requer consciência dos riscos e conduta disciplinada para mitigá-los.

No geral, apesar das poucas e fracas correlações, encontramos evidências preliminares da existência de associação entre os cinco grandes fatores de personalidade e as variáveis examinadas neste estudo. Seria importante seguirmos investigando esse fenômeno, afinal precisamos tornar mais efetivas as intervenções para promoção de conhecimento e de comportamentos de cibersegurança. Kennison e Chan-Tin (2020) sugerem que programas de treinamento em segurança cibernética podem reduzir frequência de comportamentos inseguros, mas deveriam incorporar perfis de personalidade para uma abordagem mais eficaz. Para tanto, primeiro precisamos compreender melhor essa relação, conduzindo outros estudos como este.

6. Conclusão

O objetivo deste estudo foi caracterizar conhecimentos e comportamentos de cibersegurança, avaliando a sua relação com a personalidade. Na presente amostra, observamos escores mais elevados de amabilidade e abertura, acompanhados de baixo grau de neuroticismo. As notas de conhecimento foram de "moderado a bom", com pequena vantagem para os participantes da área de informática. Sobre o comportamento de cibersegurança, notamos baixa frequência e destaque positivo daqueles da área de informática. Ao examinar as relações entre essas variáveis, identificamos evidências de uma associação fraca entre traços de personalidade e as dimensões de conhecimento e comportamento de cibersegurança. Isso pode ser útil na orientação de capacitações customizadas para as características dos alunos, bem como para a construção de modelos de recomendação de condutas em função das características de personalidade do usuário.

Para estudos futuros, observamos que uma das limitações desta pesquisa foi a homogeneidade da amostra, pois eram, predominantemente, de um único estado brasileiro. Novas investigações devem contemplar uma amostra maior e mais diversa. Ademais, consideramos importante, atendendo ao chamado de diversos pesquisadores [Egelman and Peer, 2015; Parsons et al., 2017; Rahman et al., 2021], que comecem a ser desenvolvidos instrumentos psicométricos específicos para a área de cibersegurança. Eles poderão auxiliar na avaliação de eficiência de intervenções educacionais para a promoção de comportamentos de cibersegurança, bem como na sua caracterização e investigação das variáveis que os determinam. Importa, ainda, contemplar nesses instrumentos conhecimento produzido pela indústria sobre cibersegurança.

7. Referências

Alanazi, M., Freeman, M., and Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*(107376), 1-14. https://doi.org/10.1016/j.chb.2022.107376

Aljohani, M., Alruqi, M., Alboqomi, O., and Alqahtani, A. (2020). An experimental study to understand how users choose password. In: *Proceedings of the 4th International*

Conference on Future Networks and Distributed Systems (ICFNDS '20) (pp. 1–5). New York: ACM. https://doi.org/10.1145/3440749.3442643

Andrade, J. M. (2008). *Evidências de Validade do Inventário dos Cinco Grandes Fatores de Personalidade para o Brasil* (Tese de doutorado apresentada ao Programa de Pós-graduação em Psicologia Social, do Trabalho e das Organizações, Universidade de Brasília, Brasília). Recuperado de: https://repositorio.unb.br/handle/10482/1751

Banaco, R. A., Vermes, J. S., Zamignani, D. R., Martone, R. C., and Kovac, R. (2012). Personalidade. Em: M. M. C. Hübner, & M. B. Moreira, *Temas clássicos da psicologia sob a ótica da Análise do Comportamento (pp. 144-153)*. Rio de Janeiro: Guanabara Koogan.

Bošnjak, L., Sreš, J., and Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1161-1166)*. Opatija, Croatia. https://doi.org/10.23919/MIPRO.2018.8400211

Cain, A. A., Edwards, M. E., and Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

Egelman, S., and Peer, E. (2015). Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS). In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15, pp. 2873–2882)*. New York: ACM. https://doi.org/10.1145/2702123.2702249

Glory, F. Z., Aftab, A. U., Tremblay-Savard, O., and Mohammed, N. (2019). Strong password generation based on user inputs. In: *IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (p. 416-423)*. https://doi.org/10.1109/IEMCON.2019.8936178

Gouveia, V. V., Guerra, V. M., Sousa, D. M. F., Santos, W. S., and Costa, J. M. (2009). Escala de Desejabilidade Social de Marlowe-Crowne: evidências de sua validade fatorial e consistência interna. *Avaliação Psicológica*, *8*(1), 87-98. Recuperado de http://bit.ly/39mRvqK

Guilherme, L. P., Ferreira, M. F., Fonseca, G. M., and Lazarin, N. M. (2021). Uma breve noção sobre o comportamento dos internautas em relação à segurança na rede. In: *Anais da VII Escola Regional de Sistemas de Informação do Rio de Janeiro (pp. 1-7)*. Porto Alegre: SBC. https://doi.org/10.5753/ersirj.2021.16972

Hartwig, K., and Reuter, C. (2021). Nudge or restraint: How do people assess nudging in cybersecurity - A representative study in Germany. In: *Proceedings of the 2021 European Symposium on Usable Security (EuroUSEC '21) (pp. 141–150)*. New York: ACM. https://doi.org/10.1145/3481357.3481514

Hoepers, C. (2024). A Importância dos Fatores Humanos para a Cibersegurança. *Computação Brasil*, *52*, 61–66. https://doi.org/10.5753/compbr.2024.52.4604

Ji, S., Yang, S., Hu, X., Han, W., Li, Z., and Beyah, R. (2017). Zero-Sum Password Cracking Game: A Large-Scale Empirical Study on the Crackability, Correlation, and Security of Passwords. *IEEE Transactions on Dependable and Secure Computing*, *14*(5), 550-564. https://doi.org/10.1109/TDSC.2015.2481884

Kennison, S. M., and Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.546546

Lin, X., Araujo, F., Taylor, T., Jang, J., and Polakis, J. (2023). Fashion Faux Pas: Implicit Stylistic Fingerprints for Bypassing Browsers' Anti-Fingerprinting Defenses. In: *IEEE Symposium on Security and Privacy (SP) (pp. 987-1004)*. San Francisco, CA, USA. https://doi.org/10.1109/SP46215.2023.10179437

Lopes, R., Maciel, B., Soares, D., Figueiredo, L., and Carvalho, M. Análise e reflexões sobre a diferença de gênero na computação: podemos fazer mais? In: *Anais do XVII WIT (pp. 68-79)*, Porto Alegre: SBC, 2023. https://doi.org/10.5753/wit.2023.230819

Mansur-Alves, M., and Saldanha-Silva, R. (2019). Teoria dos Cinco Fatores de Personalidade (TCF): Uma introdução teórico-conceitual e aplicada para avaliação. Em: Baptista M. N. et al. (orgs.), *Compêndio de Avaliação Psicológica (pp. 507-520)*. Petrópolis, RJ: Editora Vozes.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

Rahman, T., Rohan, R., Pal, D., and Kanthamanon, P. (2021). Human factors in cybersecurity: A scoping review. In: *Proceedings of the 12th International Conference on Advances in Information Technology (IAIT '21, pp. 1–11)*. Association for Computing Machinery, New York, NY, USA, Article 5. https://doi.org/10.1145/3468784.3468789

Ruoslahti, H., Coburn, J., Trent, A., and Tikanmäki, I. (2021). Cyber Skills Gaps – A Systematic Review of the Academic Literature. *Connections: The Quarterly Journal*, *20*(2), 33-45. https://doi.org/10.11610/Connections.20.2.04

Soares, H., Araújo, N., and de Souza, P. (2020). Privacidade e segurança digital: Um estudo sobre a percepção e o comportamento dos usuários sob a perspectiva do paradoxo da privacidade. In: *Anais do I WICS (pp. 97-106)*. Porto Alegre: SBC. https://10.5753/wics.2020.11040

Švábenský, V., Vykopal, J., and Čeleda, P. (2020). What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE conferences. In: *The 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*. https://doi.org/10.1145/3328778.3366816

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., and Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE Access*, *10*, 39325–39343. https://doi.org/10.1109/access.2022.3162594

Teles, M., Saraiva, L., Freires, M., Rocha, M., and Marques, A. Mentoria acadêmica como aliada à integração de alunas de Computação no ambiente acadêmico. In: *Anais do XVII WIT (pp. 194-204)*, Porto Alegre: SBC, 2023. https://doi.org/10.5753/wit.2023.230784