Estratégias de incentivo e ensino de comportamentos de cibersegurança: Relato de experiência em uma universidade

Paulo F. da Silva Júnior[1], Marcelo H. O. Henklain[1], Pedro V. da S. Ribeiro[1], João R. R. C. Cunha[1], Felipe L. Lobo[1], Eduardo L. Feitosa[2]

[1]Depto. de Ciência da Computação – Universidade Federal de Roraima (UFRR)
Av. Cap. Ene Garcês, 2413 – Aeroporto, Boa Vista – RR, Brasil

[2]Instituto de Computação – Universidade Federal do Amazonas (UFAM)
Manaus, Brasil

{juniorrkcm, silvapv7, jrobertocunharr}@gmail.com

{marcelo.henklain, felipe.lobo}@ufrr.br, efeitosa@icomp.ufam.edu.br

Abstract. *Cyberspace is pervasive, and with that comes the need for everyone to learn how to navigate it safely. This study aimed to evaluate two interventions (a lecture and a consultation) for promoting, and one (a course) for teaching, cybersecurity behaviors in the context of a public university. We found favorable evidence of the effectiveness of these strategies, though future studies are needed to refine them.*

Resumo. *A presença do ciberespaço é pervasiva e, com isso, surge a necessidade de que todos aprendam a lidar com ele de forma segura. Neste estudo, o objetivo foi avaliar duas intervenções (palestra e consultoria) para incentivo e uma (curso) para ensino de comportamentos de cibersegurança em contexto de universidade pública. Encontramos evidências favoráveis de eficiência dessas estratégias, sendo necessário aperfeiçoá-las em estudos futuros.*

1. Introdução

No século XXI, a presença do ciberespaço é pervasiva e isso traz inúmeros benefícios, mas também a ampliação de ameaças como ciberataques [Nogueira 2024, CERT.br 2024]. Para lidar com esse cenário, além de aperfeiçoar tecnologias, precisamos capacitar as pessoas para a vida digital, incluindo o ensino sistemático de comportamentos de cibersegurança, pois sem esse suporte o usual é que elas apresentem comportamentos inseguros [Guilherme et al. 2021, Hoepers 2024].

Apesar dessa demanda urgente por capacitação, ainda são escassos os estudos sobre educação em cibersegurança [Rahman et al. 2021, Ruoslahti et al. 2021]. Por isso, neste estudo exploratório o nosso objetivo foi avaliar duas intervenções (palestra e consultoria) para incentivo e uma (curso) para ensino de comportamentos de cibersegurança em contexto de universidade pública. Buscamos responder às seguintes perguntas de pesquisa: (1) Em que medida a palestra foi satisfatória, tendo potencial para incentivar comportamentos de cibersegurança? (2) Em que medida a consultoria foi bem-sucedida em incentivar (e comprovar emissão de) comportamento de cibersegurança? (3) Em que medida o curso promoveu aprendizagens, aumentou a autoconfiança no próprio repertório e gerou satisfação? A nossa contribuição reside em construir e testar intervenções fáceis de aplicar e que podem melhorar a resiliência de pessoas e organizações aos ciberataques.

2. Fundamentação teórica

Adotamos neste estudo a teoria analítico-comportamental [Moreira and Medeiros 2018], que entende o ensino como a organização de condições ambientais que favorecem o aprendizado de comportamentos. O aprendizado é interpretado como uma mudança duradoura de repertório, seja pela aquisição ou aperfeiçoamento de um comportamento [Cortegoso and Coser 2023]. Comportamentos propostos como alvos do ensino são chamados de comportamentos-objetivo e orientam o trabalho docente [Kienen et al. 2021]. Neste estudo, priorizamos iniciar a proposição de comportamentos-objetivo e, a partir de condições de ensino fáceis de implementar, avaliar em que medida conseguiríamos desenvolver aprendizagens relativas à cibersegurança.

Também buscamos incentivar comportamentos, o que consiste em facilitar a sua ocorrência, seja, por exemplo, removendo barreiras ou aumentando os motivos para que seja emitido. Um exemplo de remoção de barreira pode ser "estar do lado de uma pessoa para ajudá-la a realizar uma atividade difícil". Aumentar os motivos para uma ação, por sua vez, pode ser "explicar a importância de agir de determinada maneira", tornando mais saliente a relevância da produção de uma consequência. Neste trabalho, incentivamos comportamentos a partir da palestra e da consultoria individualizada em cibersegurança.

Cumpre esclarecer, por fim, que baseados na definição de cibsersegurança de [Silva 2023], propomos definir o comportamento de cibersegurança como aquele que, diante do ciberespaço, a partir de múltiplas ações relacionadas ao uso de sistemas, favorece a preservação da própria privacidade, bem como da confidencialidade, integridade e disponibilidade dos recursos digitais do indivíduo. Em nosso trabalho, buscamos, portanto, incentivar e ensinar comportamentos de cibersegurança.

3. Trabalhos relacionados

Apresentamos nesta seção os estudos consultados e que evidenciam a lacuna existente na literatura. [Paudel and Al-Ameen 2024] avaliaram em que medida recursos visuais com estatísticas sobre riscos de certos comportamentos podem incentivar o uso de senhas fortes, encontrando resultados favoráveis. [Henderson et al. 2024] mostraram os benefícios do uso de jogos para ensinar as pessoas a lidarem com *phishing*. [Losse et al. 2024], por sua vez, criaram e avaliaram uma oficina de segurança orientada para motivar discussões sobre como solucionar desafios de cibersegurança no ambiente organizacional. Verificou-se que os funcionários propuseram e discutiram dicas e técnicas inovadoras de segurança baseadas na realidade da própria organização.

[Omoyiola et al. 2024], por fim, avaliaram um programa corporativo baseado em três pilares, criados a partir de erros comuns e ações maliciosas deliberadas: Consciência (campanhas contínuas e simulações de phishing), Educação (módulos conceituais e exercícios práticos sobre senhas fortes, gerenciadores e A2F) e Comunicação (atualizações semanais via e-mail, intranet e murais, com apoio da alta gestão). Foi observado aumento nos escores de consciência entre pré e pós-testes, altas taxas de conclusão dos treinamentos, adoção expressiva de A2F e gerenciadores de senha, além de queda na eficácia de ataques simulados de phishing, evidenciando a eficácia do modelo.

Nos estudos avaliados, encontramos baixa clareza sobre quais foram os comportamentos incentivados ou ensinados e escassez de estudos realizados em contexto aplicado

no Brasil, especificamente, em instituições de ensino. Por esse motivo, identificamos a necessidade social e científica de conduzir pesquisa testando intervenções para incentivar e ensinar comportamentos de cibersegurança.

4. Método

4.1. Visão geral do estudo

Realizamos 3 intervenções, palestra, consultoria e curso, organizadas em duas frentes de trabalho sob a responsabilidade de 2 grupos de graduandos em computação (monitores). Esta pesquisa foi aprovada pelo Comitê de Ética e todos os participantes assinaram Termo de Consentimento Livre e Esclarecido (TCLE). Dado o seu caráter exploratório, não buscamos aqui generalizar as conclusões obtidas para outros contextos, mas identificar aspectos a serem aperfeiçoados para intervenções futuras. As principais informações deste estudo estão resumidas na Tabela 1.

Tabela 1. Síntese das intervenções

Intervenção	Período	Participantes	Média Idade (DP)	Sexo	Evasão	Medidas	Critério de sucesso
Palestra	29/11/24, em 2 horários 10h-11h45 e 14h-15h45	33, 10 servidores, 3 terceirizados e 20 alunos.	29,66 (12,26)	69,70% masculino	36,54% de 52 inscritos.	Satisfação	$\geq 4{,}00$
Consultoria	11/11/24 a 14/03/25	123 servidores	43,45 (9,84)	65,04% feminino	Não se aplica.	Habilitação da A2F ou Comprovação de que já estava habilitada	Não se aplica.
Curso	30/11/24 a 14/03/25	17, 2 servidores e 15 alunos.	25,49 (8,16)	82,35% masculino	54,05% de 37 inscritos.	Acertos (Ac), Segurança (Sg), Satisfação (St) e	TDE de Ac e SG $\geq$ 0,40, St $\geq 4{,}00$

O Grupo 1, com 6 monitores (M1 ao M6), organizou palestra e curso, começando pela proposição de 8 comportamentos-objetivo baseados em [Henklain et al. 2024], a saber: (1) Identificar ameaças típicas do ciberespaço e boas práticas para mitigá-las; (2) Avaliar status de atualização de Sistema Operacional e programas utilizados em computadores e celulares; (3) Avaliar antivírus pagos e gratuitos mais promissores para uso em computadores e celulares; (4) Identificar relevância dos backups para a proteção de dados; (5) Projetar senhas fortes e memoráveis; (6) Avaliar opções existentes, vantagens e desvantagens dos gerenciadores de senhas; (7) Habilitar autenticação de dois fatores; e (8) Distinguir e-mails legítimos de tentativas de *phishing*. Considerando esses objetivos, o curso foi construído e, a partir de uma síntese dele, a palestra foi organizada.

O Grupo 2, com 10 monitores (M7 ao M14, além de M1 e M3), organizou e executou a consultoria, cujo trabalho foi realizado paralelamente ao do Grupo 1. O primeiro passo foi propor 1 comportamento de cibersegurança a ser incentivado e, então, elaborar um roteiro para implementá-lo mediante interação presencial com o usuário.

4.2. Intervenção 01: Palestra sobre cibersegurança

4.2.1. Participantes

Dentre os servidores, participaram 8 técnicos-administrativos e 2 professores de computação. Entre os terceirizados, estavam profissionais de setores administrativos. Todos os alunos inscritos eram do curso de computação. Notamos que 2 servidores e 10 alunos participaram também do curso de cibersegurança realizado.

4.2.2. Procedimento de coleta e análise de dados

A partir dos comportamentos-objetivo (CO), dividimos a palestra em 5 momentos. O Tópico 1 incentivava o CO 1, o Tópico 2 os COs 2 a 4, o Tópico 3 os COs 5 a 7, e o Tópico 4 o CO 8. Destacamos que, antes da palestra, os monitores já haviam treinado como abordar os seus temas por conta da gravação das videoaulas para o curso. Além disso, o professor responsável forneceu orientações sobre boas práticas de apresentação e auxiliou os monitores na execução da palestra. Todos usaram slides (com texto e imagens) previamente validados, cujo layout foi padronizado.

A divulgação dessa intervenção foi realizada via Instagram e WhatsApp, focando apenas a comunidade acadêmica. Após a palestra, solicitamos aos participantes que avaliassem a sua satisfação por meio de instrumento de 10 itens respondido em escala Likert, "1 = Nada Satisfeito" a "5 = Totalmente satisfeito". Calculamos média aritmética e desvio padrão considerando a pontuação nesses itens e o escore total, por tipo de participante e para toda a amostra. O nosso critério de sucesso foi obter escore maior que 4,0.

4.3. Intervenção 02: Consultoria individual em cibersegurança

4.3.1. Participantes

Nessa amostra, os servidores tinham média de 13,36 anos de atuação na instituição (DP = 9,28) e 66,67% reportaram possuir pós-graduação completa. Em sua maioria, os participantes não tinham formação em informática (71,54%) ou curso de cibersegurança (86,18%), o que revela uma demanda por capacitações. Todas as pró-reitorias e a maioria dos centros da universidade tiveram participantes neste estudo.

4.3.2. Procedimento de coleta e análise de dados

Foi avaliado em grupo que o comportamento mais simples de ser aprendido, e que poderia alavancar a segurança da universidade, era o de habilitar a autenticação de dois fatores (A2F). Por essa razão, esta intervenção foi orientada para incentivá-lo. Criamos um Formulário do Google para hospedar o instrumento de coleta de dados, que continha instruções sobre como o monitor deveria se apresentar ao servidor, que perguntas precisava fazer e como deveria, caso autorizado, proceder para habilitar a A2F.

Ficou estabelecido que os monitores não deveriam manipular senhas dos servidores, nem insistir para realizar a intervenção. Mesmo se o servidor aceitasse participar, caso demonstrasse receio ao longo do processo, a habilitação deveria ser encerrada. Para garantir um procedimento uniforme, adotamos o Google Authenticator e criamos um roteiro para sua instalação e configuração, contemplando diferentes cenários, como smartphones com Android ou IOS. Incluímos demonstração sobre como recuperar o acesso ao app em caso de perda do smartphone. Ficou definido que a A2F só poderia ser incentivada e habilitada para o e-mail institucional do servidor.

Os monitores treinaram todo o procedimento, sanaram dúvidas com o professor responsável e, só então, foram a campo, tendo consigo um crachá do projeto com sua foto e nome. Para evitar coletas em duplicidade, as pró-reitorias da universidade e seus centros foram divididos entre os monitores, sendo cada servidor abordado individualmente. A

comprovação de habilitação da A2F era feita mediante demonstração pelo servidor de sua tela da conta do Google indicando a A2F como ativada. Com os dados coletados, calculamos estatísticas de contagem, proporção, média e desvio padrão.

4.4. Intervenção 03: Curso sobre cibersegurança

4.4.1. Participantes

Entre os servidores, participaram técnicos-administrativos dos setores de planejamento e de tecnologia. Na amostra de alunos, encontramos 1 acadêmico de administração, 1 de secretariado executivo e os outros 13 eram de computação. Notamos que os 2 servidores que finalizaram o curso e 10 dos alunos de computação haviam participado também da palestra. Portanto, este curso contemplou apenas 5 pessoas diferentes em relação àquelas alcançadas pela palestra.

4.4.2. Procedimento de coleta e análise de dados

O curso foi organizado em função dos mesmos 8 comportamentos-objetivo (CO) adotados na palestra. Optamos por construí-lo em formato online e disponibilizá-lo no Moodle da instituição, para facilitar o acesso. Consideramos também que o curso nesse formato pode ser utilizado em futuras intervenções.

No Moodle, incluímos fóruns de avisos e de dúvidas, instruções sobre a estrutura do curso a partir de um vídeo de abertura e texto e, na sequência, criamos 5 módulos: (1) Ameaças no ciberespaço, que desenvolvia o CO 1 e contava com 2 videoaulas (engenharia social e malwares); (2) Boas práticas no uso de computadores e celulares - COs 2 a 4 e 3 videoaulas (atualização de software, backup e antivírus); (3) Boas práticas para proteção de dados - COs 5 a 7 e 3 videoaulas (senhas fortes, gerenciadores de senhas e A2F); (4) Boas práticas para usar e-mail e evitar phishing - CO 8 e 1 videoaula; e (5) Atitude segura, que era uma revisão e contemplava, portanto, todos os COs. As videoaulas variavam de 2 a 9 minutos e a revisão teve 1 aula de 32 minutos. Adicionalmente, selecionamos 12 vídeos para complementar conceitos, sendo a maioria produzidos pelo Senai/São Paulo (https://bit.ly/431x1S4).

Cada módulo, a exceção do último, era iniciado com um pré-teste que avaliava em que medida os COs propostos para ele já haviam sido adquiridos pelos participantes. Ao final dos módulos, aplicávamos um pós-teste, repetindo as mesmas questões do pré, para avaliar se havia ocorrido melhora de desempenho. Para os Módulos 1 a 3 criamos testes com seis itens de verdadeiro ou falso. Além de tentar acertar o item, pedíamos para o participante indicar quão seguro estava de sua resposta. Por isso, cada item tinha quatro opções: "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". No Módulo 4, utilizamos instrumento de 20 itens que estamos desenvolvendo para avaliar se uma pessoa consegue reconhecer casos de phishing, inspirada na escala de phishing do NIST [Dawkins and Jacobs 2023]. Cada item apresenta um e-mail que pode ou não ter phishing e cuja resposta é dada a partir de quatro opções: "1 = Totalmente seguro de que não é phishing", "2 = Parcialmente seguro de que não é phishing", "3 = Parcialmente seguro de

que sim é phishing" e "4 = Totalmente seguro de que sim é phishing". O Módulo 5, por ser uma revisão, não teve pré ou pós-teste, sendo finalizado com a avaliação de satisfação do curso.

O curso foi construído para ser conciso, liberando tempo para que o aluno pudesse manifestar dúvidas no fórum, ler ou assistir os materiais bônus que incluímos e, principalmente, para emitir os comportamentos-objetivo em seu cotidiano, por exemplo, melhorando a força de suas senhas. A geração do certificado foi automática, mediante realização de todos os testes e marcação no Moodle de que todas as videoaulas e vídeos complementares haviam sido vistos.

Divulgamos esta intervenção junto com a palestra. Com o pré e pós-teste de cada módulo, avaliamos os comportamentos-objetivo e o grau de autoconfiança nas próprias respostas a partir de média aritmética, desvio padrão e do teste dos postos sinalizados de Wilcoxon. No final do curso, avaliamos a satisfação com instrumento de 15 itens baseado no trabalho de [Schleich et al. 2006], cuja escala de resposta e forma de análise foi a mesma usada na avaliação da palestra. Perguntamos também se e quais comportamentos o participante havia praticado a partir do curso e contamos a frequência deles.

5. Resultados e Discussão

5.1. Intervenção 01: Palestra sobre cibersegurança

A Tabela 2 exibe os 10 itens da avaliação de satisfação e as médias e desvios padrão obtidos em relação a servidores, terceirizados, alunos e toda a amostra. Nota-se que todas as médias estão acima de 4,4 e que os desvios padrão são baixos, tipicamente, nulos, indicando nesses casos que todos forneceram a mesma nota.

Tabela 2. Resultados da avaliação de satisfação com a palestra.

N	Item	Média (DP)			
		Servidor	**Terceirizado**	**Aluno**	**Todos**
1	Compromisso dos organizadores da palestra com a qualidade da formação.	5 (0)	5 (0)	5 (0)	5 (0)
2	Metodologia de ensino utilizada pelos professores.	5 (0)	5 (0)	5 (0)	5 (0)
3	Recursos audiovisuais disponíveis na palestra.	5 (0)	5 (0)	4,95 (0,22)	4,97 (0,17)
4	Meios de divulgação de informações sobre a palestra.	4,4 (1,35)	4,67 (0,58)	4,75 (0,64)	4,64 (0,9)
5	Atendimento e clareza das informações oferecidas para apoio a audiência.	5 (0)	5 (0)	5 (0)	5 (0)
6	Currículo da palestra.	5 (0)	5 (0)	5 (0)	5 (0)
7	Domínio dos professores sobre o conteúdo que ministram.	5 (0)	5 (0)	5 (0)	5 (0)
8	Relevância do conteúdo.	5 (0)	5 (0)	5 (0)	5 (0)
9	Oportunidade de desenvolvimento pessoal oferecida pela palestra.	5 (0)	5 (0)	5 (0)	5 (0)
10	Condições oferecidas para o meu desenvolvimento profissional.	5 (0)	5 (0)	5 (0)	5 (0)
	Escore	**4,93 (0,15)**	**4,96 (0,06)**	**4,97 (0,07)**	**4,96 (0,1)**

Como regra, as notas foram 5,0 (máximo possível), sendo que os Itens 3 e 4 receberam avaliações mais baixas. Acreditamos que o interesse prévio da audiência que se inscreveu e foi presencialmente assistir à palestra, como também os temas que selecionamos e como os apresentamos possam explicar esse resultado positivo [Alanazi et al. 2022, Losse et al. 2024].

No caso do Item 3, alguns alunos avaliaram que os recursos audiovisuais adotados poderiam ser melhores. Uma hipótese para explicar esse achado é que não utilizamos

imagens especialmente desenvolvidas para o treinamento e vídeos, o que poderia ter tornado algumas demonstrações mais claras e interessantes [Paudel and Al-Ameen 2024]. No Item 4, por sua vez, todos os três tipos de participantes apresentaram pontuações mais baixas. Uma hipótese é a de que o uso de redes sociais, no caso, Instagram e WhatsApp, embora prático e sem custo, pode ser insuficiente seja porque algumas pessoas não usam essas plataformas ou porque não seguem a conta ou não estão nos grupos a partir dos quais as divulgações foram realizadas. Ademais, é preciso considerar que o volume de informações na Internet é alto, sendo difícil conseguir obter a atenção das pessoas.

Em síntese, à luz da satisfação, a palestra apresentou evidência favorável de eficiência para incentivar comportamentos de cibersegurança ou, pelo menos, interesse pelo tema. Uma demonstração disso é que muitos participantes dessa intervenção se inscreveram no curso. Destacamos, ainda, que ao final da palestra os participantes se engajaram em um diálogo proveitoso sobre cibersegurança com os monitores. Foram sanadas dúvidas sobre ameaças virtuais e a iniciativa desta intervenção foi parabenizada.

5.2. Intervenção 02: Consultoria individual em cibersegurança

A Tabela 3 exibe os resultados da consultoria, na qual servidores foram individualmente abordados e, quando autorizavam, foram auxiliados a habilitar a A2F em relação ao seu e-mail institucional, utilizando o app Google Authenticator. Em 47,97% dos casos, não conseguimos habilitar a A2F ou comprovar que já estava habilitada. Os motivos foram diversos. O principal (30,89%) foi não ter recebido a autorização para habilitar a A2F, o que respeitamos. Não obstante, em 52,03% das abordagens, obtivemos sucesso.

Tabela 3. Resultados da consultoria individualizada em cibersegurança.

Avaliação	Resultados da intervenção	Qtd.	%
Sucesso	Habilitou A2F a partir da intervenção	30	24,39
	Reportou ter habilitado A2F e comprovamos isso	34	27,64
Insucesso	Erro no processo de habilitação	3	2,44
	Não habilitou A2F porque não usa o e-mail institucional	10	8,13
	Não habilitou A2F porque não tem disponibilidade de tempo para habilitar	5	4,07
	Não habilitou A2F porque não foi dada autorização	38	30,89
	Reportou ter habilitado A2F e não autorizou verificação	3	2,44
Total		**123**	**100**

Foram 30 ações bem-sucedidas de habilitação da A2F e 34 comprovações de que esse recurso já estava habilitado. Esses dados são promissores e sugerem a eficiência da intervenção para incentivar o comportamento de habilitar A2F, comprovando a sua ocorrência, algo não alcançado pela palestra. Avaliamos que intervenções dessa natureza precisam ser aperfeiçoadas, continuar a ser realizadas e devem ser avaliadas criticamente.

Notamos que muitos servidores foram abordados em momentos de trabalho e nem sempre tinham tempo para receber os monitores. Outros ficaram com receio de realizar a habilitação da A2F e, posteriormente, ter dificuldades para acesso ao seu e-mail. Problemas dessa natureza destacam a necessidade de mais investimento de tempo, esforço e criatividade para a capacitação de pessoas em cibersegurança [Tian 2024, Henderson et al. 2024].

5.3. Intervenção 03: Curso sobre cibersegurança

A Tabela 4 exibe a média de acertos no pré e pós-teste por módulo e em relação a todo o curso, sendo 10 a nota máxima. Exibe também os percentuais de autoconfiança nas próprias respostas, cuja nota máxima é 100.

Tabela 4. Resultados das avaliações de acertos e autoconfiança.

Módulo	Acertos			Segurança		
	Pré	Pós	Diferença	Pré	Pós	Diferença
1	8,14 (1,65)	9,51 (0,98)	1,37	74,51 (24,38)	86,27 (18,85)	11,76
2	8,04 (1,69)	9,02 (1,57)	0,98	73,53 (23,61)	85,29 (18,52)	11,76
3	8,53 (1,65)	9,9 (0,41)	1,37	50 (27,64)	58,82 (22,14)	8,82
4	6,56 (1,78)	8,24 (1,58)	1,68	51,76 (31,91)	62,35 (36,02)	10,59
Todos	7,82 (1,69)	9,17 (1,13)	1,35	62,45 (26,89)	73,19 (23,88)	10,74

As notas no pré-teste foram de moderadas a altas, com médias variando entre 6,56 e 8,53. Isso pode estar relacionado ao grande número de alunos de computação compondo a amostra do curso [Henklain et al. 2024]. Não obstante, é possível notar um aumento das notas no pós-teste, que passaram a variar de 8,24 a 9,90. Observamos que o módulo que parece ter gerado mais dificuldade foi o último, sobre phishing. Provavelmente esse dado está relacionado ao fato de que o instrumento de medida adotado nele era mais refinado e tinha mais itens. Considerando os dados de todos os módulos, encontramos uma diferença estatisticamente significativa entre as médias de acertos no pré e no pós-teste ($Z = 3,621$, $p < 0,001$, $r_{pb} = 1,00$, $n = 17$), com tamanho do efeito grande. Esse dado sugere que houve aprendizagem no sentido de aperfeiçoamento do repertório dos participantes a partir de sua exposição ao curso [Kienen et al. 2021]. Os COs 2 a 4, do Módulo 2, merecem maior atenção em estudos futuros, pois foram os que apresentaram menores ganhos.

Também notamos melhora de autoconfiança entre pré e pós-teste, embora mais modesta do que a melhora de desempenho. Os Módulos 3 e 4 se destacaram como aqueles que geraram menos autoconfiança. Isso pode ter ocorrido em relação ao Módulo 3 porque os itens avaliaram conhecimentos específicos sobre criação de senhas, gerenciadores de senhas e autenticação de dois fatores, como "A entropia de senha é uma métrica comumente usada na academia para definir a força de uma senha", cuja resposta era possível identificar, mas com alguma incerteza. O Módulo 4 deve ter gerado menos certeza nas respostas pelos motivos já expostos de que eram mais itens e com construção em estágio mais avançado, sendo o gabarito menos óbvio. No geral, a melhora de autoconfiança foi estatisticamente significativa e com tamanho do efeito grande ($Z = 2,438$, $p < 0,016$,$r_{pb} = 0,673$, $n = 17$). A exposição a testes e as videoaulas criadas parecem ser os motivos pelos quais encontramos aumento de autoconfiança, conforme previsto pela teoria adotada [Cortegoso and Coser 2023].

Com relação ao grau de satisfação dos participantes com o curso, novamente notamos elevados níveis, variando de 4 a 5 entre servidores e de 4,07 a 4,67 entre alunos. O item com menor grau de satisfação foi a forma de divulgação do curso, o que é compatível com o dado encontrado em relação à palestra, pois as duas intervenções foram divulgadas

juntas e muitos participantes estiveram em ambas. Destacaram-se as pontuações positivas nos itens sobre relevância do conteúdo dos módulos (Média = 4,65; DP = 0,49) e compromisso dos organizadores do curso com a qualidade da formação (Média = 4,65; DP = 0,61). Esses resultados sugerem que o curso teve valor reforçador para os participantes, tendo potencial para incentivá-los a seguir estudando sobre cibersegurança, tal como no caso da palestra [Moreira and Medeiros 2018].

Verificamos, ainda, ao final da avaliação de satisfação que 16,67% dos participantes reportaram ter habilitado a A2F após o curso. Foram 14,81% que relataram ter melhorado a força de, pelo menos, uma senha e 14,81% começaram a cuidar mais em relação aos links nos quais clicam. Observamos que 11,11% disseram que começaram a fazer backup de seus dados e 11,11% instalaram antivírus em computador ou dispositivo móvel. Um quantitativo menor instalou gerenciador de senhas (9,26%), começou a cuidar mais da atualização de softwares (7,41%), passou a explorar softwares para aperfeiçoar a sua cibersegurança (7,41%) e refletiu sobre fornecimento de seus dados na Internet (3,70%). Apenas 2 pessoas (3,70%) reportaram não ter feito nada.

Esses resultados convergem com os comportamentos-objetivo que tínhamos por propósito ensinar. Em síntese, embora os dados sejam preliminares, podemos afirmar que o curso foi eficiente em relação a promoção de aprendizagens e autoconfiança dos 8 comportamentos-objetivo propostos, tendo, ainda, gerado satisfação. Ressaltamos, ainda, que 9 monitores avaliaram a experiência de trabalhar nesse projeto: 88,9% apresentaram satisfação $\geq$ a 4 e 77,8% voltariam a atuar em projeto análogo.

Apesar dos resultados positivos, reconhecemos que o nosso estudo possui limitações. Não podemos esquecer que o grau de evasão foi elevado na palestra e no curso, assim como tivemos dificuldade para que os servidores da universidade aceitassem participar do processo de habilitação da A2F. Nossas hipóteses para essa baixa adesão às intervenções envolvem a (1) divulgação limitada, que poderia ter sido feita in loco e por canais de comunicação oficiais, (2) associada ao fato de que não buscamos apoio prévio junto às lideranças da instituição em termos de divulgação ou organização de horários para que os servidores se dedicassem a participar de uma das intervenções. Ademais, acreditamos ser crucial para entender esse comportamento de baixo engajamento, a existência de concorrência entre as atividades laborais e aquelas propostas pela intervenção. Ou seja, o servidor teria uma tarefa adicional a desempenhar, no caso, participar da intervenção, e ainda precisaria ajustá-la à sua agenda de compromissos.

O resultado desse baixo engajamento foi coletarmos dados com pequenas amostras, o que impede generalização das nossas conclusões. Não obstante, dado o caráter exploratório dessa pesquisa, consideramos que as 33 pessoas expostas à palestra, as 17 capacitadas no curso e as 123 contatadas na consultoria representem uma amostra promissora para que pudéssemos testar preliminarmente as nossas intervenções.

Sabemos também que participaram deste estudo muitas pessoas com conhecimento de informática. Embora o contato técnico com conhecimentos de computação auxilie no desenvolvimento de comportamentos de cibersegurança, nem sempre isso é uma garantia de que eles estão bem desenvolvidos e de que são emitidos regularmente [Henklain et al. 2024]. Em nossa experiência, essa população também precisa ser capacitada e incentivada a adotar comportamentos de cibersegurança.

Com relação aos instrumentos de coleta de dados, avaliamos que precisam ser aperfeiçoados e boas práticas psicométricas podem ajudar. Também consideramos que a obtenção de tantas notas máximas em avaliações de satisfação possa indicar um viés de resposta relacionado à desejabilidade social. Esse fenômeno ocorre quando o participante busca agir em conformidade com o que ele considera ser o esperado [Gouveia et al. 2009]. Para estudos futuros, podemos incluir a aplicação de uma escala de desejabilidade social para controlar essa variável, permitindo conclusões mais seguras.

Consideramos importante também, tal como fizemos no curso, avaliar o conhecimento dos participantes antes e após as intervenções, para examinar se algum comportamento foi aprendido. Não obstante, é preciso cautela no exame desse dado porque a própria exposição ao pré-teste pode favorecer melhora de desempenho no pós, o que aponta para a necessidade de desenvolvimento de teste paralelos, de mesma extensão e dificuldade, mas com itens distintos.

6. Conclusão

O objetivo deste estudo foi avaliar duas intervenções (palestra e consultoria) para incentivo e uma (curso) para ensino de comportamentos de cibersegurança em contexto de universidade pública. Encontramos evidências favoráveis de eficiência dessas estratégias, bem como aspectos a aperfeiçoar em intervenções futuras.

Para trabalhos futuros, esperamos (1) ampliar o número de monitores e, com a fase de produção de recursos pedagógicos já superada, poderemos nos dedicar mais à divulgação das intervenções, contatando previamente líderes de cada setor para que conversem com os seus funcionários. Entendemos que essa estratégia pode garantir maior adesão às intervenções. Adicionalmente, buscaremos (2) intervir preferencialmente com pessoas sem conhecimento técnico na área de informática. Com relação aos instrumentos, (3) uma estratégia psicométrica que pode ser um primeiro passo para aperfeiçoá-los é solicitar que especialistas em educação em cibersegurança os avaliem, para indicar se estão adequados. Também é interessante que sejam criados testes paralelos para avaliação de conhecimento e que seja aplicada medida de avaliação de desejabilidade social. Além dessas ações, outros pesquisadores interessados neste estudo podem, ainda, examinar a pertinência dos comportamentos-objetivo que propusemos para orientar o desenvolvimento de intervenções no âmbito de suas realidade institucionais.

Por fim, avaliamos que a estrutura proposta de cada intervenção, os recursos pedagógicos desenvolvidos e os comportamentos-objetivo propostos neste estudo podem orientar futuras intervenções educacionais e pesquisas sobre educação em cibersegurança. Além disso, a realização dessas ações permitiu, no contexto da organização em que foram executadas, que fossem dados os primeiros passos para o desenvolvimento de comportamentos de cibersegurança, o que pode fortalecer a sua resiliência em face das ameaças do ciberespaço.

Referências

Alanazi, M., Freeman, M., and Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, 136:1–14.

CERT.br (2024). Páginas falsas utilizadas em tentativas de phishing. Recuperado de https://stats.cert.br/phishing/.

Cortegoso, A. L. and Coser, D. S. (2023). *Elaboração de programas de ensino: Material autoinstrutivo*. EdUFSCar.

Dawkins, S. and Jacobs, J. (2023). Nist phish scale user guide.

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.

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 ERSI-RJ*, pages 1–7, Porto Alegre. SBC.

Henderson, N., Pallett, H., Linden, S. V. D., Montanarini, J., and Buckley, O. (2024). The disphishinformation game: Creating a serious game to fight phishing using blended design approaches. In *AHFE (2024) International Conference*. AHFE International.

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*, pages 76–91, Porto Alegre, RS, Brasil. SBC.

Hoepers, C. (2024). A importância dos fatores humanos para a cibersegurança. *Computação Brasil*, 52:61–66.

Kienen, N., Panosso, M. G., Nery, A. G. S., Waku, I., and Carmo, J. d. S. (2021). Contextualização sobre a programação de condições para desenvolvimento de comportamentos (pcdc): Uma experiência brasileira. *Perspectivas em Análise do Comportamento*, 12(2):360–390.

Losse, M., Morais, A., Sousa, E., Cabral, R., Santos, G., and Lins, F. (2024). Cultura de segurança da informação - um relato de oficinas para conscientização de servidores em organizações públicas. In *Anais do XX SBSI*, pages 261–264, Porto Alegre, RS. SBC.

Moreira, B. M. and Medeiros, A. C. (2018). *Princípios básicos de análise do comportamento*. Artmed.

Nogueira, M. (2024). Segurança na conectividade: Protegendo redes e conexões. *Computação Brasil*, (52):30–34.

Omoyiola, B. O., Mckeeby, J., and Whyte, S. T. (2024). The strategies for mitigating the human insider factor in cybersecurity. *SSRN Electron. J.*

Paudel, R. and Al-Ameen, M. N. (2024). Priming through persuasion: Towards secure password behavior. *Proc. ACM Hum.-Comput. Interact.*, 8(CSCW1).

Rahman, T., Rohan, R., Pal, D., and Kanthamanon, P. (2021). Human factors in cybersecurity: A scoping review. In *Proceedings of the 12th IAIT '21*, pages 1–11, New York, USA. ACM.

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.

Schleich, A. L. R., Polydoro, S. A. J., and dos Santos, A. A. A. (2006). Escala de satisfação com a experiência acadêmica de estudantes do ensino superior. *Avaliação Psicológica*, 5:11–20.

Silva, M. B. F. (2023). *Cibersegurança: Uma visão panorâmica sobre a segurança da informação na Internet*. Freitas Bastos Editora.

Tian, X. (2024). Unraveling the dynamics of password manager adoption: a deeper dive into critical factors. *Information and Computer Security*, ahead-of-print.