

Segurança Cibernética para Alunas do Ensino Médio: Um Relato de Experiência

Maristela Holanda¹, Camila de S. Oliveira², Olívia H. G. Martins²,
Gisele C. R. de Carvalho², Ana Beatriz G. Lima², Manuela F. Mattos¹,
Lorena S. B. Borges¹, João Gondim², Roberto Rodrigues-Filho¹, Aleteia Araujo¹,
Carla Cavalcante Koike¹, Leticia Lopes Leite¹, Maria Emilia M. T. Walter¹

¹ Departamento de Ciência da Computação – Universidade de Brasília
Brasília – DF – Brasil

² Departamento de Engenharia Elétrica – Universidade de Brasília
Brasília – DF – Brasil

{mholanda, lorena.borges, gondim, roberto.filho}@unb.br

{aleteia, ckoike, lleite, mariaemilia}@unb.br

{oliveira-souza.so, olivia.martins, gisele.carvalho}@aluno.unb.br

{ana.goulart, manuela.mattos}@aluno.unb.br

Abstract. *This paper presents an experience report on an educational initiative aimed at promoting cybersecurity awareness among high school female students within the context of the project Meninas.comp. The workshops had two main objectives: (1) introducing women to the field of cybersecurity, and (2) helping high school students protect themselves against cyberattacks. In this way, the initiative seeks to contribute to reducing the gender gap in cybersecurity, considering the low participation of women in the field and the growing demand for qualified professionals. Educational workshops were conducted with students from public schools in Federal District, Brazil, addressing topics such as digital security, cybercrimes that affect women, and prevention strategies in online environments. The methodology included interactive presentations, dynamic activities, and the application of questionnaires before and after the workshops to assess the participants' level of knowledge and perceptions. The results indicate an increase in understanding of the presented concepts, greater awareness of digital risks, and increased interest among the students in deepening their knowledge in the field of cybersecurity.*

Resumo. *Este artigo apresenta um relato de experiência sobre uma iniciativa educacional voltada à promoção da Segurança Cibernética para alunas do ensino médio no contexto do projeto Meninas.comp. Estas oficinas tiveram dois focos principais: 1) a apresentação da área de Segurança Cibernética para mulheres e 2) a proteção das alunas do ensino médio contra os ataques cibernéticos. Desta forma, esta oficina buscou contribuir para a redução da desigualdade de gênero na área de Segurança Cibernética, considerando a baixa participação feminina no setor e a crescente demanda por profissionais qualificados. Foram realizadas oficinas educativas com estudantes de escolas públicas do Distrito Federal, abordando temas como segurança digital, crimes*

cibernéticos que afetam mulheres e estratégias de prevenção no ambiente on-line. A metodologia incluiu apresentações interativas, atividades dinâmicas e aplicação de questionários antes e após a realização das oficinas para avaliar o nível de conhecimento e a percepção das participantes. Os resultados indicam aumento na compreensão dos conceitos apresentados, maior conscientização sobre riscos digitais e interesse das estudantes em aprofundar conhecimentos na área de Segurança Cibernética.

1. Introdução

A transformação digital vem contribuindo em diversos aspectos da sociedade contemporânea, mas aumenta as vulnerabilidades cibernéticas em níveis individuais e corporativos, o que torna crítica a área de Segurança Cibernética. São muitos os desafios nessa área, especialmente com relação à atração, formação e retenção de talentos em Segurança Cibernética [World Economic Forum, Centre for Cybersecurity 2025, Sani et al. 2025, Yogarajah and Hossain 2025]. A escassez de profissionais se deve a uma combinação de fatores que incluem uma demanda crescente por serviços de segurança cibernética, que cresce mais rápido do que a força de trabalho consegue acompanhar, piorada por falta de pessoas com habilidades tecnológicas especializadas e falta de diversidade, o que limita o conjunto de profissionais disponíveis. Com isso, a educação em Segurança Cibernética tem sido uma prioridade em muitos países [Vykopal et al. 2025].

A carreira em Segurança Cibernética tem um crescimento previsto de 32% ao ano, e vem oferecendo oportunidades profissionais em áreas técnicas, estratégicas e de gestão [Nogueira 2025]. Porém, em âmbito mundial, a falta de diversidade de gênero continua sendo uma questão persistente e preocupante, com as mulheres ocupando apenas 25% das funções, apesar dos esforços para promover diversidade e inclusão delas [Techrepublic 2025, Selman-Housein and Plancher 2025, Costa et al. 2025, Elnahass et al. 2025]. Como Segurança Cibernética é uma área essencial para a proteção de informações e de infraestruturas críticas, ter mais diversidade nessa área, em particular com a inclusão de mulheres, não é apenas uma questão de equidade mas também de estratégia. Equipes diversas são mais inovadoras, eficazes e eficientes na solução de problemas, trazendo diferentes perspectivas para enfrentar ameaças cibernéticas cada vez mais sofisticadas. Para construir um futuro mais seguro, é essencial incentivar, apoiar e criar ações para que mais mulheres ingressem e se destaquem em Segurança Cibernética.

A Deloitte [Mossburg, E. and Zalis, S. 2025], em pesquisa recente, explora as razões por trás dessa lacuna de gênero nessa área, em um cenário em que a demanda por profissionais qualificados é alta. Metade das jovens profissionais interessadas em Segurança Cibernética acham que não têm conhecimento suficiente para seguir nessa carreira. Além disso, 55% das mulheres pesquisadas acreditam que o setor pode ser intimidador e 47% expressam preocupação em não serem levadas a sério. Neste artigo, as autoras confirmam que a questão de gênero constitui-se em um problema sério, pois a falta de diversidade em equipes que atuam em Segurança Cibernética pode limitar a inovação e o desenvolvimento de novas metodologias, no sentido de que muitas atividades relacionadas à Segurança Cibernética podem ser aprimoradas por interações entre pessoas com diferentes competências e formas de raciocinar.

A carência de profissionais mulheres em Segurança Cibernética foi relatada no

WIT 2025 [Holanda et al. 2025]. Nessa revisão de literatura, foi encontrado apenas um artigo sobre inclusão de mulheres nessa área no Brasil. Além disso, foram encontradas algumas ações específicas como o “Ladies in Cyber”, que realiza treinamentos, palestras e eventos [Pereira et al. 2025] e a oficina sobre Segurança da Informação e *chatbot*, ministrada pelo projeto “Include Meninas UFF” [Salgado et al. 2023]. Com isso, é evidente a necessidade de mais ações para inclusão de mulheres em Segurança Cibernética.

Neste contexto, o projeto Meninas.comp tem como objetivo apresentar a área de Segurança Cibernética para alunas de escolas públicas do Distrito Federal e atrair alunas de graduação e pós-graduação para essa área, na Universidade de Brasília.

Este artigo foi dividido nas seguintes seções. A Seção 2 apresenta a metodologia para a elaboração do material didático das oficinas com foco em alunas do ensino médio. A Seção 3 descreve a aplicação das oficinas em dois eventos, Fórum de Mulheres em STEM da América Latina e *Girls.comp Day*, analisando o conhecimento antes e após a realização da oficina. Na Seção 4, as lições aprendidas são apresentadas, após um ano de projeto. Por fim, na Seção 5, são apresentadas as conclusões deste artigo e propostos alguns trabalhos futuros.

2. Metodologia

No primeiro e no segundo semestres de 2025, foram realizadas duas oficinas, estruturadas a partir de uma metodologia que combinou estratégias educativas e investigativas. As oficinas tiveram como objetivos conscientizar as alunas do ensino básico e incentivar a participação feminina na área da Segurança Cibernética. A elaboração do material didático foi feita no âmbito da disciplina optativa de quatro créditos, em um semestre letivo, com o tema “Segurança Cibernética para Mulheres”. Neste período, a Universidade de Brasília sediou dois eventos internacionais, Fórum de Mulheres em STEM da América Latina e *Girls.comp Day*. Nos dois eventos, alunas de ensino médio de cinco escolas do Distrito Federal que possuem parceria com o projeto Meninas.comp, participaram das oficinas.

A elaboração das oficinas seguiu quatro etapas principais: elaboração do material educativo; estudo e identificação de ataques cibernéticos; aplicação das oficinas e dinâmicas; e coleta e análise de dados por meio de questionários. Cada uma dessas etapas é detalhada a seguir.

2.1. Elaboração do material educativo

O material educativo foi desenvolvido pelas alunas de graduação com a orientação de docentes da disciplina. Foi utilizado o formato de *slides*, com linguagem acessível e recursos visuais atrativos, adequados à faixa etária das estudantes do ensino médio. Essa abordagem buscou facilitar a compreensão dos conteúdos, tornando-os mais claros, dinâmicos e interessantes para o público-alvo. Inicialmente, o conteúdo dos *slides* foi organizado em três grupos: a importância da Segurança Cibernética; ataques no meio digital que afetam as mulheres; e formas de defesa por controle de acesso e autenticação.

As apresentações foram estruturadas de modo a contemplar, de forma progressiva, o panorama geral da Segurança Cibernética e sua importância, a identificação dos principais crimes digitais com ênfase nos que impactam mulheres e, por fim, as estratégias de proteção e prevenção. O foco esteve na identificação de riscos e na aprendizagem de

medidas preventivas, promovendo um uso mais seguro, crítico e consciente da Internet e das redes sociais.

2.2. Estudo e identificação de ataques cibernéticos

Nesta etapa foi realizada uma revisão bibliográfica com o objetivo de identificar e compreender os principais ataques cibernéticos direcionados às mulheres. Para isso, foram analisados artigos científicos, livros, relatórios institucionais e pesquisas recentes nas áreas de segurança digital e gênero. A revisão permitiu identificar diferentes formas de violência digital e compreender como esses ataques ocorrem, suas principais características e impactos. Entre os casos identificados destacam-se o discurso de ódio online [UNESCO 2021], o vazamento de imagens íntimas [Henry and Powell 2018], o *stalking* digital [Charan 2023] e o assédio em redes sociais [Im et al. 2023]. Outros estudos também apontam a expansão dessas formas de violência digital e seus efeitos sociais e psicológicos para as vítimas [Malanga 2021, Enock et al. 2024].

Essa fundamentação teórica foi essencial para subsidiar a elaboração do material educativo utilizado nas oficinas, exemplificado na Figura 1. A revisão da literatura permitiu identificar padrões de ataques e estratégias de prevenção, garantindo que as atividades abordassem de forma crítica e contextualizada as formas mais recorrentes de violência digital contra mulheres. Dessa forma, buscou-se proporcionar uma abordagem educativa informada e sensível às experiências das participantes durante o processo de aprendizagem [Sağlam et al. 2023].



Figura 1. Slides mostrando ataques cibernéticos às mulheres

2.3. Aplicação das oficinas e dinâmicas

Durante as oficinas, os dois focos principais foram apresentar os ataques cibernéticos mais comuns e orientar as participantes sobre como se proteger, utilizando uma linguagem apropriada ao perfil das alunas. Os conteúdos seguiram a organização descrito nas seções anteriores, tendo sido abordados os seguintes tópicos:

- Introdução à Segurança Cibernética, utilizando exemplos do cotidiano e situações noticiadas em plataformas digitais;
- Valorização de mulheres na Segurança Cibernética, destacando sua importância na área tecnológica e o impacto de sua atuação na sociedade;
- Apresentação de crimes cibernéticos, com exemplos práticos e orientações sobre como reconhecer e denunciar esses casos;
- Prevenção e controle de acesso, explorando estratégias para segurança no meio digital.

A primeira oficina foi organizada para duas turmas com aproximadamente 20 a 30 alunas, cada, com duração de cerca de 45 minutos. Já a segunda oficina contou com quase 60 alunas, com duração aproximada de 1 hora. Em ambas as oficinas, as alunas tiveram a oportunidade de escolher a Segurança Cibernética como tópico de aprendizagem no evento, tendo sido selecionadas de maneira aleatória. Nas duas oficinas, as dinâmicas foram planejadas considerando o tempo de duração, a quantidade de participantes, o perfil e a idade das alunas. As atividades foram distribuídas ao longo das apresentações, garantindo maior atenção e engajamento nos tópicos, promovendo aprendizado, tornando as palestras mais interativas e menos cansativas. Cada grupo de alunas criou uma dinâmica específica em que utilizaram como apoio livros e livretos educativos produzidos pelo CERT.br¹ (Figura 2), que foram disponibilizados para as alunas levarem para casa.



Figura 2. Uma atividade de decodificação por símbolos foi utilizada em uma das dinâmicas para estimular reflexões sobre o tema de *cyberbullying* [CERT.br]

2.4. Coleta e análise de dados por meio de questionários

Para avaliar o conhecimento e o interesse das participantes, bem como suas experiências e os conhecimentos adquiridos, foram criados dois questionários anônimos de percepção, preenchidos no início e no final das oficinas, com o consentimento de que seriam utilizados para fins de pesquisa. Os dados obtidos foram analisados de forma qualitativa para verificar a efetividade da oficina.

O material didático disponibilizado², permite que outras instituições o utilizem, após o processo de revisão. Ressalta-se que os instrumentos de coleta de informações foram direcionados especificamente à percepção e aos conhecimentos relacionados à

¹Material produzido pelo CERT.br (<https://www.cert.br/>)

²As aulas podem ser encontradas neste link (https://drive.google.com/drive/folders/1vBj5cSYk_OHy5th_DKdo_HQBf74g7UP_)

Segurança Cibernética, não tendo sido incluídas métricas ou questões destinadas à avaliação de letramento digital de forma ampla. Foi ainda garantida a anonimização e preservação da identidade das alunas.

3. Aplicando a Oficina

Esta seção apresenta o processo de realização da oficina, começando na Subseção 3.1, com o perfil das participantes, em seguida uma análise de conhecimento antes (Subseção 3.2) e após a oficina (Subseção 3.3).

3.1. Perfil das participantes

Com o objetivo de compreender as características das participantes e avaliar a adequação da atividade a esse público-alvo, foi realizada uma análise do seu perfil a partir das respostas coletadas no formulário final ($n = 24$). A caracterização do público permite identificar aspectos relevantes como faixa etária, nível de escolaridade e etapa de formação, contribuindo para a avaliação do alcance da ação e para o planejamento de iniciativas futuras.

A Figura 3 apresenta o perfil das respondentes. Foi analisada a distribuição etária de acordo com os dados coletados no formulário. Na Figura 3(a), apresenta-se o nível de escolaridade das participantes. Nota-se que 88% encontram-se matriculadas no Ensino Médio, confirmando a adequação do público alcançado em relação ao público-alvo da ação. A ocorrência de uma resposta com Ensino Superior completo está associada ao professor acompanhante. A Figura 3(b) apresenta a distribuição das alunas por série. Verifica-se a participação de estudantes do Ensino Médio, com maior concentração nos anos finais, 2º e 3º anos.

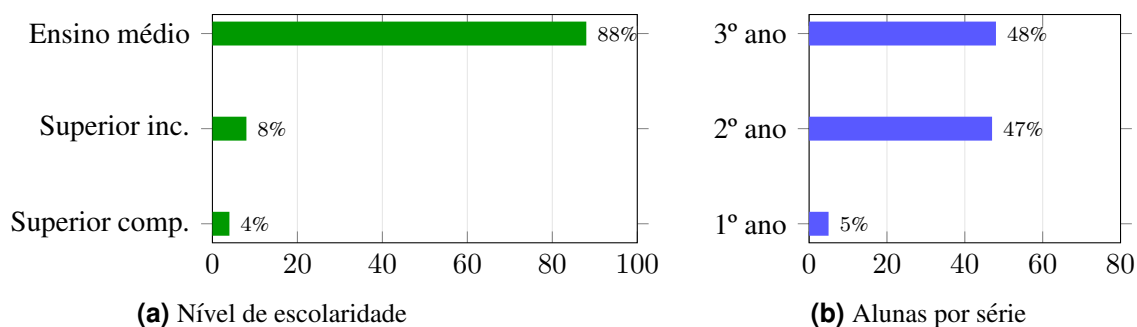


Figura 3. Perfil das participantes com relação à escolaridade, em percentuais

De modo geral, os resultados evidenciam que a atividade alcançou predominantemente estudantes em fase final do Ensino Médio, etapa caracterizada pelo processo de definição da trajetória acadêmica e profissional. Esse perfil é especialmente relevante, pois ações de sensibilização e apresentação de áreas como a Segurança Cibernética tornam-se mais efetivas nesse momento, contribuindo para estimular o interesse feminino na área de Computação e para a ampliar a participação de mulheres em tecnologias.

3.2. Percepção inicial das participantes

Antes da realização da oficina, foi aplicado um questionário com o objetivo de compreender o nível inicial de conhecimento e a percepção das participantes sobre os temas

relacionados à Segurança Cibernética. O questionário foi respondido por 38 participantes (n = 38).

A Figura 4 apresenta os resultados referentes as perguntas Q1 - "Você acha que a Segurança Cibernética é importante?", Q2 - "Você já ouviu falar de perseguição cibernética (*cyberstalking*)?" e Q3 - "Você já ouviu falar em *deepfakes*?".

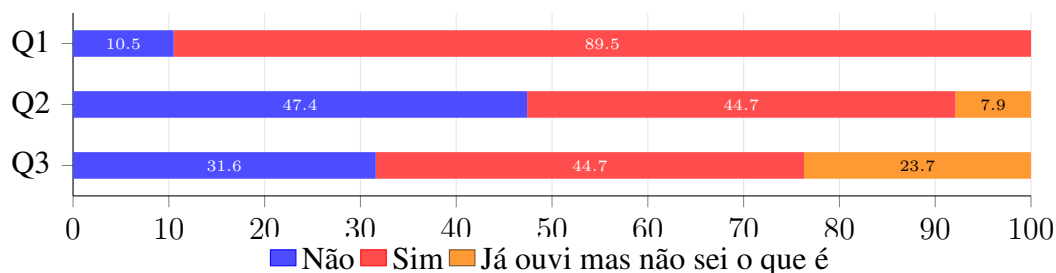


Figura 4. Percepção inicial das participantes (n=38)

Os dados da Q1 apresentados na Figura 4 mostram que a maioria das participantes (89,5%) considera a Segurança Cibernética importante, indicando que as respondentes já possuíam uma percepção inicial positiva sobre a relevância do tema no contexto digital.

Entretanto, ao analisar o conhecimento sobre ameaças específicas, foram identificadas lacunas importantes. Os resultados da Q2 apresentados na Figura 4 mostra que 47,4% das participantes declararam não conhecer o conceito de perseguição cibernética (*cyberstalking*), enquanto 7,9% afirmaram possuir apenas familiaridade superficial com o termo. Resultado semelhante pode ser observado nos dados da Q3 apresentados na Figura 4, em que 23,7% das participantes afirmaram não conhecer o conceito de *deepfakes*, e 31,6% declararam desconhecer o assunto.

As respostas abertas sobre os interesses das participantes indicam que as principais demandas estão relacionadas à aplicação prática da segurança digital. Entre os temas mais mencionados, destacam-se formas de proteção de dados pessoais e de contas em redes sociais, prevenção contra golpes e ataques virtuais, orientações sobre como agir em situações de violência ou crimes digitais e interesse em compreender, na prática, o funcionamento da Segurança Cibernética.

De forma geral, embora temas mais presentes no cotidiano digital, como vazamento de dados pessoais e violência cibernética, apresentem alto nível de conhecimento entre as respondentes, os resultados indicam menor conhecimento sobre ameaças emergentes e conceitos mais específicos da área.

3.3. Percepção final das participantes

Ao final da oficina, os dados coletados indicaram avanços significativos no conhecimento das participantes sobre Segurança Cibernética. O questionário final foi respondido por 24 estudantes (n = 24), permitindo identificar mudanças na percepção e no interesse pelo tema após a realização da atividade. A redução no número de respostas em relação ao questionário inicial ocorreu devido à participação parcial de algumas estudantes apenas na etapa inicial da oficina.

Embora a maioria das participantes tenha afirmado possuir conhecimento prévio

sobre Segurança Cibernética, a análise das respostas relacionadas aos tópicos apresentados evidencia que a oficina contribuiu para ampliar a compreensão das alunas sobre conceitos específicos da área.

Ao fazer uma avaliação sobre os conteúdos apresentados na oficina, foi criada uma escala de 1 a 5 em termos de interesse e clareza, em que 1 significa “Não gostei/não entendi” e 5 significa “Gostei muito/entendi completamente”. Os resultados mostram que os assuntos que mais se destacaram entre as alunas do ensino médio foram a “Postura no uso da internet” e a “Importância de mulheres na cibersegurança”. Isso indica que elas têm grande interesse em aprender como devem agir com segurança na Internet e nas redes sociais. Além disso, o interesse pelo tema da presença feminina demonstra que elas se identificaram com a profissão e perceberam como é importante ter mulheres atuando nessa área (Figura 5).

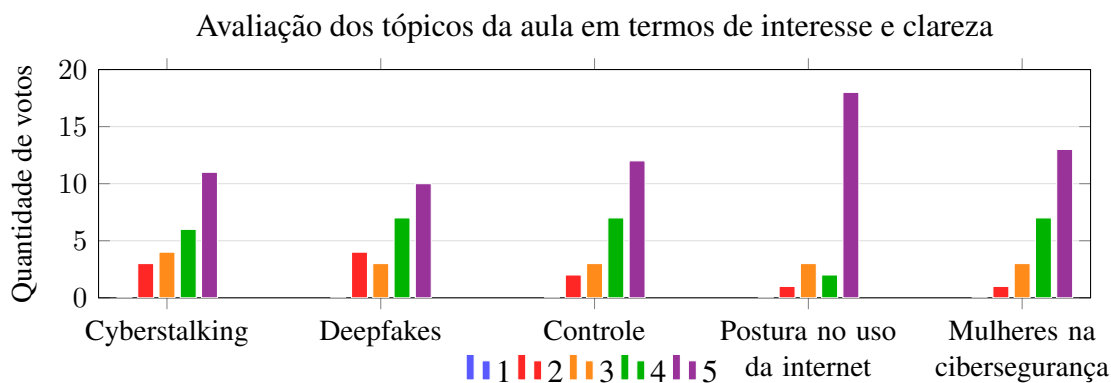


Figura 5. Respostas obtidas na avaliação dos tópicos debatidos na oficina

Em relação ao interesse em aprender mais sobre cibersegurança, 16 das 24 respondentes (66,7%) afirmaram ter se interessado em aprofundar seus conhecimentos no tema. Outras 6 respondentes (25,0%) responderam “talvez”, enquanto 2 respondentes (8,3%) indicaram não ter interesse em aprender mais sobre o assunto. Esses resultados sugerem que a oficina não apenas transmitiu informações, mas também estimulou a curiosidade e o envolvimento contínuo das participantes (Tabela 1).

Perguntas abertas referentes a definições pessoais de cibersegurança e de *cyberstalking* mostraram que muitas respondentes foram capazes de elaborar explicações próprias após a oficina, utilizando conceitos mais claros associados a situações concretas no ambiente digital. Essas repostas ajudam a identificar a apropriação dos conceitos abordados, revelando um nível mais profundo de compreensão, quando comparado à percepção inicial do grupo. A Figura 6 apresenta uma nuvem de palavras gerada a partir dessas respostas, evidenciando os termos mais recorrentes e associados à compreensão das participantes.

Em termos de importância percebida da cibersegurança, 23 das 24 respondentes (95,8%) declararam sentirem-se mais familiarizadas com a importância de compreender a violência cibernética, enquanto 1 respondente (4,2%) indicou compreender apenas parcialmente o tema. Além disso, 20 respondentes (83,3%) afirmaram que, após a oficina, passaram a considerar mais importante se proteger no ambiente virtual. Outras 3 respondentes (12,5%) relataram que nunca haviam pensado sobre essa questão anteriormente,

Tabela 1. Percepção final das participantes

Pergunta	Categoria	%
Interesse em aprender mais sobre cibersegurança	Sim	66,7
	Não	8,3
	Talvez	25,0
Familiaridade com a importância de saber sobre violência cibernética	Sim, entendi bem	95,8
	Mais ou menos	4,2
	Ainda estou confusa	0,0
Compreensão da importância de se proteger no ambiente virtual	Sim, mudei opinião após a aula	83,3
	Nunca tinha pensado nisso, mas agora estou refletindo mais	12,5
	Não e não acho seja importante	0,0
	Sim (outra resposta positiva)	4,2
Interesse em explorar carreiras/áreas de segurança cibernética	Interessada	75,0
	Muito interessada	12,5
	Pouco interessada	12,5

Nota: Percentuais calculados para $n = 24$ participantes.

mas que passaram a refletir mais sobre o tema após a atividade. Esses resultados estão apresentados na Tabela 1. Da mesma forma, quando questionadas sobre a relevância desse assunto para meninas do ensino fundamental e médio, quase todas falaram que é realmente importante aprofundar esse conhecimento desde as etapas iniciais da formação escolar. Adicionalmente, a maioria das participantes avaliou as atividades como “muito importantes” ou “importantes”, ressaltando a percepção de que iniciativas como esta são essenciais para ampliar a consciência sobre segurança no ambiente digital entre as jovens alunas. Quanto ao interesse em explorar áreas relacionadas à segurança cibernética, 18 das respondentes (75%) demonstraram curiosidade, com respostas indicando interesse ou forte interesse em seguir explorando o tema.

De modo geral, os resultados sugerem que a intervenção educativa, por meio das oficinas, não só aumentou o nível de conhecimento sobre aspectos específicos de Segurança Cibernética, como também reforçou a percepção de importância do tema e estimulou atitudes de reflexão crítica entre as participantes. Tais dados evidenciam a necessidade de ampliar o debate sobre Segurança Cibernética no contexto educacional, especialmente entre as jovens alunas do ensino básico.

4. Lições aprendidas

Após um ano de projeto, integrando pesquisa, ensino e extensão no tema de inclusão de mulheres na área de Segurança Cibernética, destacamos:



Figura 6. Nuvem de palavras com as respostas às perguntas abertas

- Criar uma disciplina optativa com essa temática fez com que as alunas da graduação pudessem aprimorar conteúdos em Segurança Cibernética e refletir sobre a necessidade de maior participação das mulheres na área;
- Elaborar uma apresentação mais dinâmica potencializou atrair a atenção das alunas de ensino médio, durante as oficinas;
- Ressaltar a importância de referências bibliográficas confiáveis permitiu criar conteúdos abordados nas oficinas com base sólida;
- Utilizar brindes é uma forma de incentivar a participação nas atividades;
- Utilizar as redes sociais e criar um perfil do evento permitiu divulgar informações relevantes às participantes;
- Utilizar materiais disponibilizados pelo projeto Meninas.com, em colaboração com o CERT.br, auxiliou nas atividades e facilitou o acesso às informações;
- Certificar que os questionários foram respondidos por todas as alunas presentes na segunda oficina, aspecto que não foi conferido na primeira oficina, permitiu incluir mais dados a serem analisados.

5. Conclusões

A Segurança Cibernética é um tema fundamental na sociedade e ter mulheres neste campo de trabalho é uma necessidade reconhecida amplamente. Para contribuir com a atração de mulheres para essa área, este artigo apresentou um relato de experiência do projeto Meninas.comp, que criou material didático específico para o ensino desse tópico em escolas de ensino médio, utilizado em oficinas. Essa ação tem dois principais objetivos, o de criar conteúdo de qualidade para auxiliar as adolescentes a se protegerem no ambiente virtual, que pode ser hostil e violento, e o de atrair alunas de graduação em computação e tecnologias para a área de Segurança Cibernética, o que contribui para incluir mais mulheres para atuarem profissionalmente nessa área.

Como trabalhos futuros, pretendemos aplicar essas oficinas em mais escolas do Distrito Federal, criar jogos com a temática de proteção de meninas no ambiente virtual e elaborar mais conteúdos didáticos no tema.

6. Uso de Inteligência Artificial

A Inteligência Artificial foi utilizada para melhorar os gráficos do artigo e figuras com a ferramenta Prism. O ChatGPT foi utilizado para auxiliar na escrita em latex.

7. Agradecimentos

Os autores agradecem à CAPES pela aprovação do projeto no Programa PROEXT-PG (processo 88881.927455/2023-01). Agradecemos também ao grupo Mulheres do Brasil (Brasília), à empresa Neospace pelo apoio ao projeto Meninas.comp e ao CERT.br pela doação dos livros.

Referências

- Charan, J. I. (2023). Cyber stalkers and cyberbullies: Protecting women in the digital age. *CYBER CRIME &*, page 119.
- Costa, G., De Francisci, S., Renieri, M., and Valiani, S. (2025). Tackling the gender gap in cybersecurity education. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1*, pages 234–240.
- Elnahass, M., Ahmed, Y., and Trinh, V. Q. (2025). Empowering women to lead cybersecurity: The effect of female executives on disclosure sentiment. *International Journal of Finance & Economics*, 30(4):3368–3394.
- Enock, F. E. et al. (2024). Understanding gender differences in experiences and concerns surrounding online harms: A short report on a nationally representative survey of uk adults. *arXiv preprint*.
- Henry, N. and Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse*, 19(2):195–208.
- Holanda, M., Lima, A., Bernardes, E., Silva, L., Mitzi, M., Araujo, A., Gondim, J., and Walter, M. E. (2025). Inclusão de mulheres na área de Cibersegurança no Brasil. In *Anais do XIX Women in Information Technology*, pages 1–12, Porto Alegre, RS, Brasil. SBC.
- Im, J. et al. (2023). Women’s perspectives on harm and justice after online harassment. *arXiv preprint*.
- Malanga, D. F. (2021). Survey of cyber violence against women in malawi. In *Proceedings of the 1st Virtual Conference on Implications of Information and Digital Technologies for Development*, pages 623–634.
- Mossburg, E. and Zalis, S. (2025). Unlocking a more resilient and secure future. <https://www.roadsec.com.br/comunidades23/cyber-security-girls-br>. Acessado em 08 mar. 2025.
- Nogueira, M. (2025). Carreiras em cibersegurança: Oportunidades no mercado em alta. *SBC Horizontes*, 1:1.
- Pereira, F., Lopes, I., and Salinas, M. (2025). Ladies in cyber: Mulheres na cibersegurança – um projeto de empoderamento feminino na Área de tecnologia. In *Anais do XXV Simpósio Brasileiro de Cibersegurança*, pages 1098–1105, Porto Alegre, RS, Brasil. SBC.

- Salgado, L., Avelino, M., Herdy, I., Santoyani, A., and Monteiro, M. (2023). Aproximando meninas da computação: Lições aprendidas em oficinas de Secbots. In *Anais do XVII Women in Information Technology*, pages 376–381, Porto Alegre, RS, Brasil. SBC.
- Sani, A. I., Olajide, A. O., Abosede, O. V., Oyebode, D. F., Vayyala, R., Alfred, J. G., Oseni, T., Jegede, E. O., Nwaogu, N. G., and Abbas, R. (2025). Cybersecurity challenges in digitizing government administration. In *Proceedings of the International Academy of Sciences*, number 1 in 2, pages 1–13.
- Sağlam, R. B., Miller, V., and Franqueira, V. N. L. (2023). A systematic literature review on cyber security education for children. *IEEE Transactions on Education*, 66(3):274–286.
- Selman-Housein, E. and Plancher, B. (2025). Improving the representation of undergraduate women in cybersecurity: A literature review. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1*, page 1043–1049.
- Techrepublic (2025). Deloitte: Why Only a Quarter of Cybersecurity Professionals are Women. <https://www.techrepublic.com/article/security-gender-pay-gap-deloitte/#:~:text=As%20of%202023%2C%20women%20make,skilled%20professionals%20in%20the%20industry>. Acessado em: 08 mar. 2025.
- UNESCO (2021). The chilling: Global trends in online violence against women journalists.
- Vykopal, J., Švábenskỳ, V., Lopez, M. T., and Čeleda, P. (2025). Cybersecurity study programs: What’s in a name? In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1*, pages 1169–1175.
- World Economic Forum, Centre for Cybersecurity (2025). The cybersecurity industry has an urgent talent shortage. <https://www.roadsec.com.br/comunidades23/cyber-security-girls-br>. Acessado em: 08 mar. 2025.
- Yogarajah, J. and Hossain, G. (2025). Optimizing cybersecurity recruitment with graph-based algorithms. In *2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC)*, pages 1–7.