SEGURANÇA CIBERNÉTICA NA EDUCAÇÃO BÁSICA: UM RELATO DE EXPERIÊNCIA NO COLÉGIO PROFESSORA HILDA MONTEIRO MENEZES

Evelly Keise Santos Lopes [1]
Roberto de Souza Freitas [2]
Damon Ferreira Farias [3]

RESUMO

Oficinas pedagógicas são atividades práticas realizadas visando uma maior compreensão dos conteúdos a serem ensinados aos alunos, com estratégias didáticas previamente planejadas e elaboradas. Com isso, este artigo, tem como objetivo sensibilizar os estudantes sobre práticas seguras no uso da internet, abordando temas como senhas fortes, privacidade nas redes sociais, reconhecimento de ameaças virtuais e uso ético da tecnologia. Autores como Amankwa (2021), Stillings (2020), Silva (2021) entre outros, estruturam a base teórica do artigo. A pesquisa é do tipo exploratória e descritiva, assumindo uma abordagem qualitativa no tratamento dos dados. Durante a execução da oficina realizada pelos pibidianos de licenciatura em ciências da computação do Instituto Federal de Educação, Ciência e Tecnologia Baiano, campus Senhor do Bonfim (BA), percebeu-se que a oficina despertou nos participantes interesse pela área. Também demonstrou que muitos adolescentes possuem conhecimentos ainda limitado sobre os riscos digitais e medidas de proteção no ambiente virtual. Por fim, verifica-se que a oficina segurança cibernética contribuiu para fomentar o pensamento crítico, o senso de responsabilidade e o protagonismo juvenil no uso das tecnologias digitais.

Palavras-chave: Pibid, Segurança cibernética, Ensino médio, atividades práticas, Tecnologia.

INTRODUÇÃO

[1] Graduando do Curso de Licenciatura em Ciências da Computação do Instituto Federal de Educação, Ciência e Tecnologia Baiano - BA, evellykeiselopes@gmail.com;
[2] Graduado pelo Curso de Licenciatura em Ciências da Computação do Instituto Federal de Educação, Ciência e Tecnologia Baiano - BA, robertosouzafreitas43@gmail.com;
[3] Doutor do Curso de Ciências e Engenharia dos Materiais da Universidade Federal de Sergipe - SE, damon.fisica@gmail.com;

Com o avanço das tecnologias digitais e o crescente uso da internet entre os adolescentes, torna-se cada vez mais essencial preparar os jovens para os desafios do mundo conectado. O ambiente virtual, embora repleto de oportunidades, também apresenta riscos significativos, como fraudes, exposição de dados pessoais, *phishing* (tentativas de enganar o usuário para obter informações confidenciais) e manipulações informacionais. Nesse contexto, a educação em segurança cibernética emerge como uma ferramenta indispensável para o desenvolvimento da consciência digital crítica e responsável (PENCHEVA 2020; PARK 2020).

De acordo com informações coletadas da pesquisa TIC Domicílios 2024, mais relevante levantamento sobre acesso a tecnologias da informação e comunicação, realizado pelo Centro Regional para o Desenvolvimento de Estudos sobre a Sociedade da Informação (Cetic.br), vinculado ao Comitê Gestor da Internet no Brasil, é possível perceber que, em 2024, os usuários de Internet representavam 84% da população com 10 anos ou mais, ou 159 milhões de pessoas, 96% dos quais utilizaram a Internet todos os dias ou quase todos os dias. Segundo a pesquisa, 60% dos usuários acessaram a Internet apenas pelo telefone celular, enquanto 40% usaram tanto o computador quanto o celular (CGI.br, 2024). Além disso, a edição de 2024 da TIC Domicílios aponta que as habilidades digitais mais realizadas pelos usuários de Internet continuam sendo a verificação de informações encontrada na Internet (52%), a adoção de medidas de segurança, como senhas fortes ou verificação em duas etapas, para proteger dispositivos e contas online (48%) e a utilização de ferramenta de copiar e colar para duplicar ou mover conteúdo, por exemplo, em um documento ou uma mensagem (45%) (CGI.br, 2024).

Nesta era de rápido avanço em multimídia e tecnologia, a internet é facilmente acessível a todas as pessoas, adultos ou crianças. Assim, as escolas devem desempenhar um papel crucial no ensino da alfabetização digital para proteger as crianças de potenciais ameaças cibernéticas pois o conhecimento e a educação sobre segurança cibernética devem ser disponibilizados desde cedo no contexto escolar por meio de atividades práticas, diálogos e recursos multimídia para criar-se uma cultura de conscientização (AMANKWA, 2021).

Este artigo apresenta um relato de experiência sobre a realização da oficina “segurança cibernética” aplicada em turmas do ensino médio do Colégio Estadual do Campo Professora Hilda Monteiro Menezes. A proposta teve como objetivo sensibilizar os estudantes sobre práticas seguras no uso da internet, abordando temas como senhas fortes, privacidade nas redes sociais, reconhecimento de ameaças virtuais e uso ético da tecnologia. Além disso, buscou-se promover a reflexão sobre os direitos e deveres no ambiente digital, contribuindo

para a formação de cidadãos mais conscientes e preparados para os desafios da era da informação.

METODOLOGIA

A pesquisa é do tipo exploratória e descritiva, assumindo uma abordagem qualitativa no tratamento dos dados coletados. Para Gil (2002), a pesquisa exploratória tem por objetivo favorecer uma maior proximidade com o tema, tornando-o mais claro, além de propiciar ao pesquisador maior intimidade com o assunto, possibilitando a compreensão do problema. Ainda conforme os autores, caracteriza-se também como descritiva, pois os fatos serão observados, analisados, registrados, classificados e interpretados, sem que o pesquisador interfira neles.

A abordagem qualitativa deste estudo se mostra pertinente aos objetivos da pesquisa. Com a proposta de ser exploratório, a escolha de analisar os dados qualitativamente permitirá que observemos os detalhes das respostas dos estudantes sobre as oficinas realizadas.

A pesquisa-ação também foi escolhida para a realização desta pesquisa, por ser uma pesquisa participativa, preocupada com a resolução de um problema coletivo, no qual pesquisadores e participantes da situação investigada estão envolvidos de modo a contribuírem com a transformação da realidade (Gil, 2002).

Para a coleta de dados, utilizou-se um questionário com quatro questões ao final da oficina. O questionário foi organizado com perguntas objetivas e teve o intuito de analisar o impacto da oficina “segurança cibernética”.

Como se observa na Tabela 1, as oficinas foram divididas em 3 (três) etapas: i) levantamento bibliográfico; ii) planejamento e definição da oficina e, por fim, iii) execução, coleta e análise dos dados da oficina. A oficina foi realizada em dois encontros com duração de 50 minutos e ocorreu nos meses de março, abril e maio de 2025 (dois mil e vinte e cinco), com participação de discentes voluntários do primeiro e segundo ano do ensino médio do Colégio Estadual do Campo Professora Hilda Monteiro Menezes da Rede Estadual da Bahia, localizado em Campo Formoso.

Tabela 1: Planejamento da Oficina.

Fase	Descrição
Levantamento bibliográfico	Levantamento bibliográfico sobre a importância da segurança cibernética na escola.
Planejamento da oficina	Foram definidos o objetivo geral, conteúdos, metodologia e recursos necessários.
Execução, coleta e análise dos dados da oficina	A execução da oficina teve como objetivo

	sensibilizar os estudantes sobre práticas seguras no uso da internet, abordando temas como senhas fortes, privacidade nas redes sociais, reconhecimento de ameaças virtuais e uso ético da tecnologia. Foram coletados dados com o objetivo de refletir a relevância da educação em segurança cibernética nas escolas.

Fonte: elaboração própria.

REFERENCIAL TEÓRICO

A segurança cibernética está intrinsecamente relacionada às atividades cotidianas, ainda que, por vezes, de forma imperceptível. Trata-se de um conjunto de práticas, normas e tecnologias voltadas à proteção de computadores, redes e dados frente a ameaças externas, ataques maliciosos e erros operacionais. Conforme enfatiza Stillings (2020), embora a digitalização tenha proporcionado avanços significativos à sociedade contemporânea, ela também introduziu desafios relevantes, notadamente em termos de privacidade, integridade e disponibilidade das informações.

De acordo com Amankwa (2021) relata que os princípios de segurança cibernética orientam como pessoas e instituições podem se proteger de ameaças cibernéticas que podem ser prejudiciais aos seus dados e informações armazenados. Dessa forma, os princípios de segurança cibernética ajudam a proteger dados e informações vitais e são agrupados em quatro categorias principais: proteger, governar, responder e detectar.

A legislação brasileira, por meio da Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 2018, estabelece que o tratamento de dados referentes a menores deve primar pelo bem-estar do indivíduo, exigindo o consentimento de pelo menos um dos responsáveis legais. Além disso, determina que o uso de dados seja transparente, seguro e orientado por finalidades legítimas, em consonância com os princípios da liberdade, da privacidade e do pleno desenvolvimento (BRASIL, 2018).

De acordo com Silva e Lopes (2021), a formação para o uso crítico e ético das tecnologias digitais deve iniciar-se precocemente, com o objetivo de fomentar uma cidadania digital consciente. A escola, nesse contexto, configura-se como espaço privilegiado para o desenvolvimento de ações pedagógicas que promovam a reflexão e a prevenção de riscos online. Incluir a segurança digital nos currículos escolares não é apenas uma demanda técnica, mas uma exigência ética e social diante das transformações tecnológicas em curso. Esses

desafios tornam-se particularmente visíveis no contexto escolar, no qual crianças e adolescentes frequentemente não dispõem do repertório técnico ou cognitivo necessário para identificar e enfrentar riscos digitais. Nesse cenário, a mediação educativa revela-se fundamental.

A Base Nacional Comum Curricular (BNCC) reconhece a relevância do tema, recomendando a inserção dos conteúdos de computação desde a educação infantil até o ensino médio. Dentre as competências trabalhadas, destacam-se o pensamento computacional, a resolução de problemas, a lógica e a análise crítica dos impactos sociais e éticos da tecnologia. No ensino médio, as discussões se ampliam, contemplando temas como ética digital, segurança da informação e as implicações do uso de dados pessoais na vida cotidiana (BRASIL, 2019).

Dentre as metodologias mais eficazes para abordar tais temáticas estão as oficinas pedagógicas, que promovem a aprendizagem ativa, colaborativa e contextualizada. Inspiradas na perspectiva freireana de educação como prática dialógica e crítica (FREIRE, 1996), essas oficinas colocam o estudante no centro do processo formativo, estimulando o protagonismo e o engajamento.

Especificamente no campo da segurança digital, as oficinas de cibersegurança possibilitam a simulação de situações reais de risco — como tentativas de fraude eletrônica, vazamento de dados ou exposição de informações sensíveis — o que permite aos estudantes compreenderem, na prática, as ameaças do ambiente virtual e desenvolverem comportamentos preventivos. A articulação entre teoria e prática fortalece a construção de conhecimentos técnicos ao mesmo tempo em que estimula a tomada de decisões éticas e fundamentadas.

RESULTADOS E DISCUSSÃO

A Base Nacional Comum Curricular (BNCC) do ensino médio aborda temas de tecnologia e computação de forma transversal em todas as áreas do conhecimento, considerando uma perspectiva interdisciplinar. Além disso, a competência geral número 1 fala na valorização de conhecimentos construídos nos mundos físico, social, cultural e digital, enquanto a número 2 ressalta a importância de fomentar nos/nas estudantes a resolução de problemas e a criação de soluções (inclusive tecnológicas). Notadamente, a competência geral número 5 explicita a necessidade de trabalhar com o tema de tecnologias digitais de

informação e comunicação (TDIC), colocando os/as estudantes como aprendizes ativos e criativos – e não apenas consumidores passivos de tecnologias:

> Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva BRASIL (2018, p.9).

Nesse sentido, a oficina de "segurança cibernética" foi realizada em duas turmas do ensino médio, primeiro ano (1°CV) e segundo ano (2°CV), no turno vespertino do Colégio Estadual do Campo Professora Hilda Monteiro Menezes, como observa-se na Figura 1.

Figura 1: Aplicação da oficina segurança cibernética.

Fonte: Acervo do autor.

No primeiro momento da oficina os pibidianos promoveram uma conscientização acerca dos riscos digitais por meio de dinâmicas participativas que integrassem teoria e prática. Inicialmente foram introduzidos conceitos sobre: segurança cibernética, *malware*, *phishing*, *ransomware* e ataques de força bruta, ver Figura 2. Vale ressaltar que trabalhar esses temas em sala de aula é vital entre os jovens usuários da Internet, pois alguns podem não estar cientes de que são vítimas de ataques cibernéticos. Também durante a oficina mostrou-se a importância de implementar vários controles de segurança para ajudar a prevenir e reduzir a vulnerabilidade a ameaças cibernéticas. Dessa forma, Normalmente, os princípios de segurança cibernética orientam como pessoas e instituições podem se proteger de ameaças cibernéticas que podem ser prejudiciais aos seus dados e informações armazenados.

Figura 2: Slide utilizado na oficina segurança cibernética.

Fonte: Acervo do autor.

De acordo com Amankwa (2021) é importante incorporar a educação em segurança cibernética nas escolas para prevenir crimes cibernéticos entre os jovens. Uma cultura de conhecimento em segurança cibernética será cultivada entre as pessoas. Mais importante ainda, o conhecimento e a educação em segurança cibernética também são cruciais na prevenção do vício em pornografia e jogos de computador disponíveis na internet. Em um segundo momento, aplicou-se um questionário composto por quatro questões objetivas para avaliar o aprendizado dos conteúdos trabalhados.

A Figura 3 mostra um comparativo de acertos das questões entre as turmas do 1ºCV e do 2ºCV. A turma do 1ºCV, observou-se que 70% dos alunos responderam corretamente à questão sobre o conceito de *malware*, reconhecendo-o como um *software* malicioso. Os 30% restantes confundiram o termo com "*hardware*", evidenciando a necessidade de reforçar a distinção entre os componentes físicos e lógicos dos sistemas computacionais. A segunda questão, que solicitava a identificação do item que não configurava *malware*, apresentou índice de acerto de 90%, indicando que a maioria dos estudantes compreendeu que hardware não se enquadra como ameaça digital.

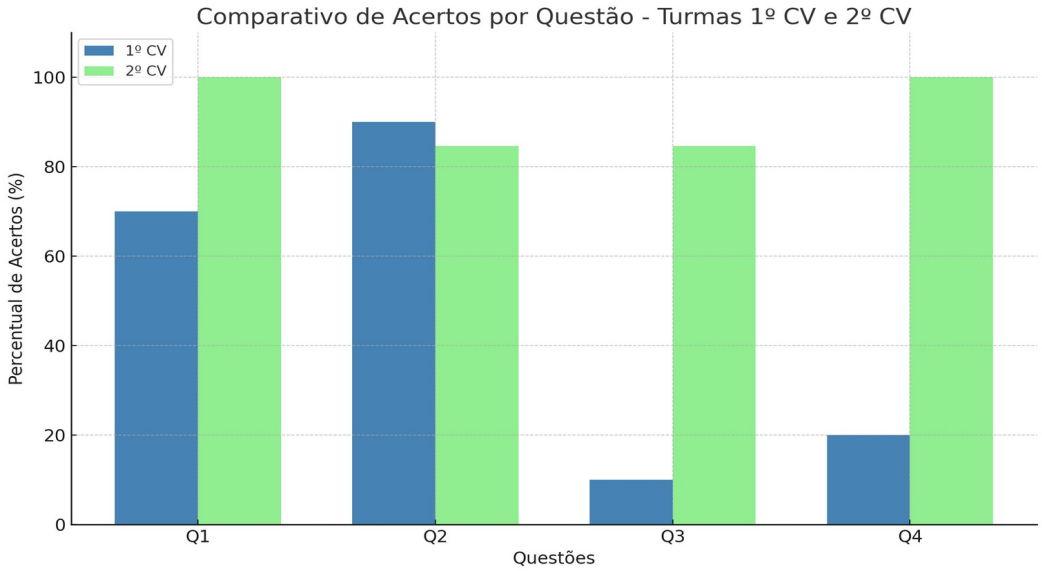
Entretanto, as maiores dificuldades concentraram-se nas questões que abordavam tipos específicos de *malware*. Na terceira pergunta, referente ao funcionamento do *ransomware*, apenas 10% dos participantes acertaram. A maioria confundiu o conceito com vírus comuns que se disseminam por redes sociais, demonstrando incompreensão acerca do mecanismo de sequestro e criptografia de dados. Na quarta questão, que tratava do *trojan*, somente 20% responderam corretamente, evidenciando desconhecimento sobre a infecção por meio do disfarce de *software* legítimo.

Por sua vez, a turma do 2º CV, que participou da mesma sequência de oficinas — agora adaptada com base na experiência anterior — apresentou desempenho significativamente superior. As questões relativas a malware e trojan obtiveram 100% de

acertos, enquanto as que tratavam de *ransomware* e identificação de ameaças alcançaram 84,62% de respostas corretas.

Essa comparação revela uma melhora substancial na compreensão dos conceitos, especialmente nas questões mais complexas (Q3 e Q4). Tal avanço pode ser atribuído a três fatores principais: (1) ajustes metodológicos implementados após a primeira aplicação; (2) reforço didático com exemplos mais contextualizados; e (3) maior ênfase em simulações práticas e discussões em grupo.

Figura 3: Comparativo de acertos por questão – turmas 1°CV e 2ºCV.



Fonte: Acervo do autor.

De acordo com a Base Nacional Comum Curricular (BNCC, 2019), é fundamental que os estudantes desenvolvam pensamento computacional e senso crítico em relação aos impactos da tecnologia. As oficinas atenderam a essa diretriz ao propiciar momentos de reflexão e protagonismo discente, conforme preconiza Freire (1996), ao conceber o aluno como sujeito ativo no processo de aprendizagem. Ademais, ao abordar a proteção de dados pessoais, o projeto estabelece diálogo com os princípios da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), que assegura a privacidade, especialmente de crianças e adolescentes, no uso das tecnologias digitais.

Assim, os resultados indicam que as oficinas de cibersegurança são eficazes não apenas como instrumento pedagógico, mas também como meio de promoção da cidadania digital e da segurança na internet. A evolução dos índices de acerto entre as turmas reforça a

importância de abordagens ativas, contínuas e contextualizadas no tratamento dessa temática nas escolas.

CONSIDERAÇÕES FINAIS

A experiência relatada neste relato de experiência evidencia a relevância da inclusão da segurança cibernética como temática pedagógica na educação básica. As oficinas realizadas com estudantes do ensino médio do Colégio Estadual do Campo Professora Hilda Monteiro Menezes demonstraram que muitos adolescentes possuem conhecimentos ainda limitado sobre os riscos digitais e medidas de proteção no ambiente virtual. Contudo, os dados indicam que é possível ampliar significativamente esse entendimento por meio de estratégias didáticas participativas, contextualizadas e fundamentadas em situações reais.

Os resultados obtidos nas turmas evidenciaram progresso expressivo na compreensão dos conceitos abordados, sobretudo na segunda aplicação, que incorporou ajustes metodológicos em resposta aos desafios identificados na primeira turma. Tal fato reforça o papel da escola como agente formador de cidadãos digitais críticos e conscientes, conforme preconizam a Base Nacional Comum Curricular (BNCC) e a Lei Geral de Proteção de Dados (LGPD), e destaca a eficácia das oficinas enquanto prática pedagógica ativa e promotora de aprendizagens significativas.

Além do domínio técnico, a proposta contribuiu para fomentar o pensamento crítico, o senso de responsabilidade e o protagonismo juvenil no uso das tecnologias digitais. A formação digital dos estudantes não deve se limitar ao uso instrumental dos dispositivos, mas deve englobar também a reflexão ética e a prevenção de riscos, fortalecendo a cidadania digital em um mundo cada vez mais conectado.

Como recomendação para futuras ações, sugere-se a continuidade e ampliação das oficinas, envolvendo outras turmas e promovendo parcerias com famílias e comunidades. Ressalta-se, ainda, a importância da formação continuada de docentes sobre o tema, com vistas a consolidar uma cultura escolar de segurança digital. Por fim, entende-se que a educação para a segurança cibernética deve ser permanente, integrada de maneira transversal e interdisciplinar ao currículo escolar.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001

REFERÊNCIAS

Amankwa, E. (2021) Relevance of Cybersecurity Education at Pedagogy Levels in Schools. ***Journal of Information Security***, 12, 233-249. doi: 10.4236/jis.2021.124013.

BRASIL. Comitê Gestor da Internet no Brasil – **CGI.br.** Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros : TIC Domicílios 2024 [livro eletrônico] / [editor] Núcleo de Informação e Coordenação do Ponto BR. São Paulo : Comitê Gestor da Internet no Brasil, 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 jun. 2025.

BRASIL. **Base Nacional Comum Curricular**: Computação na Educação Básica. Brasília: MEC, 2019. Disponível em: https://www.gov.br/mec/pt-br/assuntos/noticias/bncc-computacao-na-educacao-basica. Acesso em: 20 jun. 2025.

FREIRE, Paulo. **Pedagogia da autonomia: saberes necessários à prática educativa**. São Paulo: Paz e Terra, 1996.

GIL, ANTÔNIO CARLOS. **Métodos e Técnicas de Pesquisa Social**. 6 ed. São Paulo: Editora Atlas, 2002.

Park, H.-Ho. (2020) A Study on Cyber Crime Deterrence Recognition: The Influence of Recognition of Punishment for Cyber Crime on Intention to Report Crime. Korean Criminal **Psychology Research**, 16, 85-98. Disponível em: https://doi.org/10.25277/KCPR.2020.16.4.85. Acesso em: 27 jun 2025.

Pencheva, D., Joseph, H. and Awais, R. (2020) Bringing Cyber to School: Integrating Cybersecurity into Secondary School Education. IEEE **Security & Privacy**, 18, 68-74. Disponível em: https://doi.org/10.1109/MSEC.2020.2969409. Acesso em: 27 jun 2025.

SILVA, Eduardo; LOPES, Mariana. Segurança cibernética na educação básica: uma necessidade urgente. **Revista Brasileira de Tecnologias Educacionais**, v. 9, n. 1, p. 75-89, 2021.

STILLINGS, Nate. ***Cybersecurity essentials***. New York: Pearson, 2020.

X ENALIC

X Encontro Nacional das Licenciaturas
IX Seminário Nacional do PIBID