Proposta de uma Atividade Desplugada sobre Segurança Cibernética para a Educação Básica

André G. L. S. Lira[1], Leandro de Almeida Melo[1], Any Caroliny D. Batista de Almeida[1]

[1] Universidade de Pernambuco, Campus Mata Norte
Caixa Postal 55800-00, Nazaré da Mata - PE - Brasil

{andre.silvalira,leandro.amelo,any.caroliny}@upe.com

Abstract. *This paper presents the proposal of an unplugged activity designed for teaching cybersecurity in K–12 education. The activity was developed using a playful and pedagogical approach to foster students' understanding of concepts related to different types of malicious code. Furthermore, it encourages critical reflection and discussion on prevention strategies and ways to address threats in the context of digital navigation...*

Resumo. *Este artigo apresenta a proposta de uma atividade desplugada voltada ao ensino de segurança cibernética na Educação Básica. A atividade foi concebida com abordagem lúdica e didática, visando favorecer a compreensão de conceitos relacionados a diferentes tipos de códigos maliciosos. Além disso, a atividade promove a reflexão crítica e o debate sobre estratégias de prevenção e enfrentamento de ameaças no contexto da navegação no mundo digital.*

1. Objetivos

A Computação Desplugada tem como objetivo utilizar atividades da área de computação sem ser por aparatos digitais, mas por meio de materiais escolares simples de acordo com a atividade proposta [Bell *et al*. 2011]. Além disso, por meio da explicitação de como determinadas tecnologias funcionam, é possível atribuir um significado mais concreto aos conteúdos apresentados aos estudantes [Freire, 2017], especialmente quando associados a dinâmicas pedagógicas, considerando que os conceitos da computação são, em sua maioria, abstratos. É neste contexto que esta proposta foi criada e os seus objetivos são apresentados a seguir.

1.1 Objetivo Geral

Este trabalho tem como objetivo geral apresentar uma nova proposta de atividade desplugada desenvolvida para o ensino de segurança cibernética para crianças do ensino fundamental II. Assim, este trabalho tem o foco no ensino-aprendizagem de conceitos e características de códigos maliciosos e ataques cibernéticos. Nesse contexto, a atividade proposta foi inspirada no estilo de jogo "Quem sou eu", como uma adaptação, esta atividade desplugada chama-se de "Que vírus sou eu".

1.2 Objetivo Específicos

- Apresentar os diferentes tipos de códigos maliciosos mais comuns que podem afetar os dados das pessoas no cotidiano a fim de alertar sobre seus diferentes riscos.
- Incentivar novas dinâmicas coletivas de ensino ligadas ao mundo digital que

possam ser aplicadas no ambiente escolar, envolvendo estudantes e professores.
- Apresentar novas oportunidades de ensinar conceitos da ciência da computação no ensino básico e forma lúdica a partir de dinâmicas desplugadas inéditas.

2. Público-Alvo

Alunos dos anos finais do ensino fundamental do 7º ou 9º ano.

3. Habilidade Trabalhada

Apesar de ter sido pensada para um público alvo definido, a atividade desplugada mencionada pode ser realizada com várias faixas etárias, contudo, ela foi idealizada com um enfoque maior para turmas do Ensino Fundamental – Anos Finais tendo em vista as habilidades da Computação na Educação Básica - Complemento à Base Nacional Comum Curricular [Brasil, 2022], facilitando os planejamentos pedagógicos dos professores que decidirem utilizar deste exercício.

Tabela 1 - Habilidades e competências associadas à atividade "Que vírus sou eu"?

Eixo - Ano	Código	Habilidade
Mundo Digital - 7 ano	EF07CO07	Identificar problemas de segurança cibernética e experimentar formas de proteção.
Mundo Digital - 9 ano	EF09CO04	Compreender o funcionamento de malwares e outros ataques cibernéticos.

4. Materiais Utilizados

Nesta atividade, serão utilizados três conjuntos principais de materiais: uma tabela de conceitos, uma tabela de referências e cartas que representam os personagens do jogo, isto é, os “Códigos maliciosos”. Esses materiais são apresentados na seção seguinte e podem ser confeccionados com folhas A4, preferencialmente em papel cartão, a fim de garantir maior durabilidade. Os modelos[1] encontram-se disponíveis nesta proposta de atividade e podem ser impressos; entretanto, também é possível ser adaptados e construídos pelo professor em parceria com a turma. Por exemplo, as cartas distribuídas durante a atividade podem ser produzidas manualmente e recortadas pelos estudantes, assim novos personagens e perguntas podem ser criados e incorporados ao jogo com base em pesquisas realizadas pelos discentes, ampliando o repertório conceitual trabalhado. Ao final do processo de construção dos materiais, recomenda-se que o professor os plastifique, possibilitando sua reutilização em diferentes momentos pedagógicos.

Destaca-se que o material didático adotado como referência para a elaboração desta atividade foi fundamentado no fascículo Códigos Maliciosos, disponibilizado publicamente no website[2] do Centro de Estudos, Resposta e Tratamento de Incidentes

[1] Link com os materiais necessários para construção desta proposta de atividade: https://drive.google.com/drive/folders/1VpCcx2N3JIyYTbQ805g11Vnwimv-sN46

[2] Fonte: Fascículo de códigos maliciosos, autor CERT.br/NIC.br/CGI.br - Disponivel em: https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf . Acesso em: fevereiro de 2026.

de Segurança no Brasil (CERT.br). O referido documento apresenta a definição dos diferentes tipos de códigos maliciosos, bem como descreve o funcionamento de ataques no ambiente virtual, estabelecendo diálogos com temáticas relacionadas à Mundo Digital [Brasil, 2022]. Recomenda-se que o referido fascículo seja utilizado como material de estudo prévio e apoio pedagógico ao professor, podendo também ser disponibilizado aos estudantes em formato digital ou impresso, conforme as condições da instituição.

5. Metodologia Detalhada de Desenvolvimento da Atividade

A atividade desplugada proposta foi elaborada a partir da análise das habilidades relacionadas ao objeto de conhecimento Segurança Cibernética, conforme previsto no complemento da BNCC para a Computação [Brasil, 2022]. A escolha desse conteúdo justifica-se pela crescente utilização de recursos digitais no cotidiano, o que amplia a vulnerabilidade a ataques cibernéticos que exploram diferentes estratégias para induzir usuários a clicar em links maliciosos ou instalar softwares prejudiciais.

A atividade proposta fundamenta-se na dinâmica do jogo tradicional “Quem sou eu?”, mantendo suas características interativas e colaborativas, porém com o diferencial da mediação pedagógica do professor. No jogo tradicional, cada participante recebe a identidade de um personagem ou conceito sem ter acesso direto à informação, devendo descobri-la por meio de perguntas direcionadas aos colegas, geralmente respondidas com “sim” ou “não”. Essa estrutura favorece a formulação de hipóteses, o raciocínio dedutivo e a organização lógica do pensamento, potencializando o processo de construção do conhecimento.

Nesse sentido, a atividade tem início com a contextualização, pelo professor, do tema segurança cibernética e de sua relevância na sociedade contemporânea, introduzindo o conceito de códigos maliciosos e apresentando a diversidade de ameaças existentes. Recomenda-se ainda uma breve abordagem dos conceitos de Sistema Operacional e Antivírus, uma vez que tais termos são utilizados ao longo da dinâmica proposta. Para apoiar o professor nesse processo, disponibiliza-se nesta atividade uma tabela com os principais conceitos trabalhados (ver Figura 1). Além disso, recomenda-se a leitura prévia do Fascículo de Códigos Maliciosos, mencionado na seção anterior, como material de apoio pedagógico.

Tipo	Definição
Spyware	Projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.
Trojan	Além de executar as funções para as quais foi projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. Nome inspirado no cavalo de troia.
(...)	(...)

Figura 1 - Por limitações de espaço, a figura apresenta parte da tabela de Conceitos.

Na etapa seguinte, o professor organizará a turma em grupos, cujo tamanho poderá variar conforme o número total de estudantes, recomendando-se equipes de até cinco integrantes. Após a formação dos grupos, será apresentada a dinâmica da atividade, conforme os passos a seguir.

Passo 1: Cada grupo realizará a leitura da Tabela de Referência, que contém perguntas sobre os códigos maliciosos com respostas estruturadas em "sim" ou "não", durante um tempo previamente determinado, por exemplo, 10 minutos (1ª etapa). Recomenda-se que o professor acompanhe esse momento, incentivando o debate entre os estudantes e sugerindo estratégias que favoreçam a compreensão e a memorização das informações. O modelo da Tabela de Referência encontra-se apresentado na Figura 2.

Tipos de vírus	 Spyware	 Trojan	 Scareware	 Worm	 Ransomware	 Bot (Zumbi)
Perguntas?						
Coleta informações pessoais ou confidenciais do usuário?						
Autorreplica-se em sistemas informatizados causando danos sem a necessidade de ser ativado pela execução do usuário.						
Após infectar o dispositivo, exibe uma mensagem informando ao usuário o procedimento a ser seguido ?						

Figura 2 – Por limitações de espaço, a figura apresenta parte da tabela de referência. As imagens utilizadas foram baseadas no fascículo Códigos Maliciosos de CERT.br (2023)

Passo 2: Após o término do tempo estipulado, o professor recolherá a Tabela de Referência e organizará as cartas contendo a identificação dos códigos maliciosos (ver exemplo na Figura 3). Em seguida, um estudante de cada grupo será designado como Sistema Operacional (SO). Esse participante selecionará, de forma aleatória, uma carta e verificará qual código malicioso está indicado, representando, assim, a "infecção" do SO. O aluno designado permanecerá com a Tabela de Referência em sua posse para consulta durante a dinâmica.

Figura 3 – Exemplo de uma carta de vírus. As imagens utilizadas foram baseadas no fascículo Códigos Maliciosos de CERT.br (2023)

Passo 3: Os demais integrantes do grupo, denominados Antivírus, realizam perguntas ao estudante que representa o SO, com o objetivo de identificar qual código malicioso está associado à carta selecionada. Para isso, será disponibilizada a Tabela de Referência contendo apenas as perguntas, sem as respectivas respostas. O SO deve responder exclusivamente com "sim" ou "não". Após todos os Antivírus formularem uma pergunta, cada participante poderá apresentar sua hipótese, indicando e justificando qual código malicioso acredita estar presente no SO. Caso nenhum estudante acerte, inicia-se

uma nova rodada de perguntas, repetindo-se a dinâmica descrita neste passo até que o vírus seja corretamente identificado.

Passo 4: Após a identificação do código malicioso pelos estudantes que desempenham o papel de Antivírus, o professor realizará uma breve explicação sobre o código malicioso sorteado, abordando suas características e possíveis formas de prevenção e combate. Recomenda-se a utilização do quadro branco para sistematizar as informações e a adoção de estratégias de gamificação, como a atribuição de pontos aos alunos que identificaram corretamente o código malicioso, a fim de ampliar o engajamento. Na sequência, um novo estudante assumirá o papel de SO, reiniciando a dinâmica a partir do Passo 2. A atividade será concluída quando todos os integrantes do grupo tiverem desempenhado, ao menos uma vez, o papel de SO.

5.1. Uma variação de aplicação para turmas maiores

Turmas com número elevado de estudantes podem ser organizadas em múltiplos grupos. Contudo, essa configuração pode representar uma limitação da atividade, uma vez que dificulta o acompanhamento dos grupos pelo professor durante sua execução. Como estratégia para minimizar essa limitação, os passos apresentados na seção anterior podem ser adaptados, a partir do Passo 2, para um formato de disputa entre grupos.

Nessa variação, o papel de SO é desempenhado por um aluno e os grupos assumem coletivamente o papel de Antivírus. A atividade será concluída quando pelo menos um integrante de cada grupo tiver desempenhado o papel de SO. Recomenda-se que o professor estabeleça um tempo de debate intragrupo para a definição tanto das perguntas a serem realizadas quanto a hipótese sobre o código malicioso em questão. Essa adaptação favorece o trabalho colaborativo, estimula o debate entre os integrantes de cada grupo e possibilita que a atividade seja conduzida de forma integrada com toda a turma, mantendo o professor como mediador do processo de aprendizagem.

5.2. Do que se trata tudo isso?

Ao navegar na internet, é comum que usuários encontrem propagandas enganosas que, ao serem acessadas, podem instalar silenciosamente softwares maliciosos no dispositivo, comprometendo dados sensíveis e o desempenho da máquina. Esse tipo de situação é recorrente na contemporaneidade, em um contexto no qual informações pessoais assumem alto valor para agentes mal-intencionados.

Diante desse contexto, destaca-se a importância da formação para a Cidadania Digital, capacitando estudantes a adotarem práticas seguras, reconhecerem golpes e compreenderem os principais códigos maliciosos, suas formas de disseminação e estratégias básicas de prevenção, incluindo a importância de softwares de antivírus.

6. Avaliação

Para a avaliação das habilidades dos alunos, recomenda-se realizar observações sistemáticas da participação e engajamento dos alunos durante a aplicação da atividade e disponibilizar, ao final da atividade, de um questionário de satisfação e de autoavaliação reflexiva junto aos estudantes, com o objetivo de identificar aprendizagens, dificuldades percebidas e o nível de participação no grupo.

Referências

Bell, T., Witten, I. H., Fellows, M., Adams, R.; McKenzie, J. (2011). Ensinando Ciência da Computação sem o uso do computador. Computer Science Unplugged ORG (2011).

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br (2023). Fascículo Códigos Maliciosos: Cartilha de Segurança para Internet, julho de 2023. Disponível em: https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf . Acesso em: fevereiro de 2026.

FREIRE, Paulo. *Pedagogia do Oprimido (2017).* 64ª ed. Rio de Janeiro/São Paulo: Paz e Terra, 2017.

BRASIL (2022). Ministério da Educação. Computação na Educação Básica: Complemento à Base Nacional Comum Curricular (BNCC). Brasília, DF: MEC, 2022.