Segurança e responsabilidade no uso de tecnologia computacional – Uma proposta de abordagem de *Malwares* no primeiro ano do ensino fundamental

Raquel Moreira Machado Fernandes[1,2], Claudia Maria Francisca Teixeira[1], Claudia Lage Rebello da Motta[2] , Luiz Fernando Rust da Costa Carmo[2]

[1]Departamento de Informática Educativa – Colégio Pedro II
São Cristóvão – RJ – Brasil

[2]Programa de Pós Graduação em Informática (PPGI) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, RJ.

raquel.fernandes@ufrj.br, claudia.teixeira.2@cp2.edu.br,
claudiam@nce.ufrj.br, rust@nce.ufrj.br

Abstract. *We present a pedagogical proposal for a digital security approach in the insertion of the knowledge object "security and responsibility in the use of computer technology" in the first year of elementary school. Based on the specific skills and premises of Computing in the National Common Curricular Base (BNCC), we present an experience with the topic of malware, using active methodologies, playfulness and a maker approach.*

Resumo. *Apresentamos uma proposta pedagógica para abordagem de segurança digital na inserção do objeto de conhecimento "segurança e responsabilidade no uso de tecnologia computacional" no primeiro ano do ensino fundamental. Com base nas competências e premissas específicas da Computação na Base Nacional Comum Curricular (BNCC), apresentamos uma experiência com o tema malwares, utilizando metodologias ativas, ludicidade e abordagem maker.*

1. Descrição Geral

A internet oferece diversas possibilidades de aprendizagens e desenvolvimento cognitivo para as crianças. No entanto, apesar dos benefícios da tecnologia digital, surgem também desafios como a segurança digital.

O objetivo deste trabalho é apresentar uma proposta de abordagem de segurança digital para o 1º ano do ensino fundamental contemplando o ensino de malwares. *Malwares* são programas maliciosos projetados para danificar, controlar ou roubar informações de dispositivos e sistemas. Eles podem incluir vírus, *worms, trojans, spyware*, entre outros tipos. *Malwares* geralmente são instalados sem o consentimento do usuário e podem causar danos aos dados, comprometer a segurança e afetar o desempenho do dispositivo. São especialmente perigosos para as crianças porque muitas vezes estão disfarçados em jogos, aplicativos ou conteúdos atrativos para o público infantil. Além disso, as crianças podem ser menos experientes em identificar ameaças *online* e mais propensas a clicar em links ou baixar arquivos sem perceber os riscos associados.

2. Objetivos

I) Ensinar as crianças a reconhecer e entender o que são *malwares*, abrangendo os diferentes tipos e como eles podem se manifestar; II) Capacitar as crianças com conhecimentos básicos sobre como se proteger contra malwares; III) Discutir as consequências negativas que os malwares podem ter, tanto para os dispositivos quanto para a privacidade das pessoas IV) Promover uma cultura de responsabilidade digital, incentivando as crianças a serem conscientes e responsáveis ao usar a internet.

3. Habilidades Trabalhadas

Esta proposta contempla a habilidade EF01CO07 do objeto "Segurança e responsabilidade no uso de tecnologia computacional", que consiste em "conhecer as possibilidades de uso seguro das tecnologias computacionais para proteção dos dados pessoais e para garantir a própria segurança.

4. Materiais Utilizados

Nesta proposta, sugerimos os seguintes recursos:

- Vídeos disponibilizados pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.Br), a partir dos quais adotamos a nomenclatura "defensores" e "invasores". Além disso, também podem ser utilizados desenhos infantis, como o Episódio 121 do Super Locomoto, onde o super-herói salva o computador de um vírus.
- Materiais recicláveis, como rolinhos de papéis higiênicos, tampinhas de garrafas, papéis coloridos, lã, entre outros.
- Softwares para desenho, como Paint, TuxPaint ou Paint3D.

5. Metodologia

Delineamos um processo de ensino-aprendizagem baseado em metodologias ativas, através das quais os estudantes podem construir conhecimento de forma ativa e colaborativa através da elaboração de artefatos como personagens e desenhos, que podem ser feitos à mão ou no computador. A trilha de aprendizagem baseia-se em 4 aulas, conforme a Figura 1.

Figura 1: Proposta de trilha de aprendizagem para abordagem de malwares

Esta trilha de aprendizagem foi testada em 04 aulas. Cada aula tem 2 tempos de 50 minutos cada. A abordagem pode ser realizada da seguinte forma:

Aula 01 – Conversa sobre os invasores e seus tipos. Atividade lúdica de elaboração de um vírus de computador. As crianças devem imaginar um vírus e criá-lo a partir de materiais recicláveis em uma abordagem maker.

Aula 02 – Conversa sobre os defensores e seus tipos (Antivírus, firewall, backup, autenticação, entre outros). Atividade lúdica de elaboração de um defensor. As crianças devem imaginar um recurso defensor e criá-lo a partir de materiais recicláveis em uma abordagem maker.

Aula 03 – Nesta aula, retoma-se os conceitos abordados nas aulas 01 e 02 e propõe-se uma atividade lúdica para desenvolvimento da criatividade e competência narrativa. A atividade consiste em imaginar como seria a batalha entre um invasor e um defensor. Deve-se realizar mediações como: Quais são os poderes do defensor? O que ele irá fazer para proteger o computador? Como o invasor irá reagir? É possível trabalhar a competência narrativa e estimular a oralidade e a metacognição através da técnica da elaboração dirigida (Seminério, 1987). Nesta etapa, é possível solicitar que as crianças produzam desenhos utilizando softwares como Paint, TuxPaint ou Paint 3D para desenvolvimento da criatividade e coordenação motora. Caso a escola não possua sala de Informática, os desenhos podem ser feitos à mão.

Aula 04 – Consolidação dos conceitos e revisão através de jogos preferencialmente digitais e/ou estratégias de gamificação.

6. Avaliação

Nesta proposta, sugerimos um processo de avaliação formativa de forma contínua, cumulativa e sistemática, através da qual é possível considerar o registro e coleta das evidências produzidas pelos estudantes, bem como a participação e o conhecimento demonstrado através da oralidade. A Tabela 1 apresenta uma sugestão de correspondência entre as habilidades, como desenvolver e como avaliar.

HABILIDADE	COMO DESENVOLVER	COMO AVALIAR
CRIATIVIDADE	Através do convite à imaginação e criação de diferentes personagens e situações.	Verificar a criatividade para elaboração dos personagens e utilização dos materiais fornecidos.
VOCABULÁRIO	Através da apresentação de novas palavras e estrangeirismos do âmbito das tecnologias digitais, como “malwares”, “antivírus”, “cavalo de troia”, entre outras.	Verificar se o estudante demonstra expansão no vocabulário, compreendendo o significado de novas palavras e estrangeirismos e demonstrando apropriação e uso correto.
REPRESENTAÇÃO	Através da solicitação de construção de um modelo material de	Verificar se o estudante consegue criar um modelo de representação do

	similaridade com o imaginário.	imaginário e se consegue representar características positivas e negativas.
LINGUAGEM	Através da solicitação de apresentação das produções para o grupo e através do quiz.	Utilizar a técnica da elaboração dirigida (Seminério, 1987) para guiar as discussões e analisar aspectos relacionados à linguagem, oralidade e metacognição.
METACOGNIÇÃO	Através da solicitação de explicação de como foi realizada a atividade e quais materiais utilizados.	Verificar se o estudante consegue explicar como criou seu invasor e seu defensor e se consegue justificar as escolhas de materiais.
MEMÓRIA	Através da necessidade de retomada de conceitos para participação em quiz e/ou jogos digitais.	Verificar se o estudante lembra dos conceitos abordados nas aulas anteriores através do desempenho no quiz e/ou jogos digitais selecionados.
COORDENAÇÃO MOTORA	Através da necessidade de movimentos realizados com as mãos para realizar desenhos, recorte e colagem e manipulação dos objetos para a criação dos defensores e invasores.	Verificar se o estudante consegue realizar os movimentos necessários para a realização das atividades, tanto no computador quanto manipulando materiais, recortando e colando.

Tabela 1 - Correspondência habilidades x atividades x como avaliar

Cabe ressaltar que as atividades propostas nesta experiência pedagógica são passíveis de serem reproduzidas em diferentes contextos escolares, pois podem ser realizadas em salas de aula comuns ou na sala de Informática, onde seria possível explorar também ferramentas de desenho e softwares de animação e/ou StopMotion para a atividade da batalha.

Outras atividades poderiam ser desenvolvidas a partir dos artefatospersonagens criados, como, por exemplo, a elaboração de histórias com foco na oralidade, teatrinhos ou elaboração de histórias em quadrinhos a partir de registros fotográficos dos artefatos criados. Além disso, é possível desenvolver habilidades além das que foram privilegiadas nesta proposta.

Como desdobramentos possíveis desta experiência pedagógica, sugerimos incluir atividades de pensamento computacional com o uso de um jogo de tabuleiro no qual os personagens (invasores e/ou defensores) podem ser movimentados combinando cartas com representação de movimentos desenhados por setas, enfatizando a quantidade destes movimentos. Tal atividade pode constituir uma base teórica para o desenvolvimento, no futuro, da habilidade EF05CO02, que versa sobre representação através de grafos.

Referências

BRASIL. Ministério da Educação. Computação - Complemento a BNCC. Brasília: MEC, 2022.

Seminério, F. Elaboração dirigida - um caminho para o desenvolvimento metaprocessual da Cognição humana. Rio de Janeiro / Instituto Superior de Estudos e Pesquisas Psicossociais, Cadernos do ISOP, 1987.