

Estratégia Desplugada para o Ensino de Segurança e Privacidade Digital nos Anos Iniciais a partir do *Roblox*

Alexandre de Souza Passos¹, Ruan Carlos Pereira Barros², Lucas Bina Paulo²,
Ione de Castro Matos², João da Mata Libório Filho²

¹Núcleo de Ensino Superior de Manicoré (NESMCR) – Universidade do Estado do Amazonas (UEA) – Manicoré – AM – Brasil

² Centro de Estudos Superiores de Itacoatiara (CESIT) – Universidade do Estado do Amazonas (UEA) – Itacoatiara – AM – Brasil

{adsp.lic24, rcpb.lic25, lbp.lic25, icmatos, jlfilho}@uea.edu.br}

Abstract. *The increasing presence of children in interactive digital platforms demands pedagogical interventions focused on online safety and ethical conduct. This paper presents an unplugged activity designed for 3rd and 4th grade elementary students, using the Roblox context to foster competencies related to data protection and risk identification. Structured in three progressive stages, the methodology integrates interaction analysis, moderation exercises, and critical observation of gameplay. The proposal aligns with BNCC–Computing skills EF03CO09 and EF04CO07, promoting critical digital literacy in the early years of basic education.*

Resumo. *A crescente presença de crianças em plataformas digitais interativas demanda intervenções pedagógicas voltadas à segurança e à ética no ambiente online. Este trabalho apresenta uma proposta de atividade desplugada para estudantes do 3º e 4º ano do Ensino Fundamental, utilizando o contexto do Roblox para desenvolver competências relacionadas à proteção de dados e à identificação de situações de risco. Estruturada em três etapas progressivas, a metodologia articula análise de interações, exercício de moderação e observação crítica de gameplay. A proposta alinha-se às habilidades EF03CO09 e EF04CO07 da BNCC – Computação, promovendo letramento digital crítico nos anos iniciais.*

1. Introdução e Justificativa

O avanço das tecnologias digitais tem redefinido a forma como crianças interagem e constroem suas identidades no espaço virtual. Entre essas tecnologias, o *Roblox* se apresenta como um ambiente imersivo que combina criação de experiências digitais e socialização em rede, atraindo milhões de usuários em idade escolar. Essa característica de jogo e rede social simultaneamente amplia as possibilidades de interação, mas também expõe crianças e adolescentes a riscos relacionados à privacidade e segurança digital, exigindo atenção pedagógica e regulatória [1], em conformidade com a Lei nº 15.211/2025, que dispõe sobre a proteção de crianças e adolescentes em ambientes digitais [2]. A Base Nacional Comum Curricular (BNCC), em seu Complemento de Computação [3], reforça que a escola deve preparar os estudantes para atuar de forma crítica, ética e responsável nos ambientes digitais, o que torna pertinente a análise do *Roblox* no contexto da educação básica.

Embora o contato com plataformas digitais ocorra desde os primeiros anos escolares, é no 3º e 4º ano que os estudantes consolidam autonomia de leitura e escrita, passando a interagir de forma mais ativa em ambientes virtuais. Nesse estágio, o uso do *Roblox* intensifica a exposição a riscos como engenharia social, coleta de dados e golpes financeiros, justamente porque as crianças começam a compreender e responder a mensagens em *chats* sem supervisão constante. Estudos recentes apontam que o *Roblox* é um espaço onde se constroem sentidos sobre a infância e a socialização digital, reforçando a necessidade de abordagens críticas e pedagógicas [4]. A relevância deste trabalho consiste em antecipar práticas educativas que capacitem os alunos a reconhecer padrões de risco e a desenvolver competências de segurança digital, contribuindo para uma formação crítica ainda pouco explorada nos anos iniciais.

Neste sentido, o trabalho se configura como uma proposta pedagógica voltada para os anos iniciais do Ensino Fundamental, especificamente o 3º e 4º ano, tendo como eixo central o uso do *Roblox* para discutir privacidade e segurança digital. Avançando em relação a estudos correlatos que dependem do uso direto de jogos digitais nas telas para o ensino de segurança [5] ou de dinâmicas desplugadas voltadas a outros conteúdos [6], a presente proposta inova ao unir o engajamento do universo do *Roblox* a dinâmicas físicas de análise crítica. Assim, promove-se o letramento em segurança sem depender de infraestrutura tecnológica complexa.

2. Objetivos

Objetivo Geral: Capacitar estudantes do 3º e 4º ano a identificar e mitigar riscos de segurança e privacidade na plataforma *Roblox* através de atividades lúdicas desplugadas.

Objetivos Específicos: Diferenciar dados públicos de dados privados no contexto de interações digitais; identificar táticas de engenharia social em diálogos realizados em ambientes virtuais; compreender as possíveis consequências decorrentes de comportamentos inseguros em plataformas digitais.

3. Público-Alvo

A atividade destina-se a estudantes do 3º e 4º ano do Ensino Fundamental (8 a 10 anos). Esta faixa etária foi selecionada pois, segundo a BNCC, é o estágio onde se introduz a reflexão sobre o impacto do compartilhamento de informações, coincidindo com o aumento do uso autônomo de plataformas digitais sem supervisão parental constante.

4. Habilidades Exploradas

A proposta baseia-se nas competências específicas de Computação descritas no Complemento à BNCC: **(EF03CO09)** - 3º Ano: Reconhecer o potencial impacto do compartilhamento de informações pessoais ou de seus pares em meio digital. **(EF04CO07)** - 4º Ano: Demonstrar postura ética nas atividades de coleta, transferência, guarda e uso de dados. A proposta fundamenta-se no campo da Educação Digital e do Letramento Midiático, que compreendem a formação de sujeitos capazes de analisar criticamente conteúdos, interações e estruturas das plataformas digitais. Conforme Buckingham[7], o letramento digital não se restringe ao domínio técnico das ferramentas, mas envolve compreensão crítica dos sistemas de produção, circulação e uso da informação. No contexto da infância, Livingstone[8] argumenta que crianças não devem

ser vistas apenas como usuárias vulneráveis, mas como participantes ativos da cultura digital, necessitando de mediação pedagógica que promova autonomia segura.

Neste trabalho, adota-se a concepção de letramento digital crítico como a capacidade de identificar riscos, compreender as dinâmicas de poder nas interações *online* e tomar decisões fundamentadas em princípios éticos e de proteção de dados. Assim, a proposta não se limita à prevenção de riscos, mas busca desenvolver competências analíticas e reflexivas adequadas à faixa etária.

5. Recursos e Materiais Utilizados

A atividade utiliza uma abordagem híbrida, combinando recursos audiovisuais para análise coletiva e materiais impressos para a prática individual: Infraestrutura Multimídia: Computador com acesso à internet e projetor para exibição da interface e vídeos de *gameplay*; Matrizes de Atividades: Folhas impressas contendo (1) simulação visual de *chat* para defesa pessoal e (2) painéis de moderação para análise de conduta de terceiros; O material complementar completo encontra-se disponível no repositório <[zenodo](#)>, permitindo acesso, *download* e reutilização por outros docentes; Material de Escrita: Lápis ou caneta para marcação.

6. Metodologia Detalhada

A intervenção pedagógica estrutura-se em três aulas distintas, com complexidade progressiva (Defesa Pessoal, Moderação e Análise em Tempo Real):

6.1 Aula 1: Contextualização e Análise de Interações em *Chat* (Defesa Pessoal)

A primeira aula articula momentos expositivos e atividades práticas, com o objetivo de introduzir conceitos fundamentais relacionados à identidade digital e à proteção de dados pessoais. Inicialmente, o professor apresenta, por meio de projeção multimídia, elementos da interface da plataforma *Roblox*, utilizando-a como contexto para discutir a distinção entre identidade pessoal e identidade digital. Nesse momento, são problematizados dois conjuntos de informações: aquelas que pertencem à esfera privada do indivíduo (dados pessoais sensíveis) e aquelas que compõem sua representação no ambiente virtual (informações de perfil e elementos de personalização).

Após a contextualização teórica, realiza-se a atividade prática intitulada *Chat de Decisão*. Cada estudante recebe uma folha contendo simulações de mensagens enviadas em ambiente de *chat*. A tarefa consiste em analisar criticamente cada interação e classificá-la conforme seu nível de segurança. Para isso, o estudante deve: Assinalar positivamente as interações consideradas seguras ou adequadas ao contexto de jogo; Indicar como inadequadas aquelas que envolvam solicitação de dados pessoais, tentativa de manipulação ou outra forma de abordagem suspeita. Essa dinâmica visa desenvolver a capacidade de julgamento crítico frente a interações digitais, promovendo a internalização de critérios de segurança aplicáveis a diferentes contextos virtuais.

6.2 Aula 2: Análise de Condutas e Exercício de Moderação (Perspectiva Coletiva)

Na segunda aula, amplia-se a complexidade cognitiva da atividade ao deslocar a perspectiva do estudante: em vez de analisar interações dirigidas a si próprio, o aluno passa a assumir o papel de moderador de segurança, responsável por avaliar a conduta de

terceiros em ambiente digital. Essa mudança de foco favorece o desenvolvimento do julgamento ético e da compreensão de normas coletivas de convivência *online*.

Inicialmente, o professor retoma os conceitos trabalhados na aula anterior, especialmente os critérios utilizados para distinguir interações seguras de situações de risco. Em seguida, distribui-se uma atividade impressa contendo transcrições simuladas de diálogos entre jogadores. Os estudantes devem ler atentamente as conversas e avaliar se estão em conformidade com princípios de segurança, respeito e integridade digital.

A tarefa consiste em: Aprovar as interações que respeitem as normas de convivência e não apresentem riscos relacionados à privacidade ou à manipulação; sinalizar como inadequadas aquelas que envolvam condutas potencialmente prejudiciais, identificando e destacando o trecho específico que caracteriza a infração.

Ao exigir que o estudante justifique sua decisão com base em evidências textuais, a atividade promove a argumentação fundamentada e fortalece a compreensão das responsabilidades individuais e coletivas no ambiente digital. Dessa forma, consolida-se não apenas a percepção de risco, mas também a postura ética frente às práticas online.

6.3 Aula 3: Análise de *Gameplay* e Identificação de Situações de Risco (Percepção Dinâmica)

A terceira aula introduz um elemento de maior dinamismo, com o objetivo de desenvolver a percepção de risco em contextos audiovisuais e interativos. Diferentemente das etapas anteriores, que utilizaram materiais impressos e simulações estáticas, esta fase trabalha com trechos de *gameplay* previamente selecionados pelo professor.

Inicialmente, os estudantes são orientados a observar atentamente os comportamentos apresentados nos vídeos, considerando os critérios de segurança discutidos nas aulas anteriores. Os trechos exibidos iniciam com interações aparentemente regulares e, gradativamente, apresentam situações que podem configurar violações de normas, comportamentos inadequados ou práticas inseguras.

Durante a exibição, os alunos são convidados a: Identificar o momento em que a interação deixa de ser segura; explicar verbalmente quais elementos caracterizam a situação de risco; relacionar a ocorrência aos princípios de proteção de dados, ética digital e responsabilidade online previamente estudados.

Essa dinâmica favorece a aplicação dos conhecimentos em um contexto mais próximo da experiência real dos estudantes, estimulando a transferência do aprendizado para situações concretas. Ao integrar análise crítica, argumentação oral e observação atenta, a atividade contribui para o fortalecimento da autonomia digital e da capacidade de tomada de decisão em ambientes virtuais.

7. Avaliação

A avaliação da proposta caracteriza-se como formativa, processual e diagnóstica, ocorrendo ao longo das três aulas e tendo como finalidade acompanhar o desenvolvimento das habilidades relacionadas à segurança e à postura ética em ambientes digitais. Os instrumentos avaliativos baseiam-se nos registros produzidos pelos estudantes, nas observações sistemáticas do professor e nas manifestações orais durante as discussões coletivas.

Para fins de análise, recomenda-se a organização da avaliação em três dimensões articuladas:

7.1 Defesa Pessoal (Aula 1)

Avalia-se a capacidade do estudante de distinguir dados públicos de dados privados e de classificar adequadamente interações digitais segundo critérios de segurança. Observam-se: Correção na classificação das mensagens; Coerência entre a decisão tomada e a justificativa apresentada; Compreensão da diferença entre identidade pessoal e identidade digital.

7.2 Juízo Crítico e Ético (Aula 2)

Analisa-se a habilidade do estudante em assumir a perspectiva de moderador, identificando condutas inadequadas em interações entre terceiros. Consideram-se: Precisão na identificação do trecho que caracteriza violação de normas; Capacidade de diferenciar conflito interpessoal de infração relacionada à segurança ou privacidade; Fundamentação da decisão com base nos princípios discutidos em aula.

7.3 Percepção de Risco em Contexto Dinâmico (Aula 3)

Observa-se a aplicação dos conhecimentos em situações audiovisuais, verificando: Reconhecimento do momento em que a interação se torna insegura; Capacidade de explicitar os indícios que caracterizam risco; Transferência dos critérios aprendidos para contextos não estruturados.

Para sistematizar a análise do desempenho, recomenda-se a utilização de uma rubrica estruturada com três níveis de progressão (Iniciante, Em Desenvolvimento e Adequado), considerando critérios objetivos como: percentual de classificações corretas nas simulações; capacidade de justificar decisões com base nos princípios discutidos; identificação autônoma de situações de risco em contexto dinâmico.

Como estratégia complementar, sugere-se a aplicação de instrumento diagnóstico prévio e posterior à intervenção, contendo situações-problema semelhantes às trabalhadas em aula. A comparação entre os resultados pode fornecer evidências quantitativas do avanço conceitual dos estudantes, possibilitando futura sistematização dos dados como relato de aplicação.

Espera-se que esta proposta contribua para o desenvolvimento do letramento digital crítico, visando à proteção de dados do público-alvo. As implicações pedagógicas demonstram a viabilidade de ensinar Cultura Digital superando barreiras de infraestrutura. Para desdobramentos futuros, sugere-se aplicar a atividade para conectar a vivência em ambientes virtuais de jogos, como o *Roblox*, à conscientização prática sobre segurança digital.

Agradecimentos

Os autores agradecem à Universidade do Estado do Amazonas (UEA) pelo apoio institucional à realização deste estudo. Este trabalho está vinculado a projeto contemplado pelo Programa de Gratificação de Produtividade Acadêmica (GPA), conforme a Portaria nº 1177/2025-GR/UEA, e contou com apoio dos programas PADEX, PROTLAB-

TRAINEE, PAIC e PIBITI, no âmbito dos Editais nº 051/2024-GR/UEA, nº 131/2025-GR/UEA e nº 031/2025-GR/UEA, com financiamento da UEA, da FAPEAM e do CNPq.

9. Referências

- Cugula, J. R. G., Godoy, S. M. and Almeida, G. C. (2025) “A plataforma Roblox e o direito do consumidor brasileiro: desafios na proteção da criança e do adolescente em ambientes de consumo digitais”, *Contribuciones a las Ciencias Sociales*, v. 18, n. 11, e22324. DOI: 10.55905/revconv.18n.11-218. Available at: <https://ojs.revistacontribuciones.com/ojs/index.php/clcs/article/view/22324>.
- Brasil (2025). Lei nº 15.211, de 17 de setembro de 2025. Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/Lei/L15211.htm. Acesso em: 7 abril 2026.
- Brasil. Ministério da Educação. Conselho Nacional de Educação (2022) Base Nacional Comum Curricular: Complemento de Computação. Brasília. Available at: <http://portal.mec.gov.br/docman/fevereiro-2022-pdf/236791-anexo-ao-parecer-cneceb-n-2-2022-bncc-computacao/file>.
- Josiowicz, A. J. and Rommel Silva, M. P. (2024) “As infâncias na plataforma de videogames Roblox: transformações e permanências nas formas de jogar e de ser criança”, *La Palabra*, n. 48, e18302. DOI: 10.19053/upctc.01218530.n48.2024.18302. Available at: <https://doi.org/10.19053/upctc.01218530.n48.2024.18302>
- Farias, F. L. O.; Medeiros, N. A. A.; Rocha, S. L.; Medeiros, D. F.; Nóbrega, E. C.; Burlamaqui, A.; Madeira, C. (2019). Self Protect: Um jogo para auxílio no ensino de conceitos relacionados a Segurança na Internet para Crianças e Adolescentes. In: *Workshop de Informática na Escola (WIE)*, 25., 2019, Brasília. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, p. 246–255. DOI: <https://doi.org/10.5753/cbie.wie.2019.246>
- Simon, A. (2020). Jogos digitais ou desplugados: brincadeira ou coisa séria? *Revista Brasileira de Ensino de Ciência e Tecnologia*. <https://doi.org/10.3895/RBECT.V13N3.9972>
- Buckingham, D. (2015). Defining digital literacy: What do young people need to know about digital media? *Nordic Journal of Digital Literacy*, v. 10, p. 21–35.
- Livingstone, S. (2014). “Developing social media literacy: How children learn to interpret risky opportunities on social network sites”, *Communications*, v. 39, n. 3, p. 283–303.