

SEGURANÇA E PRIVACIDADE DIGITAL NOS ANOS INICIAIS: UM RELATO DE EXPERIÊNCIA COM ATIVIDADE DESPLUGADA A PARTIR DO ROBLOX

DIGITAL SAFETY AND PRIVACY IN THE EARLY YEARS OF ELEMENTARY EDUCATION: AN EXPERIENCE REPORT OF AN UNPLUGGED ACTIVITY BASED ON ROBLOX

SEGURIDAD Y PRIVACIDAD DIGITAL EN LOS PRIMEROS AÑOS DE LA EDUCACIÓN PRIMARIA: UN RELATO DE EXPERIENCIA CON UNA ACTIVIDAD DESENCHUFADA BASADA EN ROBLOX

Ruan Carlos Pereira Barros¹
Alexandre de Souza Passos²
Kauê Wallace Coelho Olímpio³
Adriene Chaves dos Santos⁴
Vilmar dos Santos Cavalcante Filho⁵
Ione de Castro Matos da Silva⁶
Ana Stefanne Gama Moraes⁷
Ester Figueiredo Araújo⁸
João da Mata Libório Filho⁹

1

RESUMO: Este artigo teve como objetivo analisar indícios de aprendizagem de estudantes do 3º ano do Ensino Fundamental sobre segurança e privacidade digital após a aplicação de uma intervenção pedagógica desplugada contextualizada no universo do Roblox. A pesquisa caracteriza-se como um relato de experiência, de natureza interventiva, com abordagem quantitativa e delineamento quase-experimental de grupo único, utilizando pré-teste e pós-teste aplicados a 21 estudantes. A intervenção foi desenvolvida por meio de atividades desplugadas e situações-problema relacionadas ao compartilhamento de dados pessoais, identificação de riscos em interações digitais, proteção de contas, golpes *online*, autoproteção e *cyberbullying*, buscando promover reflexões sobre comportamentos seguros e éticos em ambientes digitais. Os resultados indicaram aumento da média de acertos de 63,3% para 82,4%, diferença estatisticamente significativa entre os dois momentos avaliativos e ganhos em todas as categorias analisadas. Esses achados sugerem que situações-problema próximas das experiências digitais

¹Discente do curso Licenciatura em Computação na Universidade do Estado do Amazonas-UEA.

²Discente do curso Licenciatura em Computação na Universidade do Estado do Amazonas.

³Discente do curso Licenciatura em Computação na Universidade do Estado do Amazonas.

⁴Discente do curso Licenciatura em Computação na Universidade do Estado do Amazonas.

⁵Discente do curso Licenciatura em Computação na Universidade do Estado do Amazonas.

⁶Licenciada em Computação pela Universidade do Estado do Amazonas (UEA) – Centro de Estudos Superiores de Itacoatiara (CESIT). Trainee no Programa PROTLAB (CESIT).

⁷Graduada em Pedagogia, especialista em Educação Infantil e Gestão Escolar, mestranda em Computação.

⁸Doutora em Ciências da Educação pela Universidade do Minho, Portugal. Docente da rede estadual de ensino da Escola Estadual José Carlos Martins Mestrinho, vinculada à Secretaria de Estado de Educação e Desporto Escolar do Amazonas (SEDUC-AM).

⁹Doutor em Informática pelo Instituto de Computação da Universidade Federal do Amazonas (ICOMP/UFAM). Docente Adjunto da Universidade do Estado do Amazonas (UEA), Centro de Estudos Superiores de Itacoatiara (CESIT).

das crianças podem favorecer o desenvolvimento de noções iniciais de segurança, privacidade e conduta ética em ambientes *online*, evidenciando o potencial de atividades desplugadas contextualizadas para apoiar o letramento digital crítico nos anos iniciais do Ensino Fundamental.

Palavras-chave: Segurança digital. Privacidade digital. Roblox.

ABSTRACT: This article aimed to analyze evidence of learning among 3rd-grade elementary school students regarding digital safety and privacy after the implementation of an unplugged pedagogical intervention contextualized in the Roblox. environment. The study is characterized as an experience report of an intervention with a quantitative approach and a quasi-experimental single-group design, using a pre-test and post-test applied to 21 students. The intervention was developed through unplugged activities and problem situations related to the sharing of personal data, identification of risks in digital interactions, account protection, *online* scams, self-protection, and *cyberbullying*, seeking to promote reflection on safe and ethical behavior in digital environments. The results showed an increase in the mean score from 63.3% to 82.4%, a statistically significant difference between the two assessment moments, and gains across all analyzed categories. These findings suggest that problem situations close to children's digital experiences may foster the development of initial notions of digital safety, privacy, and ethical *online* behavior, highlighting the potential of contextualized unplugged activities to support critical digital literacy in the early years of elementary education.

Keywords: Digital safety. Digital privacy. Roblox.

RESUMEN: Este artículo tuvo como objetivo analizar indicios de aprendizaje de estudiantes del 3.º año de la Educación Primaria sobre seguridad y privacidad digital tras la aplicación de una intervención pedagógica desenchufada contextualizada en el universo de Roblox.. La investigación se caracteriza como un relato de experiencia, de naturaleza interventiva, con enfoque cuantitativo y diseño cuasiexperimental de grupo único, utilizando preprueba y posprueba aplicadas a 21 estudiantes. La intervención se desarrolló mediante actividades desenchufadas y situaciones problema relacionadas con el intercambio de datos personales, la identificación de riesgos en las interacciones digitales, la protección de cuentas, las estafas en línea, la autoprotección y el ciberacoso, buscando promover reflexiones sobre comportamientos seguros y éticos en entornos digitales. Los resultados indicaron un aumento del promedio de aciertos del 63,3 % al 82,4 %, una diferencia estadísticamente significativa entre los dos momentos de evaluación y mejoras en todas las categorías analizadas. Estos hallazgos sugieren que las situaciones problema cercanas a las experiencias digitales de los niños pueden favorecer el desarrollo de nociones iniciales de seguridad, privacidad y conducta ética en entornos en línea, evidenciando el potencial de las actividades desenchufadas contextualizadas para apoyar la alfabetización digital crítica en los primeros años de la Educación Primaria.

Palabras clave: Seguridad digital. Privacidad digital. Roblox.

INTRODUÇÃO

A presença de crianças em ambientes digitais tem se intensificado nos últimos anos, tornando a internet, os jogos *online* e as plataformas interativas parte do cotidiano infantil. Esses ambientes oferecem oportunidades de socialização, criatividade e aprendizagem, mas também expõem crianças a riscos relacionados à privacidade, ao compartilhamento indevido de dados pessoais, ao contato com desconhecidos, a golpes digitais, ao *cyberbullying* e ao acesso a

conteúdos inadequados (OECD, 2021; UNICEF, 2025). Nesse contexto, a formação para o uso seguro, crítico e responsável das tecnologias digitais torna-se uma demanda educacional relevante, especialmente nos anos iniciais do Ensino Fundamental (EF), período em que os estudantes ampliam sua autonomia no uso de dispositivos conectados e de plataformas digitais.

Entre essas plataformas, o Roblox destaca-se por combinar elementos de jogo, criação de experiências digitais e interação social, sendo utilizado em diferentes propostas educacionais por seu potencial para favorecer a criatividade, a colaboração e a participação em comunidades digitais (JOSIOWICZ e SILVA, 2024; GONÇALVES, et al., 2026). Entretanto, sua dinâmica baseada em *chats*, avatares, recompensas virtuais e interação entre usuários também pode favorecer situações de risco, como abordagens suspeitas, promessas falsas de benefícios, solicitação de dados pessoais, compartilhamento de *links* maliciosos e práticas de *cyberbullying* (CUGULA, et al., 2025; GONÇALVES, et al., 2026). Dessa forma, torna-se necessário que a escola desenvolva práticas pedagógicas que auxiliem os estudantes a reconhecerem situações inseguras, compreender formas de violência *online* e adotar decisões responsáveis em ambientes digitais (PEREIRA W e FRANÇA R, 2023).

Essa necessidade está alinhada ao Complemento à Base Nacional Comum Curricular (BNCC) – Computação, que contempla, no eixo Cultura Digital, habilidades relacionadas à segurança, à ética e à responsabilidade no uso das tecnologias digitais. Destacam-se, nesse contexto, a habilidade EF03CO09, que orienta o reconhecimento dos impactos do compartilhamento de informações pessoais em ambientes digitais, e a habilidade EF04CO07, voltada à postura ética na coleta, transferência, armazenamento e utilização de dados (BRASIL, 2022). Assim, a discussão sobre segurança e privacidade digital deve integrar a formação crítica dos estudantes para sua participação consciente nos ambientes digitais.

Apesar da relevância do tema, ainda existem desafios para o desenvolvimento de ações voltadas à segurança e à privacidade digital nos anos iniciais do Ensino Fundamental, especialmente em contextos escolares com limitações de infraestrutura tecnológica (COMITÊ GESTOR DA INTERNET NO BRASIL, 2023). Além disso, muitas iniciativas educativas concentram-se em recomendações gerais, sem explorar situações próximas da realidade vivenciada pelas crianças. Nesse sentido, atividades desplugadas contextualizadas em jogos *online* constituem uma alternativa pedagógica, pois permitem discutir riscos digitais, proteção de dados e comportamento ético sem depender do uso contínuo de dispositivos conectados.

Diante desse cenário, este estudo busca responder à seguinte questão de pesquisa: em que medida uma intervenção pedagógica desplugada, contextualizada no universo do Roblox, pode contribuir para a aprendizagem de estudantes do 3º ano do Ensino Fundamental sobre segurança e privacidade digital? Para responder a essa questão, o objetivo geral foi analisar indícios de aprendizagem após a aplicação de uma intervenção pedagógica voltada ao reconhecimento de riscos em interações digitais. Especificamente, buscou-se identificar o desempenho dos estudantes antes e após a intervenção, verificar a evolução individual dos participantes e analisar os ganhos de aprendizagem nas categorias relacionadas à proteção de dados pessoais, exposição digital, golpes *online*, proteção de contas, autoproteção e *cyberbullying*.

A principal contribuição deste estudo consiste em apresentar evidências sobre o potencial de uma atividade pedagógica desplugada, contextualizada no universo do Roblox, para o ensino de segurança e privacidade digital nos anos iniciais do Ensino Fundamental, contribuindo para o fortalecimento de práticas educativas voltadas ao uso seguro, ético e responsável das tecnologias digitais.

FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta os principais fundamentos do estudo, abordando segurança e privacidade digital infantil, sua relação com a BNCC Computação, o uso de estratégias desplugadas e estudos relacionados ao ensino de segurança em ambientes digitais.

4

Segurança e Privacidade nos Anos Iniciais

O crescimento do acesso infantil às tecnologias digitais ampliou discussões sobre segurança online, privacidade e proteção de dados. Crianças interagem cada vez mais cedo com jogos online, redes sociais e plataformas digitais, muitas vezes sem compreender plenamente os riscos envolvidos no compartilhamento de informações pessoais, em contatos inadequados e em práticas como golpes, *cyberbullying* e exposição a conteúdos impróprios.

Alves e Grané (2026) destacam que a dataficação das plataformas digitais torna crianças e adolescentes particularmente vulneráveis, enquanto Livingstone e Stoilova (2021) organizam os riscos digitais infantis no modelo dos 4Cs: conteúdo, contato, conduta e contrato. No caso do Roblox, tais riscos envolvem fragilidades de moderação, coleta de dados, exposição a conteúdos inadequados e interações potencialmente nocivas.

Dessa forma, discutir segurança e privacidade nos anos iniciais torna-se fundamental para promover comportamentos mais conscientes no uso das tecnologias digitais, contribuindo para que crianças reconheçam situações de risco e desenvolvam práticas mais seguras em ambientes online.

BNCC Computação e Letramento Digital Crítico

A discussão sobre segurança e privacidade digital na Educação Básica não se justifica apenas pela crescente presença das tecnologias no cotidiano infantil, mas também por sua relevância curricular no contexto educacional brasileiro. O Complemento à Base Nacional Comum Curricular (BNCC) Computação (BRASIL, 2022) estabelece competências relacionadas ao desenvolvimento do pensamento crítico, da cidadania digital e do uso ético e responsável das tecnologias digitais, especialmente no eixo Cultura Digital.

Esse eixo propõe que os estudantes compreendam os impactos sociais, culturais e éticos das tecnologias, desenvolvendo competências para participação consciente em ambientes digitais. Nesse contexto, o ensino de Computação na Educação Básica ultrapassa o domínio técnico das ferramentas digitais, envolvendo também reflexões sobre privacidade, segurança da informação, compartilhamento de dados e comportamento online.

5

Nos anos iniciais do Ensino Fundamental (EF), destacam-se as habilidades EF03CO09 e EF04CO07, relacionadas ao reconhecimento dos impactos do compartilhamento de informações pessoais e à adoção de posturas éticas e responsáveis no uso de dados digitais. Essas habilidades reforçam a necessidade de trabalhar, desde cedo, situações que auxiliem crianças a compreender riscos presentes em ambientes online, bem como desenvolver práticas seguras durante interações digitais.

De acordo com Neris e Hai (2023), o letramento digital envolve práticas sociais e culturais relacionadas ao uso consciente e reflexivo das tecnologias digitais. Nesse sentido, práticas pedagógicas voltadas à segurança digital contribuem para formação de estudantes mais conscientes sobre privacidade, proteção de dados e cidadania digital.

A utilização de situações próximas ao cotidiano infantil, como interações em jogos online e plataformas digitais, pode favorecer maior aproximação entre os conteúdos escolares e as experiências digitais vivenciadas pelos estudantes.

Estratégias Desplugadas e Aprendizagem Baseada em Situações-Problema

A computação desplugada consiste em estratégias pedagógicas que abordam conceitos computacionais sem depender diretamente do uso de computadores ou dispositivos digitais. Essas atividades utilizam jogos, dinâmicas, simulações e desafios para promover aprendizagem de maneira acessível, colaborativa e contextualizada.

Segundo Neris e Hai (2023), abordagens desplugadas apresentam potencial para desenvolver competências relacionadas à cultura digital mesmo em ambientes com limitações de infraestrutura tecnológica. Além de ampliarem o acesso às práticas de ensino de Computação, essas estratégias favorecem participação ativa, interação entre os estudantes e construção coletiva do conhecimento.

Entre essas abordagens, destaca-se a aprendizagem baseada em situações-problema, metodologia que estimula os estudantes a analisarem cenários, interpretar situações e tomarem decisões diante de desafios contextualizados. No campo da segurança digital, essa perspectiva possibilita discutir riscos online, privacidade e comportamento digital por meio de casos simulados inspirados em situações presentes no cotidiano infantil.

Atividades envolvendo análise de interações, exercícios de moderação e observação crítica de situações simuladas permitem que os estudantes desenvolvam percepção de risco e reflexão sobre comportamentos seguros em ambientes digitais. Essas práticas favorecem não apenas compreensão conceitual, mas também desenvolvimento do raciocínio crítico diante de problemas relacionados ao compartilhamento de dados, golpes virtuais e interações inadequadas em plataformas online.

Nesse sentido, a utilização do universo do Roblox como contexto cultural aproxima as atividades da realidade digital vivenciada pelas crianças, sem exigir o uso direto da plataforma ou de computadores durante a intervenção. Assim, estratégias desplugadas podem contribuir para o desenvolvimento do letramento digital crítico e da cidadania digital nos anos iniciais do Ensino Fundamental.

Trabalhos Relacionados

Alves e Grané (2026) analisaram riscos do Roblox para crianças e adolescentes, abordando segurança, privacidade, coleta de dados, moderação e governança. Em pesquisa

qualitativa documental, identificaram contradições entre o discurso oficial da plataforma e os riscos vivenciados por menores. Diferentemente desse estudo, esta pesquisa aplica e avalia uma intervenção pedagógica desplugada em sala de aula.

Gonçalves et al. (2026) analisaram, por revisão de literatura, potencialidades e fragilidades do Roblox na educação escolar, destacando engajamento, criatividade, colaboração e pensamento lógico, mas também riscos de segurança digital e necessidade de mediação docente. Este estudo dialoga com essa perspectiva, porém diferencia-se por aplicar uma intervenção desplugada, sem uso direto da plataforma.

Coqui et al. (2025) propuseram o Phishing Quiz, jogo educacional para conscientização sobre phishing, baseado na análise de e-mails suspeitos e feedback explicativo. A proposta indica o potencial dos jogos digitais no ensino de segurança cibernética. Esta pesquisa aproxima-se ao abordar golpes e links suspeitos, mas diferencia-se por adotar uma estratégia desplugada nos anos iniciais.

Pereira e França (2023) desenvolveram histórias em quadrinhos e uma sequência didática sobre cyberbullying, com foco no comportamento ético e no uso responsável das tecnologias digitais. Este estudo também aborda conduta ética e crueldade online, mas amplia o escopo ao integrar cyberbullying a temas como dados pessoais, phishing, proteção de senha e autoproteção em jogos online.

Em síntese, os trabalhos relacionados reforçam a relevância de discutir segurança, privacidade e conduta ética na Educação Básica. Este estudo diferencia-se por articular o contexto do Roblox a uma intervenção desplugada, aplicada no 3º ano do Ensino Fundamental, com avaliação quantitativa por meio de pré-teste e pós-teste.

MÉTODOS

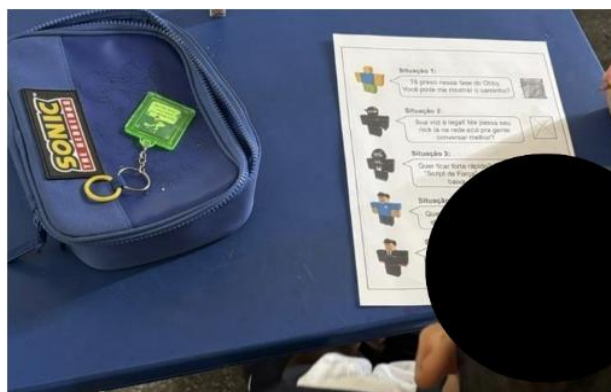
Este estudo caracteriza-se como um relato de experiência na área de Informática na Educação, de natureza interventiva, com abordagem quantitativa e delineamento quase-experimental de grupo único, utilizando pré-teste e pós-teste. A intervenção foi planejada, aplicada e avaliada em contexto real de sala de aula, com o objetivo de analisar indícios de aprendizagem relacionados à segurança e à privacidade digital nos anos iniciais do Ensino Fundamental (EF).

O estudo foi realizado com uma turma do 3º ano do Ensino Fundamental de uma escola estadual localizada no município de Itacoatiara, Amazonas. A intervenção teve como foco o ensino de conceitos relacionados à segurança digital, à privacidade, à proteção de dados pessoais e ao comportamento ético em ambientes online, utilizando situações contextualizadas no universo dos jogos digitais, especialmente em interações inspiradas no Roblox.

A pesquisa constitui uma extensão de um trabalho anteriormente publicado no SBC Educação Básica (SBC-EB 2026), no formato de resumo expandido (PEREIRA BARROS, et al., 2026). Na versão anterior, foi apresentada uma proposta pedagógica desplugada estruturada em atividades voltadas à identificação de riscos, à análise de interações e à reflexão sobre segurança e privacidade digital, sem aplicação prática em contexto escolar. Nesta pesquisa, a proposta foi aplicada em uma turma do 3º ano do Ensino Fundamental e seus resultados foram analisados quantitativamente.

A intervenção ocorreu em um único encontro, com duração aproximada de três horas, dividido em três etapas: aplicação individual do pré-teste, realização da atividade desplugada mediada pelo professor e pelos pesquisadores e aplicação individual do pós-teste. Durante a atividade, os estudantes analisaram materiais impressos contendo situações-problema inspiradas em jogos online, envolvendo conversas em chats, solicitação de dados pessoais, links suspeitos, tentativas de obtenção de senhas, bloqueio de usuários e situações de cyberbullying. Após a resolução das atividades, foi realizada uma discussão coletiva sobre as respostas apresentadas e sobre práticas seguras em ambientes digitais. As Figuras 1 e Figura 2 apresentam registros da aplicação da intervenção em sala de aula.

Figura 1-Atividade impressa de análise de situações de risco em jogos online



Fonte: Elaborado pelos autores (2026)

Figura 2- Mediação da intervenção sobre segurança e privacidade digital.



Fonte: Elaborado pelos autores (2026)

Para avaliar indícios de aprendizagem, foi utilizado um instrumento composto por dez questões objetivas, aplicado antes e após a intervenção. As questões abordaram identidade digital, dados pessoais, phishing, links suspeitos, proteção de senhas, bloqueio de usuários e cyberbullying. Para fins de análise, os itens foram organizados em quatro categorias avaliativas, apresentadas na Tabela 1. O instrumento completo encontra-se disponível no material complementar. (DOI: 10.5281/zenodo.20327109)

9

Tabela 1 – Categorias avaliativas do instrumento de pré-teste e pós-teste

Categoria avaliativa	Questões	Descrição
Identidade digital e dados pessoais	Q1, Q2, Q4	Reconhecimento de informações pessoais, distinção entre dados seguros e inseguros e compreensão sobre informações que não devem ser compartilhadas em <i>chats</i> ou jogos <i>online</i> .
Exposição e contato externo	Q3	Compreensão dos riscos associados ao compartilhamento de número de telefone e à possibilidade de contato com desconhecidos fora do ambiente do jogo.
Golpes digitais, <i>phishing</i> e proteção de conta	Q5, Q6, Q7, Q8	Identificação de situações suspeitas, <i>links</i> desconhecidos, promessas falsas de recompensas, <i>phishing</i> e solicitações indevidas de senha.
Conduta ética, autoproteção e <i>cyberbullying</i>	Q9, Q10	Reconhecimento de comportamentos inadequados em interações <i>online</i> , adoção de medidas de autoproteção e identificação de situações de <i>cyberbullying</i> .

Fonte: Elaborado pelos autores (2026)

Os dados coletados foram tabulados em planilha eletrônica e analisados no software Jamovi. Inicialmente, foram calculadas estatísticas descritivas, incluindo média, mediana, desvio-padrão, valores mínimo e máximo e intervalo de confiança de 95% para a média. Em seguida, a normalidade da distribuição dos dados foi verificada pelo teste de Shapiro-Wilk. Considerando que os mesmos estudantes responderam ao pré-teste e ao pós-teste, foram empregados testes para amostras emparelhadas com o objetivo de verificar diferenças estatisticamente significativas entre os dois momentos avaliativos.

Além da comparação entre os resultados do pré-teste e do pós-teste, foi realizada uma análise por categorias avaliativas, agrupando os itens do instrumento conforme sua proximidade conceitual. Essa estratégia permitiu analisar não apenas a evolução geral da turma, mas também os avanços dos estudantes em cada dimensão da aprendizagem relacionada à segurança e à privacidade digital.

A intervenção pedagógica foi autorizada pela Coordenadoria Regional de Educação, pela direção da escola e pelo professor regente. Os estudantes participaram mediante assentimento, e os dados foram analisados de forma agregada e anônima, preservando a identidade dos participantes e da instituição. Por se tratar de uma intervenção realizada em contexto escolar com finalidade pedagógica e posterior sistematização acadêmica dos resultados, reconhece-se como limitação do estudo a ausência de parecer prévio de Comitê de Ética em Pesquisa.

10

RESULTADOS E DISCUSSÕES

Esta seção apresenta os resultados obtidos a partir da comparação entre o desempenho dos estudantes no pré-teste e no pós-teste. A análise teve como objetivo verificar indícios de aprendizagem após a realização da intervenção pedagógica voltada à segurança e privacidade digital em ambientes de jogos online. Como os mesmos estudantes participaram dos dois momentos avaliativos, foram utilizadas análises para amostras emparelhadas.

Observa-se que a média de acertos no pré-teste foi de 63,3% (DP = 27,1), enquanto no pós-teste a média foi de 82,4% (DP = 19,5). Isso representa um ganho médio de 19,0 pontos percentuais, com intervalo de confiança de 95% entre 11,6 e 26,5 pontos percentuais. A mediana também aumentou, passando de 70,0% no pré-teste para 90,0% no pós-teste, o que indica uma melhora consistente no desempenho geral da turma (Tabela 2).

Tabela 2 – Estatística descritiva do desempenho dos estudantes no pré-teste, pós-teste e ganho.

Medida	Pré-teste	Pós-teste	Ganho
N	21	21	21
Média	63,3	82,4	19,0
IC 95%	[51,0; 75,7]	[73,5; 91,2]	[11,6; 26,5]
Mediana	70,0	90,0	20,0
Desvio-padrão	27,1	19,5	16,4
Mínimo-Máximo	10,0-100,0	40,0-100,0	0,0-70,0
Shapiro-Wilk W	0,940	0,807	0,861
Shapiro-Wilk p	0,217	< 0,001	0,007

Fonte: Elaborado pelos autores (2026)

Também houve redução da dispersão dos resultados, com desvio-padrão passando de 27,1 para 19,5, e aumento do valor mínimo de 10,0% para 40,0%, indicando melhora inclusive entre estudantes com menor desempenho inicial.

Para verificar a adequação dos testes estatísticos, foi realizado o teste de normalidade de Shapiro-Wilk. O ganho entre o pré-teste e o pós-teste apresentou violação do pressuposto de normalidade ($W = 0,861$; $p = 0,007$). Por esse motivo, adotou-se o teste de Wilcoxon para amostras emparelhadas como análise principal. O teste indicou diferença estatisticamente significativa entre os dois momentos avaliativos ($W = 153$; $p < 0,001$), com desempenho superior no pós-teste. Como análise complementar, o teste t pareado também indicou diferença significativa entre os momentos, $t(20) = 5,32$; $p < 0,001$, com tamanho de efeito elevado ($d = 1,16$). Esses resultados sugerem que a intervenção esteve associada a uma melhora expressiva no desempenho dos estudantes.

Quanto à evolução individual, 17 estudantes melhoraram seu desempenho, quatro mantiveram o percentual de acertos e nenhum estudante apresentou redução no desempenho. Esse resultado reforça que a melhora observada não foi concentrada em poucos participantes, mas ocorreu de forma ampla na turma.

Analisamos também as categorias avaliativas definidas na Tabela 1. Essa análise permite observar o desempenho dos estudantes em dimensões conceituais mais amplas, relacionadas à

segurança e à privacidade digital. A média dos percentuais de acerto das questões que compõem cada categoria é apresentada (Tabela 3).

Tabela 3 – Desempenho agregado por categoria avaliativa no pré-teste e no pós-teste.

Categoria avaliativa	Pré-teste	Pós-teste	Ganho (pontos percentuais)
Identidade digital e dados pessoais	68,3%	76,2%	+7,9
Exposição e contato externo	85,7%	100,0%	+14,3
Golpes digitais, <i>phishing</i> e proteção de conta	58,3%	82,1%	+23,8
Conduta ética, autoproteção e <i>cyberbullying</i>	54,8%	83,4%	+28,6

Fonte: Elaborado pelos autores (2026)

A análise agregada por categoria indica que houve aumento no desempenho em todas as dimensões avaliadas. O maior ganho foi observado na categoria "Conduta ética, autoproteção e *cyberbullying*", que passou de 54,8% no pré-teste para 83,4% no pós-teste, representando avanço de 28,6 pontos percentuais. Esse resultado sugere que a intervenção contribuiu para que os estudantes reconhecessem com maior clareza comportamentos inadequados em ambientes digitais e identificassem atitudes seguras, como bloquear usuários e comunicar situações de risco a um adulto de confiança.

A segunda maior evolução ocorreu na categoria "Golpes digitais, *phishing* e proteção de conta", com aumento de 58,3% para 82,1%, correspondendo a ganho de 23,8 pontos percentuais. Esse resultado é relevante porque essa categoria reúne itens relacionados à identificação de links suspeitos, promessas falsas de recompensas, tentativas de *phishing* e solicitações indevidas de senha. Assim, os dados indicam que a intervenção favoreceu a compreensão de riscos associados a golpes digitais comuns em ambientes de jogos online.

Na categoria "Exposição e contato externo", observou-se desempenho elevado já no pré-teste, com 85,7% de acertos, alcançando 100,0% no pós-teste. Embora o ganho tenha sido menor em termos absolutos, esse resultado sugere consolidação da compreensão sobre os riscos de compartilhar número de telefone e manter contato com desconhecidos fora do ambiente do jogo.

Já a categoria "Identidade digital e dados pessoais" apresentou o menor ganho, passando de 68,3% para 76,2%. Esse resultado pode estar relacionado ao fato de que parte dos estudantes já possuía conhecimentos prévios sobre o tema ou à possível dificuldade em distinguir, em determinadas situações, informações pessoais sensíveis de informações aparentemente inofensivas.

De modo geral, a análise por categoria complementa a interpretação dos resultados globais, ao evidenciar que os maiores avanços ocorreram justamente nas dimensões associadas à identificação de riscos mais complexos, como phishing, golpes digitais, proteção de conta, cyberbullying e autoproteção. Esses achados reforçam a pertinência da intervenção pedagógica, pois indicam que atividades contextualizadas em situações de jogos online podem favorecer a compreensão de problemas concretos vivenciados pelas crianças em ambientes digitais.

Os resultados sugerem que a proposta pedagógica favoreceu a aprendizagem dos estudantes sobre segurança e privacidade digital. O aumento da média, da mediana e do valor mínimo no pós-teste, associado ao resultado estatisticamente significativo do teste de Wilcoxon e ao tamanho de efeito elevado observado no teste t pareado, indica que houve melhora relevante no desempenho após a intervenção.

Como lições aprendidas, observou-se que situações-problema inspiradas em jogos online favoreceram a aproximação entre os conteúdos escolares e as experiências digitais das crianças, enquanto o uso de material impresso permitiu discutir segurança digital mesmo sem acesso individual a computadores. Também se identificou a necessidade de revisar ou ampliar itens relacionados à distinção entre dados pessoais sensíveis e informações aparentemente inofensivas, dimensão que apresentou menor ganho entre as categorias avaliadas.

Apesar dos resultados positivos, é importante reconhecer algumas limitações do estudo. A intervenção foi realizada com uma única turma e não contou com grupo controle, o que impede afirmar causalidade de forma definitiva. Além disso, o número de participantes foi reduzido, característica comum em estudos aplicados em contexto escolar, mas que limita a generalização dos achados. Portanto, os resultados devem ser interpretados como evidências iniciais de aprendizagem associadas à intervenção, recomendando-se novas aplicações com amostras maiores, diferentes turmas e, quando possível, delineamentos com grupo de comparação.

CONSIDERAÇÕES FINAIS

Este estudo apresentou a aplicação de uma intervenção pedagógica desplugada sobre segurança e privacidade digital nos anos iniciais do Ensino Fundamental, contextualizada em situações inspiradas no Roblox. Os resultados indicaram indícios positivos de aprendizagem, evidenciados pelo aumento da média de acertos de 63,3% para 82,4%, pela diferença estatisticamente significativa entre o pré-teste e o pós-teste e pela melhora individual de 17 dos 21 estudantes.

Como contribuição, o estudo reforça achados da literatura ao demonstrar, em contexto aplicado, que temas relacionados à segurança e à privacidade digital podem ser trabalhados pedagogicamente desde os anos iniciais do Ensino Fundamental. Os resultados dialogam com Pereira e França (2023), ao evidenciar a importância de práticas escolares voltadas à conduta ética e ao enfrentamento do cyberbullying, e com Coqui et al. (2025), ao confirmar a pertinência de abordar golpes digitais, phishing e links suspeitos em propostas educativas. Além disso, ao utilizar o Roblox como contexto, sem o uso direto da plataforma, a pesquisa complementa Gonçalves et al. (2026), indicando que seus potenciais pedagógicos também podem ser explorados por meio de estratégias desplugadas.

Apesar dos resultados positivos, o estudo apresenta limitações. A intervenção foi realizada com uma única turma, composta por 21 estudantes, sem grupo controle, o que limita a generalização dos resultados e impede inferências causais definitivas. Também se reconhece, como limitação ético-procedimental, a ausência de parecer prévio de Comitê de Ética em Pesquisa, embora a aplicação tenha contado com autorização institucional, assentimento dos estudantes e tratamento agregado e anônimo dos dados.

Como perspectivas para estudos futuros, recomenda-se a reaplicação da intervenção em outras turmas, escolas e anos escolares, com amostras maiores e, quando possível, grupo de comparação. Sugere-se, ainda, o aprimoramento do instrumento avaliativo, a ampliação da quantidade de itens por categoria e a incorporação de análises qualitativas das falas e justificativas dos estudantes, a fim de compreender de forma mais aprofundada os processos de aprendizagem relacionados à segurança e à privacidade digital.

REFERÊNCIAS

ALVES L, GRANÉ M. Riscos e segurança no Roblox: como proteger crianças e adolescentes no ambiente digital. *Brazilian Creative Industries Journal*, 2026; 5(2).

BRASIL. Ministério da Educação. *Computação na Educação Básica: Complemento à BNCC*. Brasília: Ministério da Educação; 2022.

COMITÊ GESTOR DA INTERNET NO BRASIL. Conectividade nas escolas brasileiras aumenta após a pandemia, mas faltam dispositivos para acesso à Internet pelos alunos, revela TIC Educação 2022. 2023.

COQUI L, et al. *Phishing Quiz: um jogo educacional para conscientização e prevenção de ataques cibernéticos. Anais Estendidos do XXIV Simpósio Brasileiro de Jogos e Entretenimento Digital*. Salvador: SBC, 2025; 139-145.

CUGULA JRG, GODOY SM, ALMEIDA GC. 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*, 2025.

GONÇALVES EAS, et al. O uso do Roblox na educação escolar e suas potencialidades e fragilidades no desenvolvimento dos estudantes. *Aurum Editora*, 2026; 97-107.

JOSIOWICZ AJ, SILVA MPR. As infâncias na plataforma de videojogos Roblox: transformações e permanências nas formas de jogar e de ser criança. *La Palabra*, 2024.

LIVINGSTONE S, STOILOVA M. *The 4Cs: Classifying Online Risk to Children*. Hamburg: Leibniz-Institut für Medienforschung – Hans-Bredow-Institut; 2021.

NERIS VA, HAI AA. Tecnologia e educação: ciências, computação (des)plugada e pensamento computacional na educação de crianças de 4 a 10 anos. *Cadernos CEDES*, 2023; 43(120): 2-4.

OECD. *Children in the Digital Environment: Revised Typology of Risks*. Paris: OECD; 2021.

PEREIRA RC, BINA PAULO L, SOUZA PASSOS A, et al. Aulas propostas. Zenodo, 2026.

PEREIRA W, FRANÇA R. *Cyberbullying na escola: entendendo e lidando com a crueldade online. Anais do III Simpósio Brasileiro de Educação em Computação*. Porto Alegre: SBC, 2023; 359-368.

UNICEF. *Childhood in a Digital World*. New York: UNICEF; 2025.