O Uso de Quizzes como Ferramenta para Educação em Cibersegurança

Ana Paula Vieira Dias[1], Laura Maria Santos[1], Raquel Arantes Valério[1], Patricia Cristiane de Souza[1], Nelcileno Virgilio Araujo[1], Aurélio Mendanha da Silva[2]

[1] Instituto de Computação – UFMT – CEP 78.060-719 – Cuiabá – MT – Brasil

[2]CISC – CEP 78.635-000 – Água Boa – MT – Brasil

apaulavieira927@gmail.com, lauramsx99@gmail.com, raquel.valerio@sou.ufmt.br, aureliomsilva1@gmail.com, (patricia, nelcileno)@ic.ufmt.br

Abstract. *Currently, several changes in the way people communicate have been taking place, culminating in the unbridled use of technologies for interaction, which also brings with it an increase in the number of cases of digital scams. As a result, social organizations, companies and educational institutions have been using Education in Cybersecurity as a way to bring knowledge to the population, so that they do not become such easy victims of digital scams. This article discusses the proposal and evaluation of quizzes as a tool for education in classification of digital scams for Internet users, using the Design Science Research (DSR) method to build the quizzes. The results obtained demonstrate greater acceptance among younger people of this quiz artifact as a way of learning about the classification of digital scams, as well as adjusting and customizing this artifact for the profiles of adults and the elderly.*

Resumo. *Na atualidade, estamos testemunhando uma crescente transformação digital na forma como as pessoas vivem e se comunicam, impulsionada pelo uso cada vez mais intenso de tecnologias de interação. Esse fenômeno tem resultado em um aumento constante no número de golpes digitais, o que agrava a vulnerabilidade de indivíduos e empresas. Uma vez que, mesmo com sistemas altamente avançados, a falta de compreensão sobre os golpes pode levar qualquer pessoa, ou até uma organização inteira, a se tornar vítima de fraudes digitais. Sendo assim, como resposta a essa realidade, instituições educacionais, empresas e organizações sociais têm adotado a educação em segurança cibernética como uma estratégia fundamental para minimizar os impactos e capacitar a população. Por conseguinte, este artigo explora a utilização de quizzes como ferramenta educacional para a conscientização sobre a classificação de golpes digitais, aplicando o método Design Science Research (DSR) no desenvolvimento desses quizzes. Os resultados obtidos revelam, de maneira clara, uma maior aceitação desse recurso entre os jovens, que demonstraram utilizá-lo de forma eficaz para aprender a identificar e classificar golpes digitais. Em contrapartida, observou-se que, embora os jovens se adaptem rapidamente à ferramenta, a aceitação entre adultos e idosos foi menos expressiva. Portanto, o estudo sugere a necessidade de adaptar e personalizar os quizzes, de modo a atender de forma mais eficaz os perfis dessas faixas etárias, ampliando, assim, seu alcance e eficácia na conscientização sobre segurança cibernética.*

1. Introdução

A tecnologia tem desempenhado um papel crucial na vida das pessoas, facilitando as tarefas do cotidiano, especialmente na área da comunicação. No entanto, essa ampla propagação também oferece oportunidades para criminosos, que utilizam equipamentos conectados à internet para aplicar golpes digitais. A informatização crescente das atividades sociais, tanto em nível individual quanto coletivo, tem proporcionado aos criminosos novas ferramentas, e seu impacto ainda não foi completamente analisado [Dias 2023]. Como resultado dessa evolução, surgiram vários tipos de golpes digitais, como fraudes aplicadas por meio de redes sociais, anúncios falsos, além das falsificações de dados financeiros e de cartões de crédito.

Nesse contexto, o conceito de "Sociedade de Risco" de Ulrich Beck é relevante, pois, segundo o autor, a modernidade reflexiva é caracterizada pela crescente conscientização dos riscos e incertezas gerados pelo próprio progresso tecnológico [Beck 2011]. Pode-se entender a sociedade de risco como uma forma sistemática de lidar com perigos e inseguranças induzidas pela modernização. Os golpes cibernéticos podem ser vistos como manifestações estruturais dessa sociedade de risco. Um risco que afeta uma parte significativa da população brasileira, que vive com o receio de ser vítima de golpes digitais, como mostram dados da Pesquisa Nacional por Amostra de Domicílios Contínua (PNAD Contínua) de 2021 [IBGE 2021]. A pesquisa revelou mudanças de hábitos, com 15% dos entrevistados dizendo evitar o uso de redes sociais ou da internet por questões de segurança.

Este medo é, em grande parte, consequência do baixo letramento digital dos usuários em relação aos golpes digitais, uma lacuna identificada por [Guilherme et al. 2021], onde 37% dos entrevistados nunca tiveram treinamento sobre navegação segura na internet. [Biadeni and Fonseca 2023] também discutem que, embora o letramento digital possa capacitar os usuários a não se tornarem alvos fáceis de desinformação, a propagação de conteúdos fraudulentos continua em crescimento. Este panorama evidencia a necessidade urgente de educar os usuários sobre cibersegurança e como se proteger contra fraudes digitais.

Uma estratégia eficaz e atual para esse tipo de educação é a gamificação. Segundo [Brazil and Baruque 2015], a gamificação está se tornando uma ferramenta importante em contextos de aprendizagem, transformando atividades educativas em experiências lúdicas que facilitam a compreensão e retenção de temas complexos. Esse conceito de gamificação tem sido amplamente utilizado para promover a educação sobre segurança digital, como demonstrado no estudo de [Scholefield and Shepherd 2019], que evidenciou a eficácia de um jogo de RPG em formato quiz na transmissão de conceitos relacionados a senhas seguras. Além disso, uma análise realizada por [Sharif and Ameen 2021], com base em diversos artigos, revelou que 34% das publicações revisadas aplicam estratégias de gamificação como método de ensino em cibersegurança. Esses achados indicam que a gamificação tem se consolidado como uma ferramenta valiosa para a educação em segurança digital, contribuindo para o engajamento e a assimilação de práticas seguras no ambiente online.

Deste modo o objetivo deste artigo é examinar o uso de quizzes como uma estratégia de gamificação para educar as pessoas sobre os padrões dos golpes digitais e como se proteger. Para tanto, utilizou-se da metodologia Design Science Research (DSR),

que visa resolver problemas práticos por meio da concepção de artefatos. Os quizzes foram divulgados no perfil do Instagram do grupo de pesquisa e foram testados por pessoas de diferentes faixas etárias e contextos de letramento digital. Os resultados, mesmo que preliminares, permitem demonstrar que há potencial de melhorar significativamente o entendimento da população sobre os golpes digitais.

Este artigo está estruturado da seguinte forma: na próxima seção é apresentado uma revisão sobre as principais pesquisas relacionadas que abordam o tema gamificação e educação em cibersegurança. Na terceira seção, é explicitada a metodologia utilizada para criação do quizzes para educação em cibersegurança. Na quarta seção, Discussão e consolidação dos resultados alcançados, são discutidos o desenvolvimento da caracterização de alguns golpes digitais, a criação do quizzes baseado na metodologia utilizada, sua aplicação para teste com alguns jogadores e o feedback obtido. E, por fim, na quinta seção, Considerações finais, é feita uma análise geral do que foi realizado e o que há por vir.

2. Trabalhos relacionados

A partir da revisão de trabalhos da literatura global sobre Gamificação —método que consiste na aplicação de elementos de jogos em contextos não lúdicos, como o ensino, para potencializar a aprendizagem do aluno a respeito de determinado conteúdo — identificaram-se estudos relevantes que abordam sua utilização na educação de jovens e adultos, especialmente para a conscientização a respeito de Golpes Digitais e Segurança Digital. Dessa forma, esses trabalhos apresentam fundamentação teórica significativa para os temas mencionados e contribuem diretamente para o embasamento desta pesquisa, fornecendo subsídios para a análise e aplicação da gamificação nesse contexto educacional.

Inicialmente, o estudo conduzido [Thornton and III 2014] teve como objetivo investigar a aplicação da gamificação no ensino de sistemas de informação e segurança, explorando como elementos de jogos podem melhorar o engajamento e a retenção de conhecimento dos alunos. Para isso, os pesquisadores desenvolveram jogos educativos e ferramentas de gamificação aplicadas em cursos universitários e de ensino médio, além de um workshop com 16 professores e instrutores. Os jogos, como Brute Force (ensino de senhas seguras) e Friend or Foe (conscientização sobre phishing), foram aplicados a 180 alunos. Utilizando o software Game Maker, os resultados mostraram que a gamificação aumentou a motivação, participação e desempenho dos alunos, melhorando a retenção e frequência às aulas. Concluiu-se que a gamificação pode ser eficaz no ensino de segurança da informação, desde que bem projetada para o público-alvo.

Posteriormente, com o objetivo de tornar o aprendizado sobre Segurança da Informação mais atrativo por meio de gamificação, [Mostafa and Faragallah 2019] conduziu um experimento com 81 estudantes de graduação dos cursos de Tecnologia da Informação, Ciência da Computação e Engenharia da Computação da Universidade de TAIF. Para a análise os estudantes foram divididos em dois grupos, sendo eles um grupo de jogos, com 42 alunos que utilizaram jogos educativos, e um grupo de controle, com 39 (trinta e nove) alunos que utilizaram apenas notas de aula, ocorrendo ao longo de seis semanas, tendo seis sessões, cada uma abordando um módulo específico de segurança da informação. Após cada sessão, os alunos realizaram pré-testes e pós-testes para avaliar a assimilação dos conteúdos, além disso os dados foram analisados utilizando ANOVA -

técnica estatística que compara as médias de dois ou mais grupos - no software SPSS 26 - software estatístico que permite a análise de dados para resolver problemas de negócios e pesquisa. Assim, a análise dos resultados indicou que o grupo de jogos teve um desempenho significativamente melhor nos pós-testes em relação ao grupo de controle, além disso, constatou-se que o gênero de jogo mais apreciado pelos participantes foi o de ação/aventura. No entanto, devido ao tamanho reduzido da amostra, não é possível inferir conclusivamente que esse seja o gênero mais adequado para a aplicação generalizada no ensino da área. Em seus resultados finais, a pesquisa revelou que jogos com conteúdos altamente integrados, como RPG e simulação, tiveram melhor desempenho do que jogos com conteúdos menos conectados, como quiz e quebra-cabeça. Com isso demonstrou que a gamificação é uma ferramenta eficaz para o ensino de Segurança da Informação, proporcionando maior engajamento e assimilação dos conteúdos pelos alunos.

Em seguida, o estudo de [Marinho and Bodê 2022] avaliou a eficácia da gamificação no treinamento em Segurança da Informação, utilizando o Kahoot! com discentes da FATEC Americana. Os resultados mostraram um aumento de 66% no desempenho dos participantes, evidenciando o potencial da gamificação para melhorar a assimilação e retenção do conhecimento, tornando-se uma estratégia eficaz para conscientização e treinamento na área.

O estudo de [Sharif and Ameen 2021] realizou uma revisão da literatura sobre os métodos de treinamento voltados para a educação em segurança da informação, analisando diferentes abordagens e identificando a mais eficaz. Por meio da revisão sistemática, constatou-se que 34% dos trabalhos analisados adotam a gamificação como estratégia central, enquanto outras pesquisas exploram o uso do RPG (role-playing game) em formato de quiz. Esses métodos demonstram um impacto positivo na conscientização dos usuários sobre segurança digital, destacando-se como abordagens promissoras para treinamentos e capacitações na área.

Além disso, o trabalho de [Silva and Vieira 2021] investigou o conceito de segurança cibernética a partir de diversas perspectivas, analisando suas definições e implicações jurídicas. Os autores examinaram os impactos dos crimes digitais e contextualizaram a legislação brasileira, com ênfase na Lei Carolina Dieckmann (Lei Nº 12.737), que tipifica crimes cibernéticos. A pesquisa também identificou os delitos mais recorrentes no Brasil, destacando a publicidade enganosa como a infração mais frequente no período analisado. Esses achados reforçam a necessidade de estratégias educativas para mitigar os riscos associados às fraudes digitais.

No que se refere às fraudes financeiras, o estudo de [Netto and Rabelo 2023] abordou os golpes envolvendo o sistema de pagamentos instantâneos Pix, analisando o receio da população em utilizá-lo. A pesquisa revelou que, apesar de 65% dos brasileiros já terem adotado essa forma de transferência bancária, ainda há uma percepção de insegurança significativa. Os resultados indicaram que quatro em cada dez cidadãos relataram já ter sido alvo de tentativas de fraude com Pix, evidenciando a relevância de medidas de conscientização e aprimoramento da segurança digital nesse contexto.

Por conseguinte, o estudo de [Santana and da S. Amorim 2024] desenvolveu e avaliou o jogo educativo Quiz60+, voltado para a capacitação de idosos em segurança digital, com foco na identificação e prevenção de golpes virtuais. O jogo foi aplicado

presencialmente e virtualmente a um grupo de cinco idosos, e a análise dos resultados apontou que 80% dos participantes consideraram a ferramenta útil para a compreensão das ameaças digitais. Esses achados reforçam o potencial das abordagens lúdicas como recurso pedagógico para públicos vulneráveis, contribuindo para o aumento da conscientização sobre segurança cibernética.

Os estudos revisados fornecem suporte teórico essencial para este projeto, reforçando a importância de soluções inovadoras que utilizem elementos lúdicos para aprimorar a educação em segurança digital e ampliar a proteção dos usuários frente às ameaças cibernéticas.

3. Metodologia

A metodologia escolhida para o desenvolvimento deste trabalho foi a Design Science Research (DSR). A DSR, conforme descrita por [Dresch et al. 2015], organiza-se em dois ciclos interdependentes: o ciclo de design, que se concentra na concepção, implementação e refinamento do artefato, e o ciclo de conhecimento, que busca gerar insights teóricos a partir das interações e avaliações realizadas durante o desenvolvimento. No contexto desta pesquisa, os ciclos de design e de conhecimento foram estruturados com duas fases cada, como mostra a Figura 1.

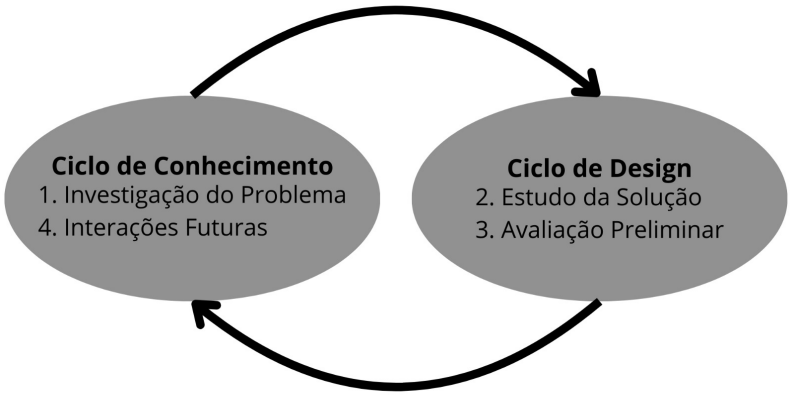

Figura 1. Ciclo da DSR

A primeira fase, Investigação do Problema, teve como base a revisão de literatura sobre golpes digitais, gamificação e o levantamento de dados sobre o impacto da falta de conhecimento em cibersegurança. Foram identificadas lacunas no letramento digital dos usuários, e com isso foram definidos os objetivos do artefato. O resultado dessa fase foi um documento com requisitos iniciais e diretrizes para o design do artefato, levando-se em consideração que seriam desenvolvidos cinco artefatos, em formato de quiz, cada um sobre um golpe digital diferente.

A segunda fase, o Estudo da Solução, teve como as entradas os requisitos definidos e princípios teóricos de gamificação. O processo foi a escolha da plataforma de desenvol-

vimento dos protótipos e criação das perguntas preliminares e mecânicas gamificadas. A saída sendo o desenvolvimento dos protótipos iniciais.

A terceira fase foi a Avaliação Preliminar, na qual as entradas foram a versão inicial dos artefatos e amostra de participantes, o processo que envolveu a aplicação dos quizzes, coleta de dados de desempenho e engajamento dos participantes. A saída obtida foi o relatório preliminar com feedback dos participantes, identificando áreas de melhoria para os protótipos.

A quarta e última fase, o planejamento das Iterações Futuras, levou em consideração o feedback obtido na avaliação preliminar e novos insights teóricos das fases anteriores, como a parte do processo que envolve a análise dos resultados e definição de ajustes e refinamentos nos artefatos. Essa fase teve como saída as diretrizes para as próximas versões dos artefatos, incluindo novas funcionalidades e ajustes pedagógicos.

Esses artefatos foram elaborados para explorar diversas situações de engajamento e aprendizagem em cibersegurança. Durante a coleta de dados, foi solicitada apenas a informação sobre a idade dos participantes, sem a coleta de outros dados demográficos ou pessoais. Essa abordagem permitiu obter feedback inicial sobre os artefatos e observar padrões gerais de participação e interação, que serão utilizados para guiar o refinamento e o aprimoramento das próximas iterações. Este caráter iterativo, inerente a natureza cíclica do DSR, assegura que a solução proposta evolua de forma contínua, atendendo progressivamente às demandas identificadas e contribuindo para a construção de um corpo de conhecimento teórico relevante.

4. Discussão e consolidação dos resultados alcançados

Seguindo o método Design Science Research, foi desenvolvida uma base de conhecimento sobre golpes digitais para promover a educação da população através da gamificação. Com apoio de um investigador da Delegacia de Água Boa - MT, analisaram-se 240 boletins de ocorrência de estelionato entre 01/02/2021 e 23/02/2022, sendo 144 relacionados a golpes eletrônicos. Uma amostra de 10% desses casos (15 registros) foi estudada para identificar padrões de comportamento dos criminosos, quantidade considerada suficiente para análise moderada [Minayo et al. 2002].

O estelionato, previsto no artigo 171 do Código Penal, consiste em enganar alguém para obter vantagem ilícita, causando prejuízo. A Lei nº 14.155/2021 passou a incluir a prática do crime por meios eletrônicos, abrangendo internet, redes sociais e aplicativos. Na pesquisa, foram analisados registros de estelionato eletrônico, incluindo crimes como falsificação de dados, injúria e racismo [Cruz and Rodrigues 2018]. A análise das narrativas identificou cinco golpes recorrentes, detalhados na Tabela 1.

A escolha pelo uso de quizzes foi inspirada no trabalho de [Mostafa e Faragallah 2019], que utilizou o jogo Be-Aware para ensinar engenharia social. Após análise, oito plataformas foram selecionadas para o desenvolvimento dos quizzes, variando entre opções simples e avançadas. Os critérios para avaliar as plataformas incluíram idioma, gratuidade, possibilidade de compartilhamento, variedade de tipos de perguntas, configuração de tempo, comentários em respostas incorretas e pontuação. Após análise, a plataforma escolhida foi a Quiz Maker, destacando-se por sua acessibilidade e jogabilidade. As perguntas dos quizzes foram elaboradas com auxílio do investigador da polícia,

adaptadas para linguagem coloquial e focadas em identificar padrões de golpes digitais. Cada quiz contém cinco perguntas, refletindo os elementos principais de cada golpe.

Ao final do quiz, o jogador recebe uma pontuação de 0 a 10, sendo cada resposta correta (Sim ou Não) equivalente a 2 pontos. A escolha da escala de 0 a 10 baseou-se em [Gjertsen et al. 2017], que destaca a importância da progressão como fator motivacional. Assim, pontuações de 0/10, 2/10 e 4/10 indicam alta chance de ser ou ter sido vítima do golpe, enquanto 6/10, 8/10 e 10/10 representam baixa probabilidade, pois refletem maior número de respostas corretas. Os quizzes foram divulgados semanalmente nas redes sociais do projeto de pesquisa, com o objetivo de disponibilizá-los durante um período de dois meses, garantindo maior participação e melhor organização.

Tabela 1. Caracterização dos golpes escolhidos para o artefato

Nome do Golpe	**Como acontece**	**Qual o meio eletrônico**	**Cuidados**
Golpe do Empréstimo	Ofertas falsas de crédito fácil e rápido, geralmente atrativas.	Solicita dados pessoais e transferência de valor antes de liberar o empréstimo.	Verifique empresas com boa reputação, desconfie de ofertas suspeitas e evite transferências antecipadas.
Falsa Foto de Perfil do WhatsApp	Uso de foto de perfil de vítima para se passar por ela.	Envia mensagens a conhecidos da vítima pedindo dinheiro.	Confirme a identidade do contato e use a autenticação em duas etapas no aplicativo.
Intermediário	Fraude em negociações prometendo altos lucros.	O golpista intermedeia a negociação, mas as transações resultam em prejuízo.	Desconfie de anúncios muito vantajosos e sempre cheque a credibilidade da negociação.
Número Novo	Alguém finge ser conhecido e solicita dinheiro.	Contato via WhatsApp informando mudança de número, seguido de pedidos de dinheiro.	Confirme o histórico de contatos e identifique a pessoa antes de realizar transferências.
Golpe da Gatinha(o)	Contas falsas pedem fotos íntimas para depois chantagear a vítima.	Falso responsável aparece alegando que a pessoa é menor de idade e exige dinheiro.	Verifique se o perfil é recente, com interações e seguidores legítimos.

Para avaliar os quizzes, foram criados formulários no Google com perguntas sobre a pontuação final, qualidade das questões e se os jogadores aprenderam os padrões dos

golpes. Os resultados indicaram que, em geral, os participantes assimilaram os padrões, mas alguns relataram dificuldades devido à formulação das perguntas, à construção do quiz e à ausência de uma "árvore de escolhas", onde cada resposta direcionasse a novas perguntas, evitando um percurso linear.

Os participantes foram divididos em três faixas etárias: "jovens adultos" (19-35 anos, 22 participantes), "adultos" (36-59 anos, 14 participantes) e "idosos" (60+ anos, 4 participantes), totalizando 40 respostas. Essa divisão foi personalizada para melhor categorizar o público, baseada em fases da vida e na distribuição etária observada. Pode-se verificar a alta taxa de "jovens adultos" que responderam o formulário, sendo 55% dos participantes, um número bem superior em relação aos idosos por exemplo.

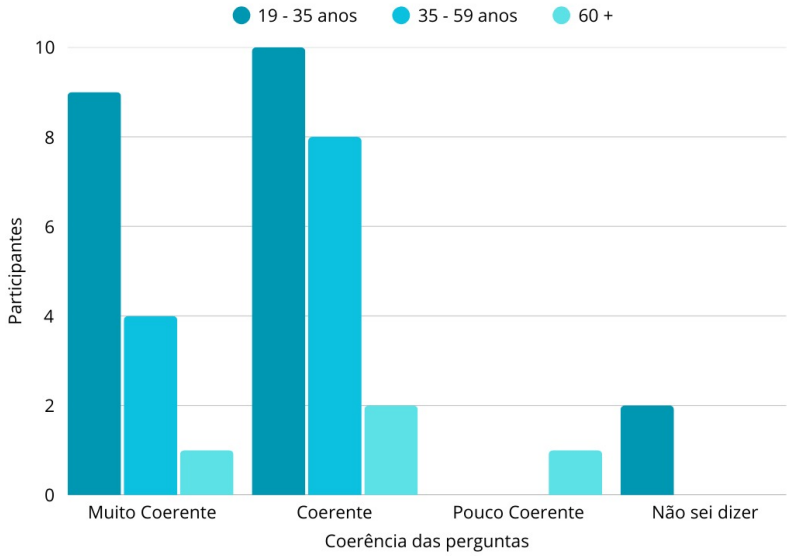

Figura 2. Coerência das perguntas

Como pode-se observar na Figura 2, a avaliação dos perguntas dos cinco quizzes, 10% dos participantes classificaram como "Razoável", 35% como "Bom" e 55% como "Muito Bom", indicando uma recepção positiva.Além disso, ao questionar se conseguiram compreender os padrões básicos dos golpes, 97,5% responderam afirmativamente, destacando a eficácia do ensino. Analisando as notas de todos os participantes, 40% do total alcançaram 8/10 pontos e apenas 25% ficaram abaixo de 6/10, com distribuições: 0/10 (7,5%), 2/10 (10%) e 4/10 (7,5%). Isso representa que os participantes aprenderam sobre os golpes e sabem identificar seus principais pontos, diminuindo a probabilidade de se tornarem vítimas.

Uma leitura interessante é feita ao se separar os grupos de idade e suas respectivas pontuações. Primeiro, ao analisar o grupo 60+, 75% dos participantes tiveram notas abaixo de 6/10 nos quizzes. E, ao preencherem o formulário de feedback, os participantes relataram ter conseguido apreender os padrões do golpe e gostaram dos quizzes. Entretanto, como se mostra na Figura 3, os participantes avaliaram positivamente as perguntas. Ao analisar os formulários de feedback, os participantes sugeriram mais perguntas para facilitar o entendimento dos golpes.

Já o grupo "adultos" mostra maior variação nas pontuações, onde 14,3% obti-

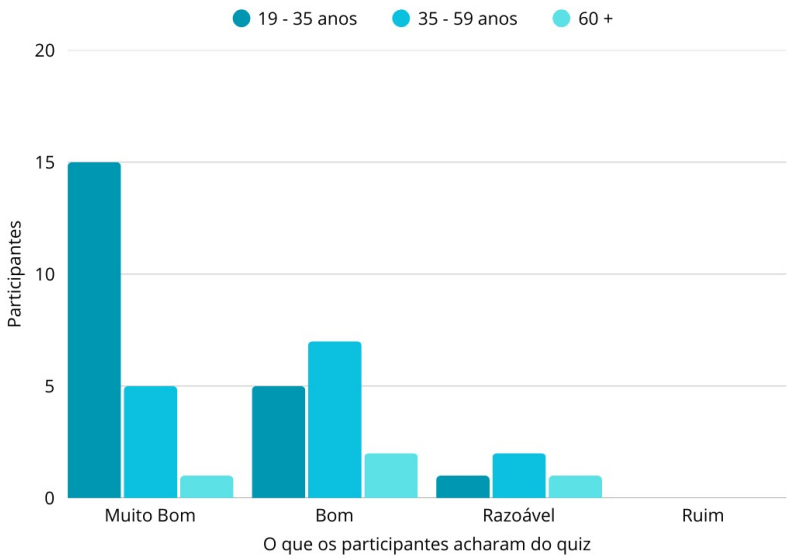

Figura 3. Opinião dos participantes sobre o quiz

veram 2/10 ou 4/10 questões, 28,6% 6/10, 21,4% 8/10 e 7,1% 10/0 questões. Embora muitos participantes tenham expressado uma visão favorável quanto ao uso do quiz como ferramenta de ensino, destacando a compreensão dos principais conceitos abordados, a análise dos feedbacks revelou a necessidade de aprimorar a formulação das perguntas. De fato, cerca de 28,57% dos respondentes relataram dificuldades em compreender algumas questões, especialmente aquelas que foram consideradas confusas ou de difícil interpretação, torna-se evidente que as pontuações abaixo de 6/10 para parte desse grupo podem ser atribuídas a uma possível falta de clareza nas perguntas.

O grupo "jovens adultos" obteve pontuações muito mais homogêneas, sendo que 54,5% obtiveram uma pontuação de 8/10 nos quizzes, as pontuações favoráveis contrastam em peso contra os 4,5% de pontuação abaixo de 6/10. Esse conjunto avaliou muito positivamente o uso de quizzes como método de ensino contra golpes digitais, com números de 72,7% avaliando o quiz como "Muito Bom".

5. Considerações Finais

Após a análise dos resultados dos quizzes e dos feedbacks, pode-se dizer que as conclusões foram encorajadores para ajudar na educação dos usuários sobre as caracterizações dos golpes digitais tratados. Sendo assim, os resultados obtidos até o momento corroboram o entendimento que o quiz é uma ferramenta eficaz para auxiliar na conscientização sobre os golpes digitais e seus padrões, principalmente para o público jovem, que se mostrou com melhores resultados dentre os três grupos de participantes.

Assim, considerando a diversidade e o surgimento de novos golpes, a pesquisa se mantém atuante em identificar e estabelecer padrões e analisar a incidência de golpes em públicos específicos, quer seja por faixa etária, sexo, condição social e/ou grau de literacia digital. Por meio de pesquisas realizadas em literatura, mais outros seis tipos de golpes foram categorizados: golpe da "Mão Fantasma"; golpe do "Smishing"; golpe de "Phishing"; golpe da "Falsa vaga de emprego"; golpe do "PIX" ou da "Falsa página";

golpe do “PIX” ou da “Falha no PIX” (Vishing).

Atualmente, o projeto tem se debruçado em dar atenção aos ajustes nas questões apresentadas no decorrer do artigo, na análise da acessibilidade dos artefatos gerados, e, no desenvolvimento de outros tipos de artefatos para o público 60+ considerando a categorização do total de onze tipos de golpes e a análise de quais são mais recorrentes com este público. O objetivo continua ser gerar artefatos em forma de jogos simples e que ajudem a educar as pessoas sobre os padrões dos golpes digitais e sobre como se proteger no mundo digital.

6. Agradecimentos

Os autores gostariam de agradecer ao Instituto de Computação - IC e a Universidade Federal de Mato Grosso.

Referências

Beck, U. (2011). *Sociedade de Risco: Rumo a uma outra modernidade*. Editora 34 Ltda., Brasil, 2 edition. Tradução: Sebastião Nascimento, 384 p.

Biadeni, B. S. and Fonseca, R. A. (2023). Fazendo pix para o influenciador preferido: relações de credibilidade e literacia midiática em golpes online. In *46º Congresso Brasileiro de Ciências da Comunicação – PUCMinas*.

Brazil, A. and Baruque, L. (2015). Gamificação aplicada na graduação em jogos digitais. In *Brazilian Symposium on Computers in Education (SBIE)*, page 677.

Cruz, P. F. and Rodrigues, L. F. C. (2018). *Crimes cibernéticos: teoria e prática*. Editora Saraiva, São Paulo.

Dias, P. (2023). A evolução cibernética e a falta de punibilidade célere dos crimes digitais: crimes digitais na plataforma whatsapp. Trabalho de Conclusão de Curso, Ciências Sociais Aplicadas: Direito, Orientador: Denise Souza, 23 p.

Dresch, A., Lacerda, D. P., and Jr., J. A. V. A. (2015). *Design Science Research: método de pesquisa para avanço da ciência e tecnologia*. Bookman.

Gjertsen, E. G. B., Gjaere, E. A., Bartnes, M., and Flores, W. R. (2017). Gamification of information security awareness and training. In *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, pages 59–70.

Guilherme, L. P., Ferreira, M. F., Fonseca, G. M., and Lazarin, N. M. (2021). Uma breve noção sobre o comportamento dos internautas em relação à segurança na rede. *SBC OpenLib (SOL)*.

IBGE (2021). Coordenação de pesquisas por amostra de domicílios. pesquisa nacional por amostra de domicílios contínua - vitimização: sensação de segurança 2021. Technical report, Rio de Janeiro. 121 p.

Marinho, A. and Bodê, J. (2022). Gamificação aplicada a programas e campanhas de conscientização de segurança da informação. In *FatecSeg - Congresso De Segurança Da Informação*.

Minayo, M. C. S., Deslandes, S. F., Neto, O. C., and Gomes, R. (2002). *Pesquisa Social - Teoria, Método e Criatividade*. Editora Vozes, Petrópolis, Rio de Janeiro, 21ª edition.

Mostafa, M. and Faragallah, O. S. (2019). Development of serious games for teaching information security courses. *IEEE Access*, 7:169293–169305.

Netto, M. and Rabelo, F. (2023). Estudo golpes com pix: Um mapeamento inédito sobre golpes financeiros via pix no brasil. Technical report.

Santana, M. C. and da S. Amorim, S. (2024). Quiz60+: Um jogo educativo para segurança digital dos usuários idosos. In *Anais do XV Seminário Jogos Eletrônicos, Educação e Comunicação (SJEEC)*, pages 114–123.

Scholefield, S. and Shepherd, L. A. (2019). Gamification techniques for raising cyber security awareness. In *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019*, HCI International Conference, HCII 2019, Orlando, FL, USA, pages 191–203. Springer International Publishing.

Sharif, K. H. and Ameen, S. Y. (2021). A review on gamification for information security training. *Institute of Electrical and Electronics Engineers - IEEE*. Editora: Instituto de Engenheiros Elétricos e Eletrônicos - IEEE.

Silva, R. L. and Vieira, A. (2021). Segurança cibernética: o cenário dos crimes virtuais no brasil. *Revista Científica Multidisciplinar Núcleo do Conhecimento*, 6(4):134–149.

Thornton, D. and III, G. F. (2014). Gamification of information systems and security training: Issues and case studies. *Information Security Education Journal*, 1(1):16–24.