# The Safest Option: Boas Práticas de Segurança da Informação no Ambientes Corporativos

***Title: The Safest Option: Best Practices for Information Security in Corporate Environments***

**Arthur Gustavo Macena Moreira[1], Matheus Pereira Lucena[1], Tadeu Moreira de Classe[1], Eduardo Gomes de Oliveira[1,2], Ronney Moreira de Castro[1,3], Henrique Prado de Sá Sousa[1], Herick Henrique Cardouzo[1]**

[1]Grupo de Pesquisa em Jogos para Contextos Complexos (JOCCOM)
Programa de Pós-Graduação em Informática (PPGI)
Universidade Federal do Estado do Rio de Janeiro (UNIRIO)
Rio de Janeiro – RJ – Brasil

[2]Instituto Federal do Sudeste de Minas Gerais (IF Sudeste MG)
Campus Ubá – Minas Gerais – MG – Brasil

[3]Departamento de Ciência da Computação (DCC)
Universidade Federal de Juiz de Fora (UFJF)
Juiz de Fora – MG – Brasil

{arthur.moreira,mthlucena}@edu.unirio.br, tadeu.classe@uniriotec.br
eduardo.oliveira@edu.unirio.br, ronney.castro@ufjf.br, hsousa@uniriotc.br
herick@edu.unirio.br

***Abstract. Introduction:*** *With increasing digitalization, human errors and social engineering attacks have become critical vulnerabilities for information security in organizations.* ***Objective:*** *This work presents the development and evaluation of an educational game aimed at raising awareness and training employees in cybersecurity best practices.* ***Methodology:*** *The Endogenous Game Design Canvas (Endo-GDC) framework was used for the design, ensuring the integration between game mechanics and instructional content. The game underwent a usability and experience evaluation with 106 participants, using questionnaires based on serious games literature.* ***Results:*** *The data indicated a broadly positive perception, with 91% of users confirming the artifact's effectiveness as a learning tool. In conclusion, the game promotes engagement and critical thinking, establishing itself as a viable pedagogical strategy for the corporate context.*
***Keywords*** *Information Security; Educational Games; Social Engineering; Corporate Awareness; Endo-GDC*

***Resumo. Introdução:*** *Com a digitalização crescente, falhas humanas e ataques de engenharia social tornaram-se vulnerabilidades críticas para a segurança da informação nas organizações.* ***Objetivo:*** *Este trabalho apresenta o desenvolvimento e a avaliação de um jogo educativo voltado à conscientização e ao treinamento de profissionais em boas práticas de cibersegurança.* ***Metodologia:*** *Utilizou-se o framework Endogenous Game Design Canvas (Endo-GDC) para o design, garantindo a integração entre mecânicas lúdicas e conteúdo instrucional. O jogo foi submetido a uma avaliação de usabilidade e experiência com 106 participantes, utilizando questionários fundamentados na literatura de jogos sérios.* ***Resultados:*** *Os dados indicaram uma percepção amplamente positiva, com 91% dos usuários confirmando a eficácia do artefato como ferramenta de aprendizagem. Conclui-se que o jogo promove o engajamento e o pensamento crítico, consolidando-se como uma estratégia pedagógica viável para o contexto corporativo.*

***Palavras-Chave*** *Segurança da Informação; Jogos Educativos; Engenharia Social; Conscientização Corporativa; Endo-GDC*

## 1. Introdução

A tecnologia tem se consolidado como uma ferramenta essencial em diversos setores, sendo parte fundamental das operações cotidianas nas empresas [Whitman et al. 2009]. Com a crescente digitalização dos processos organizacionais, as ameaças cibernéticas também se intensificaram e uma parte considerável delas explora vulnerabilidades humanas nos sistemas de segurança [Al-Badayneh et al. 2025, Pollini et al. 2022]. Pesquisas demonstram que o comportamento de usuários, decisões baseadas em heurísticas cognitivas e respostas inadequadas a ataques de engenharia social são fatores críticos na ocorrência de incidentes de segurança da informação [Khadka e Ullah 2025].

Paralelamente ao aumento das ameaças cibernéticas, a gamificação tem sido cada vez mais estudada como uma estratégia pedagógica para estimular engajamento, motivação e aprendizagem em contextos complexos de formação, incluindo a educação em segurança da informação [Pahlavanpour e Gao 2024, Krath et al. 2021]. Estudos científicos destacam que elementos lúdicos podem melhorar a experiência dos aprendizes e favorecer retenção de conteúdo quando aplicados em treinamentos, principalmente em disciplinas que exigem mudança de comportamento ou aquisição de habilidades práticas [Pahlavanpour e Gao 2024].

Diante deste cenário, este trabalho propõe o desenvolvimento de um jogo educativo focado na conscientização e treinamento em segurança da informação para ambientes corporativos. Por meio de cenários interativos que simulam riscos reais, a proposta visa não apenas fortalecer as habilidades preventivas de profissionais, mas também analisar a eficácia da gamificação para promover aprendizagem significativa, engajamento e mudanças positivas de comportamento.

Este estudo está organizado da seguinte forma: a Seção 2 aborda os conceitos essenciais para a compreensão da pesquisa. A Seção 3 aborda alguns trabalhos relacionados que deram base e inspiração ao artefato dessa pesquisa. Na Seção 4, é apresentada a organização da proposta do *design* do jogo e seu alinhamento educacional ao conteúdo. A avaliação do jogo educacional e seus resultados observados constam na Seção 5. Por fim, as conclusões do estudo e as perspectivas para pesquisas futuras são apresentadas na Seção 6.

## 2. Conceitos Fundamentais

### 2.1. Segurança da Informação

A segurança da informação é um campo da tecnologia da informação (TI) dedicado à aplicação de processos e ferramentas para prevenir, detectar e mitigar ataques a informações sensíveis, abrangendo não apenas a proteção de sistemas computacionais, mas qualquer meio em que a informação esteja armazenada, seja digital ou física [Whitman et al. 2009]. Seu objetivo é garantir que a informação mantenha três características fundamentais, conhecidas como a tríade CIA (*Confidentiality, Integrity, Availability*). A ***Confidentiality*** **- Confidencialidade** diz respeito à proteção das informações, assegurando que apenas usuários ou sistemas autorizados tenham acesso aos dados, prevenindo acessos indevidos e vazamentos, especialmente quando se trata de informações sensíveis, como dados pessoais, financeiros ou corporativos [Stallings e Brown 2017]. Já a ***Integrity*** **- Integridade** refere-se à garantia de que as informações mantêm sua exatidão, completude e confiabilidade ao longo do tempo durante seu ciclo de vida. Isso significa que os dados não foram alterados, corrompidos ou manipulados de forma não autorizada, seja de forma acidental ou intencional [Stallings e Brown 2017]. Por fim, a ***Availability*** **- Disponibilidade** diz respeito à garantia de acesso contínuo às informações por usuários e sistemas autorizados, sempre que necessário. Esse princípio está diretamente associado à continuidade dos negócios e à capacidade da organização de lidar com falhas, ataques ou desastres [Stallings e Brown 2017].

### 2.2. Jogos Educacionais e Jogos de Treinamento

Os jogos educacionais são jogos voltados para os processos de ensino e aprendizagem, tendo como foco promover a aprendizagem ativa, a motivação e a retenção de conteúdos, indo além da simples diversão [Krath et al. 2021]. Estudos comparativos têm evidenciado ganhos significativos de desempenho entre alunos que utilizam jogos educacionais em suas atividades, em relação àqueles que não fazem uso desse tipo de recurso [Pahlavanpour e Gao 2024]. Dessa forma, compreende-se que os jogos educacionais são uma ferramenta poderosa para o reforço e retenção da aprendizagem, ao mesmo tempo que aumentam a motivação e o engajamento [Krath et al. 2021].

Um dos principais objetivos dos treinamentos na indústria é fornecer aos trabalhadores o conhecimento necessário para identificar e avaliar riscos no ambiente de trabalho, bem como desenvolver habilidades para a adoção de boas práticas [Venturi et al. 2021]. Com o avanço da tecnologia, novas abordagens têm emergido, destacando-se o uso de jogos digitais como uma estratégia inovadora de treinamento (Jogos de Treinamento) [Vigoroso et al. 2021]. Tais jogos proporcionam experiências imersivas e interativas, possibilitando a simulação de situações e a prática de habilidades específicas, uma abordagem eficaz no engajamento dos participantes e na promoção da aprendizagem e retenção de conhecimentos [Lu et al. 2022].

Os Jogos de Treinamento têm sido amplamente adotados na indústria e em organizações como estratégia para capacitação de profissionais, especialmente em contextos que demandam tomada de decisão, resolução de problemas e desenvolvimento de habilidades práticas [Pahlavanpour e Gao 2024, Pollini et al. 2022]. Além disso, pesquisas indicam que estes jogos favorecem o desenvolvimento de competências comportamentais e técnicas de forma mais efetiva quando comparados a métodos tradicionais, especialmente por promoverem aprendizagem experiencial e tomada de decisão em contextos realistas [Subhash e Cudney 2018, Pahlavanpour e Gao 2024].

## 3. Trabalhos Relacionados

A utilização de jogos sérios para treinamento e conscientização em Segurança da Informação tem sido explorada na literatura, especialmente como uma estratégia para mitigar vulnerabilidades associadas ao fator humano.

Gupta et al. [2020] apresentaram um jogo voltado a público especializado, como profissionais da área de segurança. O jogo simula atividades práticas do cotidiano desses profissionais, como a identificação de ataques de *phishing* em e-mails e a análise de eventos em sistemas de monitoramento, aproximando-se de ambientes reais de operação. Hodhod et al. [2023] propuseram um jogo sério baseado em narrativa interativa com a finalidade de promover a conscientização em cibersegurança, onde o jogador progride no jogo, a partir da tomada de decisões que impactam o desenrolar da história, possibilitando diferentes trajetórias narrativas.

Como inspiração para o *design* do jogo proposto neste artigo, destaca-se o *Papers, Please*[1] , no qual o jogador assume o papel de um agente de imigração responsável por analisar documentos e tomar decisões que impactam diretamente a segurança do país. Caso contrário, podem acontecer ataques à segurança e à soberania deste país ficcional. Sendo também utilizado como base o trabalho de Pflanzl et al. [2016], o qual apresenta a ideia de jogos para conscientização e aprendizagem em processos corporativos e governamentais.

Os trabalhos concentram-se na identificação de ameaças explícitas, incentivando uma atitude mais defensiva por parte do jogador. Entretanto, no ambiente corporativo real, nem todas as situações representam riscos, sendo fundamental que o profissional desenvolva a capacidade de distinguir entre cenários legítimos e potencialmente maliciosos. Nesse contexto, este trabalho

[1] https://papersplea.se/

apresenta um jogo sério baseado em cenários do cotidiano, estruturado em tomadas de decisão e incorporando situações de risco com o objetivo de fomentar o desenvolvimento do pensamento crítico.

## 4. The Safest Option: Um Jogo Sério para Segurança da Informação

O artefato *The Safest Option*[2] foi concebido como uma ferramenta voltada à aprendizagem e conscientização em segurança da informação no ambiente corporativo, com ênfase no desenvolvimento do pensamento crítico frente a situações do cotidiano organizacional. Inspirado em abordagens de *Game-Based Learning* (GBL), o jogo busca promover a aprendizagem por meio da simulação de cenários realistas, nos quais o jogador deve tomar decisões baseadas em boas práticas de segurança.

Diferente de abordagens tradicionais que são baseadas em treinamento expositivo, *The Safest Option* traz uma experiência interativa com foco na tomada de decisão. O jogador é constantemente desafiado a avaliar situações e escolher a alternativa mais adequada. Cada decisão resulta em um *feedback* imediato com explicações, permitindo compreender não apenas se a escolha foi correta, mas também os motivos que justificam cada alternativa. Essa dinâmica favorece a aprendizagem ao conectar o conteúdo teórico a contextos práticos e próximos da realidade profissional.

O jogo foi projetado para um público amplo, incluindo estudantes e profissionais que utilizam recursos tecnológicos em suas atividades diárias, não exigindo conhecimento técnico prévio em segurança da informação. Sua estrutura é baseada em cenários independentes, que simulam situações comuns no ambiente corporativo, como tentativas de *phishing*, uso inadequado de dispositivos, compartilhamento de credenciais e acesso a redes não seguras. Esses cenários representam situações de segurança da informação, onde cada situação exige análise e julgamento por parte do jogador.

### 4.1. Projeto do Jogo

Como se trata de um jogo educacional voltado ao ensino de **Segurança da Informação e Cibersegurança**, foi necessário adotar uma abordagem estruturada para o seu planejamento. Como decisão de projeto, optou-se por realizar o *brainstorming* e a definição dos elementos do jogo por meio do *Endogenous Game Design Canvas (Endo-GDC)*, concebido especificamente para esse propósito [Taucei 2019].O Endo-GDC organiza em seções as informações necessárias para o desenvolvimento do jogo educacional, para que sejam representados: i) conteúdo educacional: problema que o jogo irá abordar; o conteúdo pedagógico; objetivos de aprendizado; *feedbacks* educativos e ii) elementos de *design* de jogo: o perfil do jogador; jogos inspiradores; história, estética, dinâmicas, mecânicas e o objetivo do jogo. Na Figura 1 é apresentada a representação do Endo-GDC para o jogo.

A ideia do jogo partiu do **problema** de fazer com que os estudantes e profissionais (**jogadores**) identifiquem os perigos e reconheçam boas práticas de segurança da informação em ambientes corporativos. A faixa etária dos jogadores teve como partida os 5 anos de idade, desde que saibam ler, uma vez que é necessário ler informações durante o jogo. Os **conteúdos pedagógicos** giram em torno da segurança da informação, como ataques de engenharia social, os diversos tipos de *malware*, ataques à cibersegurança, cuidados, compartilhamentos e boas práticas de segurança digital em ambientes corporativos. Os **objetivos educacionais** foram definidos a partir da Taxonomia de Bloom, focando em **aprender**, **reconhecer**, **identificar**, **refletir** sobre as diversas situações de vulnerabilidade digital e **entender** a importância individual de cada profissional na segurança da empresa. Por fim, são estipulados os ***feedbacks* educacionais** a partir dos objetivos, sendo considerados para esse jogo explicações sobre todas as alternativas apresentadas e o progresso do jogador seguindo sua sequência de acertos e erros.

[2] https://joccom.uniriotec.br/games/safest/

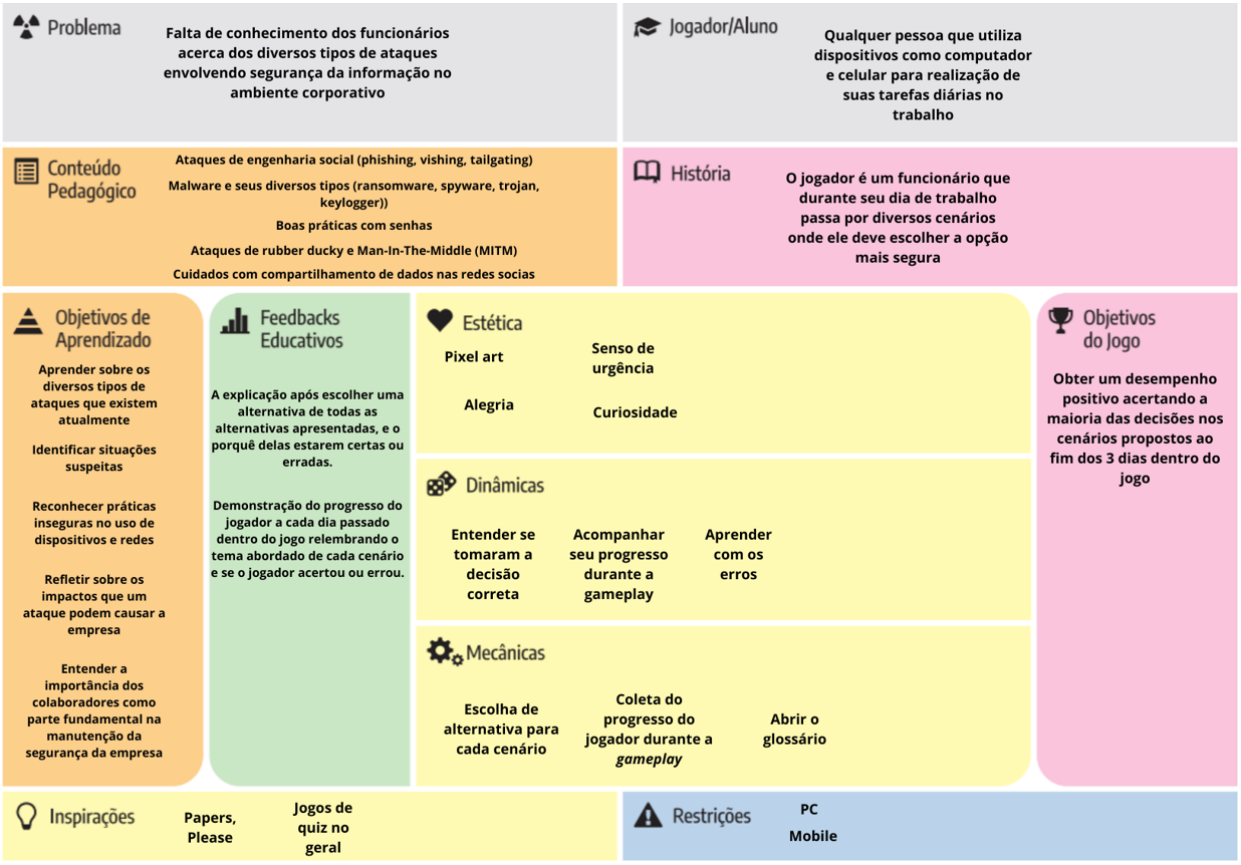


**Figura 1. Projeto do jogo organizado no Endo-GDC.**

Definidos os quadros de conteúdos educacionais, são pensados os elementos de *design* de jogo em termos de narrativa, mecânica, estética e dinâmica. Como o jogo foi inspirado em *"Papers, Please"*, ficou definido que o jogo implementaria três situações de segurança da informação por rodada (dia). A narrativa do jogo coloca o jogador no papel de um funcionário da empresa durante seus primeiros dias de trabalho, sendo submetido a diferentes situações de tomada de decisão que envolvam riscos de segurança para sua empresa (Figura 2A). Desta maneira, o objetivo do jogo, se alinha a fazer com que o jogador busque um desempenho positivo na corporação, por meio de suas decisões e ações, ao final de três dias de trabalho (estágio probatório).

Como mecânicas básicas, o jogo segue o ritmo de progresso diário, no qual, cada dia de trabalho, acontecem 3 situações de segurança da informação em que o jogador precisa tomar decisões (formato de *quiz* - Figura 2C). Cada situação apresentada é um cenário de segurança real de uma organização (Figura 2B) Cada rodada representa um dia de trabalho em uma corporação (Figura 2A). Para cada situação, também é dado o *feedback* de acerto ou erro, explicando ao jogador o possível desdobramento de suas escolhas para a corporação, estando elas certas ou não. Além das opções de ações, ao jogador também é apresentado um glossário (Figura 2D), uma espécie de guia com explicações de todas as falhas de segurança da informação que possam acontecer no ambiente corporativo e de como evitá-las. Ao fim de 1 dia (rodada), o jogador pode observar o resultado de suas ações na organização. Assim, as dinâmicas básicas de jogos levam ao jogador sensações que permeiam suas escolhas e, através delas, aprender com seus próprios erros durante o *gameplay*.

Como tecnologia, o jogo foi implementado usando a *engine GDevelop*[3], permitindo uma rápida prototipação e implementação. E, além disso, possibilitou que o jogo fosse

[3]https://gdevelop.io/


**Figura 2. *Drafts* do jogo.**

multiplataforma, uma vez que, com ela é possível fazer com que o jogo seja executado em computadores, navegadores e em aparelhos móveis, o que permite uma alta abrangência de jogadores de diferentes plataformas.

## 5. Avaliação da Atividade

### 5.1. Definição e Planejamento da Pesquisa de Opinião

Como forma de avaliação, optou-se pela aplicação de uma pesquisa de opinião, por ser um método eficaz para coletar de maneira sistemática e ágil a percepção dos participantes [Creswell e Creswell 2017]. O planejamento da pesquisa considerou as seguintes etapas: i) definição; ii) elaboração dos instrumentos; iii) seleção dos participantes; iv) execução; e v) identificação de possíveis ameaças à validade.

O escopo da avaliação foi **definido** com base na abordagem GQM (*Goal-Question-Metric*) [Basili 1992], permitindo estruturar o processo de análise de forma sistemática. Desta forma, a definição do estudo pode ser descrita como: **Analisar**: o jogo sério *The Safest Option*; **com o propósito de**: avaliação; **em relação à**: percepção de (A) experiência de *gameplay* e (B) aprendizagem do jogador; **do ponto de vista de**: jogadores (estudantes e profissionais de empresas); **no contexto** de: treinamento em segurança da informação e cibersegurança.

O **instrumento** de coleta de dados utilizado foi uma adaptação do questionário MEEGA+ [Petri et al. 2019], amplamente empregado na avaliação de jogos educacionais. Esse questionário contempla aspectos relacionados tanto à experiência de uso quanto à percepção de aprendizado. Ele é composto por uma série de afirmações que os participantes avaliam utilizando uma escala *Likert* de cinco pontos, variando de -2 (discordo totalmente) a 2 (concordo totalmente).

Os **participantes** do estudo foram alunos de graduação e pós-graduação de cursos da área de Tecnologia da Informação (TI), que atuaram como representantes do perfil de usuários finais. Eles seriam convidados a participar por e-mail e mídias sociais, caracterizando uma amostra aleatório por conveniência. Este grupo constitui o público-alvo ideal para a avaliação do *The Safest Option*, uma vez que o jogo sério foi projetado especificamente para simular desafios de Segurança da Informação no cotidiano corporativo, ambiente onde esses futuros profissionais

atuarão. Ressalta-se que a participação no estudo foi voluntária e opcional. Foram assegurados aos participantes o anonimato e a liberdade de interrupção a qualquer momento, garantindo que a atividade não tivesse qualquer impacto em seu desempenho profissional ou acadêmico, conforme os preceitos éticos de pesquisa.

Além disso, salienta-se que, por se tratar de uma pesquisa de opinião, mesmo com a participação sendo voluntária, foi apresentado aos alunos um Termo de Consentimento Livre e Esclarecido (TCLE) antes do início do estudo. Esse documento continha informações sobre os objetivos da pesquisa, possíveis riscos e as etapas de sua execução. Além disso, como o estudo se restringe à coleta de opiniões anônimas dos participantes, não foi necessária a submissão ao Comitê de Ética em Pesquisa, conforme estabelece a Resolução CNS nº 510/2016[4], que dispensa esse tipo de pesquisa desse trâmite.

Optou-se por realizar a pesquisa de opinião em três **etapas de execução**: 1) apresentação do questionário e coleta de perfil do participante (5 minutos), considerando apresentação do estudo e TCLE; 2) execução, consistindo na interação direta com o jogo *The Safest Option* durante no mínimo 10 minutos (ou o tempo que o jogador se sentisse engajado); e 3) questionário de percepção de experiência e aprendizado (5 minutos), totalizando 20 minutos de execução.

Para garantir o rigor científico, as **ameaças à validade** foram mitigadas em quatro frentes: **interna**, limitando o tempo da atividade e exigindo respostas individuais para evitar fadiga e imitação; **construção**, utilizando o modelo de avaliação validado, MEEGA+ [Petri et al. 2019]; **externa**, seguindo o *design* metodológico de Creswell e Creswell [2017]; e **conclusão**, aplicando métodos estatísticos adequados à escala *Likert*. Os resultados limitam-se ao contexto de Segurança da Informação com estudantes de TI, sugerindo a expansão para outros cenários organizacionais em trabalhos futuros.

### 5.2. Execução e Resultados

O estudo foi conduzido entre os dias 06 e 16 de junho de 2025. Durante este período, o convite para participação voluntária resultou na adesão de **106 respondentes**. Após a interação com *The Safest Option*, os usuários preencheram um questionário eletrônico via *Google Forms*, cujos dados foram compilados em uma base estruturada[5]. A análise foi realizada de forma quantitativa, utilizando métodos estatísticos para o tratamento das informações, e os resultados foram sumarizados em tabelas e gráficos, para facilitar a representação e a compreensão dos achados sobre a experiência e o aprendizado.

#### 5.2.1. Perfil dos Participantes

A caracterização dos 106 participantes que avaliaram o *The Safest Option* está detalhada na Tabela 1. A amostra possui um perfil predominantemente jovem, com 51% dos respondentes na faixa etária de 18 a 28 anos. Destaca-se uma maior participação de estudantes de graduação, que representam 42% da amostra. Além disso, a expressiva presença de jogadores habituais (75%) garante que as percepções sobre usabilidade e interface foram avaliadas por usuários com experiência prática em entretenimento digital. Essa diversidade controlada na amostra contribuiu para uma validação robusta da ferramenta em relação às diversas dimensões do modelo MEEGA+.

[4] https://www.gov.br/conselho-nacional-de-saude/pt-br/atos-normativos/resolucoes/2016/resolucao-no-510.pdf/view

[5] Em conformidade com a ciência aberta, os dados podem ser observados em: https://figshare.com/s/107b1bf82efafa85f5d1

**Tabela 1. Perfil Sociodemográfico e de Experiência dos Participantes ($n = 106$)**

| Categoria | Subcategoria / Faixa | Porcentagem (%) |
|---|---|---|
| Gênero | Masculino | 68% |
| | Feminino | 29% |
| | Outros / Não informado | 3% |
| Faixa Etária | Menos de 18 anos | 23% |
| | 18 a 28 anos | 51% |
| | 29 a 39 anos | 7% |
| | 40 a 50 anos | 8% |
| | Mais de 50 anos | 11% |
| Escolaridade | Médio Completo | 7% |
| | Médio Incompleto | 22% |
| | Superior Incompleto | 42% |
| | Superior Completo | 17% |
| | Mestrado | 9% |
| | Doutorado | 3% |
| Familiaridade com Jogos | Nunca: nunca jogo | 8% |
| | Raramente: jogo de tempos em tempos | 18% |
| | Mensalmente: jogo pelo menos uma vez por mês | 9% |
| | Semanalmente: jogo pelo menos uma vez por semana | 31% |
| | Diariamente: jogo todos os dias | 34% |

### 5.2.2. Análise de Percepção de Experiência e Aprendizado

No que tange à **percepção de experiência** em relação ao *The Safest Option*, a Figura 3 apresenta os resultados obtidos através do modelo MEEGA+. Observa-se que a vasta maioria das afirmações obteve respostas situadas entre "concordo parcialmente" e "concordo totalmente" na dimensão de **Usabilidade**. Uma exceção pontual ocorreu no item referente à personalização da aparência (fonte e cor) pelo usuário, que apresentou índices de neutralidade ou não aplicabilidade. No entanto, compreende-se que tal funcionalidade não era o foco do artefato, uma vez que o jogo foi desenvolvido com uma interface pré-definida em *Unity* para garantir a imersão na narrativa corporativa proposta. Ao analisar o conjunto das afirmações, os dados evidenciam que os participantes tiveram uma percepção de experiência amplamente positiva durante o uso do *The Safest Option*.

Quanto à **Confiança**, a percepção inicial de facilidade de uso do *The Safest Option* foi compartilhada pela grande maioria dos participantes (86%). A integração entre interface, mecânicas e estética contribuiu para que 91% dos respondentes acreditassem que o jogo resultaria em um processo de aprendizagem eficaz. Tais dados corroboram o objetivo central deste jogo sério, que busca alinhar o engajamento lúdico à efetividade educacional, fortalecendo a percepção do usuário sobre o potencial pedagógico da ferramenta.

A análise da dimensão de **Desafio** a Figura 3 revela uma heterogeneidade na percepção de desafio, atribuída à diversidade de perfis da amostra. Participantes familiarizados com Segurança da Informação reportaram menor dificuldade, enquanto usuários leigos consideraram o nível de desafio adequado. Embora 56% dos respondentes tenham identificado novos desafios nos cenários propostos, houve uma divisão quanto à monotonia do jogo. Esse resultado é consistente com a proposta de acessibilidade e universalização do conteúdo, em que o equilíbrio entre o lúdico e o educativo prioriza a clareza da instrução em detrimento da complexidade mecânica, não impactando negativamente os objetivos do projeto.

Já na dimensão de **Satisfação**, os dados apresentados na Figura 3 indicam elevados índices de satisfação e realização pessoal. Constatou-se que 74% dos participantes sentiram-se realizados ao concluir as tarefas propostas, enquanto 71% atribuíram o progresso no jogo ao seu próprio esforço, evidenciando o fortalecimento da autoconfiança do utilizador. Adicionalmente, a percepção de valor pedagógico foi expressiva: 83% demonstraram satisfação com o conteúdo aprendido e 78% afirmaram que recomendariam o *software* a terceiros. Estes resultados corroboram a eficácia do *The Safest Option* como ferramenta de disseminação de conhecimento, demonstrando que a experiência lúdica promoveu um engajamento positivo e uma recepção

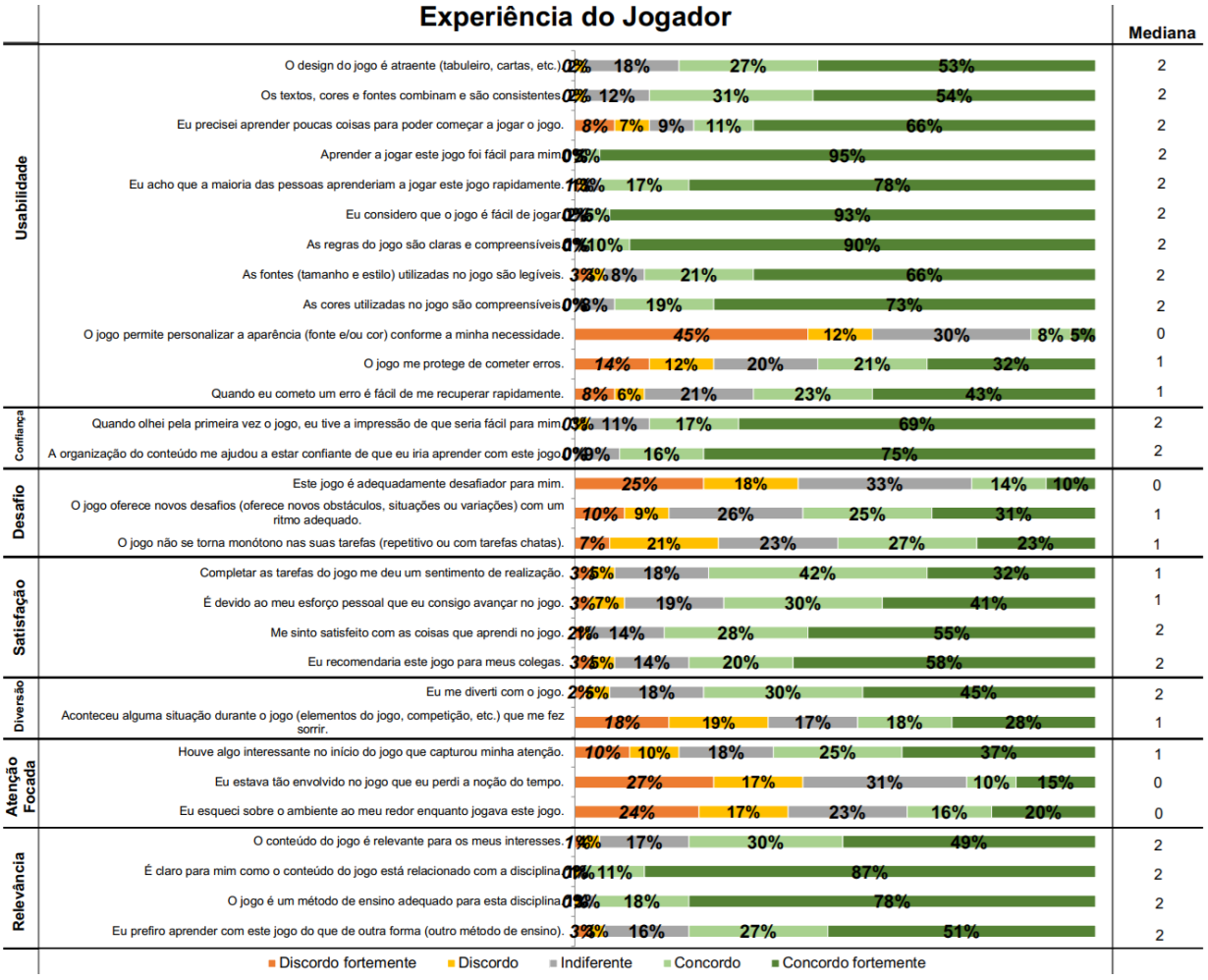


**Figura 3. Avaliação de Experiência dos Jogadores.**

favorável junto ao público-alvo.

No que concerne à dimensão de **Diversão**, a Figura 3 demonstra que 75% dos participantes se divertiram ao jogar o jogo e que uma boa parte (44%) sorriu durante a *gameplay*. Esses resultados indicam que o jogo, apesar de seu caráter educativo, preserva um elemento essencial dos jogos: a diversão.

A Figura 3 ainda indica que a dimensão de **Atenção Focada** apresentou o desempenho mais modesto entre as métricas avaliadas. Embora o jogo tenha capturado a atenção inicial de 62% dos participantes, observou-se uma divergência significativa quanto à imersão profunda (perda da noção de tempo e do ambiente externo). Apesar do desafio inerente aos jogos sérios em manter o engajamento contínuo, os dados sugerem que *The Safest Option* obteve êxito em sustentar o interesse de uma parcela considerável do público, cumprindo o objetivo de evitar o desinteresse comum em ferramentas puramente instrucionais.

Os resultados da dimensão de **Relevância** atestam o sucesso do *The Safest Option* em alinhar o conteúdo à temática de Segurança da Informação. Observou-se que 79% dos participantes demonstraram alto interesse pelo tema, enquanto 98% ratificaram a adequação do jogo como método de ensino para a disciplina. Adicionalmente, a preferência de 78% dos usuários por essa abordagem em detrimento de métodos tradicionais reforça a eficácia dos jogos sérios como ferramentas de engajamento e transmissão do conhecimento.

Por fim, quanto à **percepção de aprendizagem** (Figura 4), 84% dos participantes ratificaram a contribuição do *The Safest Option* para o conhecimento em segurança da informação,

com 75% considerando-o mais eficiente que métodos tradicionais. A eficácia pedagógica foi evidenciada pelo entendimento da distinção entre ações seguras e inseguras (92%) e pelo valor atribuído aos *feedbacks* detalhados (90%) e ao glossário de conceitos (67%). Além disso, o formato de tomada de decisão demonstrou o impacto de pequenas ações na segurança corporativa para 92% dos usuários, resultando em um incentivo à maior vigilância cotidiana para 84% deles. O jogo também promoveu o pensamento crítico e a desconstrução de percepções equivocadas sobre riscos organizacionais para a maioria dos respondentes, enquanto a estrutura narrativa dividida em dias facilitou o acompanhamento do progresso e a reflexão sobre o conteúdo aprendido.

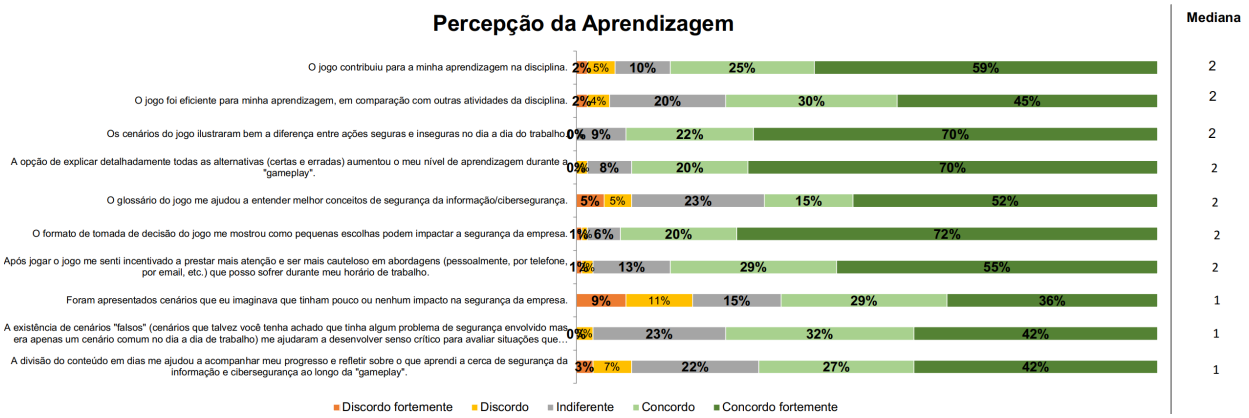


**Figura 4. Percepção de Aprendizado dos Jogadores.**

## 6. Considerações Finais

Este estudo apresentou o desenvolvimento e a avaliação do *The Safest Option*, um jogo sério digital concebido para mitigar a lacuna de conscientização em Segurança da Informação no cenário de transformação digital e trabalho remoto. Diferente de soluções correlatas, o artefato buscou oferecer uma abordagem completa e direta, alinhada aos padrões contemporâneos de consumo de informação.

A avaliação, realizada com 106 participantes de perfis heterogêneos, validou a eficácia da ferramenta. Os resultados de maior destaque referem-se à experiência do jogador, com 83% de concordância total em usabilidade, confiança e relevância. No âmbito pedagógico, a percepção de aprendizagem foi plenamente positiva, com 100% das respostas situadas entre os níveis de concordância positiva. Tais indicadores confirmam que o objetivo de desenvolver um treinamento lúdico e eficaz para o ambiente corporativo foi alcançado. Como evidência de sua maturidade e originalidade, o *software* foi registrado junto ao INPI (Processo: BR512025003028-2).

Como trabalhos futuros, pretende-se implementar melhorias de *game design* e conteúdo identificadas durante a avaliação, tais como: (i) expansão do glossário técnico e dos cenários de ataque; (ii) implementação de elementos de áudio para *feedback* imediato; (iii) randomização de alternativas para evitar a memorização; e (iv) introdução de novas mecânicas de suporte ao jogador, como sistemas de dicas com uso limitado por ciclo de jogo. Almeja-se, ainda, aumentar a extensão da narrativa para seis dias de simulação, ampliando a profundidade dos conceitos abordados.

## Agradecimentos

Os autores agradecem a Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro – FAPERJ (proc. E-26/204.478/2024 – SEI-260003/013219/2024) por financiar parcialmente esta pesquisa.

## Referências


Al-Badayneh, D. M., Al-Badayneh, D. D., e Hashish, R. K. (2025). Human factors of cybersecurity. *Journal of Posthumanism*, 5(4):1302–1314.

Basili, V. R. (1992). Software modeling and measurement: the goal/question/metric paradigm. *University of Maryland Technical Report*.

Creswell, J. W. e Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Gupta, S., Gupta, M., Chaturvedi, M., Vilkhu, M., Kulshrestha, S., Gaurav, D., e Mittal, A. (2020). Guess who?-a serious game for cybersecurity professionals. In *International Conference on Games and Learning Alliance*, pages 421–427. Springer.

Hodhod, R., Hardage, H., Abbas, S., e Aldakheel, E. A. (2023). Cyberhero: an adaptive serious game to promote cybersecurity awareness. *Electronics*, 12(17):3544.

Khadka, K. e Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal: K. khadka, ab ullah. *International Journal of Information Security*, 24(3):119.

Krath, J., Schürmann, L., e Von Korflesch, H. F. (2021). Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. *Computers in human behavior*, 125:106963.

Lu, S., Wang, F., Li, X., e Shen, Q. (2022). Development and validation of a confined space rescue training prototype based on an immersive virtual reality serious game. *Advanced Engineering Informatics*, 51:101520.

Pahlavanpour, O. e Gao, S. (2024). A systematic mapping study on gamification within information security awareness programs. *Heliyon*, 10(19).

Petri, G., Von Wangenheim, C. G., e Borgatto, A. F. (2019). Meega+: Um modelo para a avaliação de jogos educacionais para o ensino de computação. *Revista Brasileira de Informática na Educação*, 27(03):52–81.

Pflanzl, N., Classe, T., Araujo, R., e Vossen, G. (2016). Designing serious games for citizen engagement in public service processes. In *International Conference on Business Process Management*, pages 180–191. Springer.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., e Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, 24(2):371–390.

Stallings, W. e Brown, L. (2017). Computer security: principles and practice, global edition.

Subhash, S. e Cudney, E. A. (2018). Gamified learning in higher education: A systematic review of the literature. *Computers in human behavior*, 87:192–206.

Taucei, B. B. (2019). Endo-gdc: Desenvolvimento de um game design canvas para concepção de jogos educativos endógenos. Master's thesis, Programa de Engenharia de Sistemas e Computação (COPPE). Universidade Federal do Rio de Janeiro (UFRJ).

Venturi, D., Konell, A. E., e Giovanela, A. (2021). Treinamento: importância e benefícios da disponibilização de treinamento nas organizações. *Revista Científica FAMAP*, 1(01).

Vigoroso, L., Caffaro, F., Micheletti Cremasco, M., e Cavallo, E. (2021). Innovating occupational safety training: a scoping review on digital games and possible applications in agriculture. *International Journal of Environmental Research and Public Health*, 18(4):1868.

Whitman, M. E., Mattord, H. J., et al. (2009). *Principles of information security*. Thomson Course Technology Boston, MA.