FACULDADE IMPACTA TECNOLOGIA

ABNER ISRAEL SANCHES DE OLIVEIRA
ENRICO MARÇOLA FEITOZA
ENZO TAVARES LULA SILVA
JOSÉ ISAAC DA CUNHA ASENJO
SAMUEL FELIX DA SILVA

GAMIFICAÇÃO EM *SECURITY AWARENESS*: ENGAJAMENTO E APRENDIZAGEM EM AMBIENTES CORPORATIVOS

São Paulo
2026

ABNER ISRAEL SANCHES DE OLIVEIRA
ENRICO MARÇOLA FEITOZA
ENZO TAVARES LULA SILVA
JOSÉ ISAAC DA CUNHA ASENJO
SAMUEL FELIX DA SILVA

GAMIFICAÇÃO EM *SECURITY AWARENESS*: ENGAJAMENTO E APRENDIZAGEM EM AMBIENTES CORPORATIVOS

Trabalho de Conclusão de Curso apresentado à Faculdade Impacta Tecnologia como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Gilberto Perez

São Paulo
2026

RESUMO

Programas de conscientização em segurança da informação costumam enfrentar baixo engajamento, sobretudo entre profissionais de áreas não técnicas. Este trabalho, conduzido segundo o *Design Science Research*, desenvolveu um aplicativo gamificado de conscientização em segurança da informação voltado a esse público e tem como objetivo avaliá-lo quanto ao engajamento, em comparação com os treinamentos tradicionais já vivenciados pelos participantes, e quanto à percepção de aprendizado, à variação do conhecimento sobre práticas seguras e à percepção dos elementos de gamificação. O aplicativo, um *Progressive Web App* com 15 aulas, modo trivia, pontos, conquistas, ranking e explicação após cada resposta, registra os eventos de uso e aplica um questionário inicial, com a UES-SF sobre o treinamento mais recente, sete situações de conhecimento inspiradas no HAIS-Q e a escala Hexad, e um final, que repete a UES-SF, agora sobre o aplicativo, e as situações. Os dados coletados reúnem 26 questionários iniciais válidos, de participantes majoritariamente jovens e familiarizados com jogos; pouco mais da metade já havia feito treinamento em segurança, e a nota inicial nas situações de conhecimento foi alta, com mediana de 6 em 7, o que pode limitar sua variação.

Palavras-chave: gamificação; segurança da informação; conscientização de cibersegurança; engajamento; treinamento corporativo.

ABSTRACT

Information security awareness programs often struggle with low engagement, especially among non-technical professionals. Following Design Science Research, this study developed a gamified information security awareness application for this audience and aims to evaluate it in terms of engagement, compared with the traditional training participants had previously taken, as well as perceived learning, the change in knowledge of safe practices and perceptions of the gamification elements. The application, a Progressive Web App with 15 lessons, a trivia mode, points, achievements, a leaderboard and an explanation after each answer, logs usage events and administers an initial questionnaire, with the UES-SF applied to the most recent training, seven knowledge scenarios inspired by the HAIS-Q and the Hexad scale, and a final one, which repeats the UES-SF, now applied to the application, and the scenarios. The data collected comprise 26 valid initial questionnaires from mostly young participants familiar with games; slightly over half had already taken security training, and the initial knowledge score was high, with a median of 6 out of 7, which may leave little room for change.

Keywords: gamification; information security; security awareness; engagement; corporate training.

SUMÁRIO

1 INTRODUÇÃO 5
1.1 Proposta do Projeto 6
1.2 Objetivos da Pesquisa 6
1.2.1 Geral: 6
1.2.2 Específicos: 6
1.3 Justificativa para a Pesquisa 6
1.4 Contribuições da Pesquisa/Projeto 7
1.5 Esquema Geral da Pesquisa/Projeto 7
1.6 Declaração de uso de IA 7
2 REFERENCIAL TEÓRICO 8
2.1 Gamificação 8
2.1.1 Gamificação: Conceitos e Fundamentos 8
2.1.2 Gamificação em Contextos Corporativos de Aprendizagem 9
2.2 Segurança da Informação 11
2.2.1 Segurança da Informação: Conceitos e Fundamentos 11
2.2.2 Conscientização em Segurança da Informação (Security Awareness) 11
2.3 Gamificação Aplicada ao *Security Awareness* 13
2.4 Engajamento e Percepção de Aprendizado como Dimensões de Avaliação 13
3 PROCEDIMENTOS METODOLÓGICOS 14
3.1 Proposta de Desenvolvimento de Artefato 15
3.2 Análise Prévia Sobre o que foi Proposto 16
3.3 Como a solução foi implementada 16
3.4 Resultados Esperados 16
3.5 Fatores Críticos para o Sucesso (FCS) do Desenvolvimento da Proposta 17
4 APRESENTAÇÃO DOS RESULTADOS 17
4.1 Como a solução foi implementada (Etapas / Prioridades) 17
4.1.1 Arquitetura da solução 17
4.1.2 Funcionamento do aplicativo 18
4.1.3 Elementos de gamificação 23
4.1.4 Coleta de dados 24
4.2 Resultados Obtidos 25
4.2.1 Avaliação formativa 25
4.2.2 Avaliação com os participantes 25
4.3 Análise dos Resultados 26

4.4 Fatores Críticos para o Sucesso (FCS) identificados no Desenvolvimento da Solução proposta e como foram tratados 26
5 CONSIDERAÇÕES FINAIS 26
REFERÊNCIAS 28
APÊNDICE A – MATRIZ DE VALIDAÇÃO 31
APÊNDICE B – ANÁLISES DESCRITIVAS DA AMOSTRA 33

1 INTRODUÇÃO

Boa parte das falhas de segurança da informação começa no comportamento das pessoas. Senhas fracas, cliques em mensagens maliciosas e desconhecimento das políticas internas contornam controles técnicos que, sozinhos, nada podem fazer a respeito. A edição de 2026 do Data Breach Investigations Report, que analisou mais de 22 mil violações confirmadas em 145 países, identificou a participação do elemento humano em 62% dos casos (Verizon, 2026).

Um episódio ocorrido no Brasil ilustra bem o problema. Em 28 de outubro de 2020, um cientista de dados do Hospital Israelita Albert Einstein que atuava junto ao Ministério da Saúde publicou, em seu perfil pessoal no GitHub, uma planilha com usuários e senhas de acesso a sistemas do ministério, para a realização de um teste, e esqueceu de remover o arquivo da página pública (Baguete, 2020). O arquivo ficou disponível publicamente por cerca de um mês e expôs dados pessoais e clínicos de aproximadamente 16 milhões de brasileiros com diagnóstico suspeito ou confirmado de Covid-19 (Canaltech, 2020). Nenhum sistema foi invadido e nenhuma vulnerabilidade técnica foi explorada.

A conscientização em segurança da informação, conhecida pelo termo em inglês *security awareness*, é uma das respostas das organizações a esse tipo de risco. Trata-se do conjunto de ações voltadas a fazer com que os colaboradores reconheçam as ameaças a que estão expostos e saibam como agir com mais segurança no dia a dia.

A segurança da informação também vem deixando de ser vista como um assunto exclusivo da área de tecnologia. No Febraban Sec 2026, um representante do Departamento de Regulação do Sistema Financeiro do Banco Central afirmou que o órgão publicou resoluções para que a segurança cibernética deixe de ser discutida apenas pela tecnologia e passe a ser tratada no nível institucional, ou seja, pela organização como um todo (Let's Money, 2026).

Reconhecer a importância desses programas, porém, não garante que eles funcionem. Na prática, eles esbarram em três dificuldades recorrentes: baixo engajamento dos participantes, retenção limitada do conteúdo e pouca mudança efetiva de comportamento. Para Bada, Sasse e Nurse (2015), muitas campanhas falham por partir da ideia de que informar já basta para mudar conduta, deixando de lado os fatores culturais e motivacionais envolvidos. Alshaikh (2020) defende que os programas ultrapassem do cumprimento mínimo de exigências formais e passem a construir uma cultura de segurança que influencie o comportamento dos colaboradores.

Essas dificuldades podem ser maiores entre profissionais de áreas não técnicas. Com base na teoria da expectativa-valor, Gwenhure e Rahayu (2024) argumentam que esse público pode começar com menor expectativa de sucesso e ter motivações e expectativas próprias, e observam que, de um conjunto inicial de 91 artigos, apenas cinco eram empíricos e voltados especificamente a profissionais de fora da TI. Para mudar a conduta, as orientações precisam ser compreendidas e aplicadas por quem as recebe (Bada; Sasse; Nurse, 2015).

Na busca por alternativas, a gamificação tem recebido atenção crescente. O termo designa o uso de elementos de design de jogos em contextos que não são jogos (Deterding et al., 2011). A revisão de Hamari, Koivisto e Sarsa (2014) aponta efeitos positivos sobre motivação e engajamento, mas ressalva que os resultados variam conforme o contexto e o perfil dos usuários. Kapp (2012) acrescenta que a abordagem só rende quando vai além de acrescentar pontos e medalhas a um processo que já existia.

É nesse contexto que se situa este trabalho, que propõe e avalia um aplicativo gamificado de conscientização em segurança da informação voltado a profissionais de áreas não técnicas.

1.1 Proposta do Projeto

Este projeto propõe o desenvolvimento de um aplicativo de ensino voltado à conscientização em segurança da informação e a avaliação do uso de técnicas de gamificação nesse contexto, tendo como público profissionais de áreas não técnicas.

A aplicação organiza o conteúdo em aulas de texto curtas, combinando situações do cotidiano de trabalho com atividades práticas, desafios e retorno imediato sobre o desempenho. A intenção é que o usuário percorra o material de forma contínua, e não em um único treinamento pontual.

A avaliação será feita a partir da experiência dos próprios participantes, comparando o engajamento com o aplicativo ao engajamento com os treinamentos tradicionais que já realizaram. Serão observados o engajamento durante o uso, a percepção de aprendizado, a variação do conhecimento sobre práticas seguras entre os questionários inicial e final e a percepção dos participantes sobre os elementos de gamificação.

1.2 Objetivos da Pesquisa

1.2.1 Geral:

Avaliar um aplicativo gamificado de conscientização em segurança da informação voltado a profissionais de áreas não técnicas quanto ao engajamento, em comparação com os treinamentos tradicionais já vivenciados por eles, e quanto à percepção de aprendizado, à variação do conhecimento sobre práticas seguras e à percepção dos elementos de gamificação.

1.2.2 Específicos:

1) Identificar a percepção e o nível de conhecimento prévio dos participantes em relação aos treinamentos de segurança da informação
2) Desenvolver um aplicativo gamificado de conscientização em segurança da informação voltado a profissionais de áreas não técnicas
3) Comparar o engajamento proporcionado pelo aplicativo com o dos métodos tradicionais já vivenciados pelos participantes e descrever a percepção de aprendizado com o uso do aplicativo
4) Avaliar a variação do conhecimento sobre práticas seguras entre os questionários inicial e final e relacioná-la ao uso registrado do aplicativo, descrevendo também a relação entre o tipo de usuário e o recurso apontado como mais motivador
A pesquisa busca responder à seguinte pergunta: uma plataforma gamificada de *security awareness* proporciona a profissionais de áreas não técnicas uma experiência mais engajadora e agradável do que os treinamentos tradicionais que eles já vivenciaram?

1.3 Justificativa para a Pesquisa

Treinamentos de conscientização já são prática comum nas empresas, mas esbarram sempre nos mesmos problemas: pouco engajamento e pouca retenção. A gamificação aparece como alternativa promissora, mas a revisão sistemática de Gwenhure e Rahayu (2024), que reuniu cinco estudos com profissionais de fora da TI e estudantes, aponta lacunas na avaliação

de cada elemento de jogo, na adaptação das estratégias a profissionais de fora da TI e no acompanhamento dos resultados ao longo do tempo.

A mesma revisão aponta que a maioria dos estudos usou avaliações qualitativas, e não questionários quantitativos aplicados antes e depois da intervenção; este trabalho adota esse tipo de medida, com uma amostra brasileira de profissionais de áreas não técnicas. Desenvolver e avaliar uma solução pensada desde o início para esse público permite verificar, em uso real, se a gamificação sustenta o engajamento e contribui para o conhecimento sobre práticas seguras.

1.4 Contribuições da Pesquisa/Projeto

Para a área de estudo, o trabalho gera evidência empírica sobre gamificação em conscientização em segurança com um público pouco estudado e com amostra brasileira, avaliando não só o conhecimento, mas também o engajamento percebido, o uso real registrado pelo aplicativo e a percepção dos elementos de gamificação.

Na prática, entrega um aplicativo funcional, os conteúdos elaborados e os instrumentos de coleta usados na avaliação. Esse material pode ser reaproveitado ou adaptado por outras organizações e por pesquisas futuras.

Para quem trabalha com segurança da informação e treinamento corporativo, oferece um exemplo documentado de alternativa aos formatos tradicionais, descrevendo como os participantes avaliaram o aplicativo e seus elementos de gamificação.

1.5 Esquema Geral da Pesquisa/Projeto

A pesquisa segue o *Design Science Research* (Dresch; Lacerda; Antunes Jr., 2015; Hevner et al., 2004), voltado à construção e à avaliação de artefatos que resolvem problemas práticos. O trabalho está organizado em cinco etapas.

Na primeira etapa, o problema é caracterizado por meio da revisão da literatura sobre conscientização em segurança e gamificação, com a delimitação do público-alvo e das dimensões de avaliação do artefato.

Na segunda, define-se o questionário inicial, que levanta o perfil dos participantes, o conhecimento prévio e a percepção sobre os treinamentos que já fizeram. Ele é aplicado no primeiro acesso ao aplicativo, antes da primeira aula, e serve de linha de base para a avaliação.

Na terceira, o artefato é projetado: escolha dos elementos de gamificação, definição da arquitetura da aplicação e elaboração dos conteúdos e atividades.

Na quarta, o aplicativo é desenvolvido de forma incremental, com testes e ajustes a cada versão até chegar a uma versão estável.

Na quinta, os participantes têm acesso ao aplicativo e, a partir do 14º dia de uso, são convidados a responder, de forma opcional, ao questionário final, que afere o engajamento, a percepção de aprendizado, o conhecimento sobre práticas seguras e a percepção dos elementos de gamificação, comparando o engajamento com o dos treinamentos tradicionais.

1.6 Declaração de uso de IA

Na elaboração deste trabalho foram utilizadas plataformas de inteligência artificial generativa, especificamente ChatGPT, Claude, Gemini e DeepSeek.

O uso concentrou-se em revisão gramatical e de estilo, refinamento de vocabulário, organização da estrutura do texto e apoio ao desenvolvimento do aplicativo. As ferramentas

não foram empregadas para a produção autônoma de conteúdo científico nem para a formulação das conclusões da pesquisa.

Todas as sugestões incorporadas foram revisadas e validadas pelos autores, incluindo a verificação das fontes citadas, de modo a assegurar a conformidade com os critérios estabelecidos para o trabalho. A responsabilidade pelo conteúdo final é integralmente dos autores.

2 REFERENCIAL TEÓRICO

Programas de conscientização em segurança da informação enfrentam um desafio maior que apenas seu conteúdo: fazer com que as pessoas realmente se engajem. É nesse ponto que a gamificação tem atraído atenção crescente na literatura, ao propor que elementos capazes de sustentar engajamento sejam incorporados a experiências de aprendizagem.

Este capítulo discute os fundamentos conceituais dessa abordagem, sua aplicação em treinamentos corporativos e sua intersecção com o campo da segurança da informação e *security awareness*, construindo a base teórica sobre a qual se sustentam os construtos de engajamento e percepção de aprendizado avaliados neste trabalho.

2.1 Gamificação

A gamificação consiste no uso de elementos de design de jogos, como pontos, medalhas, níveis, rankings e desafios, em contextos que não são jogos (Deterding et al., 2011).

2.1.1 Gamificação: Conceitos e Fundamentos

O conceito de gamificação foi sistematizado por Deterding et al. (2011), que o definiram como o uso de elementos de design de jogos em contextos que não são jogos. Essa distinção é fundamental: na gamificação, o jogo não é o meio pelo qual o aprendizado acontece, mas sim seus elementos, como desafios, metas claras, restrições de tempo, medalhas, rankings e níveis, que são incorporados a atividades com finalidade específica.

Kapp (2012) ampliou essa perspectiva ao argumentar que a gamificação efetiva vai além da simples adição de pontos e medalhas a um processo existente. Para o autor, é necessário alinhar as mecânicas escolhidas aos objetivos pedagógicos pretendidos, sob pena de se obter apenas aparência de engajamento sem aprendizado real. Essa visão dialoga diretamente com a crítica de Nicholson (2015), que distingue a gamificação baseada em recompensas, que acrescenta medalhas, níveis, rankings, conquistas e pontos e pode reduzir a motivação intrínseca, da gamificação significativa, que usa elementos de design de jogos para construir motivação intrínseca.

Hamari, Koivisto e Sarsa (2014), em revisão de literatura de 24 estudos empíricos, identificaram que a gamificação tende a produzir efeitos positivos no engajamento dos usuários, embora esses efeitos sejam condicionados ao contexto de aplicação e às características dos usuários.

Uma forma de considerar essa influência do perfil é a escala Hexad, desenvolvida por Tondello et al. (2016) a partir do modelo de tipos de usuário proposto por Marczewski, que classifica os usuários de sistemas gamificados em seis tipos de acordo com suas motivações: filantropo, socializador, espírito livre, conquistador, disruptor e jogador. Cada tipo responde de forma distinta aos elementos de jogo: o jogador tende a valorizar pontos, recompensas e rankings, enquanto o conquistador se associa a desafios e à progressão (Tondello et al., 2016).

A versão revisada da escala, com 24 itens (Tondello et al., 2019), teve suas propriedades psicométricas investigadas em português brasileiro por Santos et al. (2022), que a consideraram próxima de uma validação completa, mas apontaram problemas na subescala do tipo disruptor. Krath et al. (2023) propuseram uma versão reduzida, a Hexad-12, com dois itens por tipo selecionados da versão de 24 itens. Como a Hexad-12 ainda não foi validada no Brasil, seu uso neste trabalho é exploratório: permite relacionar o perfil declarado dos participantes ao recurso do aplicativo que apontam como mais motivador.

Toda et al. (2019a) reuniram, a partir da literatura, elementos de gamificação para contextos educacionais e os avaliaram com 19 especialistas, chegando a uma taxonomia de 21 elementos. Em trabalho posterior, os mesmos autores organizaram esses elementos em cinco dimensões, discutidas por pelo menos cinco pesquisadores (Toda et al., 2019b): performance (pontos, níveis, progressão e reconhecimento), ecológica (acaso, escolha imposta e pressão de tempo), social (competição, cooperação, reputação e pressão social), pessoal (objetivos, novidade e quebra-cabeça) e ficcional (narrativa e storytelling). Essa taxonomia oferece uma referência estruturada para a seleção e classificação das mecânicas que serão implementadas no protótipo desenvolvido neste estudo.

Além dos elementos e categorias apresentados, é possível compreender o funcionamento da gamificação a partir da dinâmica conhecida como ciclo de engajamento. Esse ciclo, também descrito na literatura como "*engagement loop*" (Werbach; Hunter, 2012), refere-se à interação contínua entre usuário e sistema, em que a motivação leva o usuário a agir, a ação gera um retorno do sistema, como a concessão de pontos, e esse retorno motiva novas ações. Para os autores, o *feedback* é o elemento-chave desse ciclo e parte do que torna os jogos motivadores tão eficazes.

2.1.2 Gamificação em Contextos Corporativos de Aprendizagem

No contexto empresarial, Tatum (2023) observa que os treinamentos de segurança costumam ser concluídos por obrigação, e não por interesse, e que os métodos testados ao longo dos anos tiveram baixa participação; a autora pondera, porém, que gamificar apenas por gamificar não resolve esses problemas. Nesse cenário, a gamificação se apresenta como uma alternativa relevante para tornar os treinamentos corporativos mais interativos, dinâmicos e potencialmente mais eficazes na retenção do conhecimento.

Sailer e Homner (2020), em meta-análise de 38 publicações, com 40 experimentos, encontraram efeitos positivos e significativos, embora pequenos, da gamificação sobre resultados cognitivos, motivacionais e comportamentais em ambientes de ensino; a presença de narrativa e de interação social influenciou os efeitos sobre os resultados comportamentais, e apenas o efeito cognitivo se manteve estável nos estudos de maior rigor metodológico. Silic e Lowry (2020), em estudo de campo conduzido ao longo de seis meses com 420 participantes em uma organização real, verificaram que um sistema de treinamento em segurança da informação com mecânicas gamificadas produziu mudanças comportamentais positivas estatisticamente significativas, resultado que os autores associam ao atendimento das motivações dos usuários e de suas necessidades de enfrentamento (*coping*).

É importante notar, contudo, que os efeitos da gamificação dependem dos usuários (Hamari; Koivisto; Sarsa, 2014), e que profissionais de áreas não técnicas podem ter motivações e expectativas próprias (Gwenhure; Rahayu, 2024). Esse aspecto é pouco explorado na literatura, representando uma das lacunas que este trabalho busca endereçar. O quadro 1 a seguir possui a síntese dos estudos realizados sobre gamificação.

Quadro 1 – Síntese de estudos sobre Gamificação

Autor(es)	Contribuição principal	Relevância para este estudo
Deterding et al. (2011)	Definição seminal de gamificação como uso de elementos de jogos em contextos não lúdicos	Estabelece o conceito central adotado neste TCC
Kapp (2012)	Gamificação efetiva exige alinhamento entre mecânicas e objetivos pedagógicos	Fundamenta a avaliação crítica do design do protótipo
Hamari et al. (2014)	Revisão de literatura: gamificação tem efeitos positivos no engajamento, condicionados ao contexto	Fundamenta o pressuposto de maior engajamento e a atenção ao contexto e ao perfil dos participantes
Nicholson (2015)	Distinção entre gamificação baseada em recompensas (BLAP) e gamificação significativa (motivação intrínseca)	Fundamenta os indicadores sobre a gamificação baseada em recompensas, como o uso do aplicativo motivado mais pela pontuação do que pelo conteúdo
Toda et al. (2019a; 2019b)	Taxonomia de 21 elementos de gamificação avaliada por especialistas (2019a) e organizada em cinco dimensões (2019b)	Referência para seleção e classificação das mecânicas implementadas no aplicativo
Werbach; Hunter (2012)	Apresentação dos engagement loops (ciclos de engajamento), em que a motivação leva à ação, a ação gera feedback do sistema e o feedback motiva novas ações.	Fundamenta a compreensão da dinâmica de funcionamento da gamificação, auxiliando na estruturação de sistemas que incentivam a participação contínua dos usuários, aspecto incorporado no desenvolvimento do protótipo.
Sailer; Homner (2020)	Meta-análise de 38 publicações: efeitos positivos, embora pequenos, sobre resultados cognitivos, motivacionais e comportamentais em ambientes de ensino	Fundamenta a expectativa de variação positiva do conhecimento com o uso do aplicativo
Tondello et al. (2016)	Escala Hexad: seis tipos de usuário de sistemas gamificados, com preferências distintas por elementos de jogo	Fundamenta a análise de perfis e a relação entre o tipo de usuário e o recurso apontado como mais motivador

Autor(es)	Contribuição principal	Relevância para este estudo
Santos et al. (2022)	Investigação psicométrica da escala Hexad de 24 itens em português brasileiro	Fundamenta o uso da versão em português dos itens selecionados na Hexad-12 (Krath et al., 2023), aplicados no questionário inicial

Fonte: autores com base na literatura pesquisada

2.2 Segurança da Informação

Este tópico apresenta os conceitos e fundamentos da segurança da informação, abordando seus pilares estruturantes e as estratégias voltadas à capacitação e conscientização de colaboradores nas organizações.

2.2.1 Segurança da Informação: Conceitos e Fundamentos

A segurança da informação pode ser compreendida como um conjunto de práticas, políticas e mecanismos voltados à proteção dos dados contra acessos não autorizados, uso indevido, alteração ou destruição, abrangendo não apenas soluções tecnológicas, mas também a atuação conjunta de pessoas e processos ao longo de todo o ciclo de vida da informação (Whitman; Mattord, 2011).

Três pilares fundamentais, conhecidos pela sigla CID: Confidencialidade, Integridade e Disponibilidade (Hintzbergen et al., 2018), são a estrutura base da segurança da informação. A confidencialidade garante que o acesso às informações seja restrito apenas às pessoas autorizadas. A integridade diz respeito à manutenção da exatidão e consistência dos dados ao longo de todo o seu ciclo de vida, assegurando que não sofram alterações indevidas. Já a disponibilidade assegura que as informações e os sistemas estejam acessíveis sempre que necessário, mesmo após falhas ou incidentes.

2.2.2 Conscientização em Segurança da Informação (Security Awareness)

Reconhecida a centralidade do fator humano, cresce a importância dos programas voltados especificamente à educação e à mudança de comportamento dos colaboradores. Os programas de *Security, Education, Training and Awareness* (SETA), constituem uma estratégia formal para capacitar profissionais a reconhecer ameaças e adotar práticas mais seguras no cotidiano organizacional (Whitman; Mattord, 2011). Peltier (2001) dedica um capítulo à estruturação de programas de conscientização em segurança.

No Brasil, o tema ganhou relevância regulatória adicional com a Lei Geral de Proteção de Dados Pessoais, a LGPD (Brasil, 2018), que exige dos agentes de tratamento medidas de segurança, técnicas e administrativas, para proteger os dados pessoais e prevê, entre as regras de boas práticas e de governança, ações educativas. Embora a lei não torne obrigatórios os programas de conscientização, esses dispositivos reforçam sua relevância.

Apesar de sua importância reconhecida, esses programas enfrentam limitações metodológicas relevantes. Tatum (2023), em revisão integrativa da literatura sobre gamificação aplicada a programas SETA, observou que boa parte das pesquisas se concentra em campanhas de *phishing* e em jogos de aplicação única, que reproduzem a lógica de "cumprir tabela" dos treinamentos tradicionais, e recomendou estudos que acompanhem o engajamento e a mudança de comportamento ao longo do tempo. Essa lacuna evidencia a necessidade de abordagens que

articulem diferentes dimensões de avaliação, entre elas o engajamento e a percepção de aprendizado dos participantes.

Uma forma de ampliar essa avaliação é considerar, além do conhecimento, as atitudes e os comportamentos dos colaboradores. Esse é o modelo adotado pelo *Human Aspects of Information Security Questionnaire* (HAIS-Q), que mede a conscientização em sete áreas de foco: gestão de senhas, uso de e-mail, uso da internet, uso de redes sociais, dispositivos móveis, manuseio da informação e reporte de incidentes (Parsons et al., 2014). O instrumento foi validado em dois estudos adicionais, um com estudantes universitários e outro com trabalhadores; no estudo com estudantes, as pontuações se associaram ao desempenho em um experimento de identificação de *phishing* (Parsons et al., 2017).

Neste trabalho, as situações de conhecimento foram inspiradas nas sete áreas de foco do HAIS-Q: cada área orienta uma situação própria do dia a dia de trabalho, para assim poder reduzir a extensão do questionário. As situações avaliam se o participante reconhece a conduta segura diante de um caso concreto, isto é, o conhecimento aplicado e a intenção de agir. O quadro 2 possui a síntese dos estudos realizados sobre Segurança da Informação.

Quadro 2 – Síntese de estudos sobre Conscientização em Segurança da Informação

Autor(es)	**Contribuição principal**	**Relevância para este estudo**
Whitman; Mattord (2011)	Define segurança da informação como campo integrado que abrange pessoas, processos e tecnologia na proteção de dados ao longo de todo o seu ciclo de vida	Fornece a definição conceitual base adotada neste trabalho
Hintzbergen et al. (2018)	Apresenta os três pilares da segurança da informação: Confidencialidade, Integridade e Disponibilidade (CID)	Fundamenta os princípios estruturantes abordados nos conteúdos do treinamento desenvolvido
Peltier (2001)	Descreve a estruturação de programas de conscientização em segurança como parte da gestão da segurança da informação	Referência conceitual para programas de conscientização
Tatum (2023)	Revisão integrativa sobre gamificação aplicada a programas SETA; aponta a concentração das pesquisas em campanhas de phishing e em jogos de aplicação única	Fundamenta a inclusão do engajamento entre as dimensões de avaliação
Parsons et al. (2014)	HAIS-Q: conscientização medida por conhecimento, atitude e comportamento em sete áreas de foco	Inspira as situações de conhecimento aplicadas antes e depois do uso do aplicativo

Fonte: os autores com base na literatura pesquisada

2.3 Gamificação Aplicada ao *Security Awareness*

A intersecção entre gamificação e *security awareness* configura um campo de estudo relativamente recente e ainda em consolidação. Em mapeamento sistemático da literatura, com busca realizada em março de 2022, Pahlavanpour e Gao (2024) identificaram 69 artigos sobre gamificação em programas de conscientização em segurança da informação; o *phishing* foi o principal tema das ferramentas educacionais propostas, e apenas 15 artigos (21,7%) trataram de gamificação adaptativa, isto é, que leva em conta as personalidades, as necessidades e os valores de cada usuário.

Plataformas comerciais também já incorporam elementos gamificados: a KnowBe4 oferece rankings e medalhas opcionais em seus treinamentos (KnowBe4, [s. d.]).

Um aspecto particularmente negligenciado na literatura é a personalização do treinamento por perfil profissional. As evidências empíricas sobre essa personalização ainda são escassas: em revisão sistemática sobre a gamificação da conscientização para profissionais de fora da TI e estudantes, Gwenhure e Rahayu (2024) encontraram, de um conjunto inicial de 91 artigos, apenas cinco estudos empíricos voltados a esse público e observaram que a maioria das iniciativas adota uma abordagem única para todos. Este trabalho busca ampliar essas evidências ao propor um protótipo com conteúdo adaptado ao contexto de áreas não técnicas, embora a gamificação em si seja a mesma para todos os usuários, avaliando o engajamento percebido, a variação do conhecimento e a percepção dos elementos de gamificação.

2.4 Engajamento e Percepção de Aprendizado como Dimensões de Avaliação

O engajamento é um construto multidimensional que, na literatura educacional, costuma ser operacionalizado em três dimensões complementares: comportamental, baseada na ideia de participação; emocional, que abrange as reações positivas e negativas ao ambiente de aprendizagem; e cognitiva, baseada na ideia de investimento no aprendizado (Fredricks et al., 2004).

Quando o objeto avaliado é um sistema digital, o engajamento costuma ser tratado como uma qualidade da experiência do usuário. O'Brien, Cairns e Hall (2018) refinaram a *User Engagement Scale* (UES) e propuseram uma versão reduzida, a UES-SF, com 12 itens distribuídos em quatro dimensões: atenção focada, usabilidade percebida, apelo estético e recompensa. Neste trabalho, propõe-se aproximar essas dimensões das de Fredricks et al. (2004): a atenção focada aproxima-se do engajamento cognitivo, e o apelo estético e a recompensa, do engajamento emocional, enquanto o engajamento comportamental pode ser observado diretamente nos dados de uso do aplicativo.

A percepção de aprendizado, por sua vez, é a avaliação que o próprio participante faz sobre o quanto aprendeu ao longo de uma experiência. Ela não substitui medidas objetivas: em meta-análise, Sitzmann et al. (2010) observaram que autoavaliações de conhecimento se relacionam apenas moderadamente com a aprendizagem cognitiva e mais fortemente com reações e motivação. Tomadas em conjunto, essas duas dimensões se complementam: o engajamento diz respeito ao envolvimento durante a experiência, e a percepção de aprendizado diz respeito ao que o participante sente ter levado dela.

A comparação com os treinamentos já vivenciados pelos participantes, em vez de um grupo de controle, decorre de uma razão prática: formar grupos de controle com acesso controlado a treinamentos corporativos está fora do escopo deste projeto. Essa comparação restringe-se ao engajamento; a percepção de aprendizado é analisada apenas de forma descritiva, a partir do questionário final.

3 PROCEDIMENTOS METODOLÓGICOS

Este trabalho adotou como abordagem metodológica o *Design Science Research* (DSR), paradigma que orienta pesquisas voltadas à criação e avaliação de artefatos com o objetivo de resolver problemas práticos identificados em um contexto real (Hevner et al., 2004). A escolha se justificou pela natureza dupla do estudo: ao mesmo tempo que propôs o desenvolvimento de uma aplicação gamificada, buscou avaliá-la empiricamente junto a um público-alvo definido, o que demandou tanto rigor construtivo quanto avaliativo.

Para a avaliação do artefato, seguiu-se o framework FEDS (Venable; Pries-Heje; Baskerville, 2016), que orienta a escolha das estratégias de avaliação em *Design Science Research*. Adotou-se a estratégia de risco humano e efetividade (*Human Risk & Effectiveness*), indicada quando o principal risco de design é social ou ligado ao usuário (Venable; Pries-Heje; Baskerville, 2016): as avaliações formativas, de caráter artificial, consistiram em testes automatizados e em homologação interna pela equipe a cada versão, e a avaliação final foi somativa e naturalística, com profissionais em atividade utilizando o aplicativo já concluído na própria rotina, fora de um programa formal de treinamento de uma empresa.

Do ponto de vista da natureza da pesquisa, o trabalho se caracterizou como aplicado, uma vez que partiu de um problema prático, as dificuldades dos programas tradicionais de conscientização em segurança da informação, e propôs uma solução passível de implementação em contexto organizacional. Quanto aos objetivos, a pesquisa foi de caráter exploratório e descritivo, com dois testes principais definidos antes da coleta: exploratório por investigar uma abordagem com poucos estudos empíricos voltados a profissionais de fora da TI (Gwenhure; Rahayu, 2024), e descritivo por mapear percepções, uso registrado e níveis de conhecimento dos participantes antes e após a interação com o artefato.

A coleta de dados foi realizada por meio de dois questionários estruturados, aplicados no próprio aplicativo: um inicial, respondido no primeiro acesso e antes da primeira aula, e um final, liberado após o período de uso. O questionário inicial tinha 40 itens e levava cerca de 10 minutos. Ele reunia a caracterização do participante, o histórico de treinamentos em segurança, a escala de engajamento UES-SF aplicada ao treinamento mais recente, sete situações de conhecimento e a escala Hexad em sua versão reduzida, sem o tipo disruptor.

O questionário final tinha 32 itens: repetia a UES-SF (agora voltado para o aplicativo) e as situações de conhecimento, e acrescentava itens sobre os elementos de gamificação, incluindo o uso motivado pela pontuação e o desconforto com a comparação no ranking, um item de percepção de aprendizado, formulado como autoeficácia e restrito ao reconhecimento de golpes digitais, em que o participante indicava se se sentia mais preparado para reconhecê-los, o recurso mais motivador, uma comparação direta com o treinamento anterior e duas questões abertas opcionais.

As situações de conhecimento foram inspiradas nas áreas de foco do HAIS-Q (Parsons et al., 2014), com redação própria: cada uma descrevia um caso do dia a dia de trabalho e perguntava o que o participante faria, com uma alternativa correta, duas incorretas que pareciam responsáveis e a opção "Não sei o que faria", sem exibição da resposta correta. Cada acerto valia um ponto, e erro ou "Não sei" valia zero, de modo que a nota variava de 0 a 7. Por terem redação própria e uma situação por área, elas não formavam um instrumento validado; seus itens seriam descritos individualmente, e apenas a nota total entraria nos testes. Como as mesmas situações eram respondidas duas vezes, o efeito de teste não podia ser separado da variação associada ao aplicativo; a relação entre a variação e o uso registrado seria examinada, mas também poderia refletir diferenças de motivação entre os participantes.

A UES-SF passou por uma adaptação própria ao português, pois a UES-Br (Miranda; Li; Darin, 2021) traduziu e validou apenas a versão longa, e um dos itens da versão reduzida, "*I felt interested in this experience*", não fazia parte dela (O'Brien; Cairns; Hall, 2018, p. 39).

Os itens foram reescritos para dois objetos distintos, o treinamento anterior e o aplicativo, mantendo a correspondência item a item entre os questionários. A adaptação também não passou pelas etapas de retrotradução e pré-teste recomendadas por Beaton et al. (2000), o que foi reconhecido como limitação, e cada questionário incluiu um item de verificação de atenção para identificar respostas descuidadas (Meade; Craig, 2012).

A amostra foi composta por profissionais de áreas não técnicas em contexto corporativo, recrutados por conveniência a partir das redes de contato dos pesquisadores; profissionais de TI foram excluídos já no recrutamento e não se exigiu treinamento prévio, pois a variação do conhecimento seria analisada para todos os participantes. Como parte dos participantes tendia a não responder o questionário final, a meta foi recrutar de 35 a 40 pessoas para obter cerca de 20 pares de respostas completas, isto é, participantes com os dois questionários respondidos e aprovados nos itens de verificação de atenção.

O questionário inicial era obrigatório para iniciar as aulas, e a orientação aos participantes era concluir uma aula por dia. O questionário final era liberado 14 dias após a resposta ao inicial e permanecia disponível até o encerramento da coleta. Ele era opcional e podia ser respondido uma única vez. Os participantes recebiam um convite por e-mail no dia da liberação e um lembrete quatro dias depois, caso ainda não tivessem respondido.

A participação foi voluntária e condicionada ao consentimento registrado no cadastro. Os dados foram tratados conforme a LGPD: as respostas e os registros de uso foram exportados com pseudônimos, sem nome nem e-mail, e utilizados apenas para os fins desta pesquisa.

A análise dos dados quantitativos combinaria estatística descritiva e inferencial. Dois testes seriam principais: a variação da nota das situações de conhecimento, para todos os participantes com respostas completas, e a diferença na pontuação total da UES-SF entre o treinamento anterior e o aplicativo, apenas para quem já havia feito algum treinamento. Ambos usariam o teste de Wilcoxon pareado, com tamanho de efeito e correção de Holm. As subescalas da UES-SF, os itens de conhecimento, o item de percepção de aprendizado e os itens sobre os elementos de gamificação seriam analisados de forma descritiva.

De forma exploratória, os dados de uso, contabilizados até a resposta ao questionário final, seriam relacionados à percepção dos elementos de gamificação por correlação de Spearman e à variação do conhecimento por correlação parcial de Spearman, controlando o número de dias entre os dois questionários, que variaria do 14º ao 28º dia. Para avaliar o viés de abandono, quem respondeu ao questionário final seria comparado a quem não respondeu quanto às respostas iniciais e ao uso do aplicativo.

De forma exploratória e descritiva, os tipos de usuário da escala Hexad seriam cruzados com o recurso apontado como mais motivador no questionário final. Em conjunto, esses instrumentos permitiriam responder à pergunta norteadora apresentada na seção 1.2.

3.1 Proposta de Desenvolvimento de Artefato

Este trabalho adotou a *Design Science Research* como orientação metodológica por tratar-se de uma pesquisa cujo produto central era um artefato tecnológico com finalidade prática e avaliável.

A solução proposta consistiu no desenvolvimento de um aplicativo gamificado de conscientização em segurança da informação, voltado a profissionais de áreas não técnicas em ambiente corporativo. O artefato foi concebido para incorporar mecânicas de gamificação aplicadas a conteúdos de segurança relevantes para esse público, como pontos, conquistas, ranking, desafios em níveis de dificuldade, feedback imediato sobre as respostas e visualização do progresso ao longo da experiência, elementos escolhidos com base na literatura, que aponta efeitos positivos da gamificação sobre o engajamento e a aprendizagem (Hamari; Koivisto;

Sarsa, 2014; Sailer; Homner, 2020), desde que as mecânicas estejam alinhadas aos objetivos pedagógicos (Kapp, 2012).

A escolha por materializar a solução em um artefato digital, e não apenas propô-la conceitualmente, respondeu a uma das exigências centrais da DSR: a de que o conhecimento gerado pela pesquisa fosse demonstrado por meio de um produto funcional, capaz de ser avaliado em condições reais de uso (Dresch; Lacerda; Antunes Jr., 2015).

3.2 Análise Prévia Sobre o que foi Proposto

Antes do desenvolvimento do artefato, foi conduzida uma análise prévia com o objetivo de compreender, a partir da literatura, as características e as necessidades do público-alvo.

O levantamento de requisitos partiu de dois achados da literatura: para mudar a conduta, as orientações de segurança precisam ser compreendidas e aplicáveis à rotina de quem as recebe (Bada; Sasse; Nurse, 2015), e as iniciativas gamificadas raramente são adaptadas a profissionais de fora da TI (Gwenhure; Rahayu, 2024). Esse diagnóstico orientou a definição das funcionalidades prioritárias do aplicativo, com ênfase em experiências curtas, linguagem acessível e situações reconhecíveis do cotidiano corporativo.

3.3 Como a solução foi implementada

O desenvolvimento do artefato foi conduzido em etapas sequenciais, organizadas de acordo com as prioridades funcionais e os prazos disponíveis. A primeira etapa compreendeu a definição da arquitetura do sistema e a configuração do ambiente de desenvolvimento, com base na tecnologia *Progressive Web App*, escolhida por permitir acesso multiplataforma sem necessidade de instalação. O sistema foi desenvolvido com React no *frontend*, Node.js no *backend* e PostgreSQL como banco de dados relacional.

As etapas subsequentes contemplaram o desenvolvimento das funcionalidades centrais do aplicativo, priorizadas na seguinte ordem: o módulo de quiz com feedback imediato e o sistema de progressão com premiação digital. Com base na taxonomia de Toda et al. (2019b), o aplicativo combinou elementos da dimensão de performance (pontos, progressão e conquistas, estas correspondentes ao reconhecimento) e da dimensão social (ranking, correspondente à competição). Esses elementos caracterizavam o que Nicholson (2015) chama de gamificação baseada em recompensas; segundo Deci e Ryan (apud Nicholson, 2015), recompensas extrínsecas substituem a motivação intrínseca. Por isso, em vez de evitá-los, o trabalho incluiu indicadores sobre eles: o questionário final perguntou se o aplicativo foi usado mais pela pontuação do que pelo conteúdo e se a comparação no ranking causou desconforto. O ranking individual mereceu atenção particular, pois Sailer e Homner (2020) observam que a competição isolada pode ser problemática para a motivação e o desempenho dos aprendizes.

3.4 Resultados Esperados

Ao término do projeto, esperava-se entregar um aplicativo gamificado funcional, avaliado por participantes de áreas não técnicas em ambiente corporativo. Em termos de avaliação, os pressupostos, fundamentados na literatura revisada, eram que os participantes relatariam níveis superiores de engajamento em comparação aos métodos tradicionais que já vivenciaram e que haveria variação positiva do conhecimento sobre práticas seguras entre os questionários inicial e final, resultados coerentes com as evidências encontradas em estudos

sobre gamificação em contextos de aprendizagem (Hamari et al., 2014; Sailer; Homner, 2020) e de treinamento corporativo em segurança (Silic; Lowry, 2020).

Esperava-se também que a análise das respostas ao questionário pós-intervenção revelasse preferências específicas por determinadas mecânicas de gamificação e uma percepção de aprendizado favorável, entendida como média acima do ponto neutro da escala, oferecendo subsídios concretos para o aprimoramento do artefato em versões futuras. A consolidação comportamental de longo prazo, porém, ultrapassava o escopo temporal deste trabalho, sendo reconhecida como limitação e recomendação para pesquisas futuras.

3.5 Fatores Críticos para o Sucesso (FCS) do Desenvolvimento da Proposta

O sucesso do projeto esteve condicionado a um conjunto de fatores que envolviam tanto o desenvolvimento técnico do artefato quanto a condução da avaliação com os participantes. Entre os fatores favoráveis, destacaram-se a disponibilidade de ferramentas de desenvolvimento gratuitas e amplamente documentadas, a existência de literatura sobre gamificação e *security awareness* como base para as decisões de design, e o acesso a um grupo de participantes com perfil adequado para a fase de avaliação.

Por outro lado, os principais riscos identificados incluíram a dificuldade de recrutar participantes em número suficiente dentro do prazo acadêmico estabelecido; a possibilidade de viés nas respostas decorrente da natureza retrospectiva da comparação com métodos tradicionais já vivenciados; a limitação inerente a amostras de conveniência, que restringiam a generalização dos resultados para contextos organizacionais mais amplos; o abandono antes do questionário final, que poderia concentrar as respostas nos participantes mais engajados; o viés de demanda decorrente do recrutamento nas redes de contato dos autores e o poder estatístico limitado pelo tamanho da amostra. A mitigação desses riscos passou pela diversificação dos perfis recrutados e pela aplicação dos mesmos questionários, pelo próprio aplicativo, a todos os participantes, o que padronizou a coleta, embora as escalas adaptadas não tivessem sido validadas e as respostas continuassem autodeclaradas. O viés de abandono seria examinado comparando quem respondeu ao questionário final com quem não respondeu.

4 APRESENTAÇÃO DOS RESULTADOS

Foi desenvolvida uma aplicação web e mobile voltada ao ensino de boas práticas de segurança da informação e à conscientização dos usuários sobre os riscos a que estão expostos no ambiente corporativo.

A solução adotou uma abordagem gamificada como estratégia para sustentar o engajamento ao longo do uso e alcançar um público mais amplo. Nesse formato, o usuário recebeu retorno contínuo sobre sua evolução no conteúdo, seja por meio de medalhas de reconhecimento ou seja pela sua posição em um ranking geral de pontuação. Complementarmente, foram coletados dados de uso dos participantes para analisar o engajamento durante a experiência.

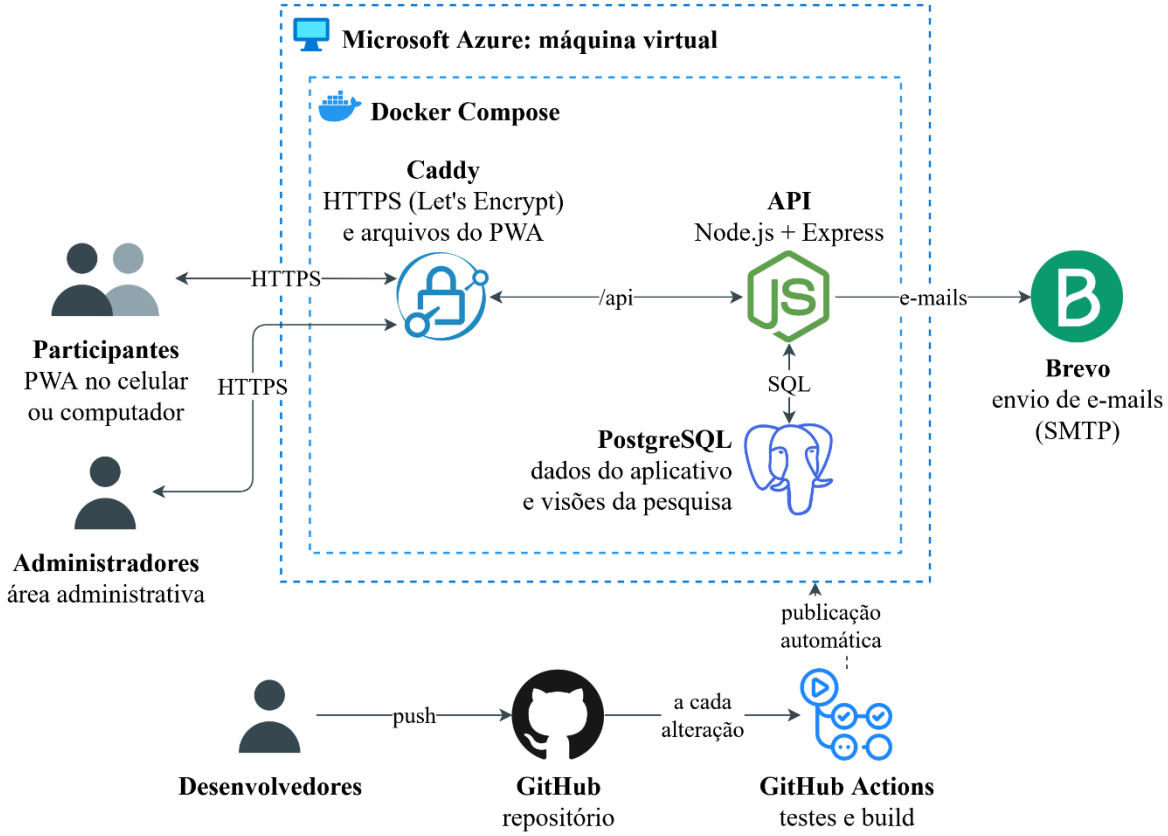
4.1 Como a solução foi implementada (Etapas / Prioridades)

4.1.1 Arquitetura da solução

A aplicação foi construída como um *Progressive Web App* (PWA), acessível pelo navegador do computador ou do celular e passível de instalação na tela inicial, sem passar por

lojas de aplicativos. Em produção, os serviços foram executados em contêineres Docker em uma máquina virtual na nuvem Microsoft Azure, com o servidor Caddy responsável pelo HTTPs e pelo encaminhamento das requisições à API, de modo que interface e API ficassem na mesma origem (Figura 1). A cada alteração no repositório, uma esteira de integração contínua verificava o padrão do código e executava os testes automatizados; as alterações aprovadas na ramificação principal foram publicadas automaticamente.

Figura 1 – Arquitetura da solução



Fonte: os autores (2026)

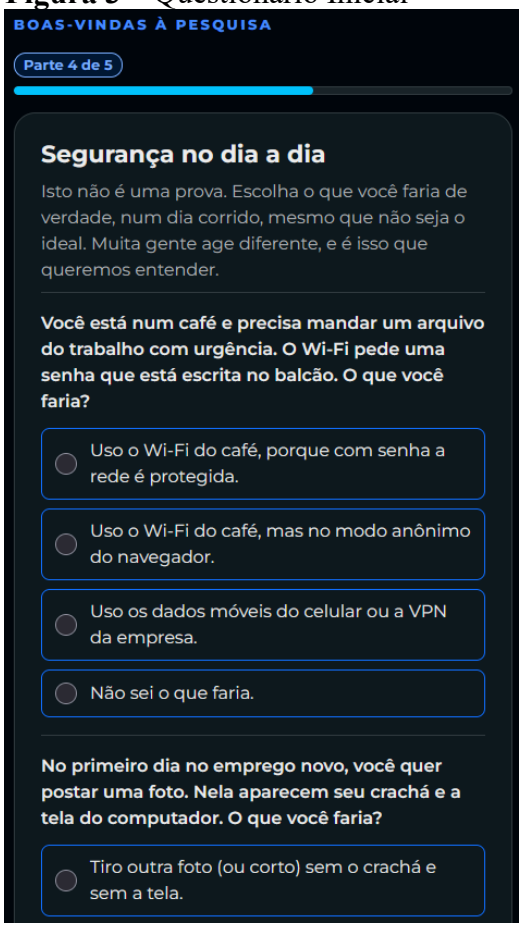
4.1.2 Funcionamento do aplicativo

No primeiro acesso, o participante cria sua conta e registra o consentimento de participação na pesquisa (Figura 2); em seguida, responde ao questionário inicial, que precisa ser concluído antes da primeira aula (Figura 3).

Figura 2 – Cadastro

Fonte: os autores (2026)

Figura 3 – Questionário Inicial



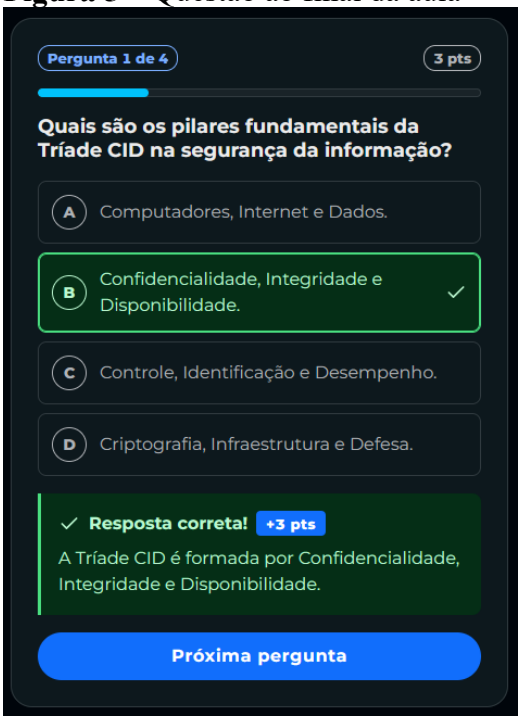
A aplicação foi estruturada em dois modos de uso: o modo aula e o modo trivia.

No modo aula, o conteúdo era apresentado em linguagem simples e contextualizada para a rotina corporativa, em uma trilha de 15 aulas liberadas em sequência: cada aula ficava disponível somente após a conclusão da anterior, e uma barra mostrava o progresso na trilha (Figura 4). Ao final de cada aula, o usuário respondia a questões de múltipla escolha destinadas a reforçar o conteúdo trabalhado e via, logo após cada resposta, a explicação correspondente (Figura 5). As respostas corretas se convertiam em pontos no ranking da aplicação, e a primeira conclusão de cada aula rendia um bônus. Questões já respondidas corretamente não geravam nova pontuação, de modo a evitar o acúmulo de pontos por repetição.

Figura 4 – Trilha de aulas

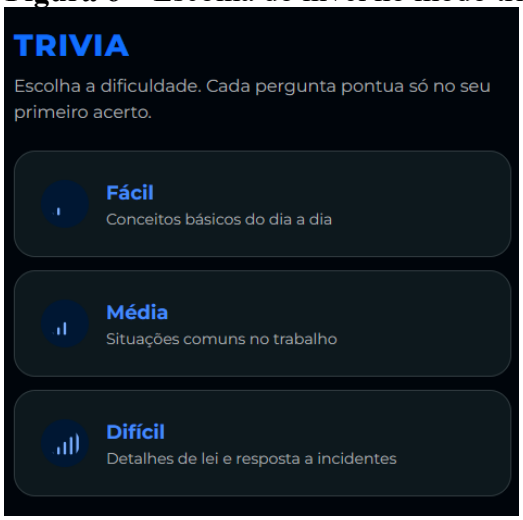
Fonte: os autores (2026)

Figura 5 – Questão ao final da aula



No modo trivia, liberado após a conclusão das 15 aulas, o usuário escolhia entre três níveis de dificuldade: fácil, médio e difícil (Figura 6). Cada rodada tinha cinco questões de múltipla escolha, com quatro alternativas e apenas uma correta. A pontuação variava conforme a dificuldade, sendo cinco pontos para as questões fáceis, dez para as médias e quinze para as difíceis, conforme as Figuras 7 a 9. As questões eram sorteadas entre as do nível escolhido e, também neste modo, repetir uma questão já acertada não gerava pontuação adicional. As questões sorteadas davam prioridade por questões ainda não respondidas antes de repetir por perguntas que o usuário já conhecia e acertara anteriormente.

Figura 6 – Escolha do nível no modo trivia



Fonte: os autores (2026)

Figura 7 – Exemplo de questão de nível fácil

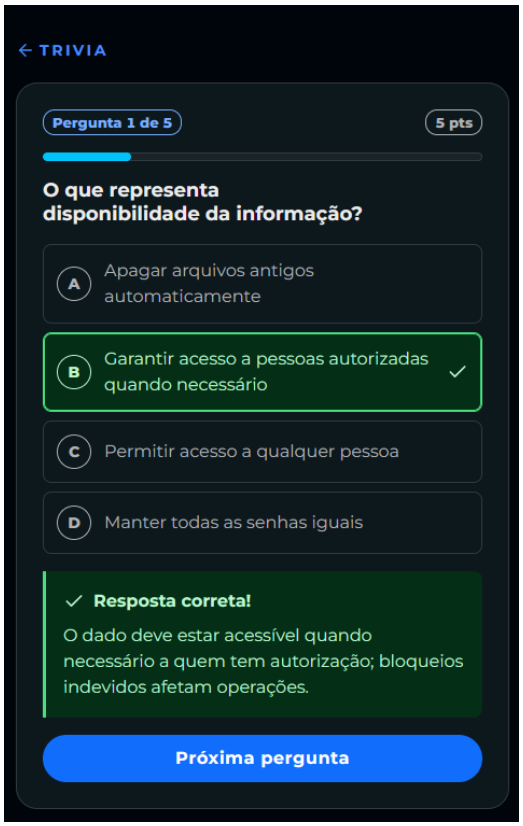


Figura 8 – Exemplo de questão de nível médio

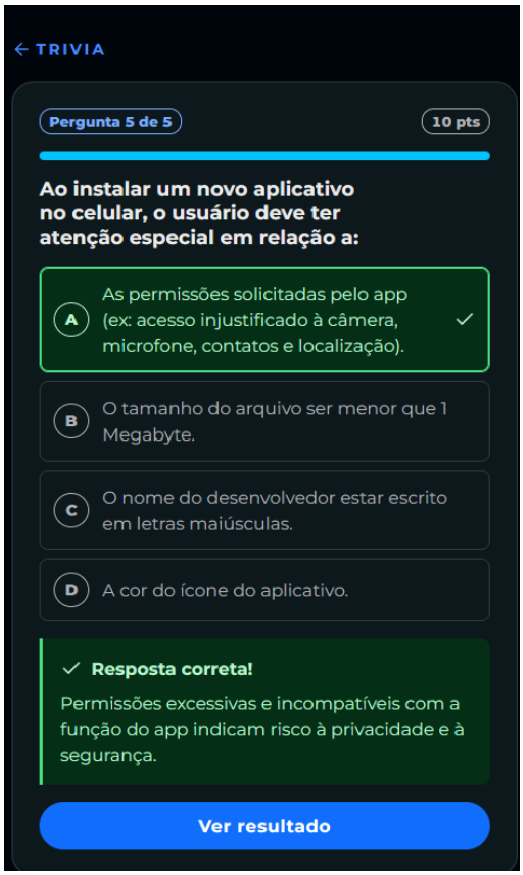
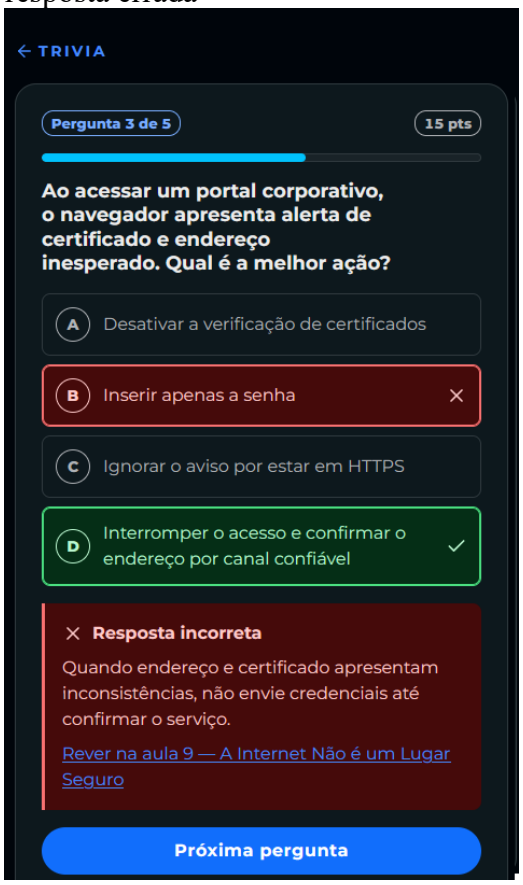


Figura 9 – Exemplo de questão difícil e resposta errada



Fonte: os autores (2026)

Os pontos acumulados nos dois modos levavam às conquistas e definiam a posição do usuário no ranking geral (Figuras 10 e 11).

Figura 10 – Conquistas

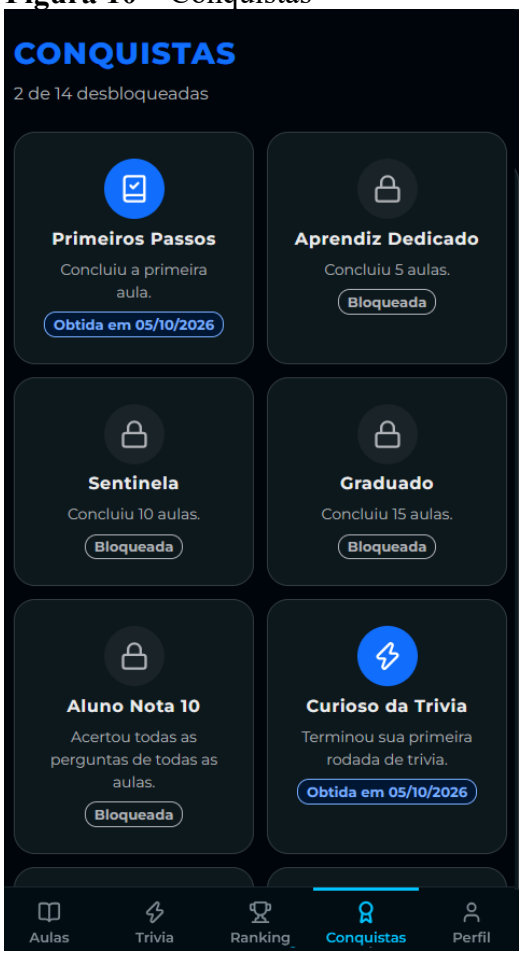
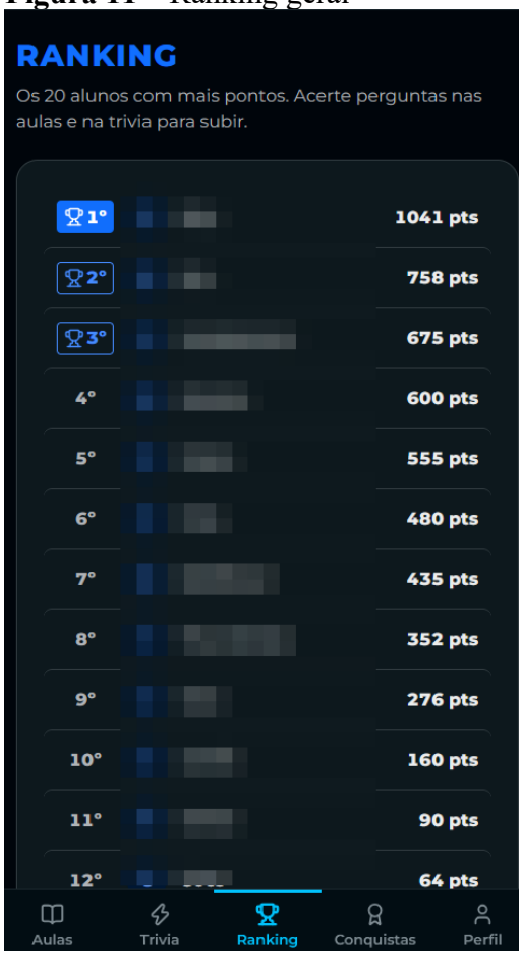


Figura 11 – Ranking geral



Fonte: os autores (2026)

4.1.3 Elementos de gamificação

O Quadro 3 relaciona os elementos de gamificação implementados às dimensões da taxonomia de Toda et al. (2019b) e aos itens do questionário final que avaliarão a percepção de cada um. O modo trivia corresponde ao elemento quebra-cabeça da dimensão pessoal, que abrange desafios e quizzes (Toda et al., 2019b, p. 7), e a explicação após cada resposta, ao feedback que sustenta o ciclo de engajamento (Werbach; Hunter, 2012).

Quadro 3 – Elementos de gamificação implementados

Elemento (dimensão)	**Implementação no aplicativo**	**Itens do questionário final**
Pontos (performance)	Pontos por questão acertada nas aulas e bônus na primeira conclusão de cada aula; 5, 10 ou 15 pontos por questão do modo trivia; cada questão pontua apenas no primeiro acerto	GAM1, EXT

Elemento (dimensão)	Implementação no aplicativo	Itens do questionário final
Progressão (performance)	Trilha de 15 aulas liberadas em sequência, com barra de progresso	—
Conquistas (performance: reconhecimento)	14 conquistas, obtidas pela conclusão de aulas, pelo desempenho no modo trivia e pela pontuação acumulada	GAM3
Ranking (social: competição)	Classificação geral dos usuários pela pontuação total	GAM2, GAM5
Desafios em níveis (pessoal: quebra-cabeça)	Modo trivia com três níveis de dificuldade	—
Feedback imediato (ciclo de engajamento)	Explicação exibida após cada resposta, nas aulas e no modo trivia	GAM4

Fonte: os autores (2026), com base em Toda et al. (2019a; 2019b) e Werbach e Hunter (2012)

Além desses itens, o questionário final perguntará se pontos, conquistas e ranking fizeram diferença na forma de uso do aplicativo (GAM6) e qual recurso mais motivou o uso (MOT), entre pontos, conquistas, ranking, Trivia e explicações.

4.1.4 Coleta de dados

Os questionários da pesquisa foram aplicados no próprio aplicativo. O questionário inicial, com 40 itens, foi exigido antes da primeira aula. O final, com 32 itens, foi liberado 14 dias após a resposta ao inicial e ficava disponível até a data de encerramento da coleta; nesse período, um aviso na tela inicial indicava que ele estava disponível e o participante recebia um convite por e-mail no dia da liberação e um lembrete quatro dias depois. Cada questionário podia ser respondido uma única vez e não rendia pontos nem conquistas.

A telemetria é implementada a partir do registro de eventos de uso, contemplando os identificadores de sessão e de login do usuário, a tela em que o evento ocorreu, o tipo de evento, como a resposta a uma questão do modo trivia ou a abertura de uma aula, o elemento acionado, o tempo de permanência na tela e os metadados associados, entre eles o acerto ou erro da questão e o nível de dificuldade selecionado.

Para a análise, os dados foram exportados pelos autores em arquivos CSV, nos quais cada participante aparecia apenas por um pseudônimo, sem nome, apelido nem e-mail.

4.2 Resultados Obtidos

4.2.1 Avaliação formativa

Conforme a estratégia de avaliação descrita no capítulo 3, a avaliação formativa foi composta por testes automatizados e pela homologação interna a cada versão, complementadas por um teste de carga.

Os testes automatizados, unitários e de integração, cobrem a interface e a API e são executados pela esteira de integração contínua a cada alteração, incluindo casos de sucesso, de erro e de borda. A interface contava com 385 testes, que cobrem 99,8% das linhas do código, e a API com 475 testes, que cobrem 100% das linhas.

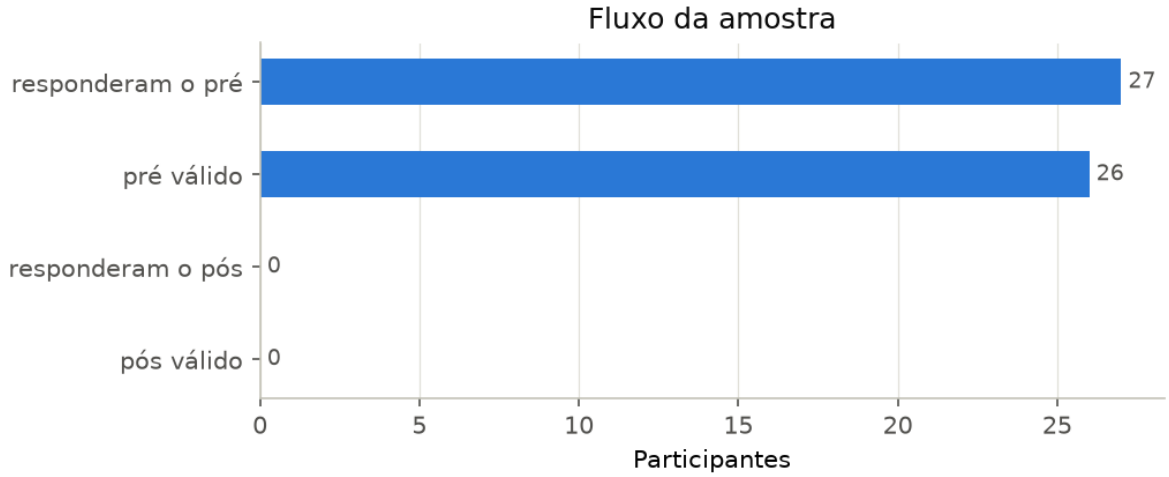
Na homologação interna, a equipe percorreu o fluxo completo do participante, do cadastro ao questionário final, no computador e no celular. Nesta homologação não foram encontrados problemas relacionados a usabilidade.

O desempenho foi verificado por teste de carga em uma cópia da máquina virtual de produção. No teste realizado com 100 usuários simultâneos navegando pelas aulas e pelo modo trivia durante três minutos, não houve nenhuma falha, e 95% das respostas da API foram entregues em até 20 ms (150 ms nas operações de autenticação).

4.2.2 Avaliação com os participantes

Esta seção apresenta dados parciais, coletados até 19 de outubro de 2026. Até 19 de outubro, nenhum participante havia respondido ao questionário final, que só é liberado 14 dias após a resposta ao questionário inicial; por isso, são apresentados apenas o fluxo dos participantes (Figura 12), um panorama do perfil da amostra e os primeiros resultados do questionário inicial, cujas tabelas completas estão no Apêndice B. Os resultados que dependem do questionário final, isto é, os dois testes principais e as análises do engajamento com o aplicativo, da percepção de aprendizado, da variação do conhecimento e da percepção dos elementos de gamificação, assim como as análises exploratórias, serão obtidos com os dados ainda em coleta e apresentados em versão posterior deste trabalho.

Figura 12 – Fluxo dos participantes



Fonte: os autores (2026)

Até 19 de outubro de 2026, 27 participantes haviam respondido ao questionário inicial; um deles foi excluído por não marcar a resposta solicitada no item de verificação de atenção, o que resultou em 26 questionários iniciais válidos (Figura 12). A amostra parcial é composta principalmente por adultos jovens: 21 dos 26 participantes (80,8%) têm entre 18 e 34 anos. Treze participantes se declararam do gênero feminino, 12 do masculino e 1 de outro gênero; 13 (50,0%) têm ensino superior completo ou pós-graduação. As áreas de atuação são variadas: nenhuma reúne mais de 5 participantes (19,2%), e apenas a área jurídica não teve representantes (Tabela B.2, no Apêndice B). Quanto à familiaridade com jogos, 19 participantes (73,1%) jogam no celular, no computador ou em console ao menos algumas vezes por mês, e 23 (88,5%) já usaram o Duolingo, a plataforma de ensino com pontos, medalhas ou ranking mais citada (Tabela B.3).

Pouco mais da metade dos participantes (14; 53,8%) informou já ter feito algum treinamento em segurança da informação. Nesse grupo, o treinamento mais recente havia sido obrigatório para 12 dos 14 participantes e realizado no último ano também por 12 participantes; o formato principal mais citado foi vídeo ou curso online (10 de 14) (Tabela B.4). Esses 14 participantes também avaliaram esse treinamento pela UES-SF: o escore total teve mediana 3,5, em escala de 1 a 5, e a consistência interna da escala, estimada pelo alfa de Cronbach, foi de 0,95 (n = 14). Nas situações de conhecimento do questionário inicial, a nota, que varia de 0 a 7, teve mediana 6 (n = 26) (Tabelas B.5 e B.6). Esses resultados são descritivos e preliminares; a comparação entre os questionários inicial e final será feita após o encerramento da coleta.

4.3 Análise dos Resultados

Esta seção confrontará os resultados com os pressupostos da seção 3.4: maior engajamento com o aplicativo do que com os treinamentos tradicionais já vivenciados, variação positiva do conhecimento sobre práticas seguras e percepção de aprendizado acima do ponto neutro da escala. Os resultados também serão comparados aos de estudos sobre gamificação em contextos de aprendizagem (Hamari; Koivisto; Sarsa, 2014; Sailer; Homner, 2020) e de treinamento corporativo em segurança (Silic; Lowry, 2020), considerando as limitações descritas no capítulo 3.

4.4 Fatores Críticos para o Sucesso (FCS) identificados no Desenvolvimento da Solução proposta e como foram tratados

O principal fator crítico identificado no desenvolvimento foi a integridade da pontuação. Como pontos, conquistas e ranking dependem dela, uma pontuação calculada no aparelho do usuário poderia ser manipulada, distorcendo o ranking e os dados de uso da pesquisa. Por isso, a regra de pontuação ficou no servidor, e o banco de dados aceita apenas o primeiro acerto de cada questão e um único bônus de conclusão por aula, mesmo que o usuário repita a ação ou envie várias requisições ao mesmo tempo.

Outro fator crítico foi o recrutamento e participação ativa dos usuários do aplicativo que responderam ao questionário inicial e navegaram no aplicativo.

5 CONSIDERAÇÕES FINAIS

Este trabalho desenvolveu um aplicativo gamificado de conscientização em segurança da informação voltado a profissionais de áreas não técnicas, com o objetivo de avaliá-lo quanto ao engajamento, em comparação com os treinamentos tradicionais já vivenciados pelos

participantes, e quanto à percepção de aprendizado, à variação do conhecimento sobre práticas seguras e à percepção dos elementos de gamificação. Como a coleta de dados ainda está em andamento, as considerações a seguir são conclusões iniciais e serão revistas quando os dados do questionário final estiverem disponíveis.

O segundo objetivo específico, de desenvolver o artefato, foi alcançado. O aplicativo foi construído como um *Progressive Web App*, com uma trilha de 15 aulas, o modo trivia em três níveis de dificuldade, pontos, conquistas, ranking e explicação após cada resposta, além do registro dos eventos de uso.

Quanto ao primeiro objetivo específico, os dados parciais do questionário inicial, com 26 respostas válidas até 19 de outubro de 2026, permitiram descrever o perfil dos participantes e seu conhecimento prévio. A amostra é composta principalmente por adultos jovens, de áreas de atuação variadas e familiarizados com jogos e com plataformas de ensino gamificadas. Pouco mais da metade já havia feito algum treinamento em segurança da informação, em geral obrigatório e no formato de vídeo ou curso online, e atribuiu ao treinamento mais recente escore total mediano de 3,5 na UES-SF, em escala de 1 a 5. A nota nas situações de conhecimento foi alta já no questionário inicial, com mediana de 6 em 7, o que indica que boa parte dos participantes reconheceu a conduta segura na maioria das situações e pode limitar a margem para a variação positiva prevista na seção 3.4.

Os demais objetivos específicos, que tratam de comparar o engajamento com o aplicativo ao dos treinamentos anteriores, descrever a percepção de aprendizado, avaliar a variação do conhecimento e sua relação com o uso registrado e relacionar o tipo de usuário ao recurso apontado como mais motivador, dependem das respostas ao questionário final, assim como a análise da percepção dos elementos de gamificação. Por isso, a pergunta de pesquisa, isto é, se uma plataforma gamificada de *security awareness* proporciona a profissionais de áreas não técnicas uma experiência mais engajadora e agradável do que os treinamentos tradicionais que eles já vivenciaram, ainda não pode ser respondida, e nenhuma conclusão sobre o efeito do aplicativo é apresentada nesta etapa.

Na continuidade do trabalho, após o encerramento da coleta, serão realizados os testes principais e as análises descritivas e exploratórias previstas no capítulo 3, e os resultados serão confrontados com os pressupostos da seção 3.4. Essas análises deverão considerar as limitações já descritas: a amostra por conveniência, recrutada nas redes de contato dos autores, e o número reduzido de participantes; a ausência de grupo de controle; a comparação retrospectiva com os treinamentos já vivenciados; o uso de escalas adaptadas sem validação e de respostas autodeclaradas; o efeito de responder duas vezes às mesmas situações; e o possível abandono antes do questionário final.

Para trabalhos futuros, sugere-se acompanhar o comportamento dos participantes por um período mais longo, utilizar o aplicativo em um programa formal de treinamento de uma empresa, com grupo de comparação, e adaptar os elementos de gamificação ao perfil de cada usuário.

REFERÊNCIAS

ALSHAIKH, M. **Developing cybersecurity culture to influence employee behavior**: a practice perspective. Computers & Security, v. 98, art. 102003, 2020.

BADA, M.; SASSE, A. M.; NURSE, J. R. C. Cyber security awareness campaigns: why do they fail to change behaviour? In: **INTERNATIONAL CONFERENCE ON CYBER SECURITY FOR SUSTAINABLE SOCIETY**, 2015, Coventry. Anais... Coventry: [s. n.], 2015. p. 118-131. Disponível em: https://arxiv.org/abs/1901.02672. Acesso em: 5 out. 2026.

BAGUETE. **Vazamento expõe dados de quem fez teste da Covid-19**. 26 nov. 2020. Disponível em: https://www.baguete.com.br/noticias/vazamento-expoe-dados-de-quem-fez-teste-da-covid-19. Acesso em: 5 out. 2026.

BEATON, D. E. et al. Guidelines for the process of cross-cultural adaptation of self-report measures. **Spine**, v. 25, n. 24, p. 3186-3191, 2000.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 out. 2026.

CANALTECH. **Vazamento de senhas do Ministério da Saúde expõe pacientes da COVID, diz jornal**. Fidel Forato, 26 nov. 2020. Disponível em: https://canaltech.com.br/hacker/vazamento-de-senhas-do-ministerio-da-saude-expoe-pacientes-da-covid-diz-jornal-175307/. Acesso em: 5 out. 2026.

DETERDING, S. et al. From game design elements to gamefulness: defining "gamification". In: **PROCEEDINGS OF THE 15TH INTERNATIONAL ACADEMIC MINDTREK CONFERENCE: ENVISIONING FUTURE MEDIA ENVIRONMENTS**, 2011, Tampere. Anais... New York: ACM, 2011. p. 9-15.

DRESCH, A.; LACERDA, D. P.; ANTUNES JR., J. A. V. **Design Science Research**: método de pesquisa para avanço da ciência e tecnologia. Porto Alegre: Bookman, 2015.

FREDRICKS, J. A.; BLUMENFELD, P. C.; PARIS, A. H. School engagement: potential of the concept, state of the evidence. **Review of Educational Research**, v. 74, n. 1, p. 59-109, 2004.

GWENHURE, A. K.; RAHAYU, F. S. Gamification of cybersecurity awareness for non-IT professionals: a systematic literature review. **International Journal of Serious Games**, v. 11, n. 1, p. 83-99, 2024.

HAMARI, J.; KOIVISTO, J.; SARSA, H. Does gamification work? A literature review of empirical studies on gamification. In: **HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES**, 47., 2014, Hawaii. Anais... IEEE, 2014. p. 3025-3034.

HEVNER, A. R. et al. Design science in information systems research. **MIS Quarterly**, Minneapolis, v. 28, n. 1, p. 75-105, 2004.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. Definições e conceitos de segurança. In: HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018. cap. 3.

KAPP, K. M. **The gamification of learning and instruction**: game-based methods and strategies for training and education. San Francisco: Pfeiffer, 2012.

KNOWBE4. **Learner Experience (LX) Guide**. [S. l.]: KnowBe4, [s. d.]. Disponível em: https://support.knowbe4.com/hc/en-us/articles/360014116634-Learner-Experience-LX-Guide. Acesso em: 5 out. 2026.

KRATH, J. et al. Hexad-12: developing and validating a short version of the gamification user types Hexad scale. In: **CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI '23)**, 2023, Hamburg. Anais... New York: ACM, 2023. art. 677, p. 1-18.

LET'S MONEY. **BC alerta: segurança cibernética precisa sair de TI**. Gabriel Pereira, 19 mar. 2026. Disponível em: https://www.letsmoney.com.br/noticias/bc-alerta-seguranca-cibernetica-precisa-sair-de-ti/. Acesso em: 5 out. 2026.

MEADE, A. W.; CRAIG, S. B. Identifying careless responses in survey data. **Psychological Methods**, v. 17, n. 3, p. 437-455, 2012.

MIRANDA, D.; LI, C.; DARIN, T. UES-Br: translation and cross-cultural adaptation of the User Engagement Scale for Brazilian Portuguese. **Proceedings of the ACM on Human-Computer Interaction**, v. 5, n. CHI PLAY, art. 278, 2021.

NICHOLSON, S. A RECIPE for meaningful gamification. In: REINERS, T.; WOOD, L. C. (Ed.). **Gamification in education and business**. Cham: Springer, 2015. p. 1-20.

O'BRIEN, H. L.; CAIRNS, P.; HALL, M. A practical approach to measuring user engagement with the refined user engagement scale (UES) and new UES short form. **International Journal of Human-Computer Studies**, v. 112, p. 28-39, 2018.

PAHLAVANPOUR, O.; GAO, S. A systematic mapping study on gamification within information security awareness programs. **Heliyon**, v. 10, n. 19, e38474, 2024.

PARSONS, K. et al. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). **Computers & Security**, v. 42, p. 165-176, 2014.

PARSONS, K. et al. The Human Aspects of Information Security Questionnaire (HAIS-Q): two further validation studies. **Computers & Security**, v. 66, p. 40-51, 2017.

PELTIER, T. R. **Information security policies, procedures, and standards**: guidelines for effective information security management. Boca Raton: Auerbach Publications, 2001.

REVILLA, M.; OCHOA, C. Ideal and maximum length for a web survey. **International Journal of Market Research**, v. 59, n. 5, p. 557-565, 2017.

SAILER, M.; HOMNER, L. The gamification of learning: a meta-analysis. **Educational Psychology Review**, New York, v. 32, n. 1, p. 77-112, 2020.

SANTOS, A. C. G. et al. Psychometric investigation of the gamification Hexad user types scale in Brazilian Portuguese. **Scientific Reports**, v. 12, art. 4920, 2022.

SILIC, M.; LOWRY, P. B. Using design-science based gamification to improve organizational security training and compliance. **Journal of Management Information Systems**, v. 37, n. 1, p. 129-161, 2020.

SITZMANN, T. et al. Self-assessment of knowledge: a cognitive learning or affective measure? **Academy of Management Learning & Education**, v. 9, n. 2, p. 169-191, 2010.

TATUM, D. C. **Gamification of security awareness training programs**: a literature review. 2023. Research Paper (Doctor of Science in Information Technology) – School of Computing, Middle Georgia State University, Macon, 2023.

TODA, A. M. et al. A taxonomy of game elements for gamification in educational contexts: proposal and evaluation. In: **IEEE INTERNATIONAL CONFERENCE ON ADVANCED LEARNING TECHNOLOGIES (ICALT)**, 19., 2019, Maceió. Anais... Los Alamitos: IEEE, 2019a. p. 84-88.

TODA, A. M. et al. Analysing gamification elements in educational environments using an existing gamification taxonomy. **Smart Learning Environments**, v. 6, n. 1, art. 16, p. 1-14, 2019b.

TONDELLO, G. F. et al. The gamification user types Hexad scale. In: **ANNUAL SYMPOSIUM ON COMPUTER-HUMAN INTERACTION IN PLAY (CHI PLAY '16)**, 2016, Austin. Anais... New York: ACM, 2016. p. 229-243.

TONDELLO, G. F. et al. Empirical validation of the gamification user types Hexad scale in English and Spanish. **International Journal of Human-Computer Studies**, v. 127, p. 95-111, 2019.

VENABLE, J.; PRIES-HEJE, J.; BASKERVILLE, R. FEDS: a framework for evaluation in design science research. **European Journal of Information Systems**, v. 25, n. 1, p. 77-89, 2016.

VERIZON. **2026 Data Breach Investigations Report**. Verizon Business, 2026. Disponível em: https://www.verizon.com/business/resources/T161/reports/2026-dbir-data-breach-investigations-report.pdf. Acesso em: 5 out. 2026.

WERBACH, K.; HUNTER, D. **For the win**: how game thinking can revolutionize your business. Philadelphia: Wharton Digital Press, 2012.

WHITMAN, M. E.; MATTORD, H. J. **Principles of information security**. 4. ed. Boston: Cengage Learning, 2011.

APÊNDICE A – MATRIZ DE VALIDAÇÃO

Título: **GAMIFICAÇÃO EM *SECURITY AWARENESS*: ENGAJAMENTO E APRENDIZAGEM EM AMBIENTES CORPORATIVOS**
Proposta/Projeto de Pesquisa

Objetivos da pesquisa		***Fundamentação teórica***	***Pontos de Ação*** *O que fazer?* Informações necessárias	***Etapas / Prioridades***	***Resultados Esperados***
Geral	***Específicos***				
Avaliar um aplicativo gamificado de conscientização em segurança da informação voltado a profissionais de áreas não técnicas quanto ao engajamento, em comparação com os treinamentos tradicionais já vivenciados por eles, e quanto à percepção de aprendizado, à variação do conhecimento sobre práticas seguras e à percepção dos elementos de gamificação.	Identificar a percepção e o nível de conhecimento prévio dos participantes em relação aos treinamentos de segurança da informação	Parsons et al. (2014) O'Brien, Cairns e Hall (2018) Santos et al. (2022) Krath et al. (2023)	Aplicar questionário pré-intervenção com escala tipo Likert e questões de conhecimento para mapear o perfil e a percepção inicial dos participantes	Elaborar instrumento; Aplicar com participantes; Tabular respostas	Compreender o ponto de partida dos participantes em relação a conhecimento e experiências anteriores com treinamentos de segurança
	Desenvolver um aplicativo gamificado de conscientização em segurança da informação voltado a profissionais de áreas não técnicas	Kapp (2012) Toda et al. (2019b) Nicholson (2015) Werbach; Hunter (2012) Gwenhure; Rahayu (2024)	Desenvolver um aplicativo educacional gamificado voltado à segurança da informação, com mecânicas alinhadas aos objetivos de aprendizagem e atenção aos riscos da gamificação baseada apenas em recompensas	Prototipar o app; Homologar internamente; Publicar o app	Entregar um artefato funcional, avaliável em condições reais de uso, com mecânicas de engajamento incorporadas
	Comparar o engajamento proporcionado pelo aplicativo com o dos métodos tradicionais já vivenciados pelos participantes e descrever a percepção	O'Brien, Cairns e Hall (2018) Fredricks et al. (2004) Venable, Pries-Heje e Baskerville (2016)	Aplicar questionário pós-intervenção com escala tipo Likert para avaliar engajamento (incluindo usabilidade), percepção de aprendizado e percepção dos elementos de gamificação	Aplicar questionário pós-uso; Analisar respostas; Comparar com dados pré-intervenção	Verificar se o engajamento com o aplicativo supera o relatado para os treinamentos tradicionais e descrever a percepção de aprendizado, os pontos fortes e as limitações do artefato

Objetivos da pesquisa		***Fundamentação teórica***	***Pontos de Ação*** *O que fazer?* Informações necessárias	***Etapas / Prioridades***	***Resultados Esperados***
Geral	***Específicos***				
	de aprendizado com o uso do aplicativo	Silic; Lowry (2020)			sob a perspectiva dos próprios usuários
	Avaliar a variação do conhecimento sobre práticas seguras entre os questionários inicial e final e relacioná-la ao uso registrado do aplicativo, descrevendo também a relação entre o tipo de usuário e o recurso apontado como mais motivador	Hamari et al. (2014) Sailer; Homner (2020) Parsons et al. (2014) Tondello et al. (2016)	Comparar as situações de conhecimento pré e pós-intervenção e relacionar a variação ao uso registrado no aplicativo e cruzar o recurso apontado como mais motivador com os tipos da escala Hexad	Aplicar questionário pré e pós Analisar variação de desempenho Confrontar com dados de uso do app	Identificar se a experiência gamificada se associa a ganho de conhecimento sobre práticas seguras e quais elementos de gamificação foram percebidos como mais motivadores

APÊNDICE B – ANÁLISES DESCRITIVAS DA AMOSTRA

Este apêndice reúne as análises descritivas completas do questionário inicial, com os dados coletados até 19 de outubro de 2026. Os percentuais foram calculados sobre os 26 questionários iniciais válidos, exceto quando indicado, e arredondados para uma casa decimal; por isso, a soma dos percentuais de uma variável pode diferir de 100%. O apêndice será atualizado com os dados do questionário final após o encerramento da coleta.

A Tabela B.1 apresenta o fluxo dos participantes e as regras de qualidade aplicadas às respostas. As Tabelas B.2 a B.4 descrevem o perfil dos participantes, as plataformas de ensino com pontos, medalhas ou ranking que já usaram e o histórico de treinamentos em segurança da informação. A Tabela B.5 apresenta a confiabilidade das escalas, e a Tabela B.6, as estatísticas descritivas dos escores do questionário inicial.

Tabela B.1 – Fluxo dos participantes e qualidade das respostas

Etapa ou regra	n
Responderam ao questionário inicial	27
Excluídos por não marcar a resposta solicitada no item de verificação de atenção	1
Questionários iniciais válidos	26
Responderam ao questionário final	0
Mesma resposta em todos os itens da Hexad (sinalizados, não excluídos)	2
Mesma resposta em todos os itens da UES-SF (sinalizados, não excluídos)	0

Fonte: os autores (2026)

Tabela B.2 – Perfil dos participantes

Variável	Categoria	n	%
Faixa etária	18–24	8	30,8
	25–34	13	50,0
	35–44	2	7,7
	45–54	3	11,5
	55 ou mais	0	0,0
Gênero	Feminino	13	50,0
	Masculino	12	46,2
	Outro	1	3,8
	Prefiro não informar	0	0,0
Escolaridade	Até o ensino médio (completo ou não)	3	11,5
	Superior incompleto	10	38,5
	Superior completo	9	34,6
	Pós-graduação	4	15,4

Variável	Categoria	n	%
Área de atuação	Administrativo	4	15,4
	Financeiro ou contábil	2	7,7
	Recursos humanos	1	3,8
	Comercial ou vendas	5	19,2
	Marketing ou comunicação	5	19,2
	Jurídico	0	0,0
	Atendimento ao cliente	2	7,7
	Operações ou logística	2	7,7
	Outra	5	19,2
Frequência com que joga jogos digitais	Nunca	1	3,8
	Raramente (menos de 1 vez por mês)	6	23,1
	Algumas vezes por mês	6	23,1
	Algumas vezes por semana	7	26,9
	Todos os dias	6	23,1

Fonte: os autores (2026)
Nota: n = 26.

Tabela B.3 – Plataformas de ensino com pontos, medalhas ou ranking já usadas

Plataforma	n	%
Duolingo	23	88,5
Kahoot!	6	23,1
Quizizz	4	15,4
Khan Academy	4	15,4
Treinamento da empresa com pontos, medalhas ou ranking	2	7,7
Outra	4	15,4
Nenhuma	3	11,5

Fonte: os autores (2026)
Nota: n = 26. Pergunta de múltipla escolha; por isso, a soma dos percentuais passa de 100%. Número de plataformas marcadas por participante: nenhuma, 3; uma, 9; duas, 10; três, 2; quatro, 2.

Tabela B.4 – Treinamentos anteriores em segurança da informação

Variável	Categoria	n	%
Já fez treinamento (n = 26)	Sim	14	53,8
	Não	11	42,3
	Não lembro	1	3,8

Variável	Categoria	n	%
Tempo desde o mais recente (n = 14)	Menos de 6 meses	5	35,7
	Entre 6 meses e 1 ano	7	50,0
	Entre 1 e 2 anos	1	7,1
	Mais de 2 anos	1	7,1
	Não lembro	0	0,0
Formato principal (n = 14)	Vídeo ou curso online	10	71,4
	Palestra ou aula presencial	0	0,0
	Material para leitura	2	14,3
	Simulação de e-mail falso (phishing)	0	0,0
	Jogo ou quiz com pontos ou ranking	1	7,1
	Outro	1	7,1
Era obrigatório (n = 14)	Sim	12	85,7
	Não	2	14,3
	Não lembro	0	0,0

Fonte: os autores (2026)
Nota: as perguntas sobre o treinamento mais recente foram feitas apenas aos 14 participantes que já haviam feito algum treinamento; os percentuais dessas perguntas usam esse total.

Tabela B.5 – Confiabilidade das escalas no questionário inicial

Escala	Itens	n	Coeficiente
UES-SF: total	12	14	0,95
UES-SF: atenção focada	3	14	0,94
UES-SF: usabilidade percebida	3	14	0,82
UES-SF: apelo estético	3	14	0,93
UES-SF: recompensa	3	14	0,86
Situações de conhecimento	7	26	0,64

Fonte: os autores (2026)
Nota: alfa de Cronbach para a UES-SF e suas dimensões; KR-20 para as situações de conhecimento, cujas respostas são certas ou erradas.

Tabela B.6 – Estatísticas descritivas dos escores do questionário inicial

Medida	n	Média	DP	Mediana	Q1	Q3	Mín.	Máx.
UES-SF: atenção focada (1–5)	14	2,60	1,23	2,50	1,75	3,50	1,00	5,00
UES-SF: usabilidade percebida (1–5)	14	3,81	0,90	4,00	3,67	4,25	1,33	5,00
UES-SF: apelo estético (1–5)	14	3,31	1,15	3,83	2,50	4,00	1,00	5,00
UES-SF: recompensa (1–5)	14	3,45	1,05	3,50	3,00	4,00	1,67	5,00
UES-SF: total (1–5)	14	3,29	0,96	3,50	2,62	3,81	1,42	5,00
Situações de conhecimento (0–7)	26	5,50	1,53	6,00	4,25	7,00	2,00	7,00
Hexad: filantropo (2–14)	26	12,50	1,45	13,00	11,25	13,75	9,00	14,00

Medida	n	Média	DP	Mediana	Q1	Q3	Mín.	Máx.
Hexad: socializador (2–14)	26	10,19	2,90	11,00	8,25	12,00	4,00	14,00
Hexad: conquistador (2–14)	26	12,04	1,66	12,00	11,25	13,75	8,00	14,00
Hexad: jogador (2–14)	26	11,62	2,00	12,00	10,25	13,00	6,00	14,00
Hexad: espírito livre (2–14)	26	12,58	1,45	13,00	12,00	14,00	9,00	14,00

Fonte: os autores (2026)

Nota: DP = desvio padrão; Q1 e Q3 = primeiro e terceiro quartis. Entre parênteses, o intervalo possível de cada escore. A UES-SF foi respondida apenas por quem já havia feito treinamento e refere-se ao treinamento mais recente.