WRSeg 2024 - 8º Workshop Regional de Segurança da Informação e de Sistemas Computacionais (WRSeg). DOI: 10.5753/errc.2024.4684

ARTIGO COMPLETO/FULL PAPER

Proposta de uma ferramenta para o apoio ao processo de ensino-aprendizagem de cibersegurança

Proposal for a Tool to Support the Cybersecurity Education and Learning Process

Guilherme Goulart • guilhermedomingues.aluno@unipampa.edu.br
Universidade Federal do Pampa (Unipampa)
Érico Amaral • ericoamaral@unipampa.edu.br
Universidade Federal do Pampa (Unipampa)
Marcelo Cordeiro • marcelo_1411@hotmail.com
Universidade Federal do Pampa (Unipampa)
Mateus Soares • mateus123soares@hotmail.com
Universidade Federal do Pampa (Unipampa)
Thiago Leal • thfleal@gmail.com
Universidade Federal do Pampa (Unipampa)

RESUMO. Este artigo apresenta a proposta de um jogo educativo 2D, baseado em RPGs de mesa com o uso de cartas, que simula uma situação de invasão em uma organização empresarial. O objetivo do jogo é promover o ensino de conceitos relacionados à segurança cibernética, com o intuito de auxiliar na formação profissional dos participantes, impulsionando seu processo de aprendizagem e despertando o interesse de mais estudantes para o campo da cibersegurança. Dessa forma, almeja-se aumentar o número de profissionais qualificados no mercado, a fim de suprir a atual escassez de especialistas nessa área específica.

ABSTRACT. This article presents a proposal of a 2D educational game, based on tabletop RPGs using cards, which simulates an invasion situation in a business organization. The objective of the game is to promote the teaching of concepts related to cybersecurity, in order to assist in the professional training of participants, boosting their learning process and awakening the interest of more students in the field of cybersecurity. In this way, the aim is to increase the number of qualified professionals in the market, in order to supply the current shortage of specialists in this specific area.

PALAVRAS-CHAVE: Cibersegurança • Jogos Sérios • Teoria de aprendizagem
KEYWORDS: Cybersecurity • Serious Game • Learning theory

1 Introdução

Ao analisar o mercado de trabalho em cibersegurança, é notável o número crescente de vagas disponíveis em diversas funções, com empresas ao redor do mundo buscando profissionais qualificados. Essa demanda é impulsionada por uma escassez significativa de talentos no setor. O relatório de 2024 da ISC2 (*International Information System Security Certification Consortium*) destaca que a lacuna global na força de trabalho de cibersegurança é de 4,8 milhões de profissionais, representando um aumento de 19% em relação ao ano anterior. Esse dado evidencia a necessidade urgente de expandir a mão de obra especializada para proteger adequadamente as organizações contra ameaças cibernéticas. Além disso, o estudo revela que 90% dos líderes de segurança que participaram da pesquisa reconhecem que a falta de habilidades adequadas expõe suas empresas a riscos consideráveis, o que reforça a necessidade de soluções de ensino eficazes para mitigar este problema [1].

O número de ciberataques está crescendo a uma taxa alarmante, com um aumento de 28% nos ataques no primeiro trimestre de 2024 em comparação ao trimestre anterior, enquanto a oferta de profissionais qualificados para enfrentar essas ameaças não acompanha a demanda [2]. O relatório de 2024 da ISC2 citado anteriormente aponta que, embora a necessidade de especialistas em cibersegurança continue a aumentar, a força de trabalho capacitada teve um crescimento de apenas 0,1% em 2024. Esse crescimento é substancialmente menor quando comparado ao aumento recorde de 8,7% registrado em 2023, o que evidencia a disparidade entre a escalada das ameaças e a formação de profissionais preparados para combatê-las. Esse descompasso entre a necessidade de mão de obra especializada e a oferta disponível está resultando em uma escassez significa-

tiva de profissionais, o que compromete a capacidade das empresas de se protegerem de forma eficaz contra ataques. Sabendo que há uma grande insuficiência de profissionais de cibersegurança no mercado, o presente trabalho traz a proposta de um jogo sério com o objetivo de ensinar tópicos importantes de cibersegurança em sala de aula, assim auxiliando na formação profissional do aluno, em sua construção do aprendizado e atraindo o interesse de mais estudantes para cibersegurança, de modo que cada vez mais profissionais sejam inseridos no mercado, para assim suprir o déficit atual. A cada dia que passa, pessoas mal intencionadas conhecidas como cibercriminosos encontram formas cada vez mais sofisticadas de enganar as pessoas e invadir organizações, geralmente com o objetivo de obter grandes lucros através de seus ataques ou simplesmente causar caos. A sociedade atual necessita de uma linha de frente altamente capacitada e com suficiente número de membros para protegê-la contra estes cibercriminosos.

Para alcançar o objetivo desta pesquisa, o texto está organizado em: (II) metodologia, (III) referencial teórico, (IV) proposta de jogo sério, (V) validação do jogo e resultados e (VI) considerações finais.

2 Metodologia

A classificação desta pesquisa baseado em seu objetivo é a exploratória, pois envolve levantamento bibliográfico e a análise de exemplos que estimulem a compreensão, com o objetivo de proporcionar uma maior familiaridade com o problema com a intenção de torná-lo mais explícito ou a constituir hipóteses [3].

Quanto à classificação da abordagem, a pesquisa busca levantar dados de fontes confiáveis e, na sequência, traz uma aplicação prática e análise dos resultados, coletando e analisando dados tanto do ponto de vista qualitativo quanto quantitativo. Trata-se, portanto, de uma abordagem quali-quantitativa, que interpreta as informações quantitativas por meio de símbolos numéricos e os dados qualitativos por meio da observação, interação participativa e interpretação do discurso dos sujeitos [4].

Em relação a natureza desta pesquisa, trata-se da natureza aplicada, pois existe a necessidade de uma aplicação prática dos conhecimentos obtidos para solucionar o problema inicialmente proposto.

No que diz respeito ao procedimento técnico da pesquisa, esta se caracteriza como uma pesquisa experimental, pois envolve a testagem e avaliação de um novo material educativo e bibliográfico. No entanto, é necessária uma pesquisa bibliográfica adicional em outros materiais para revisar informações e dados que servirão como base para a investigação. Esse tipo de pesquisa requer a aplicação constante de testes da ferramenta, permitindo a coleta de dados tanto quantitativos quanto qualitativos, além da análise dos resultados. O objetivo é possibilitar uma avaliação da ferramenta em relação ao seu propósito e comprovar sua efetividade no ensino proposto.

Para alcançar os objetivos da pesquisa, foi implementado uma metodologia de pesquisa em oito etapas: (I) Definição do problema de pesquisa; (II) Levantamento do referencial teórico; (III) Definição dos requisitos e ferramentas; (IV) Modelagem da solução; (V) Implementação da solução; (VI) Testes e validação; (VII) Análise dos resultados; (VIII) Considerações finais;

A coleta de dados foi realizada por meio de dois experimentos com protótipos do jogo, seguido da aplicação de um formulário de avaliação com 16 perguntas, baseado no modelo de Savi et al. (2010), que integra elementos dos frameworks de Kirkpatrick, ARCS, UX em jogos e a Taxonomia de Bloom. Esse modelo visa avaliar a eficácia educacional do jogo, captando dados qualitativos e quantitativos [5]. O processo de validação envolveu análise dos questionários e observação do desempenho dos participantes, com ajustes no jogo feitos com base no feedback. No entanto, o processo de validação ainda não foi totalmente finalizado, tendo em vista que há planos para futuros testes onde um questionários envolvendo perguntas de cibersegurança será disponibilizado para os participantes antes e depois de uma partida, para assim comparar a taxa de acertos e ver se existe uma melhoria no aprendizado. A análise dos dados qualitativos e quantitativos permitiu identificar melhorias e medir a percepção dos alunos sobre o jogo.

3 Referencial teórico: Cibersegurança, teorias de aprendizagem e correlatos

As organizações precisam de meios eficazes para proteger o ativo mais importante: a informação. A segurança da informação, formada por orientações, normas, políticas e procedimentos, visa garantir a proteção dos dados e minimizar o risco de roubo e danos à empresa. Segundo a norma ABNT NBR ISO/IEC 27001:2013, a segurança da informação é essencial para a continuidade dos negócios, mitigando riscos e maximizando o retorno sobre investimentos. Ela protege dados críticos contra ameaças, assegurando que a informação correta e disponível seja usada de forma eficiente, evitando perdas que possam prejudicar o funcionamento da organização e afetar sua imagem publicamente devido a incidentes de segurança [6].

Teorias de aprendizagem, também conhecidas como ciência do comportamento humano [7], são uma área que estuda as formas de aprendizagem do ser humano, levando em conta suas particularidades como desenvolvimento motor, efetivo e cognitivo [8]. No seguinte trabalho, foram utilizadas três teorias de aprendizagem para a criação da dinâmica do jogo sério: A teoria construtivista de Jerome Bruner que destaca a interação entre professor e aluno, com o aluno adquirindo conhecimento de forma autônoma, mas recebendo orientação do professor quando necessário [9], a teoria sociocultural de Lev Vygotsky que enfatiza a importância da interação social no desenvolvimento do indivíduo, afirmando que o conhecimento surge primeiro no grupo e depois é internalizado pelo indivíduo [7] e a aprendizagem baseada em problema (PBL) que incentiva a resolução de problemas em grupo como forma de construção do conhecimento, em contraposição ao ensino passivo em sala de aula [10].

A fim de identificar o estado da arte dos trabalhos que atualmente estão sendo publicados, nesta pesquisa identificou-se quatro trabalhos principais que estão alinhados com a área de ferramentas voltadas ao ensino, sendo eles o *Creative Journey*, TH3_0FF1C3, *Control-Alt-Hack* e *Backdoors & Breaches*, com este ultimo sendo a principal fonte de inspiração para o presente trabalho.

O trabalho de Maria Elizabeth Bárcena Silva nomeado de "*Creative Journey*: Uma Ferramenta de Auxílio ao Ensino de Lógica e Programação para Crianças" apresenta um game de aventura 2D que serve como uma ferramenta de auxílio em sala de aula para o ensino de lógica e programação para crianças. A autora utiliza conceitos de teorias de aprendizagem e gamificação, além de metodologias específicas voltadas para o desenvolvimento de jogos sérios como a *Digital Game Based Learning -Instructional Design* (DGBL-ID) e a *Design, Play, and Experience* (DPE) para construir uma ferramenta de ensino competente, sendo capaz de atingir o objetivo que foi proposto, servindo como uma ferramenta de auxílio ao ensino de lógica e programação para crianças do ensino fundamental [11].

A dissertação de pós-graduação de Francis Mallmann Schappo nomeada "TH3_0FF1C3: Um jogo de tabuleiro educacional para o ensino de conceitos da segurança da informação" realiza a apresentação de um jogo de tabuleiro físico, tendo como objetivo principal o desenvolvimento do aprendizado de alunos para tópicos relacionados a segurança da informação. Nele os estudantes fazem parte de uma empresa fictícia recém contratada, eles devem coletar recursos e controlar os ataques virtuais para vencer. Os jogadores devem trabalhar em conjunto para que o nível de ameaças virtuais não chegue no máximo, pois se ele chegar significa que o servidor central da empresa está totalmente exposto para um ataque. Este trabalho utiliza o que é chamado de atividade desplugada, que seria uma atividade que não requer o uso de qualquer tipo de dispositivo eletrônico para ser executada. Como esse trabalho foi desenvolvido durante a pandemia, o autor Francis Schappo também sentiu a necessidade de criar uma versão digital do game, porém o foco dele sempre foi a versão física. O jogo de tabuleiro foi aplicado no curso de Sistemas de Informação na disciplina de Segurança e Auditoria de Sistemas de Informação na Instituição Antônio Meneghetti Faculdade (AMF), com os participantes tendo idades entre 18 e 29 anos. O jogo sério obteve resultados positivos quanto a sua eficiência no ensino dos tópicos abordados durante as partidas [12].

O *game Control-Alt-Hack*, com sua mecânica de jogo sendo desenvolvida pela empresa Steve Jackson Games, é um jogo de cartas sobre os "hackers do chapéu branco" ou "hackers éticos", que são hackers que trabalham para empresas tentando identificar possíveis vulnerabilidades em seus sistemas. As organizações contratam esses hackers para que eles utilizem todo o seu conhecimento para invadir os sistemas, porém sem causar qualquer dano, já que o objetivo é apenas expor falhas de segurança. O game é dividido em diversas missões, onde os jogadores necessitam utilizar todo seu conhecimento de hacking para atingir o objetivo final e vencer [13].

O jogo *Backdoors & Breaches* (B&B), desenvolvido pela *Black Hills Information Security* e pela *Active Countermeasures*, é um *card game* de resposta a incidentes que visa conduzir diversos exercícios relacionados à segurança da informação. Seu propósito é testar a eficiência dos profissionais contratados e treiná-los para detectar diferentes situações de incidentes que podem ocorrer dentro da organização, além de estabelecer políticas de segurança para evitar possíveis brechas no sistema de defesa da empresa. O foco deste jogo sério está voltado para o ambiente profissional, avaliando a eficácia da equipe de segurança da organização em que está sendo aplicado [14].

A ferramenta de apoio ao processo de ensino-aprendizagem em cibersegurança que está sendo desenvolvida utiliza diversos conceitos de *Backdoors & Breaches*, no entanto, embora fortemente inspirada em B&B, essa ferramenta é totalmente adaptada para o ambiente escolar, com o objetivo de aprimorar a formação dos estudantes, atrair novos alunos para a área de cibersegurança e auxiliar os professores na sala de

aula, mantendo a atenção dos discentes e facilitando a interação entre aluno e professor.

4 Proposta de jogo sério

Don't Get Hacked (DGH) é um jogo educativo com foco em cibersegurança, que proporciona a seus jogadores novas formas de aprendizado. A ferramenta estimula a interação dos jogadores provendo inspiração para um cenário de invasão ao professor utilizando quatro cartas de diferentes categorias, com a narrativa sendo algo original construído pelo próprio docente no começo de cada partida. O professor age como um narrador e fonte de informações, enquanto que os alunos, divididos em até três equipes de cinco membros, agem como funcionários da empresa que foi invadida, tentando identificar como essa invasão aconteceu. O *game* pode ser utilizado em ambientes educacionais como escolas e universidades, para ensinar conteúdos importantes de forma divertida e efetiva, permitindo ao professor analisar o nível de conhecimento individual ou geral da turma, identificar possíveis dificuldades e induzir os alunos a utilizarem seus conhecimentos de forma ativa, fornecendo uma aplicação prática com diversos possíveis cenários para os alunos testarem seus conhecimentos, fugindo da rotina padrão das salas de aula onde muitas vezes o aluno não aplica em situações reais o conhecimento adquirido.

Como ilustra a Figura 1, DGH é composto por seis tipos diferentes de cartas, sendo quatro deles utilizados para a construção da narrativa, um para aplicar efeitos específicos na dinâmica do jogo e o azul sendo os procedimentos aos quais os defensores tem acesso, utilizado para revelar as quatro cartas usadas na construção da narrativa. As cartas são baseadas no formato de cartas do *Backdoors & Breaches* [14]. O objetivo dos defensores é, atraves de perguntas e discussões, além de dicas dadas pelo professor, executar procedimentos para identificar as quatro cartas da narrativa. Cada equipe possui sua própria rodada para realizar uma pergunta ao professor e tentar executar um procedimento, com essa tentativa envolvendo a justificativa com o motivo pelo qual a equipe deseja executar aquele procedimento, além da rolagem de um dado de 20 lados para definir se o procedimento será executado ou algum imprevisto acontecerá durante a execução. Após a equipe realizar uma pergunta para o professor e selecionar o procedimento que deseja executar, o professor escolherá um membro da equipe para explicar a lógica por trás da escolha, incentivando os alunos a prestarem mais atenção no jogo e realizarem trocas de conhecimento entre si, além de permitir que o professor avalie o conhecimento do aluno selecionado. Caso o aluno selecionado não seja capaz de prover uma explicação que faça sentido com os detalhes inicias da narrativa apresentada e todas as informações adquiridas através de perguntas durante a partida, o professor poderá finalizar a rodada sem que a equipe seja capaz de executar o procedimento. Vence a equipe que revelar o maior número de cartas.

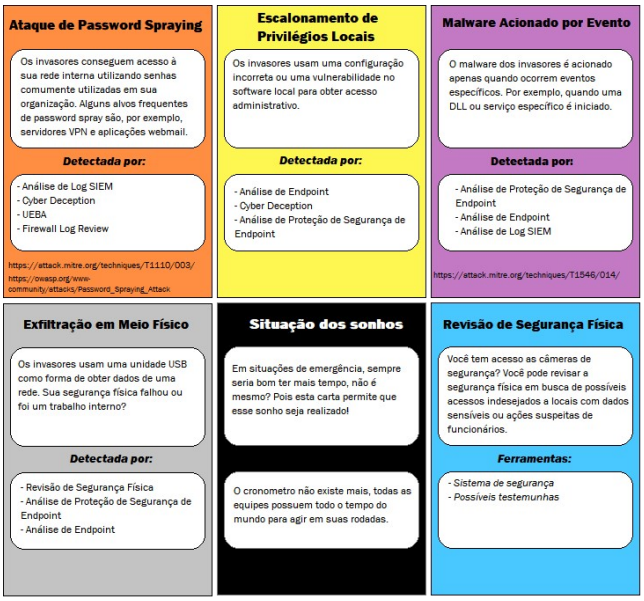

Figura 1. Exemplo de Cartas (Protótipo)

O jogo está sendo desenvolvido na *engine Unity* que é uma *engine* de desenvolvimento de jogos baseada em *scripts*, utilizando a linguagem C# para o desenvolvimento dos *scripts*, Node.js para o servidor que permite a interação com o banco de dados, e a *API Mirror* para a implementação do *multiplayer peer-to-peer*. Contará também com um banco de dados MySQL para armazenar informações de contas e sugestões de narrativas acessíveis a outros usuários. A versão digital de DGH está atualmente em desenvolvimento, com a maior parte de seus assets já definidos, suas dinâmicas e regras estabelecidas e seus elementos de prototipação como requisitos funcionais e não funcionais, diagramas de sequência, casos de uso e diagrama entidade relacionamento já estabelecidos. A previsão de conclusão da versão digital é para o primeiro trimestre de 2025.

A Figura 2 apresenta um exemplo de um dos elementos de prototipação do sistema do jogo, sendo este o diagrama de sequência referenciando algumas telas e *scripts* contidos na *Unity*. Esse diagrama captura, de forma simplificada e adaptada para o sistema de scripts da unity, todas as ações que ocorrem em uma rodada completa de *Don't Get Hacked*, visto da perspectiva do jogador classificado como professor.

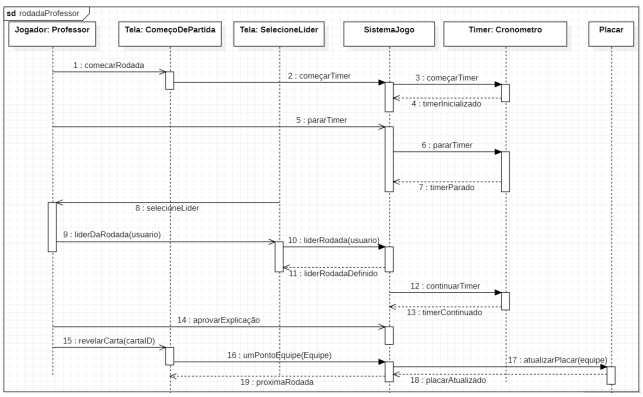

Figura 2. Diagrama de sequência adaptado (rodada inteira como professor)

5 Experimentos iniciais e resultados

Para realizar uma validação inicial da proposta do jogo sério e testar suas mecânicas e dinâmicas, além de coletar um *feedback* inicial sobre categorias importantes, como relevância do conteúdo, nível de interesse dos alunos, diversão e eficácia no ensino, foram realizados dois experimentos utilizando protótipos do jogo. Participaram um total de onze alunos do curso de engenharia de computação da Unipampa Campus Bagé, que jogaram uma partida completa de DGH. Os alunos foram divididos em até três equipes e a partida foi conduzida por um profissional da área de cibersegurança, que atuou como professor.

Ao final de cada partida, um formulário foi enviado aos participantes, contendo dezesseis perguntas baseadas em um modelo de avaliação de jogos educativos proposto por Savi et al. (2010). Esse modelo integra elementos do *framework* de avaliação de treinamentos de Kirkpatrick, o ARCS, UX em jogos e a Taxonomia de Bloom, definindo quais características seriam utilizadas para criar um modelo próprio e mais abrangente de avaliação de jogos educacionais [5]. As perguntas do formulário apresentavam três opções de resposta: 'sim', 'não' e 'outros'. A terceira opção foi incluída para permitir que os participantes fornecessem respostas mais detalhadas ou intermediárias, caso tivessem uma opinião mista ou desejassem elaborar mais suas respostas. A última pergunta consistia em um espaço livre para comentários sobre a experiência e sugestões de melhorias, não incluindo as opções 'sim' e 'não'. Além disso, foi realizada uma roda de conversa ao final de cada teste. Alguns resultados e questões estão ilustrados na Figura 3, onde "sim" representa tanto a seleção da opção correspondente quanto respostas positivas dos participantes que optaram por "outros". Por outro lado, "não" abrange tanto a escolha dessa opção quanto respostas negativas por escrito em "outros".

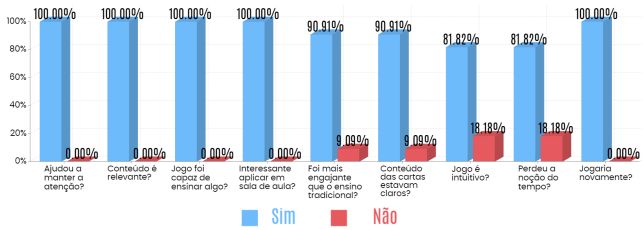

Figura 3. Questionário: Exemplos e alguns resultados

Com base no *feedback* dos experimentos, diversas alterações foram feitas na dinâmica e no conteúdo de DGH. Para tornar as partidas mais rápidas, foi introduzido um limite de tempo de 1 minuto e 30 segundos por rodada e alterado o critério de sucesso da rolagem de dado, que passou a exigir um valor acima de 5, em vez de 10, reduzindo a taxa de falhas de 50% para 25%, eliminando a alta frustração entre os jogadores. A duração de uma partida completa, que no primeiro teste durou cerca de 60 minutos, foi reduzida para 35 minutos após esses ajustes. O cronômetro incentivou as equipes a se prepararem de forma mais eficiente, além de ter aumentado a imersão ao criar uma sensação de urgência em meio a um incidente. Ajustes ocorreram no conteúdo das cartas, visando melhorar a clareza, e um manual foi desenvolvido para facilitar o aprendizado prévio. Além disso, efeitos nas rolagens de dado foram testados, onde a equipe recebia alguma vantagem ao rolar números ímpares ou 20. No entanto, esses efeitos foram removidos após o segundo teste, pois os jogadores os ignoraram por ser muito confuso. Nos questionários de feedback, 100% dos participantes afirmaram que o jogo é interessante, mantém a atenção, aborda tópicos relevantes e é aplicável em sala de aula, além de preferirem-no em relação ao modelo tradicional de ensino. Todos também afirmaram que o jogo foi divertido e que jogariam novamente.

6 Considerações finais

Embora a ferramenta digital ainda não esteja finalizada, os dados coletados nos testes iniciais indicam que ela tem grande potencial como ferramenta de ensino de cibersegurança. O jogo se mostrou eficaz em engajar os alunos, oferecendo uma maneira divertida de aprender conceitos da área. Contudo, o processo de validação não foi concluído, pois estão previstos testes futuros que incluirão questionários de cibersegurança sendo aplicados antes e depois das partidas, permitindo comparar a taxa de acertos e avaliar possíveis melhorias no aprendizado dos participantes.

Declarações complementares

Referências

1 (ISC)². *ISC2 Cybersecurity Workforce Study (2024)*. 2024. Disponível em: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study. Acesso em: 31 out. 2024.

2 Intelligence, C. *Report Shows Record Increase in 2024 Cyber Attacks*. 2024. Disponível em: https://www.cybersecurityintelligence.com/blog/report-shows-record-increase-in-2024-cyber-attacks-7607.html. Acesso em: 15 nov. 2024.

3 Gil, A. C. *Como Elaborar Projetos De Pesquisa*. 4. ed. São Paulo: Atlas S.A., 2002.

4 Do Rosario Knechtel, M. *Metodologia Da Pesquisa Em Educação: Uma abordagem teórico-prática dialogada*. Intersaberes, 2014. ISBN 9788582129005.

5 Savi, R. *et al.* Proposta de um modelo de avaliação de jogos educacionais. *Renote*, v. 8, n. 3, 2010.

6 Fontes, E. *Segurança da informação*. Saraiva Educação S.A., 2017. ISBN 9788502122192. Disponível em: https://books.google.com.br/books?id=FyprDwAAQBAJ.

7 Aposo, R.; Vaz, F. *Introdução as Teorias de Aprendizagem*. 2002. Disponível em: http://www.nce.ufrj.br/ginape/publicacoes/trabalhos/t_2002/t_2002_renato_aposo_e_francine_vaz/teorias.htm. Acesso em: 19 out. 2024.

8 Santos, J. A. S. Teorias da Aprendizagem: comportamentalista, cognitivista e humanista. *Revista Sigma*, v. 2, p. 97–111, 2006.

9 Marques, R. *A pedagogia de Jerome Bruner*. 2002. Disponível em: http://www.eses.pt/usr/Ramiro/docs/etica%5C_pedagogia/A%5C%20Pedagogia%5C%20de%5C%20JeromeBruner.pdf. Acesso em: 12 set. 2022.

10 Sebrae. *Conheça o que é PBL, o ensino basedo em problemas*. 2019. Disponível em: https://cer.sebrae.com.br/blog/pbl-o-ensino-baseado-em-problemas/. Acesso em: 17 set. 2022.

11 Silva, M. E. B. CREATIVE JOURNEY: Uma Ferramenta de Auxilio ao Ensino de Logica e Programação Para Crianças. *Curso de Engenharia de Computação, Universidade Federal do Pampa*, p. 129, 2022.

12 Schappo, F. M. TH3_0FF1C3: Um Jogo de Tabuleiro Educacional Para o Ensino de Conceitos da Segurança da Informação. *Mestrado em Tecnologias Educacionais em Rede, Universidade Federal de Santa Maria*, p. 161, 2022.

13 Denning, T. *et al.* Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. *In*: PROCEEDINGS of the 2013 ACM SIGSAC conference on Computer & communications security. 2013. P. 915–928.

14 Security, Black Hills Information and Countermeasures, Active. *Backdoors & Breaches*. 2019. Disponível em: https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/. Acesso em: 1 set. 2022.