Artículo Original

Th3_0ff1c3: Um jogo de tabuleiro educacional para o ensino de conceitos da segurança da informação

Th3_0ff1c3: an educational board game for teaching information security concepts

Francis Mallmann Schappo[1], Roseclea Duarte Medina[1]

[1] Universidad Federal de Santa María, Santa Maria - RS, Brasil

francismallmann@gmail.com, roseclea.medina@gmail.com

Recibido: 08/12/2022 | **Corregido**: 26/09/2023 | **Aceptado**: 16/11/2023

Cita sugerida: F. Mallmann Schappo, R. Duarte Medina, "Th3_0ff1c3: Um jogo de tabuleiro educacional para o ensino de conceitos da segurança da informação," *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología*, no. 38, pp. 88-95, 2024. doi:10.24215/18509959.38.e9.

Resumo

Este artigo apresenta um jogo de tabuleiro educacional moderno com a temática de Segurança da Informação chamado de Th3_0ff1c3, o jogo simula ataques por vários tipos de Malwares e de ações de criminosos virtuais. Se trata de um jogo de tabuleiro de estratégia baseada em turnos onde os alunos precisam trabalhar colaborativamente na defesa de um grande escritório contra Malwares e ação de ataques virtuais. O jogo se destaca pela grande interação entre os jogadores e a capacidade de elucidar diversos conceitos de Segurança da Informação.

Palavras chaves: Tecnologia educacional, segurança da informação, lgpd, jogo de tabuleiro, th3_0ff1c3.

Abstract

This paper presents a modern educational board game with the theme of Information Security called Th3_0ff1c3, the game simulates attacks by several types of Malware and cybercriminal actions. It is a turn-based strategy board game where students need to work collaboratively in defending a large office against Malware and cyber-attack action. The game stands out for the great interaction between players and the ability to elucidate various concepts of Information Security.

Keywords: Educational technology, Information security, LGPD, Board game, Th3_0ff1c3.

1. Introdução

A sociedade atual tem se transformado em um ritmo acelerado e dinâmico pelas novas Tecnologias de Informação e Comunicação (TIC), que afetam diretamente as áreas sociais, políticas e econômicas.

A grande rede mundial de computadores (Internet), foi a realização tecnológica essencial para as bases do conhecimento da sociedade atual, sendo a ferramenta mais utilizada para a troca de conhecimentos.

Para Castells [1], a Internet é uma ferramenta de comunicação que revolucionou a forma dos indivíduos interagirem e se socializarem. Esse formato de interação e socialização é conhecido como sociedade em rede ou sociedade da informação.

A Internet nasceu como um ambiente livre para a troca de informações entre as pessoas, com o grande volume de informações e dinamicidade da grande rede é fácil comprometer a segurança da informação (SI) de cada usuário de um dispositivo eletrônico conectado.

A SI tem um papel cada vez mais central na preocupação das empresas e usuários domésticos, os conceitos de segurança virtual têm trazido muitas dúvidas para as

pessoas que utilizam dispositivos eletrônicos na Internet, e com cada vez mais ataques elaborados por criminosos virtuais com as mais variadas motivações. Atualmente existem uma variedade de ferramentas virtuais para a quebra da segurança virtual, como vírus, cavalos de Tróia, Phishing, sniffers, DDOS, os temidos Ransomwares, entre outros. Como exemplo os Ransomwares têm tido um papel central na mídia nos últimos tempos, segundo Kaspersky [2] estimou-se que haveria um ataque de Ransomware a cada 11 segundos em 2021 causando até 20 bilhões de dólares em prejuízos, principalmente devido à utilização cada vez maior da internet. A cada dia, os cibercriminosos encontram maneiras mais sofisticadas de enganar os internautas e obter lucros maiores com seus ataques.

Vivemos em uma sociedade dependente da tecnologia e cada vez mais conectada, com seus smartphones, computadores e equipamentos de Internet of Things (IoT) ou Internet das Coisas. Essa dependência atrai a atenção de criminosos que buscam uma vantagem de roubar dados, interromper serviços e roubar riquezas.

Segundo Kayworth e Whitten [3], nenhuma solução ou mecanismo tecnológico é suficiente para garantir a eficácia da segurança da informação nas organizações, pois esta eficácia só pode ser atingida através da aplicação de uma estratégia corporativa de segurança que envolva aspectos técnicos e sociais.

Este trabalho tem como finalidade auxiliar no conhecimento para usuários finais de como identificar possíveis ataques e métodos de prevenção, evitando assim maiores prejuízos. Como produto foi desenvolvido um jogo de tabuleiro educacional moderno sobre segurança da informação.

2. Metodologia, material e métodos

Este trabalho de pesquisa classifica-se por ser do tipo aplicada, que se caracteriza pela geração de conhecimento com uma aplicação prática e imediata, buscando a solução de problemas específicos que é de geral interesse das pessoas envolvidas.

Neste capítulo é elucidado todo o processo de elaboração do trabalho e sua metodologia e foi realizado em algumas etapas: Pesquisa, desenvolvimento, aplicação e análise de resultados.

O processo de pesquisa foi realizado com um processo de revisão sistemática da literatura (RSL), conforme Kitchenham [4], a revisão sistemática da literatura é uma pesquisa metodologia onde todos os estudos empíricos sobre um determinado tópico são agregados de forma sistemática, facilmente repetível e imparcial. Este processo permite uma melhor compreensão do assunto e fornece respostas para questões de pesquisa relacionadas a ele.

No processo de buscas foi utilizado um software gratuito de apoio chamado de Publish or Perish [5] onde foi configurado os critérios de inclusão e exclusão de artigos científicos, revistas, livros e sites. A busca teve como palavras chaves os termos para inclusão na busca de artigos as seguintes palavras: “segurança da informação”, “cyber segurança”, “cyber security”, “educational boardgames”, “tabuleiros educacionais”, “jogos de tabuleiro modernos”. Também foi configurado como inclusão de buscas os artigos publicados entre os anos de 2015 até 2021.

Como critério de exclusão foi especificado artigos publicados abaixo do ano de 2015 e sem as palavras chaves contidas na busca. As buscas foram realizadas nos portais de pesquisa como Web of Science, SBGames, IEEE Xplore, IEEE Educon, Scielo, Scopus, Google Acadêmico, ACM Digital Library e Science Direct.

Pela conclusão da pesquisa foi desenvolvido uma ferramenta em forma de jogo de tabuleiro moderno que utiliza conceitos da segurança da informação, o jogo de tabuleiro se aplica para usuários com e/ou sem conhecimento nas áreas da computação, o produto foi desenvolvido com material digital e impresso. As informações foram produzidas da forma mais clara e acessível a todos os níveis de usuários.

A aplicação realizou-se utilizando o jogo de tabuleiro Th3_0ff1c3 no formato digital em um ambiente para jogos digitais e na forma desplugada utilizando o tabuleiro físico do jogo que apresentou alguns conceitos de boas práticas da segurança da informação, como questões de malwares, incidentes de segurança, percas financeiras e de dados por ataques virtuais, entre outros. O trabalho foi aplicado e testado em uma turma de nível superior do 8º semestre na disciplina de Segurança e Auditoria de Sistemas de Informação do curso de Bacharelado em Sistemas de Informação na Antônio Meneghetti Faculdade – AMF que se situa na cidade de Restinga Seca no Estado do Rio Grande do Sul.

A aplicação foi realizada no dia 05 de junho de 2021, a turma teve um total de 8 alunos participantes durante a execução da aplicação do jogo de tabuleiro. A aplicação foi realizada durante a manhã com o início da disciplina as 8h e finalizado as 12h.

Durante o processo de aplicação inicialmente foram executados um questionário demográfico e uma avaliação de conhecimento inicial para a aquisição de dados dos participantes. Após os questionários iniciais, foi realizada uma breve explicação sobre o trabalho da pesquisa e demonstração de jogos de tabuleiro modernos como o Catan e o Mansion of Madness, após isso foi realizado a explicação de regras e mecânicas do jogo de tabuleiro Th3_0ff1c3, em sequência foi realizada a execução do jogo de tabuleiro Th3_0ff1c3 na forma física e digital.

Ao finalizar o jogo, foi aplicado novamente o questionário da avaliação e a ferramenta de avaliação de jogos educacionais MEEGA+ [6].

3. Desenvolvimento do jogo de tabuleiro Th3_0ff1c3

Nesta seção são apresentados os principais aspectos do jogo educacional desenvolvido. Como características principais planejadas para o jogo de tabuleiro foram construídas para que o jogo deve ser jogável entre 2-4 pessoas, com a idade de pessoas com mais de 14 anos. O jogo deve também ser aplicável em um tempo aproximado de 45 minutos, o equivalente a uma hora/aula em média, ele deve ser um jogo não digital para possibilitar a jogada sem uso de computadores, estimulando também a interação social entre as pessoa e que também tenha uma versão digital, para ser utilizada em modalidades de cursos não presenciais, atendendo aos protocolos da pandemia da Covid-19. O jogo também foi criado tendo em suas mecânicas, regras ou elementos que façam com que haja cooperação entre os componentes, e que consigam não ser derrotados pela mecânica do jogo e que haja cooperação entre os jogadores para elaborar estratégias e a construção do conhecimento deles.

O jogo de tabuleiro foi montado em mesa conforme figura 1, disposto para 4 jogadores, com a montagem dos hexágonos adicionando primeiro o hexágono correspondente ao servidor central na mesa de jogo e adicionando adjacentes os outros hexágonos em sentido anti-horário por cada jogador. Formando um espiral até o último hexágono ser posto em mesa.

Figura 1. Tabuleiro montado

Após a montagem inicial do jogo de tabuleiro é iniciado a sequência da mecânica do jogo que pode ser vista da figura 2 com o fluxograma da sequência de um turno completo dentro do jogo.

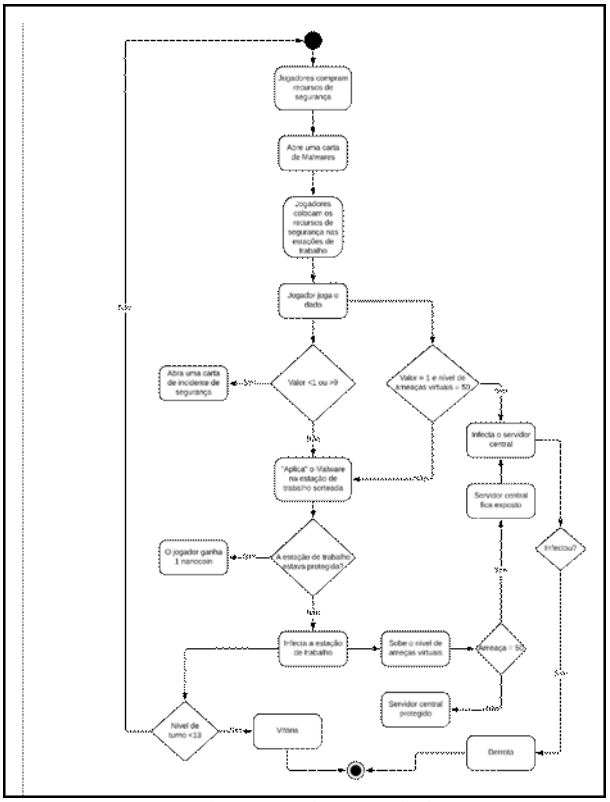


Figura 2. Fluxograma de sequência de um turno

Para um melhor entendimento das mecânicas e temáticas do jogo educacional de tabuleiro está listado na tabela 1 as principais características do jogo.

Tabela 1. Características do jogo

Características do jogo	
Objetivo do jogo	O jogador vai escolher a empresa de segurança que irá representar e terá que resolver os problemas que se apresentarão em cada turno.
Gênero	Estratégia e administração de recursos.
Plataforma	Jogo não-digital de tabuleiro.
Modo de interação	Jogo *multiplayer* híbrido cooperativo e competitivo.
Regras	Em cada início de turno, um jogador irá retirar uma carta de malware do topo que mostrará o tipo de ataque virtual que irá ocorrer na rodada, cada jogador decidirá onde investir e aplicar os recursos de segurança (representados por tokens) em suas respectivas cores nos hexágonos que representam baias de trabalho com computadores. Após aplicada as medidas de segurança é jogado um dado D10, onde o número que for

	sorteado será o número do computador atingido, ou o IP do computador atacado. Se o computador estiver protegido pelo recurso de segurança, o jogador irá receber 1 nanocoin por cada defesa bem-sucedida. Se não conseguir proteger o computador, o malware irá causar o prejuízo ao jogador ou aos jogadores. Se o dado cair no número 0, será revelada uma carta de incidentes de segurança durante a rodada. A cada infecção bem-sucedida por ataques de malwares a barra de nível de ameaças irá subir, e se chegar ao máximo, o servidor central estará exposto a ataques virtuais, se ele for infectado todos perdem o jogo. O jogo termina em 13 turnos (0-12).
Mecânica	O jogo se desenvolve em turnos, onde os jogadores devem administrar seus recursos resolvendo os problemas de segurança utilizando seus tokens e comprando novos recursos, usando seus "nanocoins".
Narrativa	O jogo começa com cada jogador escolhendo sua empresa, após começa a montagem do tabuleiro, onde o servidor central é o hexágono com o IP 192.168.0.1 que ficará centralizado no tabuleiro, depois em sentido anti-horário cada jogador colocará um hexágono, até que todos os hexágonos estejam inseridos no tabuleiro.
Recursos do jogo	Botões que representam "nanocoins" Tokens de Recursos de Segurança
Personagens	
	Os personagens são os jogadores que representam 4 empresas de segurança e os atacantes virtuais que são anônimos, representados pela mecânica do jogo.
Outros elementos do jogo	
Hexágonos	Compõem o tabuleiro com 4 cores distintas, vermelho, amarelo, azul e verde.
Cartas de Malwares	Representam os ataques virtuais contra a empresa.
Cartas de Incidentes de Segurança	Cartas que causam modificações dentro ou no próximo turno.
Token de Malwares	Representam a ameaça sorteada na compra da carta de malware, são colocadas em cima do hexágono sorteado.
Token de Recurso de Segurança	Representam uma defesa, ou imunização contra o ataque causado por Malware.
Vitória, derrota e feedback educacional	
Critérios de vitória	A vitória ocorrerá no final do 13º turno.
Critérios de derrota	A derrota irá acontecer se o servidor foi infectado por um malware.
Feedback educacionais ao jogador	O jogo não fornece feedback ao jogador durante o jogo. O feedback ocorre ao final do jogo, em uma discussão entre jogadores e professor sobre o resultado do jogo.

3.1 A simulação dos ataques virtuais e suas defesas

O jogo de tabuleiro Th3_0ff1c3 simula um escritório que é formado por hexágonos, na qual, cada hexágono é uma baia de trabalho, que contém um usuário utilizando um computador.

Durante a execução do jogo este computador está conectado a uma rede fictícia, que é formado por faixas de IPs. Cada jogador escolhe sua cor e consequentemente uma faixa de IP no início do jogo.

Como por exemplo o jogador vermelho, recebe sua faixa de IP com o endereço 192.168.1.1 até o intervalo 192.168.1.9, que pode ser visto na figura 3.

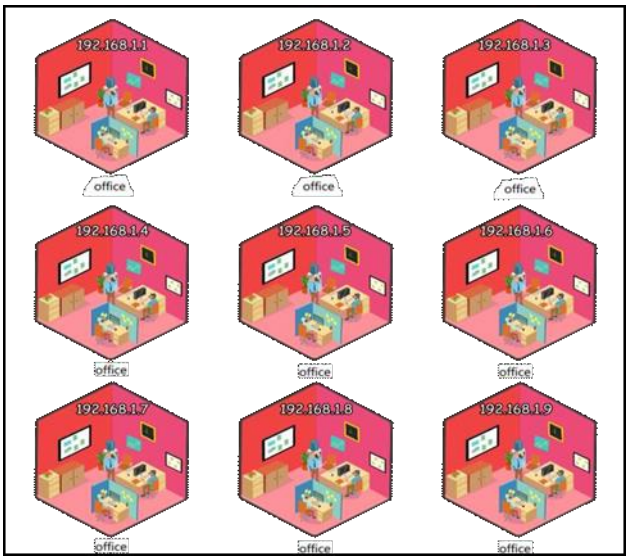


Figura 3. Hexágonos correspondentes ao jogador vermelho

As hexágonos seguem a construção com o jogador verde recebendo a faixa de IP 192.168.2.1, o jogador amarelo que recebe o IP inicial 192.168.3.1 e o jogador azul recebe o IP inicial 192.168.4.1.

No início de um turno de jogo, cada jogador deve decidir quais defesas devem ser aplicadas durante a rodada, utilizando seus recursos eles podem aplicar um treinamento contra Phishing para o funcionário fictício, para que ele consiga identificar e não cair em um ataque de Phishing trazendo prejuízos para a empresa. O jogador pode investir em um antivírus para que o computador não seja infectado

por um vírus, sendo necessário um gasto adicional para a desinfecção do computador. A atualização do sistema operacional para dificultar a infecção por Malwares do tipo Worms, que podem infectar e depois tentar infectar outras baias não atualizadas explorando falhas de software. O jogador também pode optar por se defender contra Spywares utilizando um antispyware que protege contra prejuízos financeiros para cada início de turno. O jogador poderá optar pelo uso de um firewall para dificultar o uso de Cavalos de Tróia pelos atacantes, que se infectado abre portas ocorrendo prejuízos para o jogador e por fim o jogador poderá optar pelo uso de um Backup de sistema, podendo defender o computador contra um ataque de Ransomware, sendo possível uma rápida recuperação da baia de trabalho.

Após a aplicação dos recursos de segurança e defesas contra-ataques virtuais, um dos jogadores deve pegar uma carta de Malwares e ler em voz alta a ação dela durante a rodada, os computadores que serão atacados são sorteados durante o lançamento do dado. As cartas de Malwares podem ser vistas na figura 4.

Figura 4. Cartas de ação dos Malwares

Também para aumentar a complexidade do jogo, foi desenvolvido cartas de incidentes de segurança, que podem modificar o turno, a mecânica e estratégias. As cartas de incidentes de segurança são ativadas quando o jogador que jogar o dado ter um número fora da faixa de IP, que pode ser o número 0 ou o número 10, dependendo do dado utilizado.

Os ataques que podem ocorrer durante um incidente de segurança pode ser o ataque por uso de dispositivos conhecidos como Bad USB que trará prejuízos financeiros para todos os jogadores. O jogador também poderá retirar a carta de ataque por DDOS que irá trazer prejuízos financeiro para o escritório, diminuindo os pagamentos para cada jogador. Ou também poderá ser uma carta de um vírus mutável que irão aumentar o número de Malwares que irão atacar o escritório durante o turno e uma temida falha do Dia Zero, que irá deixar exposto o servidor central da empresa, que se for infectado irá encerrar o jogo e todos os jogadores irão ser derrotados.

As mecânicas de cartas tentam simular os vários tipos de ataques virtuais existentes e trazem a aleatoriedade que pode ocorrer durante um ataque virtual, onde as pessoas não esperam ser atacadas e sempre irão ter algum tipo de prejuízo ou dificuldade pela ação de criminosos virtuais.

3.2 Desenvolvimento da versão digital

Conforme o decreto estadual Nº 55.852, de 22 de abril de 2021 em decorrência da pandemia de COVID-19, foi estabelecido o uso de ensino a distância para metade do total de alunos dentro de sala de aula. Com essa demanda foi necessário o desenvolvimento de uma versão digital do jogo de tabuleiro Th3_0ff1c3, seguindo todas as mecânicas e designs do tabuleiro físico, foi construído a versão digital no site de simuladores de jogos de tabuleiros chamado Tabletopia[1].

O jogo foi criado na plataforma digital seguindo as regras para 4 jogadores que foram assumidos por 4 alunos na aplicação da pesquisa. Sendo criado o tabuleiro de jogo conforme as recomendações de início do jogo conforme o manual do jogo que pode ser vista na figura 5.

Figura 5. Jogo de tabuleiro Th3_0ff1c3 na versão digital

O acesso ao jogo de tabuleiro Th3_0ff1c3 está disponibilizado na plataforma Tabletopia pelo seguinte endereço: https://tabletopia.com/games/th3-0ff1c3- bhp3jq/play-now

4. Aplicação e análises de resultados

O trabalho foi aplicado no curso de Sistemas de Informação na Antônio Meneghetti Faculdade (AMF) da cidade de Restinga Seca no Estado do Rio Grande do Sul no dia 5 de junho de 2021, no turno da manhã. A aplicação teve a participação de um total de 8 pessoas, sendo 7 alunos do sexo masculino e 1 aluna do sexo feminino na modalidade de aula presencial e a distância. A aplicação do projeto de pesquisa teve um total de 50% da turma presencial e outros 50% na modalidade a distância. O projeto foi aplicado na mesma data e horário para todos os alunos com o jogo de tabuleiro físico e em formato digital, visto nas figuras 6 abaixo. Os alunos na modalidade de ensino a distância

conectaram-se pelo aplicativo Zoom e foi compartilhado os slides da apresentação, os áudios e o uso da câmera da sala de aula presencial, o jogo de tabuleiro foi disponibilizado em forma de sala de jogo digital pelo site Tabletopia, que podem ser vistas nas figuras 7. Todos os participantes receberam no dia anterior uma cópia do manual do jogo de tabuleiro e receberam recomendações de estudá-lo.

Figura 6. Aplicação do jogo de tabuleiro físico

Figura 7. Aplicação do jogo de tabuleiro digital

Como critério de aplicação foram selecionados os participantes de um curso superior na área da computação, segundo os resultados da aplicação do questionário de avaliação demográfico constatou-se que a maioria dos participantes da aplicação tinham experiência profissional na área da computação, apenas 1 aluno se classificou como apenas estudante, os demais trabalham em meio período ou tempo integral, segundo o gráfico 1.

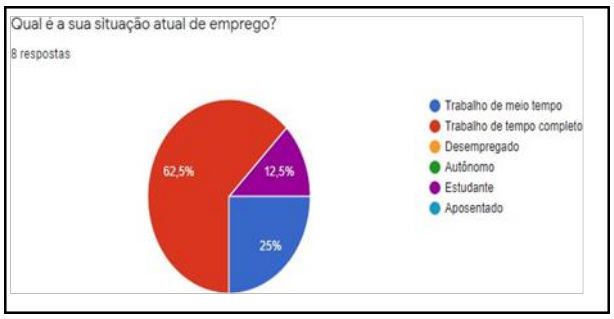


Gráfico 1. Situação atual de emprego dos participantes

Antes e após a aplicação do jogo de tabuleiro Th3_0ff1c3 foram realizadas duas avaliações de conhecimento dos participantes utilizando 10 questões objetivas, abertas e de múltipla escolha que compreendem vários conceitos sobre malwares e riscos à segurança da informação, para tentar entender o atual conhecimento dos participantes e se a aplicação do jogo de tabuleiro Th3_0ff1c3 trouxe algum benefício para o desenvolvimento do conhecimento na área de segurança da informação, ou se o jogo de tabuleiro foi um auxiliador para relembrar as matérias já ministradas em aula, já que segundo o professor da disciplina foram vistos no decorrer da disciplina. As alternativas foram sorteadas para dificultar que o participante decorasse a resposta correspondente entre as aplicações e não passar a resposta correta adiante.

Na tabela 2 foram tabuladas as somas de todos os acertos na primeira avaliação de conhecimento e todas os acertos na segunda avaliação de conhecimento. A média total de respostas corretas na 1ª avaliação foi com uma pontuação de 68,75% de acertos contra a média geral de 78,75% de respostas corretas na segunda avaliação, tendo um aumento de 10% no total de respostas corretas entre a primeira e a segunda avaliação de conhecimento.

Tabela 2. Total de acertos e média geral da avaliação de conhecimento

	Total de Acertos	Média geral
1ª Avaliação de Conhecimento	55	68,75%
2ª Avaliação de Conhecimento	63	78,75%

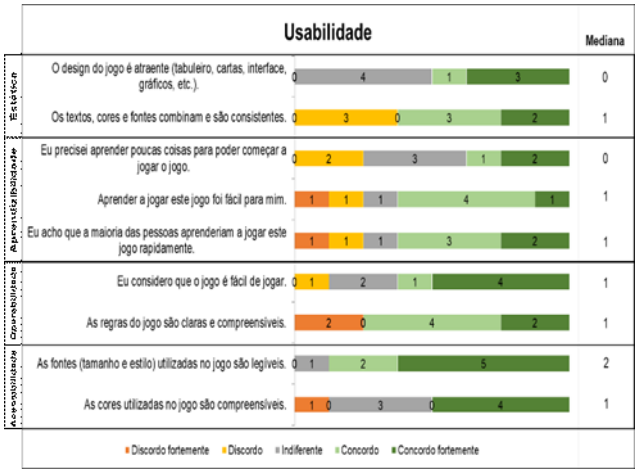
Os dados apresentados pelas estatísticas demonstram uma melhora significativa após a aplicação do projeto de pesquisa utilizando o jogo de tabuleiro Th3_0ff1c3 em alunos de um curso na área da computação com conhecimento prévio de segurança da informação.

O jogo de tabuleiro educacional Th3_0ff1c3 foi avaliado utilizando o método MEEGA+ desenvolvido pelo autor Petri. Segundo Petri [6], existem poucos modelos ou métodos que forneçam um suporte sistemático para a avaliação de jogos educacionais. Com isso foi utilizado o método MEEGA+ para a avaliação da versão do jogo de tabuleiro em formato físico e digital. O método MEEGA+ foi desenvolvido pelo autor Petri et al. em 2018, utilizando uma pesquisa multi-método.

A tabela 3 demonstra resultados em que houve resultados positivos na facilidade de uso do jogo de tabuleiro Th3_0ff1c3 e outras neutras ou negativas em relação a qualidade gráfica, design e as cores do jogo, espelhando a opinião de participantes de jogadores dos jogos digitais, que utilizam recursos de imagens em alta definição, sons, músicas, gráficos 3d, entre outros, no qual não temos em uma aplicação de não digital.

A mediana para cada tabela demonstra a maioria das escolhas, onde uma mediana de -2 refere-se à opção de Discordo totalmente, a mediana de -1 refere-se a opção de Discordo, a mediana de número 0 concerne a opção de Indiferente, a mediana de número 1 indica a opção de Concordo e a mediana do 2 compete a opção de Concordo Totalmente.

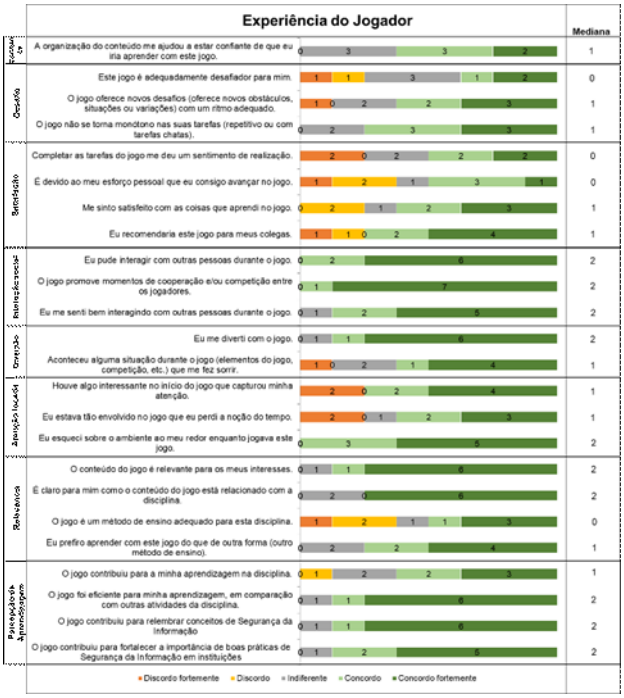
Tabela 3. O jogo auxiliou a relembrar algum conceito de SI?



Para a avaliação da experiência do jogador compilados na tabela 4 tivemos excelentes resultados na questão da interação social e diversão, que houve durante a aplicação do jogo na turma a distância e no formato presencial em sala de aula sendo observado pelo autor deste trabalho. O jogo de tabuleiro também foi bastante recomendado para ser utilizado por outras turmas e colegas da turma de Sistemas de Informação, que se mostrou uma ótima ferramenta educacional para relembrar conceitos de segurança da informação já vistos durante o curso e até aprendizado de novos conceitos e exemplos das ações de malwares e ataques virtuais no modo de um jogo de tabuleiro.

O jogo de tabuleiro Th3_0ff1c3 não teve resultados positivos na questão da dificuldade do conteúdo e não foi desenvolvido para ser um método central de ensino de segurança da informação dentro de um curso de Sistemas de Informação, mas sim uma ferramenta de apoio educacional para ser utilizado em disciplinas das áreas da computação.

Tabela 4. O jogo auxiliou a relembrar algum conceito de SI?



Conclusões

Vivemos diversos desafios dentro da sociedade, com vários facilitadores e dificultadores. O crescimento tecnológico e do saber crescem exponencialmente nas mais diversas áreas do conhecimento, e a computação veio como uma grande auxiliadora para os desafios da sociedade, mas também trouxe alguns problemas.

Os surgimentos de ameaças contra a segurança digital das pessoas cresceram junto com a tecnologia, trazendo diversos problemas como fraudes de informação, prejuízos financeiros e contra a imagem dos indivíduos, quebra da privacidade cada vez mais explorada para obtenção e criação de tendências dentro da sociedade, espionagem a nível mundial no mundo virtual feito contra governos e países e muitos outros tipos de crimes virtuais.

E o jogo Th3_0ff1c3 tentou retratar um cenário prático onde os jogadores podem ter contato com a área de segurança da informação.

Os jogos no geral têm um papel cada vez mais importantes na formação e no manter cultural da sociedade. Segundo Huizinga [7], no prefácio de sua obra Homo Ludens, é declarado que “há muitos anos que vem crescendo em mim a convicção de que é no jogo e pelo jogo que a civilização surge e se desenvolve”.

Os jogos de tabuleiro são uma interessante ferramenta educacional que pode ser utilizada nos trabalhos pedagógicos em diversas instituições, como salas de aula dos mais variados níveis de ensino como o fundamental, médio e superior. Pode ser aplicado em empresas de diversas áreas, setores industriais, representações governamentais e dentro de toda a sociedade.

O jogo Th3_0ff1c3 teve bons resultados nas avaliações de conhecimento e a avaliação de qualidade do jogo educacional bastante positiva em relação a qualidade do jogo de tabuleiro Th3_0ff1c3, sendo recomendado pelos participantes como uma ferramenta educacional para ser um auxiliador no aprendizado de SI.

Notas

[1] https://tabletopia.com/

Referências

[1] M. Castells, *A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade*. Rio De Janeiro: Jorge Zahar Ed, 2003.

[2] "Principais ataques de Ransomware," *www.kaspersky.com.br*, Feb. 18, 2022. https://www.kaspersky.com.br/resource-center/threats/top-ransomware-2020

[3] T. Kayworth, D. Whitten, Effective "Information Security Requires a Balance of Social and Technology Factors." *MIS Quarterly Executive*, vol. 9, no. 3, pp. 163-175, 2010.

[4] B. A. Kitchenham, D. Budgen, and P. Brereton, *Evidence-based software engineering and systematic reviews*. Boca Raton: CRC Press/Taylor & Francis Group, 2016

[5] A.W. Harzing, Publish or Perish, 2007, Disponível em: https://harzing.com/resources/publish-or-perish

[6] C. Gresse von Wangenheim, G. Petri, and A. Ferreti Borgatto, "MEEGA+KIDS: A Model for the Evaluation of Games for Computing Education in Secondary School," *RENOTE*, vol. 18, no. 1, Jul. 2020, doi: 10.22456/1679-1916.105938.

[7] J. Huizinga, *Homo ludens*

Informações de contatos dos autores

Francis Mallmann Schappo
PPGTER – UFSM
Santa Maria - RS
Brasil
francismallmann@gmail.com
https://orcid.org/0000-0002-8725-7647

Roseclea Duarte Medina
PPGTER – UFSM
Santa Maria – RS
Brasil
roseclea.medina@gmail.com
https://orcid.org/0000-0003-0888-6961

Francis Mallmann Schappo
Graduado em Sistemas de Informação pela UFSM (2016), Mestre em Tecnologias Educacionais em Rede (UFSM). Participante do Grupo de Redes e Computação Aplicada (GRECA - UFSM)

Roseclea Duarte Medina
Possui mestrado em Computação pela Universidade Federal do Rio Grande do Sul (1995) e doutorado em Informática na Educação pela Universidade Federal do Rio Grande do Sul (2004). Atualmente é professora Titular da Universidade Federal de Santa Maria