UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE EDUCAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIAS
EDUCACIONAIS EM REDE – MESTRADO PROFISSIONAL

Francis Mallmann Schappo

***TH3_0FF1C3*: UM JOGO DE TABULEIRO EDUCACIONAL PARA O ENSINO DE CONCEITOS DA SEGURANÇA DA INFORMAÇÃO**

Santa Maria, RS
2022

Francis Mallmann Schappo

TH3_0FF1C3: UM JOGO DE TABULEIRO EDUCACIONAL PARA O ENSINO DE CONCEITOS DA SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Tecnologias Educacionais em Rede, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Mestre em Tecnologias Educacionais em Rede.**

Orientadora: Profª Drª. Roseclea Duarte Medina

Santa Maria, RS
2022

Schappo, Francis Mallmann
TH3 0FF1C3: UM JOGO DE TABULEIRO EDUCACIONAL PARA O ENSINO DE CONCEITOS DA SEGURANÇA DA INFORMAÇÃO / Francis Mallmann Schappo.- 2022.
155 p.; 30 cm

Orientadora: Roseclea Duarte Medina
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Educação, Programa de Pós-Graduação em Tecnologias Educacionais em Rede, RS, 2022

1. Tecnologia educacional 2. Segurança da Informação 3. Jogo de tabuleiro educacional I. Medina, Roseclea Duarte II. Título.

sistema de geração automática de ficha catalográfica da UFSM. dados fornecidos pelo autor(a). sob supervisão da direção da divisão de processos técnicos da biblioteca central. bibliotecária responsável paula schoenfeldt patta crb 10/1728.

Declaro, FRANCIS MALLMANN SCHAPPO, para os devidos fins e sob as penas da lei, que a pesquisa constante neste trabalho de conclusão de curso (Dissertação) foi por mim elaborada e que as informações necessárias objeto de consulta em literatura e outras fontes estão devidamente referenciadas. Declaro, ainda, que este trabalho ou parte dele não foi apresentado anteriormente para obtenção de qualquer outro grau acadêmico, estando ciente de que a inveracidade da presente declaração poderá resultar na anulação da titulação pela Universidade, entre outras consequências legais.

Francis Mallmann Schappo

TH3_0FF1C3: UM JOGO DE TABULEIRO EDUCACIONAL PARA O ENSINO DE CONCEITOS DA SEGURANÇA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Tecnologias Educacionais em Rede, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Mestre em Tecnologias Educacionais em Rede.**

Aprovado em 28 de setembro de 2022:

Rosecléa Duarte Medina, Dra. (UFSM)
(Presidente/Orientadora)

Gilliane Bernardi, Dra. (UFSM)

Erico Marcelo Hoff do Amaral, Dr. (UNIPAMPA)

Santa Maria, RS
2022

Para a minha esposa Sol e minha filha Alana, vocês foram a minha base para construir esse trabalho.

AGRADECIMENTOS

Agradeço a Aquele que criou os Céus e a Terra, por me iluminar no descortinar da sabedoria e do conhecimento.

Agradeço a minha família que me apoiou e deu esteio em todo esse tempo de crescimento, alegrias e dificuldades. A minha amada Sol que permitiu eu ter essa paixão por jogos de tabuleiro e minha querida filha Alana que gosta muito de brincar de “dodo” com o papai, vocês foram uma inspiração e um auxílio em todos os obstáculos.

A minha Orientadora Profe Rose, que confiou e acreditou nas minhas ideias, dando todo o apoio e a paciência que foram necessárias. Nunca esquecerei.

Para o Programa de Pós-Graduação em Tecnologias Educacionais em Rede, que me deram uma visão mais completa sobre o lado das humanas e da educação, me tornando uma pessoa mais completa.

A todos os amigos e colegas que não conseguirei citar aqui, mas que foram muito importantes neste caminho.

Muito obrigado!

RESUMO

TH3_0FF1C3: UM JOGO DE TABULEIRO EDUCACIONAL PARA O ENSINO DE CONCEITOS DA SEGURANÇA DA INFORMAÇÃO

AUTOR: Francis Mallmann Schappo
ORIENTADORA: Roseclea Duarte Medina

O atual projeto foi desenvolvido na linha da pesquisa de Desenvolvimento de Tecnologias Educacionais em Rede, no Programa de Pós-graduação de Tecnologias Educacionais em Rede da Universidade Federal de Santa Maria. Tem como objetivo o desenvolvimento de um jogo de tabuleiro educacional para a aplicação e aprendizado de conceitos sobre segurança da informação para pessoas com e sem o domínio do conhecimento. Baseando na nova Lei Geral de Proteção de Dados Pessoais que entrou em vigor para todas as empresas no ano de 2021, e a crescente onda de ataques virtuais que ocorrem a nível mundial, a atual pesquisa tenta responder à pergunta de “Uma atividade desplugada em forma de jogo de tabuleiro poderia ser um facilitador no aprendizado sobre boas práticas de Segurança da Informação?”. A pesquisa foi aplicada em usuários de computadores para jovens universitários com ou sem experiência no mercado de trabalho. Para o desenvolvimento deste trabalho foi realizada uma pesquisa bibliográfica, construção de um protótipo e aplicação do jogo de tabuleiro. Os dados para análise foram adquiridos por meio de questionários de avaliação compilados e demonstrados no capítulo de resultados, onde houve respostas positivas após a aplicação como uma ferramenta educacional para auxílio no desenvolvimento do conhecimento. O jogo de tabuleiro educacional contendo conhecimentos de segurança da informação é um produto aberto e acessível a toda a comunidade no formato físico e digital.

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

ABSTRACT

TH3_0FF1C3: AN EDUCATIONAL BOARD GAME FOR THE TEACHING OF INFORMATION SECURITY CONCEPTS

AUTHOR: Francis Mallmann Schappo
ADVISOR: Roseclea Duarte Medina

The current project was developed in line with the Research Development of Educational Technologies in Network, in the Postgraduate Program of Educational Technologies in Network of the Federal University of Santa Maria. Its objective is the development of an educational board game for the application and learning of concepts about information security for people with and without the domain of knowledge. Based on the new General Law for the Protection of Personal Data that came into force for all companies in 2021, and the growing wave of cyberattacks that occur worldwide, the current research tries to answer the question of “An unplugged activity in a could a board game be a facilitator in learning about good Information Security practices?”. The research was applied to computer users for university students with or without experience in the job market. For the development of this work, bibliographic research was carried out, construction of a prototype and application of the board game. Data for analysis were acquired through evaluation questionnaires compiled and demonstrated in the results chapter, where there were positive responses after application as an educational tool to aid in the development of knowledge. The educational board game containing information security knowledge will be an open-end product accessible to the entire community in both physical and digital format.

Keywords: Educational Technology, Information Security, LGPD, board game, th3_0ff1c3

LISTA DE ILUSTRAÇÕES

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KIPS	Kaspersky Interactive Protection Simulation
LGPD	Lei Geral de Proteção aos Dados
NBR	Norma Brasileira
SI	Segurança da Informação
UFSM	Universidade Federal de Santa Maria

SUMÁRIO

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.

Após a revolução industrial dos séculos XVIII e XIX que mudaram a sociedade europeia com o advindo das máquinas e do trabalho assalariado, iniciou-se a revolução da informação, a necessidade de busca de novos conhecimentos.

Essas grandes mudanças sociais começaram o processo da globalização mundial, que foi um facilitador e propagador da informação e do conhecimento, ocorrendo rápidas transformações nos campos sociais e tecnológicos, permitindo que novos conhecimentos se propaguem em grande velocidade na sociedade mundial.

A 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 (2003), 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 (CASTELLS, 2003; MATTELART, 2002).

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 existe 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 Afrikatec (2017) ao longo dos últimos anos, o número de ciberataques registrados em todo o mundo tem crescido em níveis alarmantes em mais de 74 países, 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 (2010), 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 pensado o desenvolvimento de um jogo de tabuleiro moderno sobre segurança da informação.

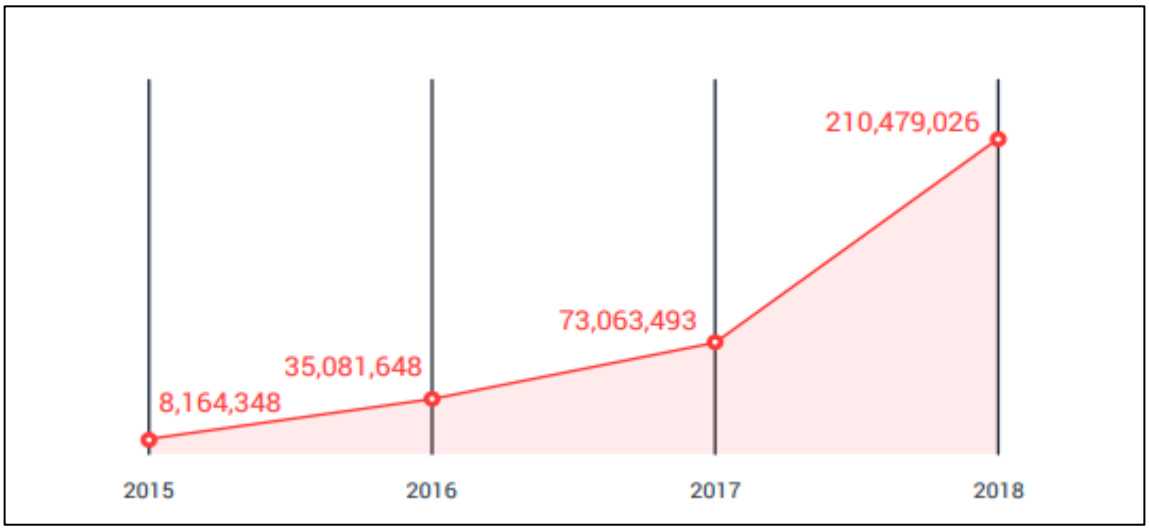
1.1 PROBLEMA DE PESQUISA E HIPÓTESE

Vivemos uma tendência mundial no aumento da quantidade de ataques cibernéticos na grande rede mundial de computadores que tem crescido a cada ano. Segundo o relatório realizado pelo laboratório de segurança *dfndr lab*[1] da empresa Psafe no ano de 2018, o Brasil teve 120,7 milhões de ataques só no primeiro semestre de 2018, com um aumento de 95,9% em relação ao ano anterior, praticamente o dobro de aumento de ataques.

O uso de técnicas para roubos de dados como o *phishing*, no qual o criminoso cria um website idêntico ao original para enganar o usuário, continua a crescer em ação pelo mundo. No gráfico 1, pode-se ver o número de bloqueios que o software de segurança da empresa Trend Micro[2] realizou nos últimos anos em todos os países de mundo.

[1] Ver https://www.psafe.com/dfndr-lab/
[2] Ver https://www.trendmicro.com/pt_br/business.html

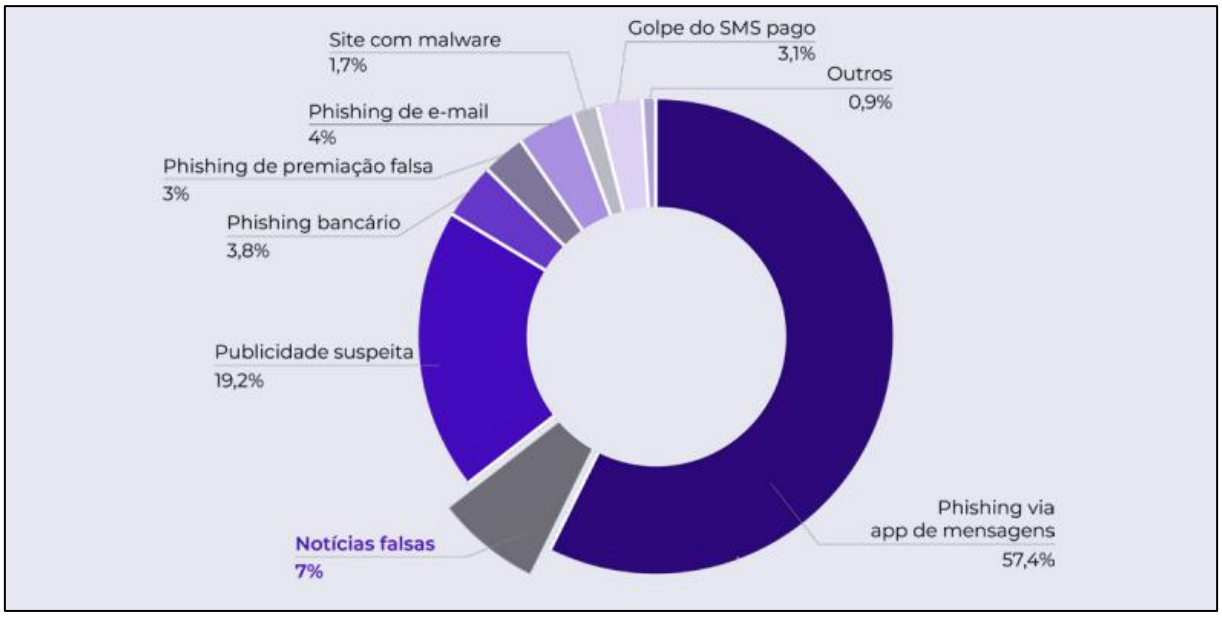
Gráfico 1 - Aumento dos bloqueios de tentativas de phishing



Fonte: Trend Micro Security Predictions for 2019 (2019, p. 6).

A exploração do uso de informações falsas para tentativas de roubos de informações está sendo bastante utilizado, principalmente em aplicativos de trocas de mensagens por celular, causando prejuízos para a sociedade. No gráfico 2, criado pelo laboratório de segurança *dfndr lab,* mostra as diversas técnicas que tiveram crescimento.

Gráfico 2 - Utilização de informações falsas



Fonte: dfndr lab (2018, p. 3).

Segundo o relatório *The Fraud Beat* de 2019 da empresa de segurança Cyxtera[3], houve um aumento de 500% nos casos de *ransomwares*, com a previsão de um ataque a cada 14 segundos, no qual o criminoso sequestra os dados com a utilização de criptografia, e exige um valor de resgate para a vítima, geralmente cobrado utilizando moedas virtuais, como as *bitcoins*, estima-se que ocorram prejuízos de U$ 11,5 bilhões por ano pelas empresas.

As tendências de crescimentos nos ataques contra a segurança da informação apontam para a necessidade de criar uma cultura educacional de boas práticas de segurança da informação na sociedade. Em consequência disso ainda existem muitas dúvidas e até mesmo o desconhecimento dos possíveis prejuízos dos golpes causados por criminosos virtuais que poderiam ser minimizados com a utilização de ferramentas educacionais.

Para o desenvolvimento deste projeto, foi definida a seguinte pergunta para o problema de pesquisa: “A utilização de um jogo de tabuleiro, construído com conceitos da segurança de informação e mecânicas de jogos de tabuleiro modernos, pode ser um auxiliador ou ferramenta no processo de ensino e aprendizagem sobre conceitos de Segurança da Informação?”.

1.2 OBJETIVOS

1.1.1 Objetivo Geral

Desenvolver um jogo de tabuleiro educacional para ser uma ferramenta facilitadora do aprendizado sobre a Segurança da Informação em ambientes empresariais e da educação.

1.1.2 Objetivos Específicos

a) Realizar uma pesquisa bibliográfica sobre os jogos de tabuleiros educacionais com o tema de segurança da informação;
b) Desenvolver um protótipo de um jogo de tabuleiro educacional com o tema de segurança da informação;

[3] Ver https://www.cyxtera.com/

c) Aplicar o jogo de tabuleiro no meio acadêmico;

d) Avaliar os conhecimentos adquiridos pelos participantes;

e) Avaliar o jogo de tabuleiro utilizando o método MEEGA+;

1.3 JUSTIFICATIVA

Para o ensino de boas práticas na área de segurança da informação precisamos um produto inovador que seja interessante a todos os tipos de usuários. Tenho trabalhado na área de Tecnologia da Informação por mais de 15 anos, e tenho percebido muitas dúvidas de todos os tipos de usuários de computadores em empresas, e um aumento nos prejuízos causados por pragas virtuais.

Segundo a nova Lei Geral de Proteção aos Dados[4] (LGPD), todas as empresas brasileiras deverão se adequar a proteger os dados e a privacidade das pessoas envolvidas, desde clientes á funcionários, garantindo a segurança da informação e o anonimato de dados pessoais.

A conscientização para a cultura de proteção aos dados é algo processual e seria interessante o uso de ferramentas, como por exemplo o projeto de pesquisa e o produto desenvolvido nesse trabalho.

O autor deste trabalho realizou algumas palestras[5] e uma breve pesquisa sobre segurança da informação durante o tempo de graduação em Sistemas da Informação na UFSM, na disciplina de Computadores e Sociedade", para variados tipos de usuários. A aplicação da pesquisa atendeu os cursos superiores como a Medicina Veterinária e cursos técnicos no Colégio Politécnico da UFSM, a aplicação por palestras revelou muitas dúvidas e bastante interesse por parte dos alunos sobre o tema, assim gerou-se a ideia de dar continuidade na pesquisa utilizando uma abordagem diferente. A ferramenta utilizada para a aplicação da nova abordagem foi o desenvolvimento de um jogo de tabuleiro moderno e educacional pela proximidade do autor com vários tipos de jogos de tabuleiro modernos.

Pudemos acompanhar nos últimos anos o aparecimento de ataques mais sofisticados, como por exemplo os sequestros de dados (*ransomwares*), que pararam empresas, órgãos públicos, serviços críticos etc.

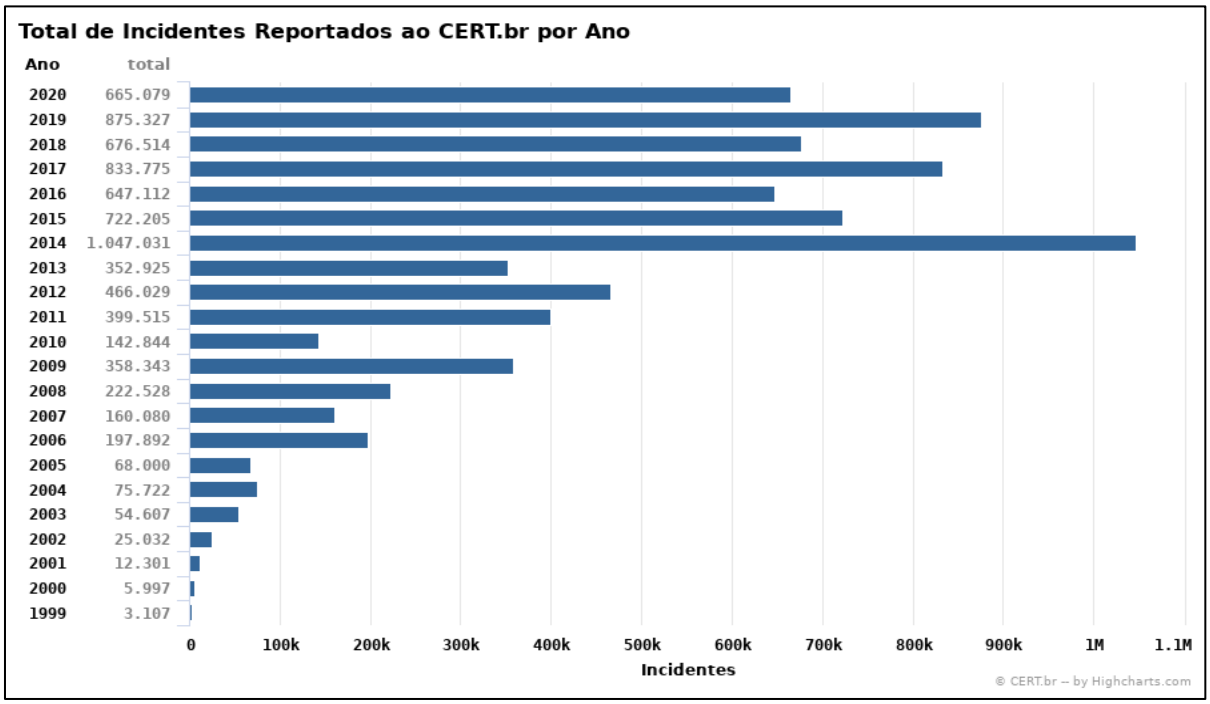
---

[4] Ver http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

[5] Ver https://www.youtube.com/watch?v=pbgrje8oy3o

Segundo o gráfico 3, pode-se ver um aumento no número de incidentes em segurança da informação, tanto na esfera pessoal e empresarial que foram reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT, 2021).

Gráfico 3 - Total de Incidentes reportados até o ano de 2020



Fonte: CERT (2021).

Os ataques de roubos financeiros são diários, e visam enganar os usuários, se passando por serviços bancários oficiais gerando bilhões em prejuízos anuais. E os prejuízos vão além do financeiro, atingindo muitas vezes a imagem de pessoas e empresas que sofreram ataques como os vazamentos de informações causada por ataques virtuais bem-sucedidos, ocorrendo inclusive suicídios por vazamento de fotos intimas na rede mundial, como ocorreu em uma família de Utah no ano de 2018, no qual o filho de 21 anos se suicidou após o vazamento de fotos intimas e os criminosos fizerem extorsões financeiras (FOX, 2017).

Este trabalho tenta conscientizar e dar conhecimento a todos os tipos de usuários de computador por meio de um jogo de tabuleiro moderno e educacional com a temática de segurança da informação para ser um auxiliador no aprendizado sobre técnicas de SI em diversos ambientes, como salas de aula, ambientes coorporativos, industriais, entre outros.

2 SEGURANÇA DA INFORMAÇÃO

Segundo a norma brasileira da ABNT NBR ISO/IEC 17799 o conceito de SI é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades do negócio (ABNT NBR ISO/IEC 17799:2005, p. IX).

A NBR ISO/IEC 27.002:2005 define segurança da informação como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio e estabelece como objetivo da segurança da informação a preservação da confidencialidade, da integridade e da disponibilidade da informação (ASSOCIAÇÃO, NBR ISO/IEC 27.002, 2005).

Esses termos estão assim definidos na NBR ISO/IEC 27.001:2006 (ASSOCIAÇÃO, NBR ISO/IEC 27001, 2006):

- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;
- Integridade: propriedade de salvaguarda da exatidão e completeza de ativos;
- Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

Não se pode negar que a informação é uma ativo muito importante para as empresas públicas, privadas e usuários de dispositivos conectados em geral, tendo valor de integridade e financeiro, como por exemplo os bancos de dados de sistemas que podem guardar informações sigilosas sobre pessoas, como por exemplo hospitais, laboratórios de análises, serviços governamentais, serviços bancários etc. Na qual se houver um vazamento de informações, ou alterações e danos aos dados, ocorrerá riscos a vida de pessoas e grandes prejuízos financeiros.

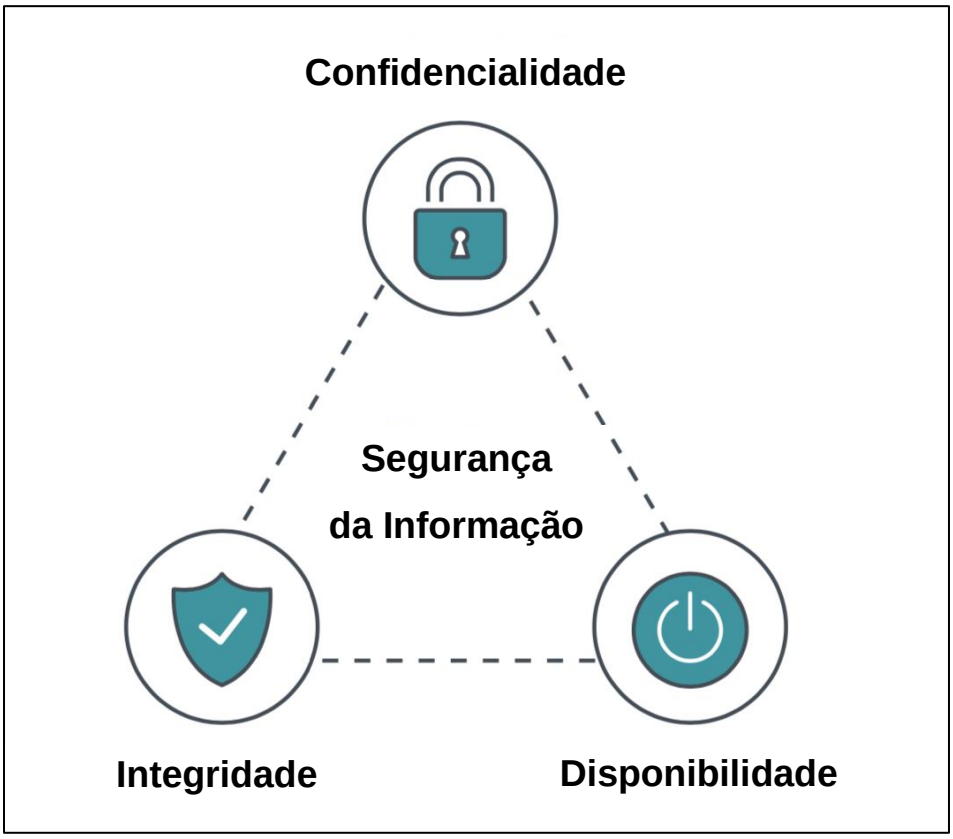
Segundo Jacobson e Idziorek (2013), podemos classificar a segurança da informação em uma tríade:

> **Confidencialidade:** Impedir que usuários não autorizados leiam ou acessem informações. Confidencialidade é o que a maioria das pessoas pensam

> quando se refere à segurança da informação. Uma perda de confidencialidade incluiria um invasor aprendendo sua senha ou número do cartão de crédito.
> **Integridade:** Garantir que um usuário não autorizado não altere as informações. Um saldo de conta bancária é um exemplo sólido de informação que requer muita integridade. Uma perda de integridade nesse caso seria prejudicial para o banco ou seus clientes.
> **Disponibilidade:** Garantir que as informações possam ser acessadas quando necessário por usuários autorizados. Se um disco rígido fosse apagado como resultado de uma infecção por malware, esse tipo de ação seria considerado uma perda de disponibilidade.

Conforme a figura 1, a tríade da segurança da informação precisa estar em unidade para não ocorrer o risco de incidentes de segurança para o usuário de tecnologia.

Figura 1 – Tríade da Segurança da Informação



Fonte: ESET (2019, tradução nossa).

2.1 TIPOS DE ATACANTES VIRTUAIS

Os tipos de atacantes virtuais podem ser classificados em diversas categorias no mundo da segurança da informação que estão explanadas a seguir.

2.1.1 Hackers

O termo *hacker* começou a ser utilizado na década de 60, nos Estados Unidos da América, na qual classificava qualquer solução inovadora para um problema utilizando a palavra *hack*. Em pouco tempo a palavra foi atribuída aos programadores de computador (BRASIL ESCOLA, 2018). Em 1980, um artigo da *Psychology Today* usou o termo “hacker” em seu título: “*The Hacker Papers*” que discutia a natureza viciante do uso do computador.

Mais tarde, em 1982, o filme americano de ficção científica *Tron* mostra o protagonista descrevendo suas intenções de quebrar o sistema de computadores da empresa ao invadi-lo. O enredo de um outro filme lançado no ano seguinte, *WarGames*, era baseado na invasão de um computador utilizado por um adolescente ao Comando de Defesa Aeroespacial Norte-americano (NORAD). Tratava-se de uma ficção que introduzia a figura dos hackers como uma ameaça à segurança nacional (Malwarebytes, 2019).

A introdução da ideia *hacking* na cultura norte-americana trouxe diversos movimentos de ataques virtuais contra instituições governamentais, bancos, hospitais, entre outros, sendo utilizada a palavra *hacker* de forma pejorativa nos grandes meios de notícias.

Com a impulsão das mídias mundiais, criou-se várias gangues de criminosos virtuais em todo o mundo, fazendo os governos criarem leis anti-hacking e atraindo a atenção das grandes empresas de desenvolvimento de sistemas operacionais, como Microsoft, IBM e Apple a investirem em segurança da informação em seus produtos.

O termo não pejorativo para a palavra *hacker*, remete-se a pessoas com grande conhecimento em uma área de atuação, não necessariamente na área da computação, que em outras palavras classifica-se como um especialista na função que desempenha. Na área da computação classifica-se como *hacker* alguém com muito conhecimento, domínio de determinadas ferramentas e sistemas e grande

conhecimento em segurança da informação. Um *hacker* tem uma boa capacidade analítica para encontrar e resolver falhas nos sistemas de informação, em nível de software e hardware. Geralmente utilizam seus conhecimentos na solução de problemas em empresas e na sociedade em geral e não para causar danos estruturais e financeiros, como por exemplo o hacker ético, que pode trabalhar como consultor de segurança da informação, descobrindo falhas de segurança em sistemas e assessorando em corrigi-las.

2.1.2 Classificação dos tipos de Hackers

Segundo EGOV (2016), existem três classificações gerais para hackers na área da computação, que são os chamados *white hat* (chapéu branco), *black hat* (chapéu preto) e *gray hat* (chapéu cinza):

a) *White hat*: São os profissionais da área de segurança da informação que atuam com serviços de hacker éticos, analisando os sistemas das empresas a procura de falhas e problemas de segurança, buscando soluções para o contratante. A ética de um White hat não permite a exploração da vulnerabilidade para ganhos pessoais e tão pouco a venda ou disponibilização da informação sobre a falha de segurança.
b) *Black hat*: Ao contrário dos *White hats,* os *black hats* trabalham para explorar as falhas em sistemas das instituições, com o intuito de roubar dados sigilosos, senhas, dados bancários, derrubar serviços essenciais, como servidores de páginas web e/ou de aplicações etc. Suas motivações são os ganhos financeiros, pessoais e a espionagem cibernética. Alguns autores classificam como *crackers*.
c) *Gray hat*: Os chapéus cinza, ou *gray hat,* são pessoas que trabalham dos dois lados, investigam as falhas de segurança nas empresas, mas também divulgam elas publicamente. Os chapéus cinzas não trabalham de forma ética para as empresas, geralmente não informando sobre os problemas encontrados.

Ainda existem mais algumas classificações para atacantes virtuais dentro da comunidade hacker:

a) *Cracker*: O termo foi criado para descrever as pessoas que utilizam seus conhecimentos na área de redes e computação para modificar, destruir ou capturar dados como benefício próprio, vingança ou sabotagem. Para realizar danos na economia, infraestruturas críticas e o bem da sociedade em geral (WEBSTERS, 2006).
b) *Script Kiddie*: Os atacantes virtuais classificados como “script kiddie” são as pessoas com as ferramentas de ataque, mas sem o conhecimento profundo da ação que estão realizando, por isso que são facilmente descobertos (BASHAM, 2005). Ou seja, são pessoas que utilizam softwares prontos para realizar ataques quase sempre aleatórios nas redes de computadores.
c) *Phreaker*: Os atacantes conhecidos como Phreaker utilizam os sistemas de telefonia fixa e de celulares para benefícios próprios. Podendo realizar ligações gratuitas, desativar linhas e outras fraudes na telefonia (GONÇALVES, 2012).

2.1.3 Motivações para os ataques virtuais

Os ataques virtuais são motivados pelas mais diversas razões, e muitas vezes até desconhecidas. Por isso a importância de manter os sistemas de segurança atualizados e sempre ativos.

Para Matos (2018), é possível resumir as razões dos ataques nos seguintes itens do quadro 1:

Quadro 1 - Razões e motivações para cometer ataques virtuais.

Razões e Motivações	Características
Motivações financeiras	Os crimes com vista à obtenção de vantagens financeiras são, habitualmente, dirigidos a alvos específicos, ou identificados em ações massificadas, para recolher informações e acessos pessoais através de endereços de internet e informações falsas, tentado fazer-se passar por entidades reais (phishing). Para além da ação de criminosos de forma isolada, têm surgido dados que indiciam a existência de redes

	organizadas para perpetrar este tipo de crimes. Frequentemente estes crimes visam a fraude, roubo ou extorsão.
“Hacktivismo”	Considerar-se “hacktivistas” aqueles que encetam ataques através do ciberespaço com motivações políticas, sociais, ambientais etc., sendo os alvos preferenciais organizações públicas e privadas. Estes ataques podem implicar a negação de serviços ou a alteração da imagem das organizações visadas, bem como o roubo de dados. Não é comum identificarem-se motivações financeiras associadas a este tipo de iniciativas.
Subversão	As razões desta categoria de ataques e exploração de vulnerabilidades estão, muitas vezes, associadas ao “hacktivismo”. Os ataques podem igualmente ser dirigidos a organizações públicas e privadas.
Religião ou nacionalismo	Nesta categoria são, habitualmente, identificados indivíduos e organizações que se intitulam de “ciberguerreiros” tendo por base razões religiosas ou ideologias normalmente associadas ao patriotismo ou nacionalismo extremos.
Terrorismo	À semelhança da categoria anterior, com a intenção de provocar medo e ataques de dimensão considerável, encontram-se indivíduos e organizações, normalmente de forma coordenada, com múltiplas motivações, entre as quais a religião ou o nacionalismo. Em alguns casos, estas ações incluem motivações financeiras.
Desafio	A tentativa de desafiar ou de superar sistemas de proteção e segurança são razões que levam indivíduos, habitualmente de forma isolada, a efetuar ataques de diversa natureza no ciberespaço contra organizações. É possível encontrar referências que denominam esta motivação como “script kiddies”.

Notoriedade	Muitas vezes associado ao desafio e à superação dos sistemas de proteção e segurança está, também, o desejo de ser conhecido. A tentativa de conquistar um grau de respeito dentro das comunidades hackers ou das comunidades da cibersegurança costuma estar, igualmente, associado a estes ataques.
Vingança	A vingança contra pessoas ou organizações é uma das razões de ataques ou roubo de informação que, algumas vezes, quando se trata de organizações ou empresas, podem ser perpetrados por pessoas internas, isto é, que, por alguma razão, por forma a se vingarem, obtêm indevidamente, expõem ou danificam informação ou infraestruturas das organizações a que pertencem ou pertenciam.
Espionagem	A exploração de vulnerabilidades motivada por espionagem pode ocorrer de diversas formas (phishing, malware, agentes internos, entre muitas outras) e, não descartando organizações sem fins lucrativos ou de caráter social, é essencialmente dirigida a organizações dos setores público e privado. Estados e empresas são alvos altamente apetecíveis para estes atores dadas as vantagens políticas, estratégicas, concorrenciais e financeiras que poderão advir da informação obtida por via de ataques informáticos ou exploração de vulnerabilidades. Estas razões e motivações podem estar na origem da ação não só de indivíduos ou redes organizadas de indivíduos, mas também dos próprios Estados visando outros Estados ou empresas localizadas em outros Estados, e ainda de empresas contra empresas concorrentes.

Fonte: MATOS (2018).

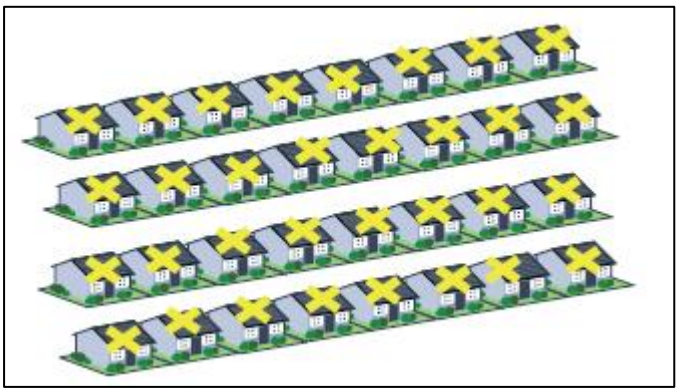
O quadro acima demonstra as variadas e complexas razões e motivações dos ataques virtuais contra as empresas e sociedade em geral. A multiplicidade de atores, razões e ameaças fazem da segurança da informação um problema complexo e atual dentro das organizações.

2.1.4 Métodos de ataque

Segundo Jacobson e Idziorek (2015), existem 5 tipos de ataques virtuais onde o atacante pode conseguir acessar informações das suas vítimas. As vulnerabilidades, *exploit*, códigos de ataque, ataques e os *exploits* do dia zero.

a) Vulnerabilidade: A vulnerabilidade é uma fraqueza em computadores que pode ser usada em um ataque para comprometer as informações. Podem existir vulnerabilidades de design, na implementação ou na configuração de computadores. As vulnerabilidades de design são quando o atacante pode ignorar toda a segurança nos computadores. Como por exemplo, na figura 2, um desenvolvedor construísse várias casas com portas, mas sem fechaduras. Se um atacante descobrisse o erro de design, entraria em todas as casas.

Figura 2 - Vulnerabilidade de design

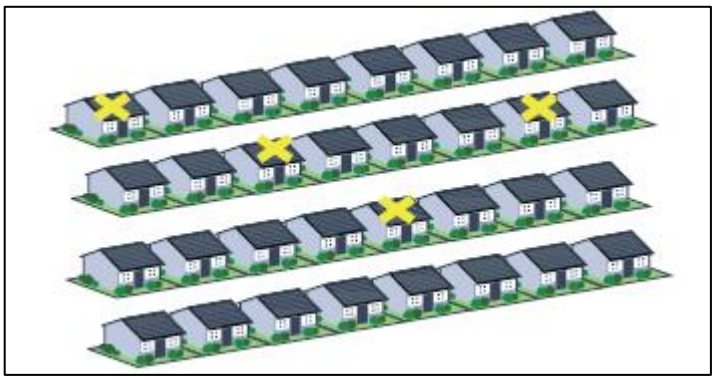


Fonte: JACOBSON E IDZIOREK (2015, p. 33).

A vulnerabilidade de implementação existe quando os desenvolvedores cometem erros ao implementar os designs dos produtos. Continuando com o exemplo de casas, na Figura 3, enquanto os planos do desenvolvedor continham projetos para todas as casas serem equipadas com fechaduras, as fechaduras foram instaladas incorretamente ou não foram instaladas pelos

contratados. Nesse caso, em vez de todas as casas estiverem usando os mesmos planos que eram vulneráveis a arrombamentos, apenas as casas construídas por um determinado contratado seriam vulneráveis. As vulnerabilidades de implementação no software podem ser difíceis de encontrar, mas uma vez descobertas, elas são fáceis de resolver com uma atualização de software.

Figura 3 - Vulnerabilidade de implementação

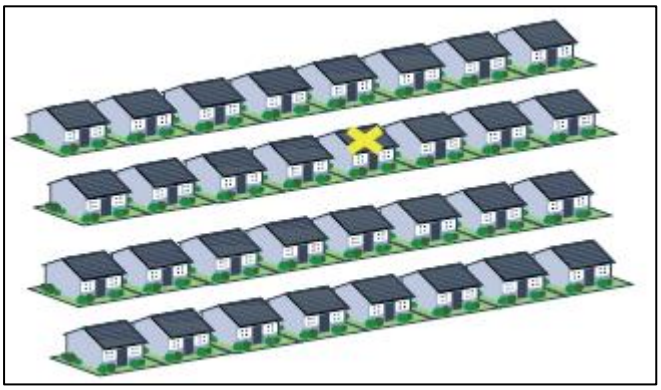


Fonte: JACOBSON E IDZIOREK (2015, p. 33).

As vulnerabilidades de configuração ocorrem quando o usuário configura incorretamente, ou mantém padrões do sistema. Com a ideia dos exemplos das casas, uma vulnerabilidade de configuração, é quando as casas estão construídas com portas e fechaduras bem instaladas, mas o usuário não tranca a fechadura, facilitando o ataque, visto na figura 4.

As vulnerabilidades de configuração mais comuns, são quando o usuário coloca senhas comuns e de fácil descoberta, ou usa uma senha padrão, ou até nem utilize alguma senha.

Figura 4 - Vulnerabilidade de configuração

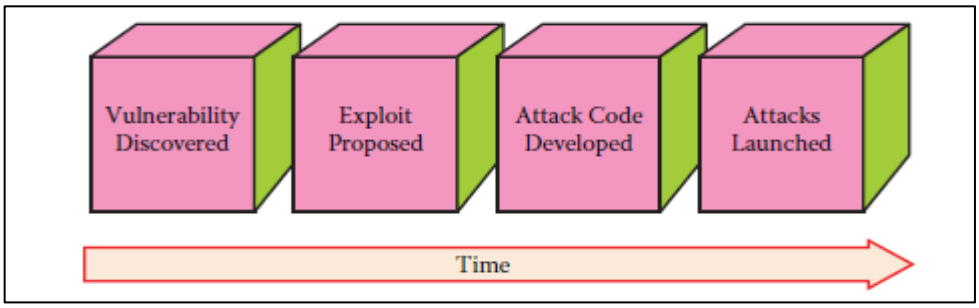


Fonte: JACOBSON E IDZIOREK (2015, p. 33).

b) Exploit: Um exploit, ou exploração é um método não implementado ou algoritmo que é capaz de tirar proveito de uma vulnerabilidade em um sistema de computador. Usando o exemplo da fechadura da porta, uma exploração pode consistir em saber que, se você fizer uma chave de segurança, uma chave sem entalhes, ela abrirá certas fechaduras, mas você não possui ou sabe como fazer a chave. Portanto, uma exploração é uma ameaça em potencial subjacente a um ataque em potencial.
c) Código de ataque: Um código de ataque, ou *attack code*, é um programa ou outra implementação de uma exploração usada para atacar uma vulnerabilidade em um sistema de computador.
d) Ataques: É o uso do código de ataque contra um sistema ou a exploração de uma vulnerabilidade. É o mesmo que usar uma chave de segurança para abrir uma porta vulnerável.

A Figura 5 mostra a relação cronológica entre vulnerabilidades, explorações, código de ataque e ataques. As vulnerabilidades permanecem inativas nos programas de software por anos antes de serem descobertas. Mesmo quando são descobertos, pode não haver uma maneira fácil de explorá-los. O intervalo de tempo entre o momento em que uma vulnerabilidade é descoberta e uma exploração é projetada pode variar de dias a meses ou até mais. Depois que a exploração for identificada, pode demorar um pouco até que o código de ataque seja criado. Às vezes, a exploração é descoberta diretamente através da criação do código de ataque, e o tempo entre a exploração e o código de ataque é zero.

Figura 5 - Relação cronológica de um ataque



Fonte: JACOBSON E IDZIOREK (2015, p. 34).

e) Exploit ou exploração do dia zero: Quando o código de ataque é usado para direcionar um sistema antes que a vulnerabilidade ou exploração seja descoberta ou conhecida pela comunidade de segurança (ou seja, defensores ou mocinhos), essa ação é conhecida como exploração "dia zero". Explorações de dia zero são particularmente perigosas porque os profissionais de segurança são inicialmente indefesos contra esses ataques.

Outro método de ataque é o chamado *Phishing*, onde o atacante tenta obter dados pessoais ou financeiros de sua vítima, utilizando métodos de engenharia social e meios técnicos.

A engenharia social pode ser descrita da seguinte forma:

> A engenharia social é uma técnica que pode ser utilizada para convencer as pessoas a divulgar informações sobre elas mesmas, suas empresas ou organizações. Ao fazer uma pesquisa prévia, um hacker pode induzir alguém a revelar detalhes que normalmente não revelariam. Se um hacker chama uma empresa de provimento de TV do Texas e tentar solicitar o canal premium da HBO para George Bush, o agente teria uma maior probabilidade de concluir o pedido quando o endereço e o número de telefone corretos de Bush foram fornecidos. (VARSALONE E MCFADDEN, 2012, p. 309, Tradução nossa).

2.1.5 Tipos de Malwares

Os Malwares, ou códigos maliciosos, são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador (CERT, 2016).

Tem como característica a autoinstalação, ou seja, muitas vezes não tendo a interação com o usuário, sendo difícil a detecção em computadores por usuários leigos.

Segundo CERT (2016), algumas formas de infecção por malwares são:

a) Realizando a exploração de vulnerabilidades existentes nos programas instalados;
b) Utilizando a auto execução de mídias removíveis infectadas, como pen-drives;
c) Pelo acesso a páginas Web maliciosas, utilizando navegadores vulneráveis;
d) Pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
e) Executando arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores (através do compartilhamento de recursos).

Os principais tipos de malwares, e que serão utilizados no jogo de tabuleiro deste trabalho são: Vírus de computador, *worms*, *spywares*, *ransomwares* e cavalos de Tróia.

2.1.5.1 Vírus de computador

Um vírus de computador é um programa ou trecho de código projetado para danificar seu PC através da corrupção de arquivos do sistema, utilização de recursos, destruição de dados ou sendo, de algum outro modo, um aborrecimento ao usuário (TORRES, 2017).

Segundo CERT (2016), os vírus de computador podem ser classificados como:

> **Vírus propagado por *e-mail*:** recebido como um arquivo anexo a um *e-mail* cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os *e-mails* encontrados nas listas de contatos gravadas no computador.
> **Vírus de *script*:** escrito em linguagem de *script*, como *VBScript* e *JavaScript*, e recebido ao acessar uma página *Web* ou por *e-mail*, como um arquivo anexo ou como parte do próprio *e-mail* escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador *Web* e do programa leitor de *e-mails* do usuário.
> **Vírus de macro:** tipo específico de vírus de *script*, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam

> esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).
> **Vírus de telefone celular:** vírus que se propaga de celular para celular por meio da tecnologia *bluetooth* ou de mensagens MMS (***M****ultimedia* ***M****essage* ***S****ervice*). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares.

2.1.5.2 Worms

A característica principal do *worm* é a auto propagação em redes de computadores, normalmente explorando uma falha do tipo *exploit* em sistemas operacionais ou de aplicações.

Ao contrário do vírus, um *worm* não infecta arquivos ou *softwares* em computadores, mas executa diretamente sua própria cópia.

Segundo CERT (2016), o processo de infecção de um *worm* ocorre na seguinte sequência:

> **Identificação dos computadores alvos:** após infectar um computador, o worm tenta se propagar e continuar o processo de infecção. Para isto, necessita identificar os computadores alvos para os quais tentará se copiar, o que pode ser feito de uma ou mais das seguintes maneiras:
> - Efetuar varredura na rede e identificar computadores ativos;
> - Aguardar que outros computadores contatem o computador infectado;
> - Utilizar listas, predefinidas ou obtidas na Internet, contendo a identificação dos alvos;
> - Utilizar informações contidas no computador infectado, como arquivos de configuração e listas de endereços de e-mail.
>
> **Envio das cópias:** após identificar os alvos, o worm efetua cópias de si mesmo e tenta enviá-las para estes computadores, por uma ou mais das seguintes formas:
> - Como parte da exploração de vulnerabilidades existentes em programas instalados no computador alvo;
> - Anexadas a e-mails;
> - Via canais de IRC (Internet Relay Chat);
> - Via programas de troca de mensagens instantâneas;
> - Incluídas em pastas compartilhadas em redes locais ou do tipo P2P (Peer to Peer).
>
> **Ativação das cópias:** após realizado o envio da cópia, o worm necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:
> - Imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas sendo executados no computador alvo no momento do recebimento da cópia;
> - Diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu computador;
> - Pela realização de uma ação específica do usuário, a qual o worm está condicionado como, por exemplo, a inserção de uma mídia removível.
>
> **Reinício do processo:** após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de agora, o

> computador que antes era o alvo passa a ser também o computador originador dos ataques.

2.1.5.3 Spyware

O malware do tipo spyware foi desenvolvido para monitorar as ações dos usuários de computadores e enviar as informações coletadas para terceiros, definido por KASPERSKY (2022) com a seguinte característica:

> O spyware é definido de maneira geral e imprecisa como um software destinado a coletar dados de um computador ou outro dispositivo, e encaminhá-los a terceiros sem o consentimento ou o conhecimento do usuário. Muitas vezes, envolve a coleta de dados confidenciais, como senhas, PINs e números de cartões de crédito, o monitoramento de pressionamentos de teclas, o rastreamento de hábitos de navegação e a coleta de endereços de e-mail.

Pode ser usada de forma legitima ou maliciosa em sistemas de computadores. Como por exemplo, a forma legitima é quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado.

E a forma maliciosa é quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha) (CERT, 2016).

A classificação de spywares pode ser dada por:

> **Keylogger:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.
> **Screenlogger:** similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet Banking.
> **Adware:** projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito. (CERT, 2016).

2.1.5.4 Ransomware

Os ransomwares são tipos de malwares que fazem sequestros de dados do usuário por meio de criptografia ou bloqueios, deixando o sistema inacessível, e pedem um pagamento para liberação dos dados.

> Ransom malware, ou ransomware, é um tipo de malware que impede os usuários de acessarem seu sistema ou arquivos pessoais e exige o pagamento do resgate (ransom) para recuperar o acesso. As primeiras variantes do ransomware foram desenvolvidas no final da década de 1980, e o pagamento deveria ser enviado via correio tradicional. Hoje, os autores do ransomware demandam que o pagamento seja enviado via criptomoeda ou cartão de crédito.
> (MALWAREBYTE, 2018).

Existem três tipos principais de *ransomware*, os *scarewares*, bloqueadores de tela e *ransomware* de criptografia. Os tipos variam em termos de severidade, desde um perigo levemente perturbador até a destruição de arquivos e grandes prejuízos financeiros.

Segundo MALWAREBYTES (2018), as três principais classificações de *ransomwares* podem ser descritas como:

> Os scarewares, vem do termo “scary”. Incluem softwares de segurança trapaceiros e fraudes de suporte técnico. Você pode receber uma mensagem pop-up alegando que o malware foi descoberto e a única maneira de se livrar dele é pagando. Se você não fizer nada, provavelmente continuará sendo bombardeado por pop-ups, mas seus arquivos estão, em essência, seguros. Um programa legítimo de segurança cibernética não faria solicitações aos clientes dessa maneira. Se você ainda não possui o software desta empresa no seu computador, então eles não monitorarão seu computador em relação à infecção por ransomware. Se você possui um software de segurança, você não precisaria pagar para remover a infecção - você já pagou o software para fazer esse trabalho.
>
> Bloqueadores de tela:
> Atualize para o nível de alerta laranja contra esses caras. Quando o ransomware de bloqueio de tela invade seu computador, isso significa que você está completamente paralisado fora do seu PC. Ao inicializar o seu computador, uma janela do tamanho da tela aparecerá, muitas vezes acompanhada por selo do FBI ou do Departamento de Justiça Americano, que aparenta ser oficial, dizendo que uma atividade ilegal foi detectada em seu computador e você deve pagar uma multa. No entanto, o FBI não impediria seu acesso ao computador ou exigiria o pagamento por conta de atividades ilegais. Se eles suspeitassem de pirataria, pornografia infantil ou outros crimes cibernéticos, eles utilizariam os meios legais apropriados.
>
> Ransomware de criptografia:
> Este é o tipo de coisa realmente desagradável. Estes são os caras que pegam seus arquivos e os encriptam, exigindo pagamento para descriptografar e devolver. A razão pela qual esse tipo de ransomware é tão perigoso é porque, uma vez que os criminosos cibernéticos tomam posse dos seus arquivos,

> nenhum software de segurança ou restauração do sistema pode devolvê-los. A menos que você pague o resgate - para a maioria deles, eles se foram. E mesmo que você pague, não há garantia de que os criminosos cibernéticos vão lhe dar esses arquivos de volta.

2.1.5.5 Cavalos de Tróia

O Cavalo de Tróia[6], ou trojan, é um programa malicioso que tem por finalidade executar instruções no computador, sem o consentimento do usuário, e criar uma vulnerabilidade para que o atacante tenha acesso total ao computador da vítima.

O malware tem como característica necessitar ser instalado pelo usuário de computador, que o baixou da internet na forma de um software legitimo, um protetor de telas para computador, arquivo de fotos, jogos etc. (CERT, 2016).

O cavalo de Tróia tem classificações de acordo com suas funções maliciosas, categorizados por programas antimalwares. Segundo CERT (2016), pode ser descrito as seguintes classificações:

> **Trojan Downloader:** instala outros códigos maliciosos, obtidos de sites na Internet.
> **Trojan Dropper:** instala outros códigos maliciosos, embutidos no próprio código do trojan.
> **Trojan Backdoor:** inclui backdoors, possibilitando o acesso remoto do atacante ao computador.
> **Trojan DoS:** instala ferramentas de negação de serviço e as utiliza para desferir ataques.
> **Trojan Destrutivo:** altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação.
> **Trojan Clicker:** redireciona a navegação do usuário para sites específicos, com o objetivo de aumentar a quantidade de acessos a estes sites ou apresentar propagandas.
> **Trojan Proxy:** instala um servidor de proxy, possibilitando que o computador seja utilizado para navegação anônima e para envio de spam.
> **Trojan Spy:** instala programas spyware e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante.
> **Trojan Banker ou Bancos:** coleta dados bancários do usuário, através da instalação de programas spyware que são ativados quando sites de Internet Banking são acessados. É similar ao Trojan Spy, porém com objetivos mais específicos.

Existem os mais variados tipos e ferramentas de malwares, com as mais variáveis funções com o objetivo de enganar as pessoas e cometer crimes virtuais como danificar e roubar dados, roubos financeiros, espionagem, sabotagens, entre outros.

---

[6] O "Cavalo de Troia", segundo a história grega, foi uma grande estrutura em forma de cavalo, utilizada como instrumento de guerra pelos gregos para obter acesso à cidade de Troia. A estátua do cavalo foi recheada com soldados que, durante a noite, abriram os portões da cidade possibilitando a entrada dos gregos e a dominação de Troia.

A tabela 1, faz uma comparação entre os tipos de malwares apresentados neste trabalho, suas características e comportamentos.

Tabela 1 - Resumo comparativo entre os códigos maliciosos.

	Vírus	*Worm*	*Trojan*	*Spyware*	*Ransomware*
Recebido automaticamente pela rede		✓			
Recebido por *e-mail*	✓	✓	✓	✓	✓
Baixado de *sites* na Internet	✓	✓	✓	✓	
Compartilhamento de arquivos	✓	✓	✓	✓	✓
Uso de mídias removíveis infectadas	✓	✓	✓	✓	
Redes sociais	✓	✓	✓	✓	
Mensagens instantâneas	✓	✓	✓	✓	
Inserido por um invasor		✓	✓	✓	✓
Ação de outro código malicioso		✓	✓	✓	
Execução de um arquivo infectado	✓				
Execução explícita do código malicioso		✓	✓	✓	✓
Via execução de outro código malicioso					✓
Exploração de vulnerabilidades		✓			✓
Insere cópia de si próprio em arquivos	✓				
Envia cópia de si próprio automaticamente pela rede		✓			✓
Envia cópia de si próprio automaticamente por *e-mail*		✓			✓
Não se propaga			✓	✓	
Altera e/ou remove arquivos	✓		✓		✓
Consome grande quantidade de recursos		✓			
Furta informações sensíveis			✓	✓	✓
Instala outros códigos maliciosos		✓	✓		
Possibilita o retorno do invasor					✓
Envia *spam* e *phishing*					✓
Desfere ataques na Internet		✓			✓
Procura se manter escondido	✓			✓	✓

Fonte: Adaptado de CERT (2016).

2.3 JOGOS DE TABULEIRO

O conceito de jogo é bastante amplo na nossa sociedade, envolvendo diversas tarefas do dia a dia das pessoas. Para PEREIRA (2016) a aplicabilidade do termo jogo se adapta em muitas atividades:

> A palavra “jogo” envolve uma gama enorme de atividades, muitas delas triviais e tão presentes em nosso dia a dia que às vezes sequer notamos que elas são, de fato, jogos. Fazer palavras cruzadas, assistir futebol, brincar de “esconde-esconde”, jogar videogames, todas essas atividades podem ser consideradas jogos.

Os jogos acompanham a humanidade por toda a sua história, existem relatos de que os egípcios jogavam um tipo de jogo de tabuleiro, com algumas características, muito parecidas com o que jogamos hoje, chamado Senet[7], representado na figura 6 há mais de 5000 anos (PICCIONE, 1980, p. 55-58).

Figura 6 - Representação da Rainha Nefertari jogando Senet

Fonte: Science Magazine (2020).

As mais variadas formas de jogo existem hoje, desde os chamados analógicos como jogo de cartas e tabuleiros, e os digitais, como vídeo games, jogos em dispositivos móveis, jogos de realidade aumentada e jogos de simulação em mundos virtuais.

Neste capítulo será dissertado o atual momento dos jogos classificados como tabuleiros modernos, ou também conhecidos como *tabletop game*[8], que tiveram diversas mudanças com novos componentes, regras, mecânicas e ideias. Os jogos de tabuleiro, ou jogos de mesa (*Boardgames*), têm como principal característica a

[7] https://www.sciencemag.org/news/2020/02/original-board-game-death

[8] A tradução mais próxima na língua portuguesa para o termo tabletop game seria “jogo de mesa”.

utilização de um tabuleiro de papel, madeira ou metal e seus complementos, como dados, marcadores, cartas, miniaturas, fichas de recursos, tokens etc.

Seguindo uma série de regras, instruções e mecânicas, os jogadores precisam emergir em uma realidade alternativa para atingir um determinado objetivo para pontuar ou vencer o jogo. Que pode ser de forma competitiva, um jogador contra o outro, ou de forma cooperativa, onde os jogadores precisam se ajudar para alcançar o objetivo.

Pode-se dizer que a definição dos jogos é “um sistema de regras no qual agentes competem ao realizarem decisões ambíguas”. (BURGUN, 2012, p. 1, tradução nossa).

Jesse Schell (2008, p. 37, tradução nossa) em seu livro “*The Art of Game Design: A Book of Lenses, Schell*” propõe que: "Um game é uma atividade de solução de problemas, abordada com uma atitude de play." e que "Play é uma manipulação que satisfaz curiosidade". A definição de Schell é interessante por apresentar jogos como uma atividade de solução de problemas e por tentar fazer uma clara distinção dos termos game e play.

Para Huizinga (1990), os jogos trazem uma certa ordem, onde os jogadores submergem em uma realidade diferente, no qual tomam decisões para benefício próprio, ou cooperando com outros participantes.

Ainda existe bastante escassez de informações mais aprofundadas e seguras sobre as classificações de jogos de tabuleiro modernos na pesquisa cientifica de artigos ou livros no Brasil, que não sejam somente os jogos mais antigos como por exemplo o livro “The Oxford History of Board Games” (o qual ainda não possui tradução para o português), mas que contenham também os considerados “jogos modernos” (FILHO, LIMA e SOUZA, 2015).

> A via digital é onde mais se localizam informações sobre o tema, existem muitos artigos de interessados no assunto, editoras de jogos, publicadoras, designers de games, ilustradores, e mesmo aspirantes, que escrevem sobre em seus blogs, revistas digitais, websites, e até mesmo fóruns, além é claro, de entrevistas com pessoas do ramo disponibilizadas em sites que divulgam os jogos de tabuleiro mundo afora (FILHO, LIMA e SOUZA, 2015).

Os jogos de Tabuleiro Modernos surgem entre 1820 e 1869, motivados diretamente pela revolução industrial. Pequenos fabricantes começaram a produzir

versões dos jogos clássicos e novos jogos, com o intuito de atender a demanda da classe média emergente, tanto dos Estados Unidos como na Europa (GRECA, 2013).

Woods classifica três tipos principais de jogos de tabuleiro: os *classical game*s, *mass-market games* e *hobby game*s. Os jogos de tabuleiro conhecidos como Classical games são jogos sem autoria atribuída e sem a reivindicação de patente por alguma empresa ou organização, sendo o xadrez e dama um exemplo, ou seja, jogos clássicos e bastante antigos. Os jogos *Mass-market game*s definem quando existe um autor definido, produzidos em massa e voltados para o público em geral, como Monopoly, ou Banco Imobiliário no Brasil e Jogo da vida. E por fim, os *hobbys games* remetem aos jogos surgidos a partir da segunda metade do século XX, desenvolvimento que ocorreu fora do mercado de massa e, consequentemente, fora da grande indústria dos jogos e direcionado a segmentos particulares da sociedade. Para o Aleknevicus, o mercado de *hobby games* podem ser divididas em quatro pilares: wargames, role-playing games, collectible card games e eurogames (WOODS, 2012 apud ALEKNEVICUS, 2008, p. 21).

Os jogos de tabuleiro mais conhecidos são os jogos temáticos e os jogos estratégicos, que geralmente contém vários outros elementos de classificação como o RPG, exploração, miniaturas, cooperação, entre outros. Que serão exemplificados nos itens abaixo.

2.3.1 Jogos de tabuleiro temáticos

Os jogos de tabuleiro americanos temáticos têm como principal característica a construção de uma experiência dramática para todos os jogadores, onde ocorre uma narrativa com histórias, heróis, facções, surgimento de conflitos, com muitas variáveis de acontecimentos durante a partida (INBOARD GAMES, 2016). São conhecidos pelo apelido de *ameritrash* pela comunidade de jogadores de tabuleiro.

Como exemplos de jogos de tabuleiro temáticos temos o jogo *Zombicide* e o *Mansions of Madness*. Na figura 7 é possível ver o jogo de tabuleiro *Zombicide*, onde um grupo de sobreviventes, controlado por cada jogador, deve sobreviver a um ataque de mortos-vivos e atingir um objetivo, o jogo é cooperativo, de exploração e com vários elementos de jogos de RPG.

O jogo de tabuleiro *Zombicide* conta com várias versões, desde ambientes, armas e miniaturas futuristas à ambientes medievais, com algumas alterações em suas regras de jogo.

Figura 7 - Jogo de tabuleiro Zombicide

Fonte: Coopboardgames (2016).

Na figura 8, é possível ver o jogo de tabuleiro *Mansions of Madness*, que é ambientado dentro das histórias de terror do escritor Howard Phillips Lovecraft, no qual os jogadores assumem o papel de investigadores que entram em salas obscuras de mansões assombradas de Arkham e em outras localidades sinistras para desvendar segredos forâneos, solucionar quebra-cabeças ardilosos e lutar contra perigos sobrenaturais.

O jogo tem a necessidade do uso de um aplicativo que indica as instruções que os jogadores devem realizar, missões, resolução de enigmas e quebra-cabeças, inclusive criando uma ambientação sonora para a decorrência das jogadas.

Figura 8 - Jogos de tabuleiro Mansions of Madness

Fonte: Galapagos (2017).

2.3.2 Jogos de tabuleiro estratégicos

Os jogos de tabuleiro estratégicos, ou conhecidos com o termo *eurogames* são muito populares entre os jogos de tabuleiro. Esse estilo busca valorizar mais a estratégia, reduzindo assim o fator sorte e conflitos diretos. Apesar do nome, nem todo *eurogame* é necessariamente europeu, o termo ganhou forma quando o jogo *The Settlers of Catan*, um jogo de origem alemã, foi publicado nos Estados Unidos em 1995 e fez um sucesso jamais feito anteriormente (BODOGAMI, 2017).

A Alemanha tem um papel fundamental na popularização de jogos de tabuleiro no mundo todo. Segundo PEREIRA (2016), a forte cultura de jogos de tabuleiro na sociedade, impulsionadas pela mídia, trouxe um caso de sucesso no desenvolvimento de produção de jogos de tabuleiro:

> Segundo Stewart Woods (2012, p. 63), até por volta de 1980, a indústria de jogos de tabuleiro na Alemanha não se diferenciava de forma significativa da de outros países europeus ou da dos EUA. Contudo uma série de influências no mercado de jogos alemão, entre os anos de 1982-1994 posicionou o país como o centro da atenção mundial no que se relaciona a jogos de tabuleiro. Woods (2012) sugere que a tradição do país como fabricante de brinquedos, e uma mídia interessada em promover os jogos analógicos como um lazer positivo para todas as idades (incluindo, até hoje, a análise de jogos

> analógicos nos jornais diários), auxiliou no desenvolvimento de uma cultura única e muito favorável para estes produtos.

Com esse sucesso se desenvolveu diversas e importantes associações de desenvolvedores de jogos como a SAZ[9], feiras internacionais como a *Essen Games Fair*[10], centros de pesquisa e documentação de jogos analógicos, e o prêmio mundialmente conhecido *Spiel des Jahrs*[11], que premia os melhores jogos de tabuleiro do ano no mundo todo, sendo uma das maiores honraria que um jogo pode receber.

Para Woods, os jogos de tabuleiro classificados como *eurogames*, buscam a cultura da pacificidade entre os jogadores, como uma forma de mudança cultural para o pós-guerra na Europa, que pode ser vista abaixo:

> Enquanto títulos de jogos de tabuleiro americanos como Risk (1957) focado em formas diretas de competição jogador a jogador, os jogos de tabuleiro de estilo alemão foram desenvolvidos para se concentrar em formas mais indiretas de conflito. Em vez de lutar contra um adversário, os eurogames foram desenhados em torno da ideia da habilidade individual de um jogador para maximizar a eficiência. Se os títulos de jogos de tabuleiro americanos do pós-guerra estivessem focados na guerra e conflito, os jogos de tabuleiro de estilo alemão eram focados na simulação de conflitos pacíficos, escambo, comércio e troca (Woods, 2012).

Também segundo Woods, os jogos categorizados como *eurogames* apresentam as seguintes características:

> Os Eurogames podem, neste contexto, ser classificados por um conjunto de características comuns. Quando comparados aos jogos de tabuleiro de estilo americano, os eurogames tentam não esconder nenhuma informação do jogador (todo jogador está ciente de que movimentos você pode e não pode fazer), envolve muito pouca sorte e normalmente não elimina jogadores do jogo. (Woods, 2012).

O jogo de tabuleiro *The Settlers of Catan,* visto na figura 9*,* é vendido no Brasil com o nome Catan e produzido e distribuído pela empresa Devir, foi desenvolvido pelo alemão Klaus Teuber, tem como característica o seu tabuleiro formar uma ilha, montadas por hexágonos de papel, onde os jogadores precisam colonizar, tendo que administrar recursos e territórios. O jogo classifica-se como competitivo, pois cada jogador tem como papel ser um povo disputando a “ilha de Catan”, e como regra é permitido a negociação de recursos entre os jogadores para atingir seus objetivos de

[9] *Spieleautorenzunft*. Ver www.spieleautorenzunft.de
[10] Ver www.merz-verlag-en.com
[11] Ver www.spiel-des-jahres.com

pontuação. O primeiro jogador que atingir a pontuação estabelecida nas regras é o vencedor do jogo.

Figura 9 - Jogo de tabuleiro Catan

Fonte: Devir (2019).

Outro jogo de tabuleiro muito conhecido para exemplificar os jogos estratégicos é o jogo Carcassonne, que leva o nome da cidade medieval de Carcassonne na França. O jogo, que pode ser visto na figura 10, foi desenvolvido pelo alemão Klaus-Jürgen Wrede no ano 2000, e publicado em português no Brasil pela empresa Devir no ano de 2002. Atualmente o jogo de tabuleiro vendeu mais de 10 milhões de cópias em todo o mundo.

Figura 10 - Jogo de tabuleiro Carcassonne

Fonte: Devir (2015).

O jogo inicia com apenas uma peça virada para cima, e outras 71 que serão sorteadas no decorrer da partida por cada jogador e colocadas adjacentes a peça já colocada, formando um grande tabuleiro, interligando estradas, cidades, campos e igrejas.

Após o jogador colocar a peça, ele pode reivindicar o território colocando um "*meeple*[12]", derivado do inglês "*my people*" ou conhecido também como seguidor, uma peça de madeira em forma de pessoa. Que será utilizada para a contagem de pontos no final de uma partida.

[12] https://mykindofmeeple.com/what-is-a-meeple/

3 TRABALHOS CORRELATOS

Nos capítulos sequentes dessa seção, serão expostos alguns trabalhos com jogos de tabuleiro educacionais com a temática de segurança da informação, os jogos são analógicos e não digitais, ou como a literatura classifica como desplugados, alguns jogos necessitam um aplicativo para auxiliar na mecânica do jogo. Existem jogos educacionais comerciais e gratuitos para aplicação.

3.1 JOGO DE TABULEIRO KASPERSKY INTERACTIVE PROTECTION SIMULATION

O jogo de tabuleiro Kaspersky Interactive Protection Simulation (KIPS)[13], é um jogo desenvolvido pela empresa de segurança da informação Kaspersky Lab. O KIPS é um jogo de simulação de equipe, onde os participantes têm a tarefa de lidar com uma série de ameaças cibernéticas inesperadas, enquanto tentam maximizar lucros e manter a confiança do mercado.

A ideia do jogo é construir uma estratégia de defesa cibernética, fazendo escolhas dentre os melhores controles proativos e reativos disponíveis.

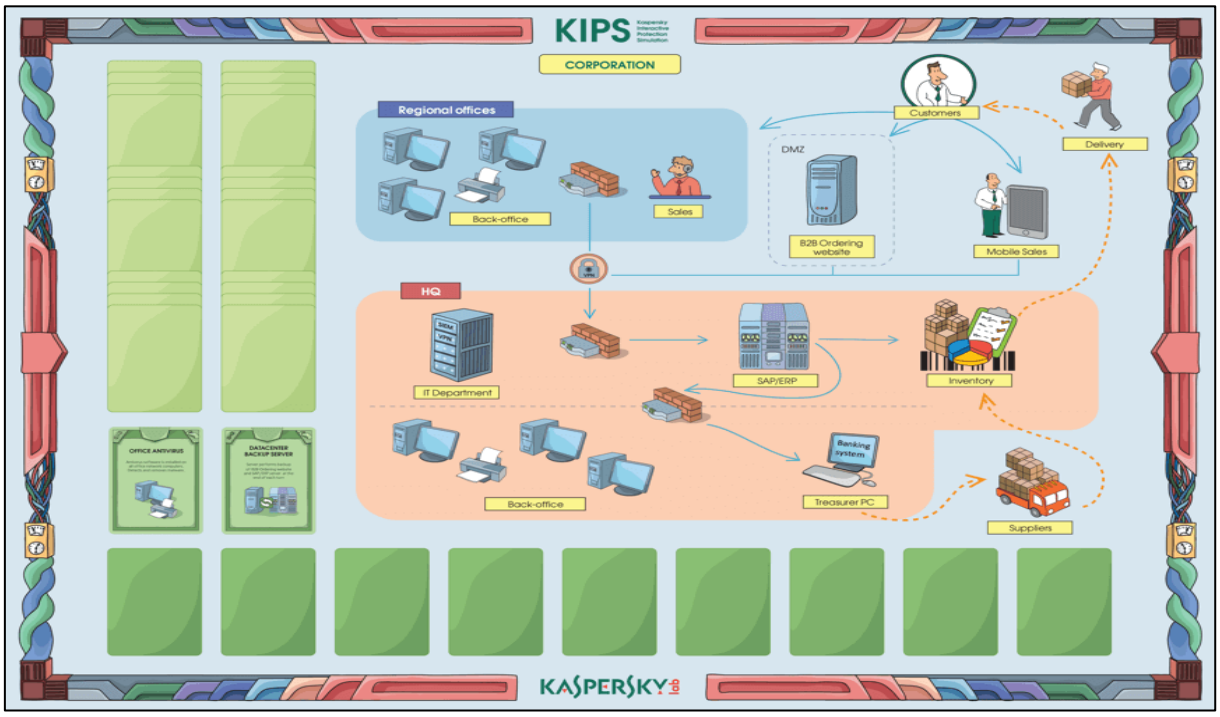
Segundo Kaspersky, o jogo KIPS tem as seguintes vantagens para o treinamento em empresas:

a) Oferece uma nova abordagem viável da segurança cibernética;
b) É divertido, envolvente e rápido (2 horas);
c) Cria cooperação através do trabalho em equipe;
d) Promove habilidades de iniciativa e análise através da concorrência;
e) Permite descobertas e erros na construção de segurança cibernética e comportamento cibernético para ser feito e analisado com segurança através da jogabilidade.

O jogo contém vários cenários de simulação para diversos ambientes que ele pode ser aplicado, como empresas (figura 11), usinas de energia elétrica (figura 12), setores públicos governamentais (figura 13) e setores financeiros (figura 14), e mais alguns como estações de tratamento de água, refinarias de petróleo e gás, e transporte (Kaspersky, 2019).

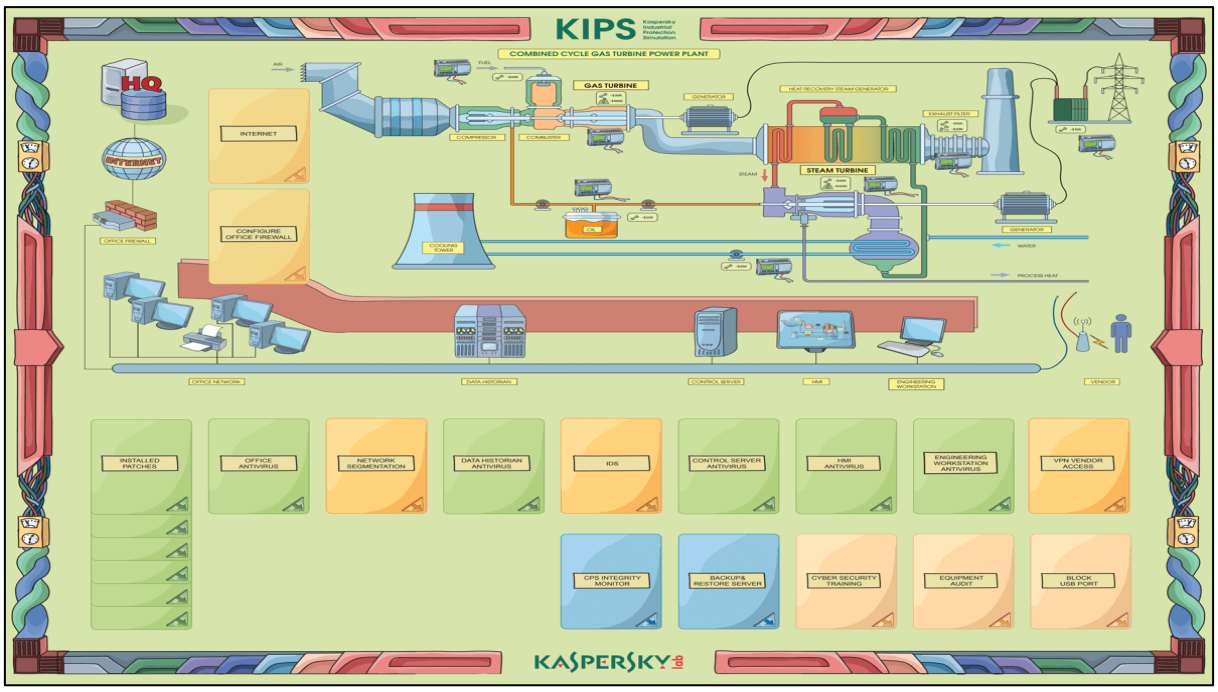
[13] Ver https://www.kaspersky.com/enterprise-security/security-awareness

Figura 11 - Tabuleiro KIPS para empresas ou corporações



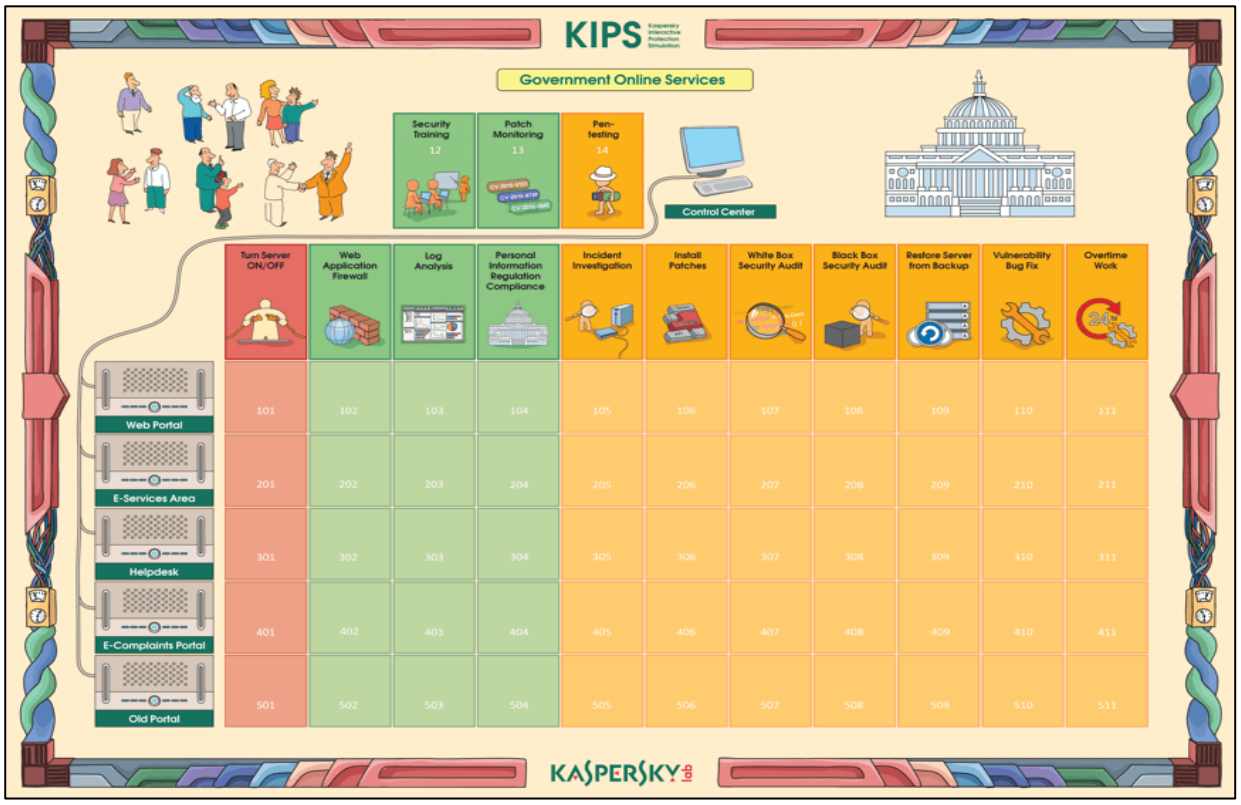
Fonte: Kaspersky (2019).

Figura 12 - Tabuleiro KIPS para usinas de energia elétrica



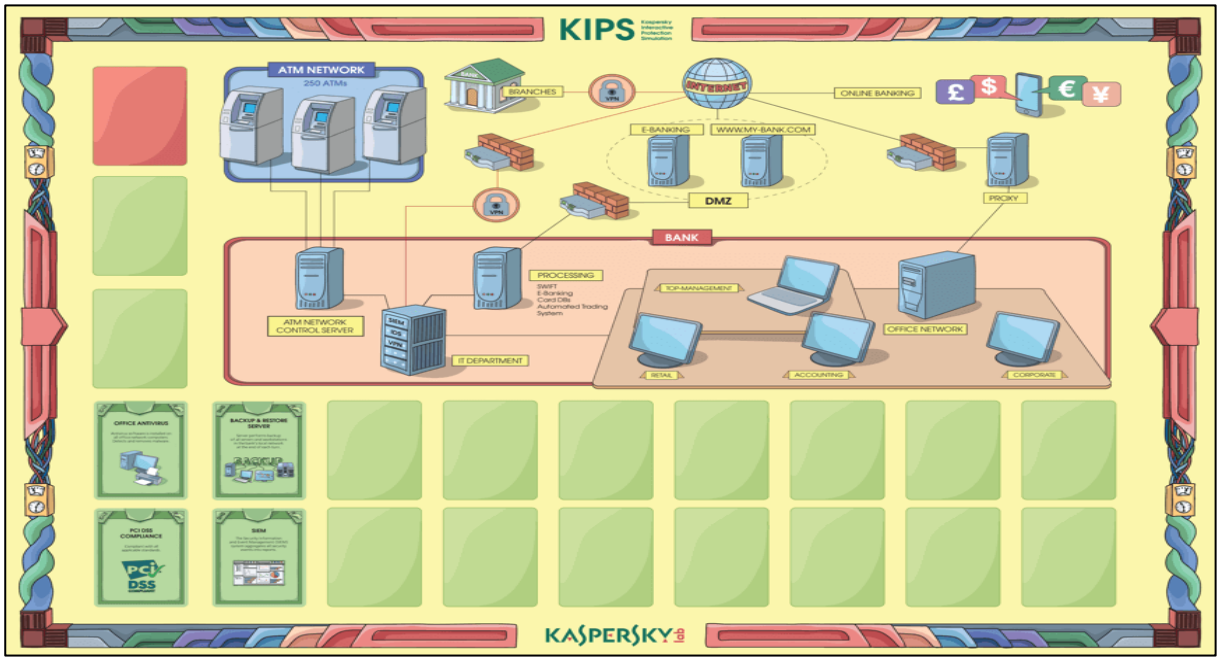
Fonte: Kaspersky (2019).

Figura 13 - Tabuleiro KIPS para os setores governamentais



Fonte: Kaspersky (2019).

Figura 14 - Tabuleiro KIPS para os setores financeiros



Fonte: Kaspersky (2019).

O jogo de tabuleiro KIPS conta com várias cartas, que podem ser vistas na figura 15, sendo elementos do jogo de tabuleiro que representam recursos de segurança na simulação, com custos e tempo para a implantação.

Figura 15 - Cartas do jogo KIPS

Fonte: Tomsk (2018).

O Instituto Nacional de Tecnologia do Japão (KOSEN)[14] utilizou o jogo de tabuleiro KIPS para medir sua eficácia no ensino da segurança de informação dos seus alunos.

Segundo YONEMURA *et al* (2018), a prática de resultados experimentais mostrou que o jogo contribui para o efeito educacional positivo e foi encontrada a possibilidade de transferência positiva de habilidades.

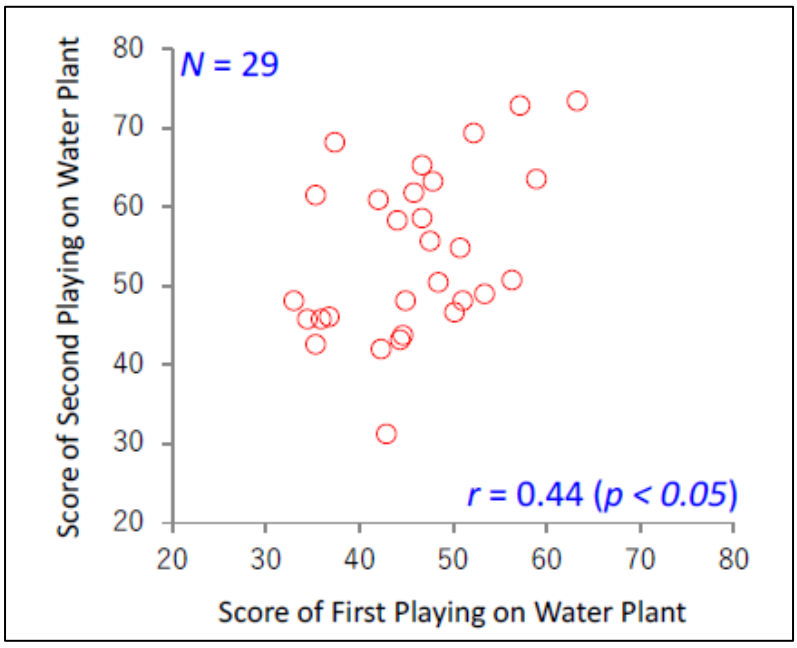
O jogo foi aplicado em alunos das turmas de engenharia elétrica e eletrônica. Inicialmente, com uma média de 30 alunos e com quatro partidas realizadas, duas com a versão do tabuleiro de estação de tratamento de água e outras duas com a versão do tabuleiro coorporativo. Após três dias repetiram o jogo com a versão da estação de tratamento de água e após quatro dias com a versão do tabuleiro coorporativo.

Para YONEMURA *et al* (2018), houve um crescimento das habilidades e do conhecimento dos participantes pela repetição do uso do jogo e a medida da pontuação.

[14] Ver https://www.akashi.ac.jp/english/kosen

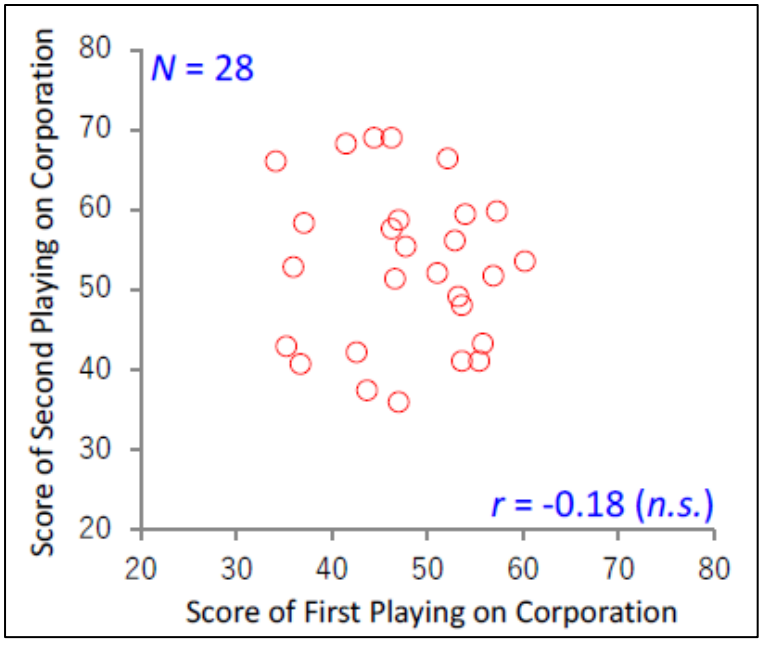
O trabalho de YONEMURA (2018) fez comparações com gráficos de dispersão entre as partidas utilizando o tabuleiro da estação de tratamento de água, gráfico 4. E a partida com o tabuleiro da corporação, no gráfico 5. Nestes dois testes não foi possível comparar a pontuação por ser jogos de ambientes diferentes.

Gráfico 4 - Primeiro teste utilizando o jogo KIPS com a estação de tratamento de água



Fonte: YONEMURA (2018).

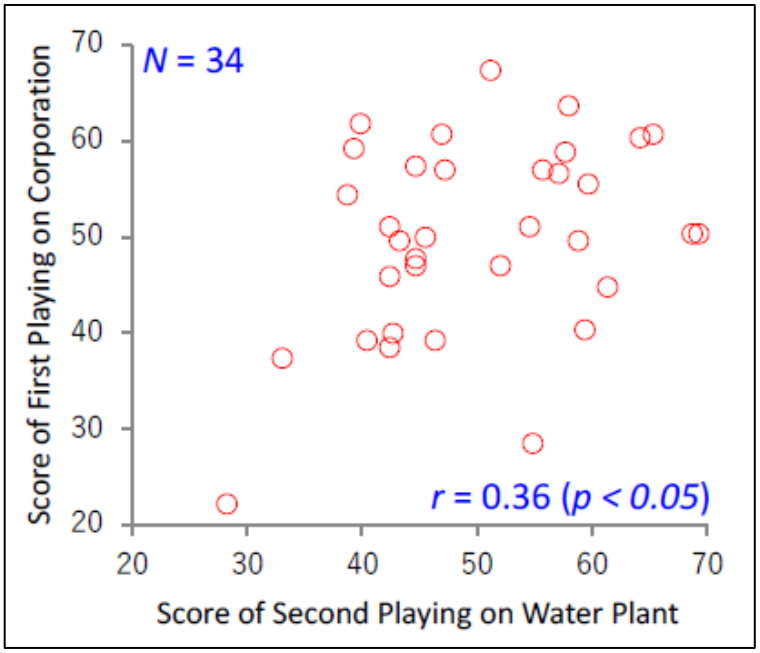
Gráfico 5 - Primeiro teste utilizando o jogo KIPS com a corporação



Fonte: YONEMURA (2018).

Após os primeiros testes foi realizado um segundo teste com o tabuleiro da estação de tratamento de água, tendo alteração para uma maior pontuação entre os participantes, no gráfico 6:

Gráfico 6 - Segundo teste utilizando o jogo KIPS com a estação de tratamento de água



Fonte: YONEMURA (2018).

Para YONEMURA (2018) houve um grande acréscimo de conhecimento e habilidades entre os participantes do teste.

3.2 JOGO DE TABULEIRO [D0X3D!]

O [d0x3d!] é um jogo de tabuleiro de código aberto projetado para envolver um corpo discente diverso na terminologia de segurança de rede, mecânica de ataque e defesa e construções básicas de segurança. Sua mecânica apresenta um jogo cooperativo, coleção de cenários, poderes variáveis de jogador em um sistema de pontos de ação e um tabuleiro modular que simula uma topologia de rede. O jogo de tabuleiro [d0x3d!] foi criado por Zachary Peterson e Mark Gondree e inspirado no jogo de tabuleiro *Forbidden Island*, criado por Matt Leacock e publicado pela *Gamewright*. Na figura 16 é ilustrado o tabuleiro montado para o jogo.

Figura 16 - Tabuleiro de [d0x3d!]

Fonte: Boardgamegeek (2012).

Segundo Gondree e Peterson (2012), o design do jogo foi pensado para ser divertido, acessível, colaborativo, significativo, discreto, modificável e catalítico.

3.3 THE AGILE APP SECURITY GAME

O jogo foi desenvolvido pela equipe Security Lancaster, para auxiliar na programação de aplicativos e gerenciamento de projetos, o jogo faz com que os jogadores assumam o papel de gerentes de produtos para desenvolver um aplicativo seguro.

Os jogadores selecionam entre uma variedade de opções com funcionalidades de segurança para implementar e descobrem se suas escolhas impedem os ataques. O jogo requer um coordenador e precisa de cartas impressas e recortados com antecedência.

3.4 BACKDOORS AND BREACHES

O jogo “*Backdoors and Breaches, an Incident Response Card Game*” é um jogo educacional com a temática de segurança da informação de cartas desenvolvido pela empresa Black Hills Information Security.

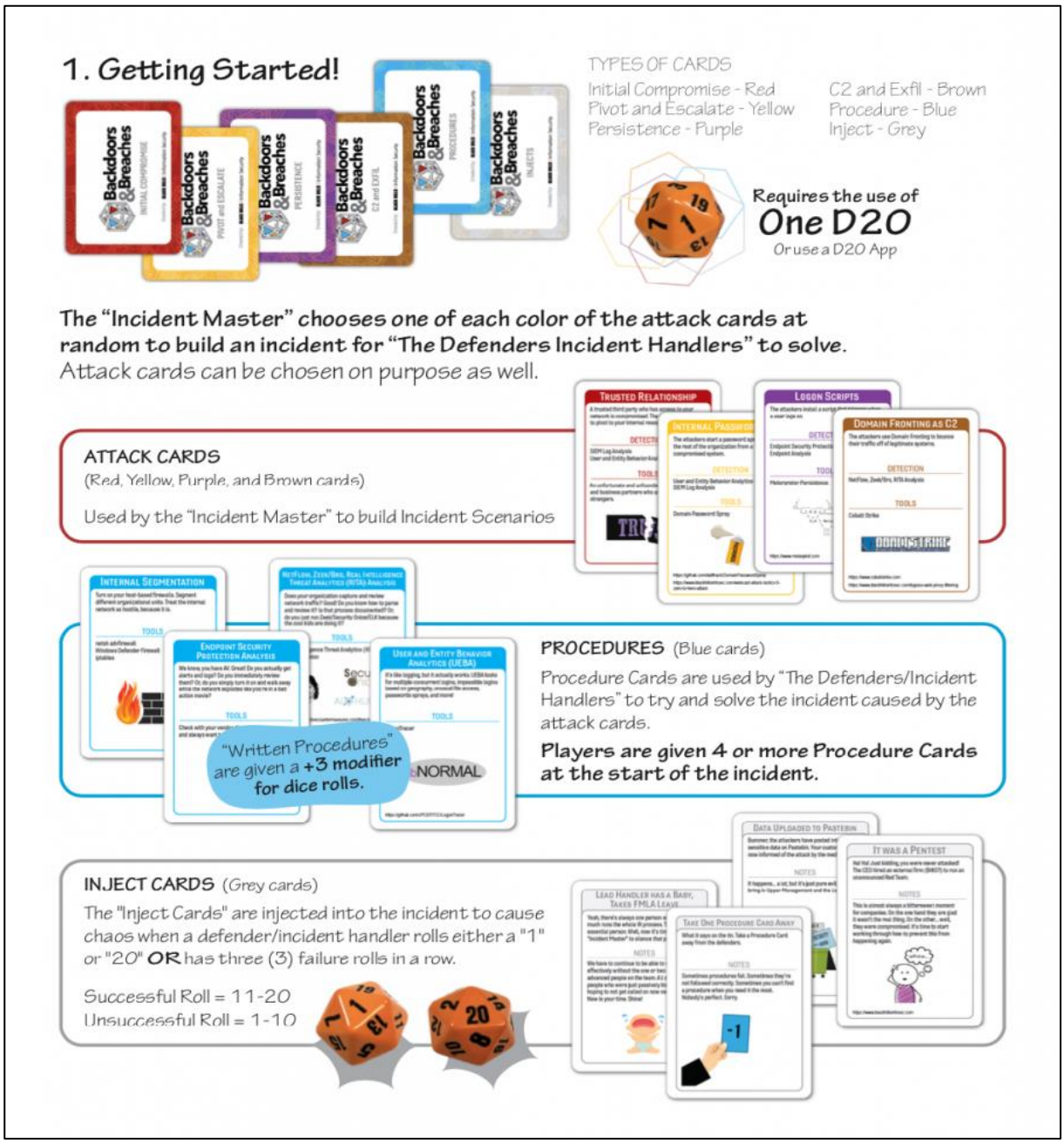
O jogo simula incidentes de segurança dentro de uma empresa, fazendo os jogadores tomarem decisões para resolver as falhas de segurança. Uma descrição do jogo pode-se ser lida abaixo:

> Procurando uma maneira de tornar os exercícios de mesa mais divertidos? Confira Backdoors & Breaches, um novo jogo de cartas para resposta a incidentes da Black Hills Information Security. Backdoors e breaches ajudarão você e sua equipe a entender os principais componentes, procedimentos e tecnologias necessários para solucionar um incidente. O B&B fornece tudo o que você precisa para desenvolver todo o incidente, desde o ataque inicial, ao pivô e escalada, movimento lateral e C2. Backdoors & Breaches contém 52 cartões exclusivos para ajudá-lo a realizar exercícios de mesa de resposta a incidentes e aprender táticas, ferramentas e métodos de ataque. São necessárias quatro cartas para construir um incidente, uma de cada categoria de ataque. (Compromisso inicial, rotação e escalonamento, persistência e C2 e Exfil) 3.840 cenários de incidentes. Sabemos que este jogo de cartas continuará a melhorar e evoluir ao longo do tempo com base nos seus comentários e ao ser jogado e modificado pela comunidade infosec. Requer um dado de 20 lados ou um aplicativo de dados de 20 lados gratuito instalado no seu telefone (BLACK HILLS INFORMATION SECURITY, 2019).

O jogo está em constante evolução, sendo adicionadas novas expansões, com novas cartas e cenários, dependendo dos pedidos da comunidade *infosec*, que é um grupo situado em Madison nos Estados Unidos da América que lutam contra os crimes virtuais, ou crimes cometidos na INTERNET.

Segundo o site da empresa produtora, Black Hills, o jogo conta com três grupos de cartas para tratar sobre incidentes de segurança, que são as cartas de ataque (vermelhas), cartas de procedimentos (azuis) e cartas de injeção (cinzas). Na figura 17 é possível vê-las:

Figura 17 - Instruções e tipos de cartas Backdoors & Breaches



Fonte: Blackhillsinfosec (2019).

3.5 CIA: COLLECT IT ALL

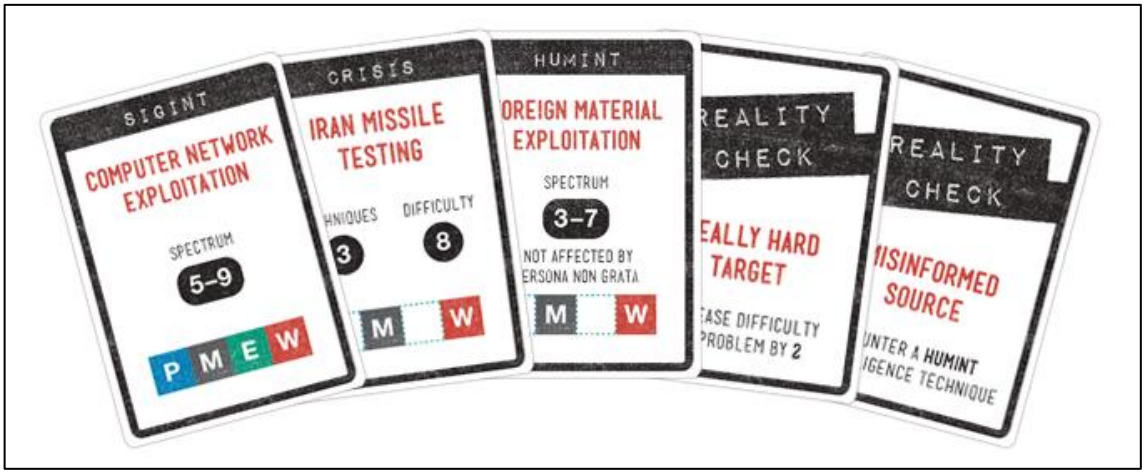
Collect It All, ou CIA, é um jogo de cartas competitivo desenvolvido pela empresa Diegetic Games, baseado nos baralhos de coleção da CIA (*Central*

Intelligence Agency) ou Agência Central de Inteligência dos EUA. O jogo atualmente é utilizado para treinamento de agentes da CIA, e ele simula um ambiente onde os agentes precisam coletar informações de inteligência e enfrentar ameaças de segurança em cada rodada, uma descrição do jogo pode ser vista abaixo:

> ...um baralho de mais de 150 cartas, os jogadores começam cada rodada com uma mão cheia de táticas de inteligência e devem elaborar estratégias para resolver com êxito várias crises. Todas as táticas e crises contêm aspectos - políticos, militares, econômicos e armas - e os jogadores só podem enfrentar crises se tiverem táticas com aspectos correspondentes. No entanto, jogadores rivais também têm cartas de "verificação da realidade" que podem ser usadas para complicar os esforços de seus oponentes (LUBIN, 2016).

Na Figura 18, é ilustrado algumas cartas do jogo CIA: Collect It All, o jogo está na língua inglesa conforme os textos das cartas.

Figura 18 - Cartas do jogo Collect it all



Fonte: Diegetic Games (2016).

3.6 CONTROL-ALT-HACK

Control-Alt-Hack é um jogo de tabuleiro sobre hackers de chapéu branco (White hat), baseado na mecânica de jogos da poderosa empresa de jogos Steve Jackson Games que também desenvolveu os jogos Munchkin, Car Wars, Illuminati e Hacker (CONTROLALTHACK, 2012).

O jogo simula uma pequena empresa de segurança chamada Hackers, Inc. onde os jogadores realizam o papel de hackers éticos (também conhecidos como chapéu branco) que realizam auditorias de segurança e prestam serviços de consultoria. O lema da empresa é: "Você nos paga para invadir você".

Os jogadores devem cumprir missões - tarefas que exigem seja aplicado as habilidades de hacker para ter sucesso. Como o uso de Engenharia Social, invasão de redes, alteração da programação de dispositivos etc.

Na figura 19 é possível ver o jogo de cartas Control-Alt-Hack e seus componentes:

Figura 19 - Jogo de tabuleiro Control-Alt-Hack

Fonte: Control-Alt-Hack (2012).

3.7 CRYPTO GO

Crypto Go é um jogo de cartas educacional projetado para ensinar criptografia simétrica atualizada. O Crypto Go foi projetado para envolver os jogadores com criptografia simétrica e ensiná-los sobre o uso correto e o nível de segurança das ferramentas simétricas. Ele conscientiza os jogadores da natureza efêmera dos níveis e padrões de segurança e os estimula a aprender mais sobre criptografia do mundo real (Gonzáles, 2018). O jogo pode ser baixado e impresso para uso educacional, e está disponível na língua inglesa e espanhola.

3.8 COMPARATIVO DOS JOGOS DE TABULEIRO EDUCACIONAIS

Todos os jogos educacionais apresentados neste capítulo apresentam conceitos de SI em suas aplicações, tendo características diferentes em suas mecânicas de jogo, classificação do tipo de jogo, língua que é apresentado e diferentes cenários. Os jogos KIPS, Th3_0ff1c3 e [D0X3D!] são classificados como jogo de tabuleiro ou *boardgame*, que se difere por ter um tabuleiro utilizado pelos jogadores além de marcadores, dados e cartas. Os demais jogos apresentados são caracterizados por ter o objeto de uso principal pelos jogadores o uso de cartas, classificando como jogo de cartas, ou *cardgames.* Os jogos de cartas geralmente apresentam regras mais simples e são executados em menos tempo, além de ter um valor menor para a confecção do jogo.

Todos os jogos apresentados neste capítulo não estão no idioma português, sendo na maioria no idioma inglês. Apenas o jogo TH3_0ff1c3 desenvolvido neste trabalho encontra-se no idioma português, facilitando a utilização na maioria das regiões do Brasil.

O jogo de tabuleiro Th3_0ff1c3 foi construído para ser colaborativo e competitivo, além de ser classificado na área de jogos de tabuleiro como um eurogame que utiliza a alocação de recursos e um American game que traz competitividade entre os jogadores em sua estratégia de pontuação, sendo híbrido em todas as formas. O jogo KIPS segue um estilo semelhante na classificação de colaborativo e competitivo, onde cada grupo de jogadores colabora e compete entre si pela pontuação final. Onde a mecânica pode trazer incentivos na interação social e a diversão entre os jogares participantes.

4 METODOLOGIA DA PESQUISA

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 (BARROS; LEHFELD, 2014).

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 (2009), 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*[15] onde foi configurado os critérios de inclusão e exclusão de artigos científicos, revistas, livros e sites. A busca teve como palavras-chave 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.

Com o resultado da pesquisa foram demonstrados nos capítulos de referencial teórico, trabalhos correlatos e de desenvolvimento do jogo de tabuleiro educacional apresentado neste trabalho.

[15] Disponível em: https://harzing.com/resources/publish-or-perish

Pela conclusão da pesquisa foi desenvolvido um jogo de tabuleiro moderno educacional 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_off1c3 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.

O processo compreendeu com as seguintes etapas sequenciais:

- Aplicação de teste demográfico;
- Aplicação de avaliação de conhecimento inicial;
- Apresentação do trabalho de pesquisa com demonstração de jogos de tabuleiro modernos;
- Explicação de regras e mecânicas do jogo Th3_0ff1c3 para toda a turma de alunos;
- Execução do jogo de tabuleiro Th3_0ff1c3;
- Aplicação de avaliação de conhecimento final;
- Aplicação de ferramenta de avaliação de jogos educacionais.

Para a coleta de dados e análise de resultados foram aplicados três questionários para obtenção das informações que foram nomeados com os seguintes títulos:

- Questionário demográfico (Apêndice B);
- Questionário de conhecimento (Apêndice C);
- Questionário de avaliação de qualidade de jogos (Apêndice D);

A utilização de questionários, segundo Gil (1999, p.128), pode ser definido “como a técnica de investigação composta por um número mais ou menos elevado de questões apresentadas por escrito às pessoas, tendo por objetivo o conhecimento de opiniões, crenças, sentimentos, interesses, expectativas, situações vivenciadas etc.”

Essa abordagem busca a obtenção de informações de cunho empírico, tentando entender como a pesquisa aplicada pode trazer resultados satisfatórios na sua execução.

O questionário demográfico é composto por 10 questões no formato de questões abertas, múltipla escolha e dicotômicas, onde foi possível verificar a atual situação social de cada participante da pesquisa. As variáveis demográficas são avaliadas com frequência nas pesquisas e descrevem características das pessoas, como etnia, idade, sexo e status socioeconômico (SHAUGHNESSY; ZECHMEISTER; ZECHMEISTER, 2012).

O segundo questionário desenvolvido para a aplicação da pesquisa foi o questionário de conhecimento, onde foram desenvolvidas 11 questões de formato aberto, múltipla escolha e dicotômicas, que compreendem alguns conceitos de SI aplicados com definições e algumas afirmações. O questionário coletou dados de conhecimento dos participantes de antes da aplicação da pesquisa e após a aplicação para analisar a efetividade educacional do jogo de tabuleiro Th3_0ff1c3.

O terceiro questionário avaliou a qualidade do jogo de tabuleiro com um total de 41 questões no formato aberta e utilizando a escala de Likert.

> A escala de Likert apresenta uma série de cinco proposições, das quais o respondente deve selecionar uma, podendo estas ser: concorda totalmente,

> concorda, sem opinião, discorda, discorda totalmente. É efetuada uma cotação das respostas que varia de modo consecutivo: +2, +1, 0, -1, -2 ou utilizando pontuações de 1 a 5. É necessária atenção quando a proposição é negativa. Nestes casos a pontuação atribuída deverá ser invertida. (CARMO, 2013).

Para o desenvolvimento do protótipo do jogo Th3_0ff1c3 e seus itens pertencentes a execução do jogo foram utilizados os seguintes softwares:

- Microsoft PowerPoint (Criação da primeira prototipação dos hexágonos que formam o tabuleiro);
- Photoshop CS6 (Criação das fichas dos jogadores, marcadores de segurança e marcadores de malwares);
- Strange Eons (Criação das cartas de Malwares e cartas de Incidentes de segurança);
- Photoscape X Pro (Ajustes de cores e retoques nas imagens).

A versão de prototipação da montagem do tabuleiro foi desenvolvida na língua inglesa para buscar profissionais de design gráfico em outros países para a criação de ideias e temas para a qualidade gráfica do jogo de tabuleiro Th3_0ff1c3.

O material gráfico do jogo de tabuleiro foi desenvolvido pelo autor do trabalho, e apenas as artes feitas nos hexágonos que compõem a construção do tabuleiro foram desenvolvidas pelo designer gráfico Emerson Eduardo Lima de Sa, no qual foi firmado contrato para a criação. Os detalhes do desenvolvimento do jogo de tabuleiro Th3_0ff1c3 podem ser vistos no capítulo seguinte deste trabalho.

Os resultados do trabalho estão publicados nesta dissertação e o jogo de tabuleiro está disponível na forma digital e na forma física para a impressão para a toda a comunidade.

4.1 CONTEXTO DE INVESTIGAÇÃO DA PESQUISA

A execução do projeto desenvolveu um jogo de tabuleiro moderno com conceitos de segurança da informação, que foi aplicado para universitários estudantes do curso da área da Computação.

4.2 ETAPAS DA PESQUISA

Etapa 1: Realizou-se um levantamento bibliográfico sobre as áreas de Segurança da Informação e jogos de tabuleiros educacionais.

Etapa 2: Os dados da pesquisa foram analisados conforme a revisão sistemática da literatura proposto por B. Kitchenham (2009).

Etapa 3: Foi desenvolvido uma ferramenta educacional para ensino de segurança da informação em forma de um jogo de tabuleiro educacional moderno com a temática de segurança. Em decorrência das restrições impostas pela Covid19 foi desenvolvido o jogo de tabuleiro no formato digital.

Etapa 4: O jogo de tabuleiro foi aplicado e testado em uma turma de alunos do curso de Sistemas de Informação, na disciplina de Segurança e Auditoria de Sistemas de Informação.

4.3 INSTRUMENTOS PARA COLETA DE DADOS

Para a realização deste estudo, foram utilizados como instrumentos de coleta de dados: foi obtido fotos, vídeos, um questionário demográfico, um questionário de avaliação de conhecimento antes e após aplicação do produto final e um questionário de avaliação baseado no método MEEGA+ do autor Petri et al. em 2018. O questionário foi aplicado individualmente para cada participante utilizando a plataforma Google Forms.

4.4 AMOSTRA, POPULAÇÃO-ALVO E CRITÉRIOS DE INCLUSÃO E EXCLUSÃO

A população em estudo para a aplicação da pesquisa foi composta por estudantes da computação de nível superior na cidade de Santa Maria - RS, contendo profissionais de diversas empresas, maiores de 18 anos do sexo masculino e feminino. A aplicação foi realizada no ano de 2021 com turma hibrida na forma presencial e online.

Os critérios de inclusão são os alunos do curso de graduação em Sistemas de Informação da Instituição Antônio Meneghetti Faculdade da disciplina de Segurança e Auditoria de Sistemas de Informação do 8º semestre. Como critério de

exclusão são as pessoas não alunas do curso de graduação em Sistemas de Informação da Instituição nomeada acima.

5 DESENVOLVIMENTO DO JOGO EDUCACIONAL

Neste capítulo é descrito o processo de prototipação e desenvolvimento do jogo de tabuleiro educacional com a temática de SI chamado Th3_0ff1c3 como continuidade do processo metodológico do trabalho.

5.1 ANÁLISE DO JOGO

Foi planejado e desenvolvido os seguintes requisitos para o jogo de tabuleiro Th3_0ff1c3:

- Como requisito do jogo, foi definido que ele deve ser jogável entre 2-4 pessoas;
- O jogo deve também ser aplicável em um tempo aproximado de 45 minutos, o equivalente a uma hora/aula em média;
- Deve ser um jogo não-digital para possibilitar a jogada sem uso de computadores, estimulando também a interação social entre as pessoas;
- Deve ter uma versão digital, para ser utilizada em modalidades de cursos não presenciais, atendendo aos protocolos da pandemia da Covid-19;
- Possuir em sua mecânica, 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.

5.2 Concepção do jogo

Nesta seção são apresentados os principais aspectos do jogo educacional desenvolvido. No quadro 2 a seguir são apresentadas as principais características do jogo.

Quadro 2 - 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/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.

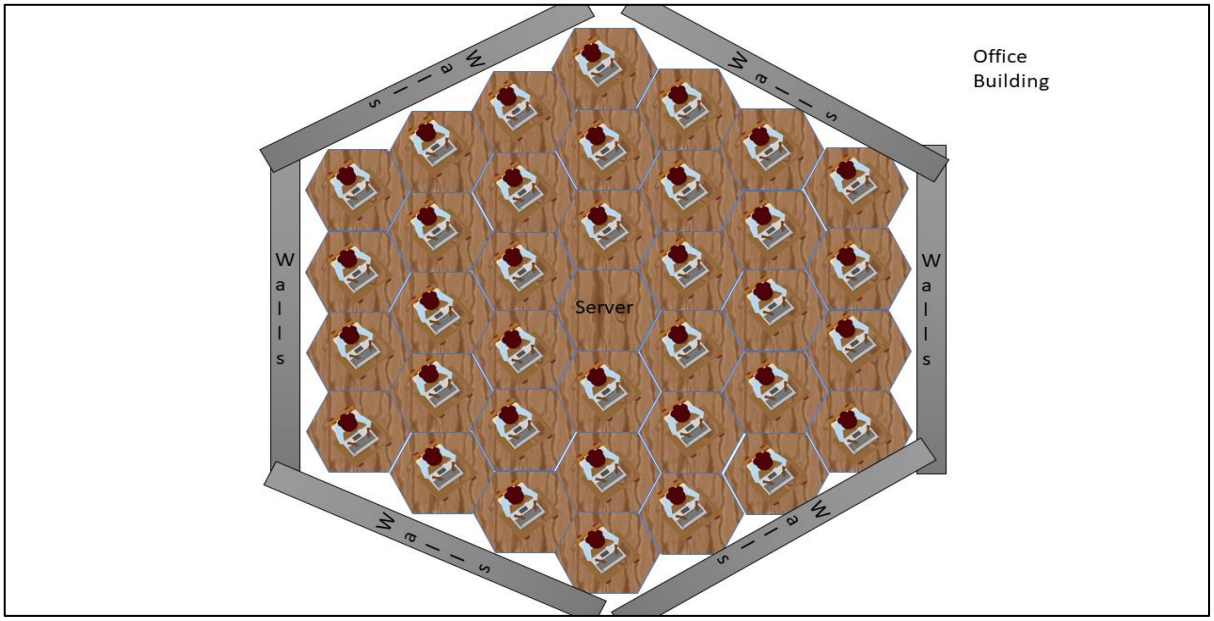
Fonte: Autoria própria.

5.3 DESIGN DO JOGO

Nesta seção é descrita a evolução do desenvolvimento do jogo de tabuleiro “Th3_0ff1c3” de protótipo até a sua versão final. O jogo segue desde o início do seu desenvolvimento a ideia de que o jogador deve coletar recursos para vencer e controlar os ataques virtuais. Na primeira versão, os hexágonos foram desenhados no software PowerPoint[16], com a ideia do tabuleiro montado. Utilizando a ideia de um tabuleiro modular, com um total de 37 hexágonos, onde um hexágono representa o servidor central da empresa fictícia, e outros 36 hexágonos que foram divididos em 4 cores dos possíveis jogadores, dando o resultado de 9 hexágonos para cada jogador. O tabuleiro central do jogo foi inspirado no tabuleiro do jogo “Catan”. A ideia inicial da montagem do tabuleiro pode ser vista na figura 20.

Os protótipos iniciais estão marcados com a língua inglesa para facilitar o contato com designers gráficos para as melhorias gráficas durante o desenvolvimento do jogo de tabuleiro, foi buscado pessoas dentro do Brasil e em outros países para melhorias estéticas das imagens.

Figura 20 - Tabuleiro montado com 37 hexágonos.



Fonte: Autoria própria.

Na segunda versão foi desenhada a ideia dos hexágonos para a construção do tabuleiro e as cartas de Malwares. Os hexágonos com o design gráfico de um

[16] https://products.office.com/pt-br/powerpoint

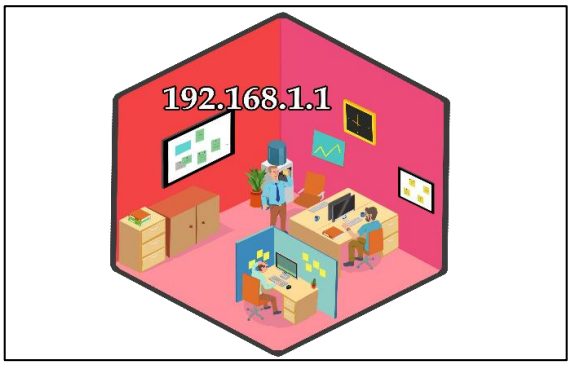
escritório foram utilizados do site “*dreamstime*[17]”, visto na figura 21, e a coloração foi modificada pelo software de edição de imagens “*PhotoScape X Pro*[18]”.

Figura 21 - Hexágono com o design gráficos de um escritório.

Fonte: Dreamstime (2020).

Para uma melhor qualidade na estética e experiência dos jogadores do jogo de tabuleiro, foi desenvolvido junto do designer gráfico Emerson Eduardo Lima de Sa, novos modelos de hexágonos que compõe a criação do tabuleiro de jogo, visto na imagem 22. Trazendo elementos gráficos únicos para o jogo de tabuleiro Th3_0ff1c3.

Figura 22 - Hexágono com o design gráficos de um escritório



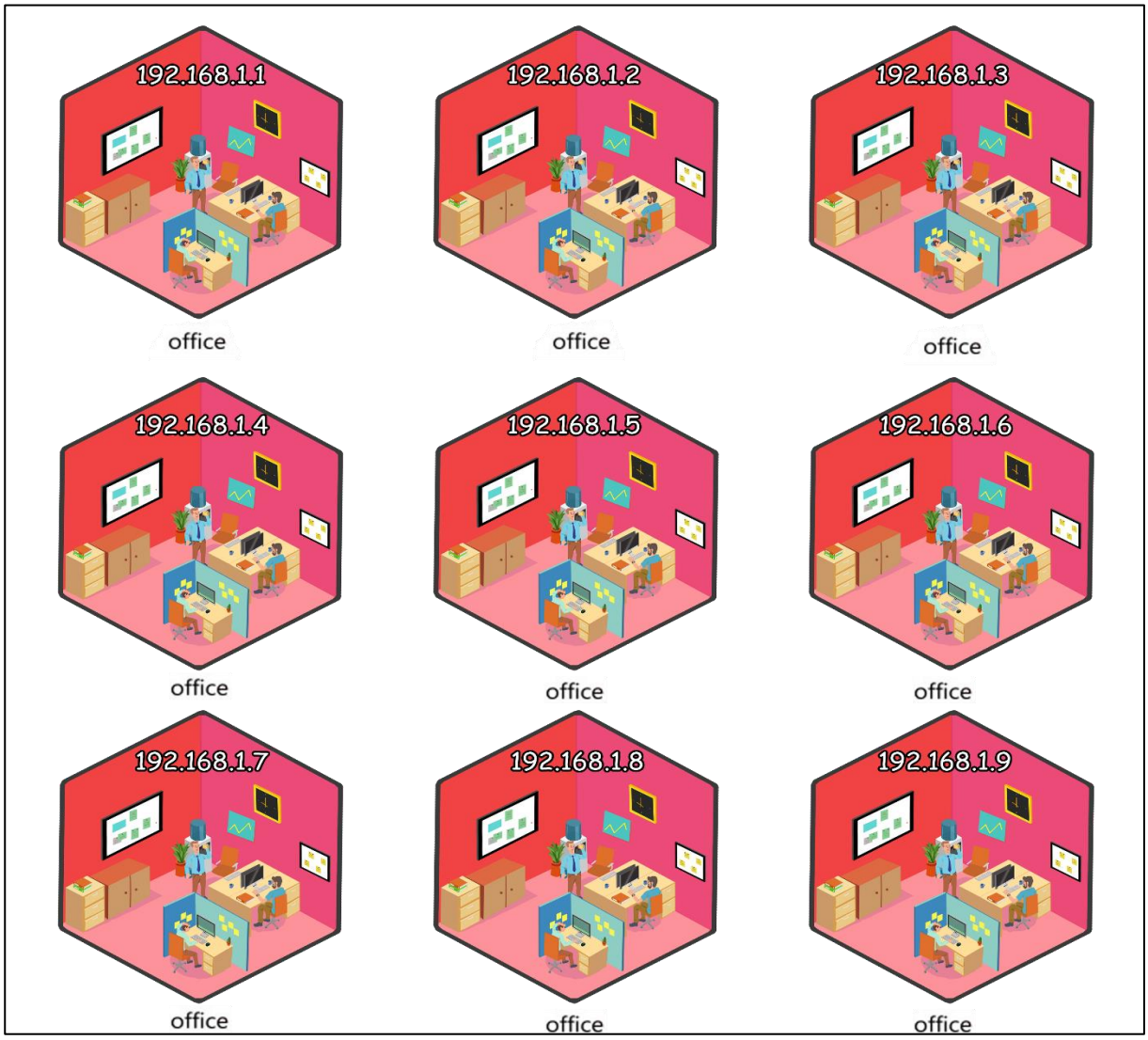
Fonte: Sa (2021).

A coloração para a divisão dos hexágonos para cada jogador são: vermelho, azul, amarelo e verde. Foi adicionado um hexágono neutro, não pertencendo a

[17] Ver https://pt.dreamstime.com/ilustra%C3%A7%C3%A3o-stock-conceito-abstrato-isom%C3%A9trico-liso-dos-departamentos-interiores-do-assoalho-do-escrit%C3%B3rio-d-image71360547
[18] Ver http://x.photoscape.org/

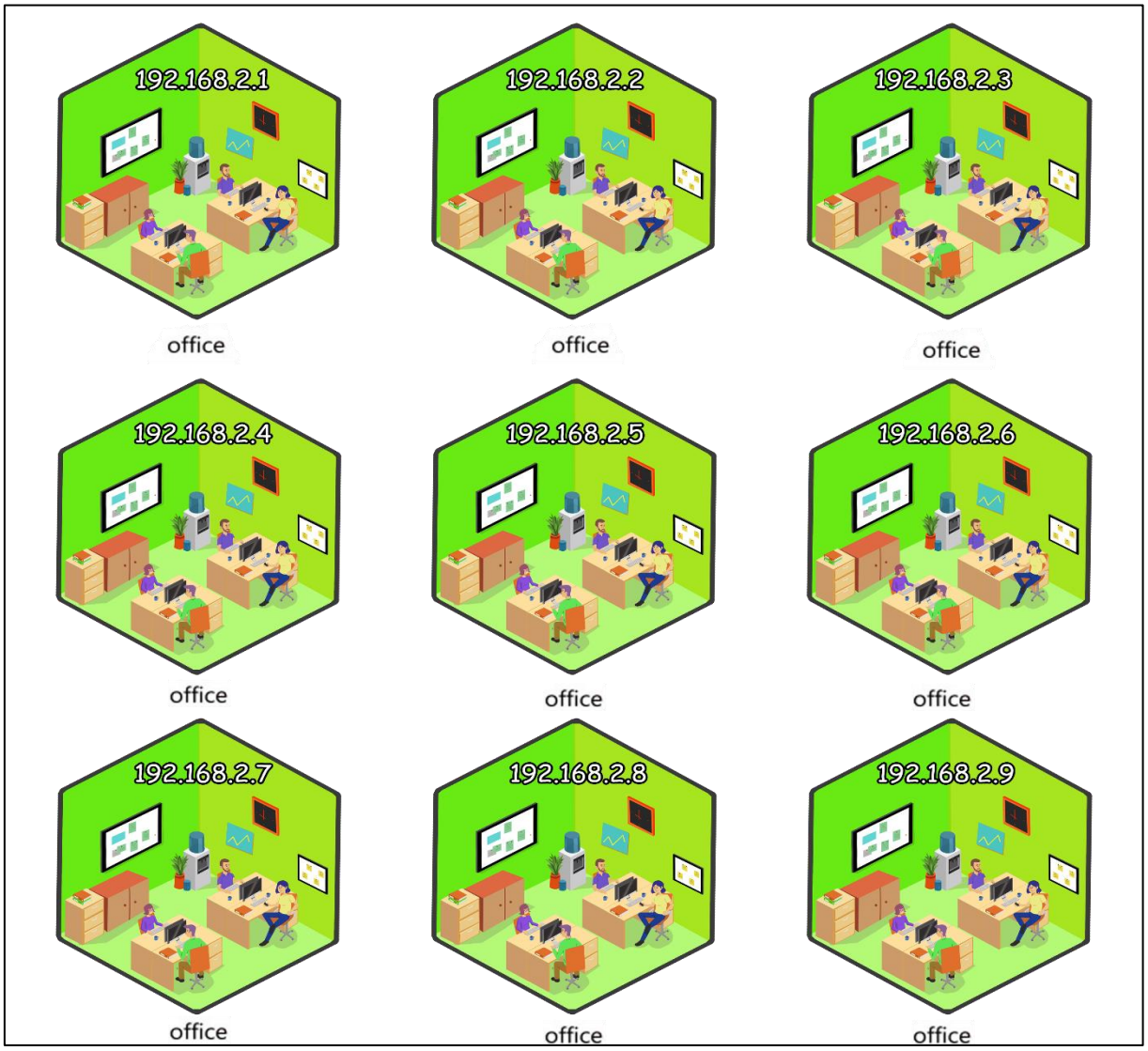
nenhum jogador, mas sendo o mais importante do tabuleiro, que é o servidor central da empresa. Foi adicionado um endereço de IP diferente para cada hexágono, onde o jogador 1 recebeu a cor vermelha com a sequência de IP 192.168.1.1 até 192.168.1.9, que pode ser visto na figura 23. O jogador 2 recebeu a cor verde com a sequência de IP 192.168.2.1 até 192.168.2.9, que pode ser visto na figura 24. O jogador 3 recebeu a cor amarela com a sequência de IP 192.168.3.1 até 192.168.3.9, visto na figura 25. E o jogador 4 recebeu a cor azul, com a sequência de IP 192.168.4.1 até 192.168.4.9, visto na figura 26.

Figura 23 - Hexágonos do Jogador 1



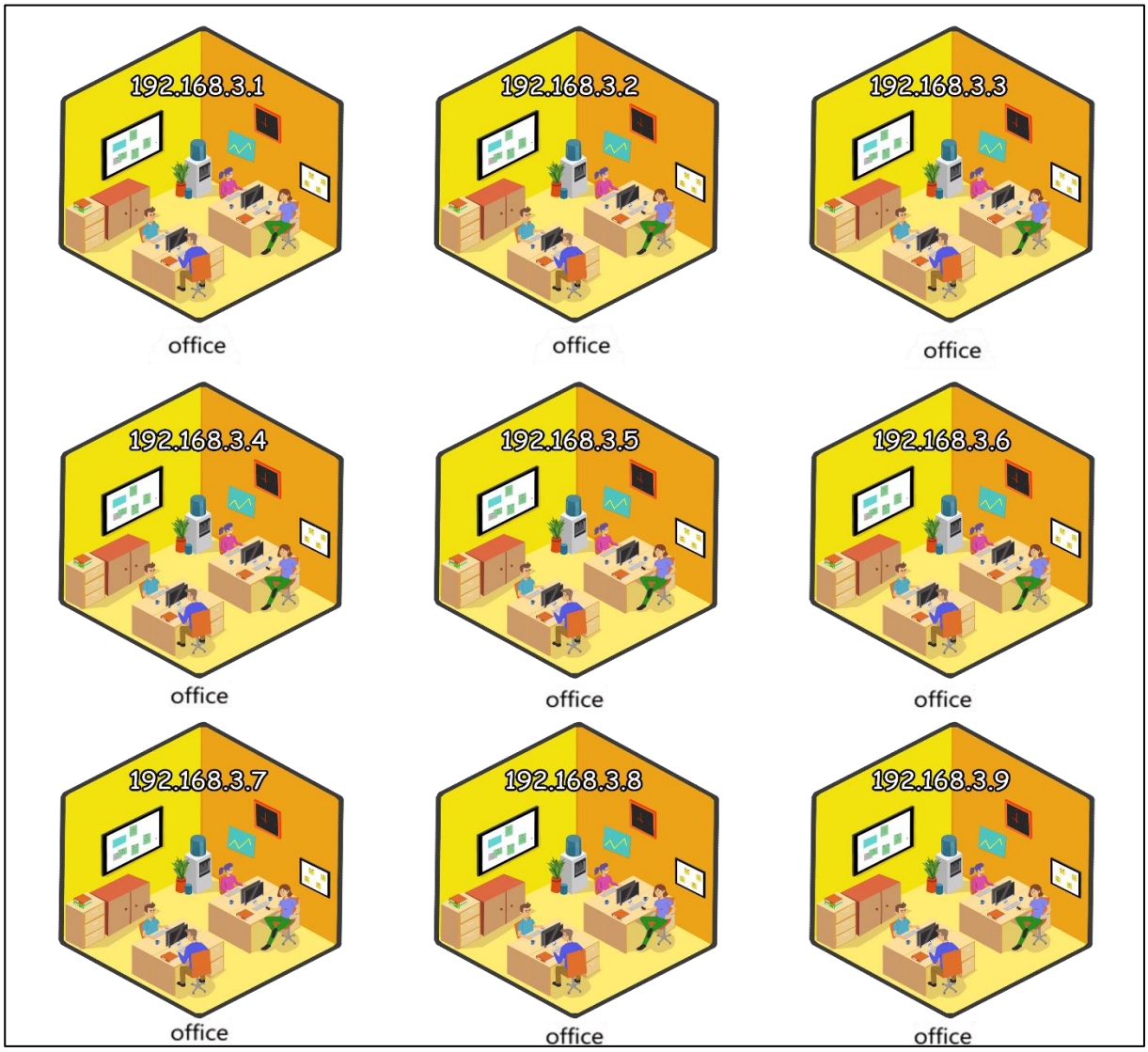
Fonte: Autoria própria.

Figura 24 - Hexágonos do Jogador 2



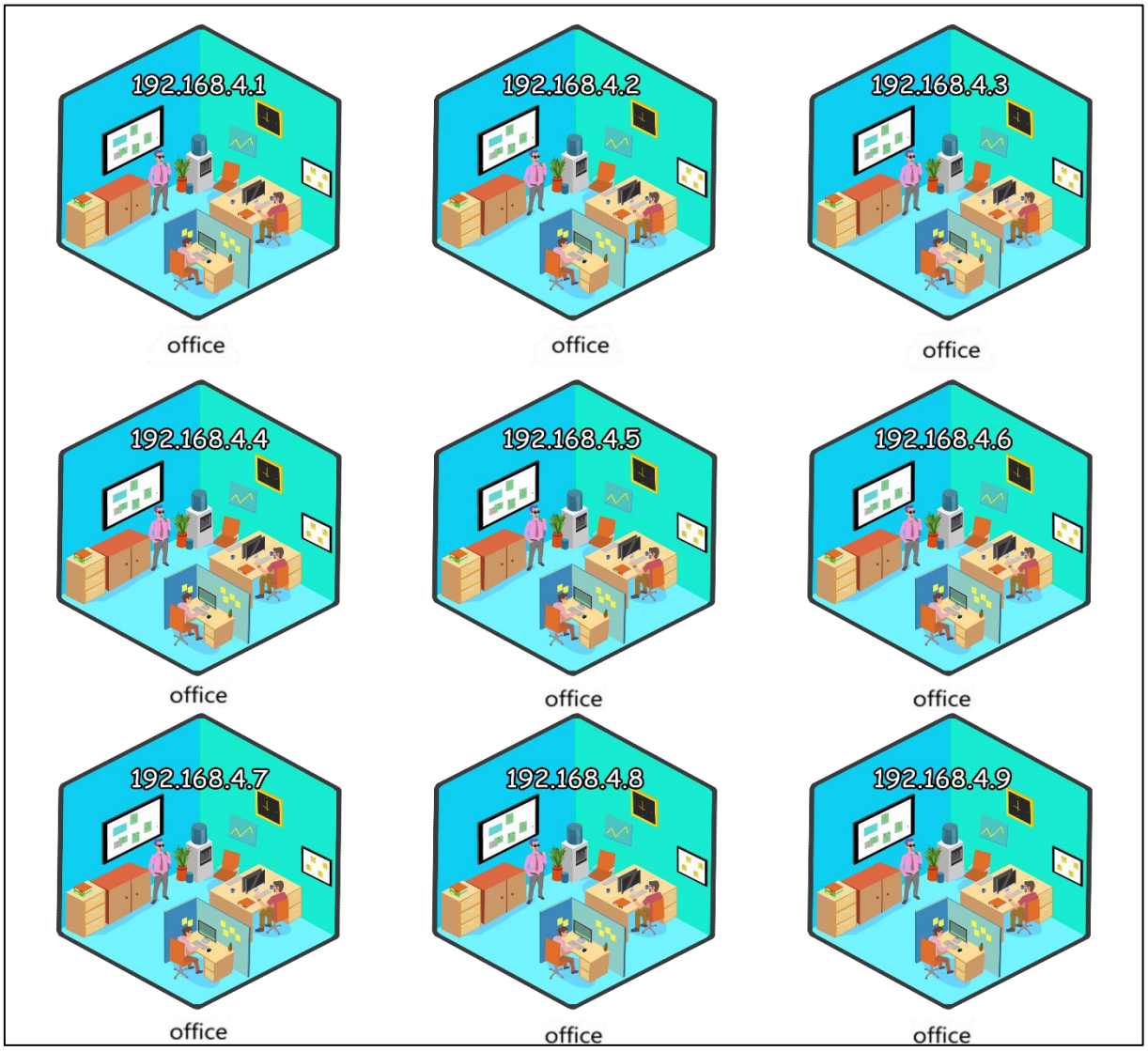
Fonte: Autoria própria.

Figura 25 - Hexágonos do Jogador 3



Fonte: Autoria própria.

Figura 26 - Hexágonos do Jogador 4



Fonte: Autoria própria.

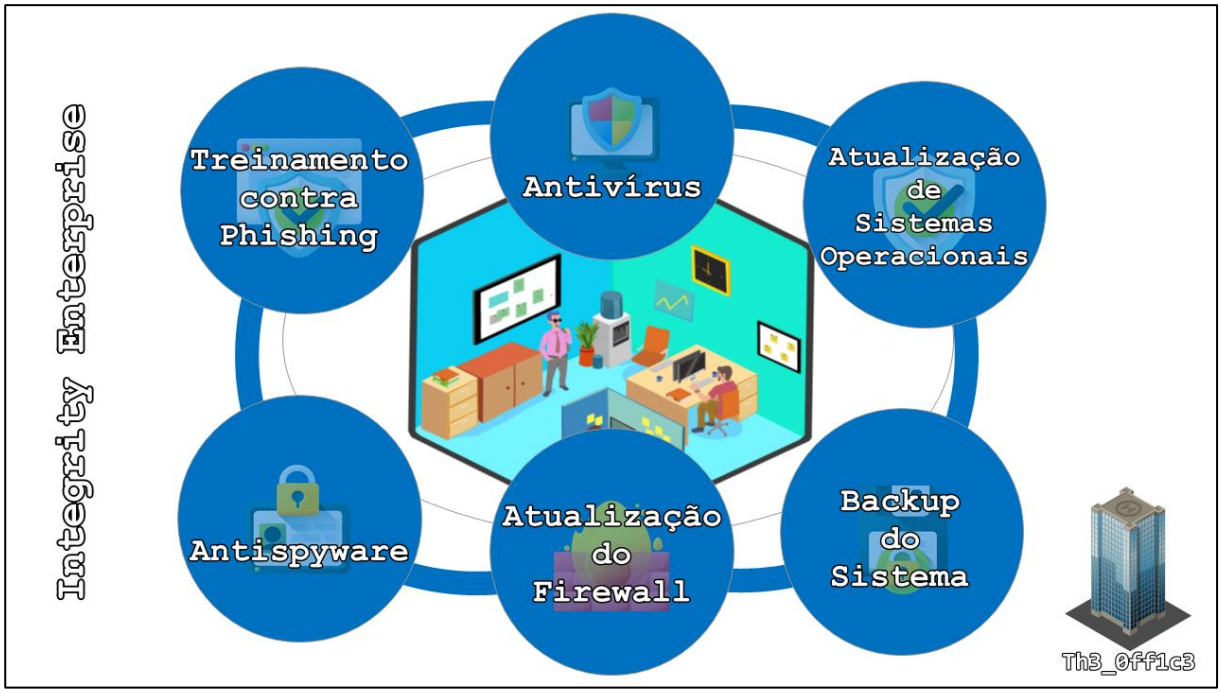
Cada jogador representa e administra uma empresa de segurança dentro do jogo, e foi desenvolvido no software de edição de imagem *Photoshop*[19], 4 pequenos tabuleiros para cada jogador, com espaços para guardar e gerenciar os tokens de recursos de segurança. A empresa do jogador 1 recebeu o nome de *"Confidenciality Enterprise"*, visto na figura 27. O jogador 2 recebe a empresa com o nome de *"Integrity Enterprise"*, visto na figura 28. O jogador 3 recebe a empresa com o nome de "*Disponibility Enterprise*", visto na figura 29. E o jogador 4 recebe a empresa com o nome de "*Information Enterprises*", visto na figura 30. Os nomes foram inspirados na tríade da segurança da informação: Confidencialidade, Integridade e Disponibilidade.

[19] Ver https://www.adobe.com/br/products/photoshop.html

Figura 27 - Cartão do jogador 1

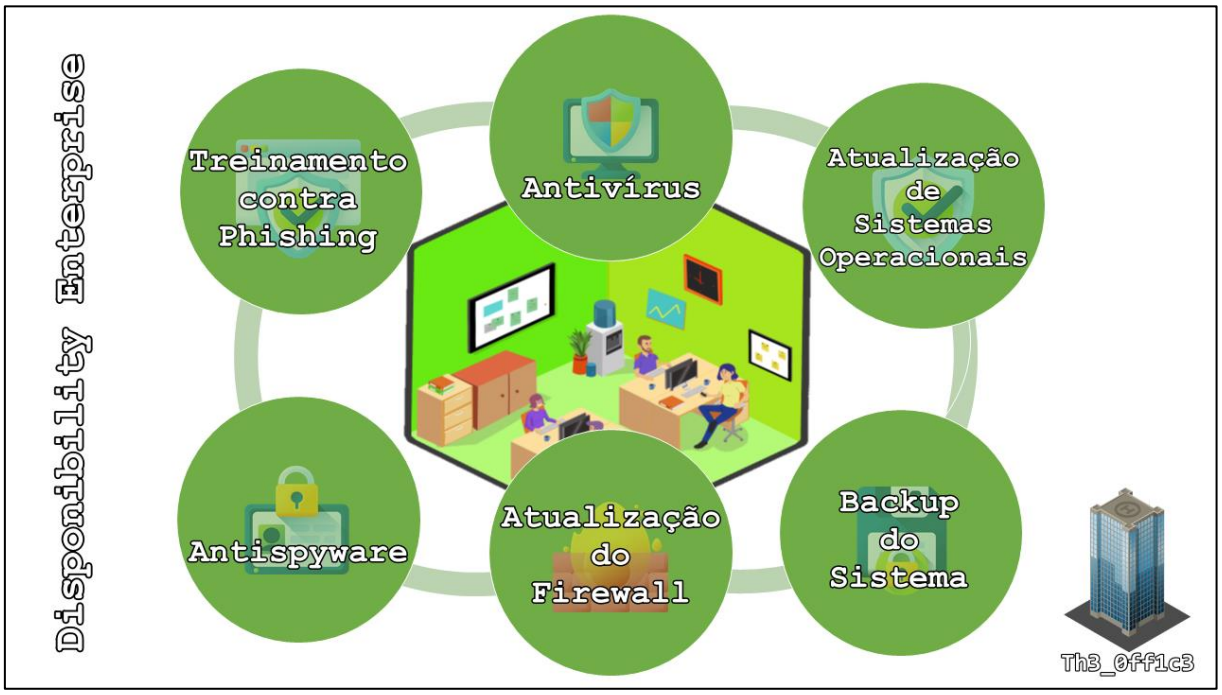
Fonte: Autoria própria.

Figura 28 - Cartão do jogador 2



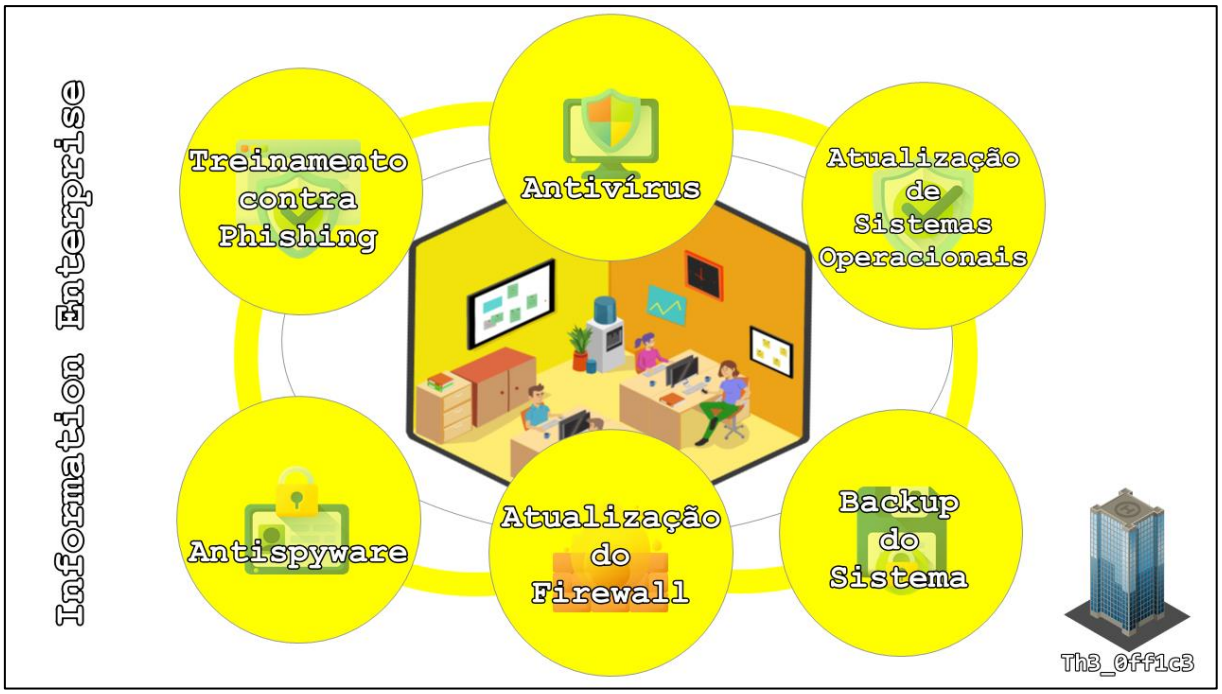
Fonte: Autoria própria.

Figura 29 - Cartão do jogador 3



Fonte: Autoria própria.

Figura 30 - Cartão do jogador 4



Fonte: Autoria própria.

As cartas de Malwares foram desenvolvidas no software "*Strange Eons 3*[20]", com as cartas representando *ransomware*, *phishing*, *worm,* cavalo de Tróia, vírus e *spyware,* representadas na figura 31*.* As cartas descrevem o que cada Malware ocasiona em um ataque real e seus efeitos dentro do tabuleiro.

Figura 31 - Cartas de Malwares

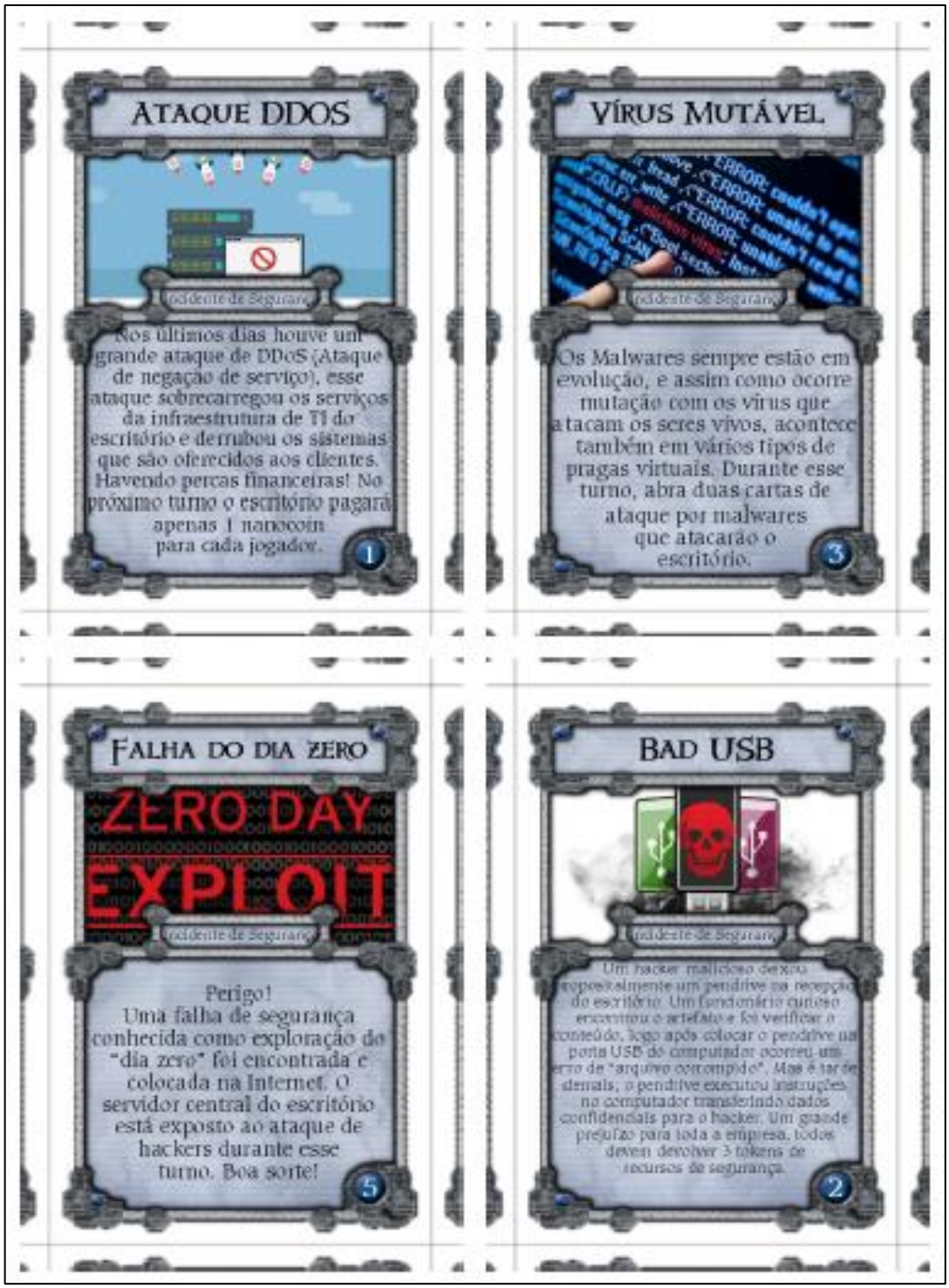
Fonte: Autoria própria.

O jogo também utiliza uma mecânica de alteração de algumas regras, causadas por incidentes de segurança, para esses casos foram desenvolvidas algumas cartas para representar eventos que simulam incidentes de segurança, como

[20] Ver https://cgjennings.ca/eons/

ataques de negação de serviço, mutação de malwares, uso de equipamento do tipo "*Bad USB"*, entre outros, vistas na figura 32.

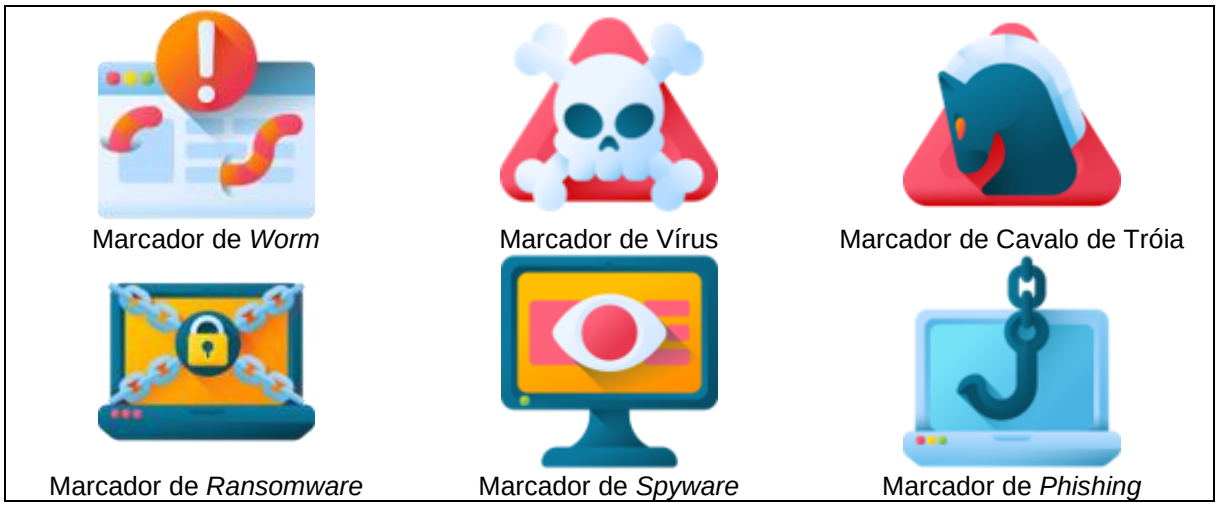
Figura 32 - Incidentes de segurança



Fonte: Autoria própria.

Para representar as ameaças virtuais e os recursos de segurança no tabuleiro, foram escolhidas algumas imagens que retratam os tipos de malwares aplicados pelas cartas de Malwares e os recursos de segurança para resolvê-los, os *tokens*, ou marcadores, foram escolhidos no site Flaticon[21]. Que pode ser visto nas figuras 33 e 34.

Figura 33 - Tokens de Malwares



Fonte: Flaticon (2020).

Figura 34 - Tokens de Malwares e recursos de segurança

Fonte: Flaticon (2020).

[21] https://www.flaticon.com/packs/cyber-security-54

O jogo de tabuleiro foi montado em mesa conforme figura 35, 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 35 - Tabuleiro montado

Fonte: Autoria própria.

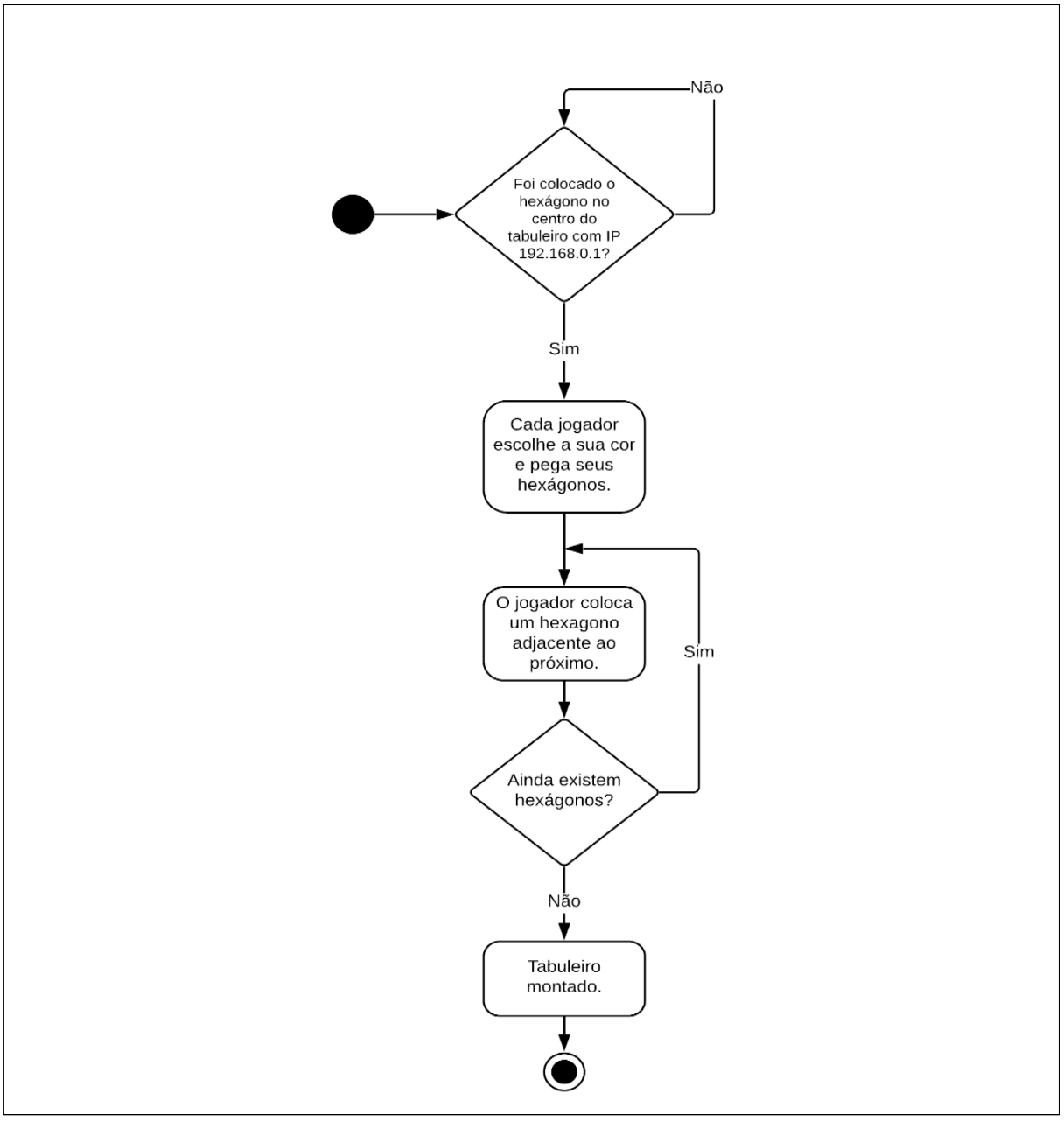
Para o entendimento das regras, componentes e conceitos do jogo de tabuleiro foi produzido um manual de instruções que pode ser visto no apêndice A deste trabalho.

5.4 MODELAGEM DO JOGO

Com objetivo de modelar o jogo e o entendimento das mecânicas e lógicas apresentadas durante a execução do jogo de tabuleiro é construído o fluxograma que descreve as etapas de início do jogo e as iterações iniciais até o final do jogo.

No fluxograma da figura 36 descreve-se a sequência da montagem do tabuleiro inicial, no qual é colocado na mesa cada hexágono adjacente sequencialmente até a sua finalização.

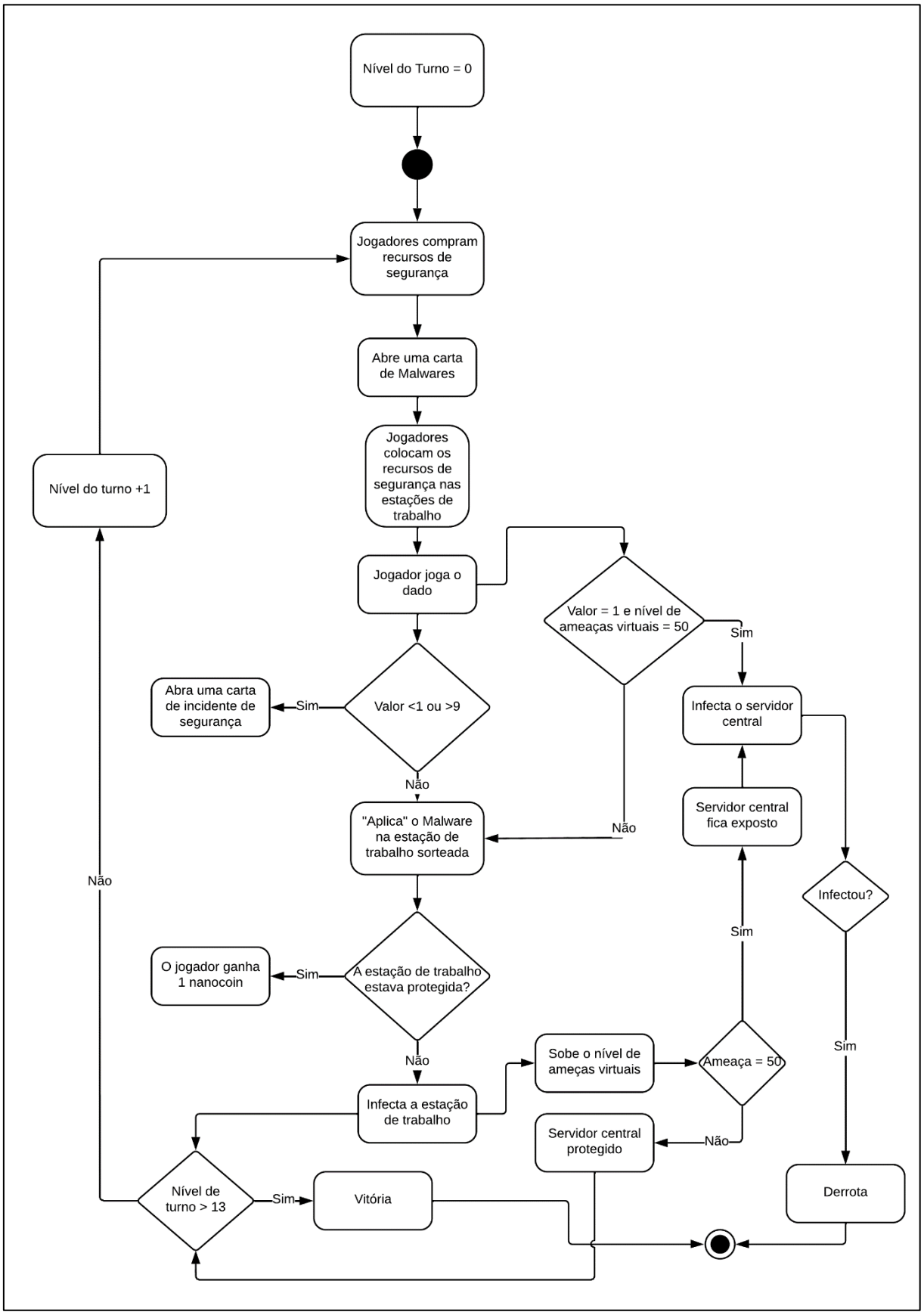
Figura 36 - Fluxograma da montagem do tabuleiro



Fonte: Autoria própria.

Após a montagem inicial do tabuleiro inicia-se a sequência da mecânica do jogo que pode ser vista da figura 37 com o fluxograma da sequência de um turno dentro do jogo.

Figura 37 - Fluxograma de sequência de um turno



Fonte: Autoria própria.

5.5 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 todos as mecânicas e designs do tabuleiro físico, foi construído a versão digital no site de simuladores de jogos de tabuleiros chamado Tabletopia[22].

O jogo foi criado e testado pelo autor do trabalho na plataforma digital seguindo as regras para 4 jogadores que durante a aplicação do jogo e da pesquisa foram assumidos pelos alunos na modalidade a distância. No qual o tabuleiro foi montado conforme as recomendações de início do jogo descritos no manual do jogo que pode ser vista na figura 38.

Figura 38 - Jogo de tabuleiro Th3_Off1c3 na versão digital

Fonte: Autoria própria.

[22] https://tabletopia.com/

6 APLICAÇÃO E ANÁLISES DE RESULTADOS

O jogo de tabuleiro Th3_0ff1c3 foi aplicado no curso de Sistemas de Informação na disciplina de Segurança e Auditoria de Sistemas de Informação na Instituição 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 foi realizada na mesma data e horário para todos os alunos com o jogo de tabuleiro físico e em formato digital, visto na figura 39 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[23] de jogo digital pelo site Tabletopia, que pode ser vista na figura 40. Todos os participantes receberam no dia anterior uma cópia do manual do jogo de tabuleiro e receberam recomendações de estudá-lo.

Figura 39 - Aplicação do jogo de tabuleiro físico para a turma presencial

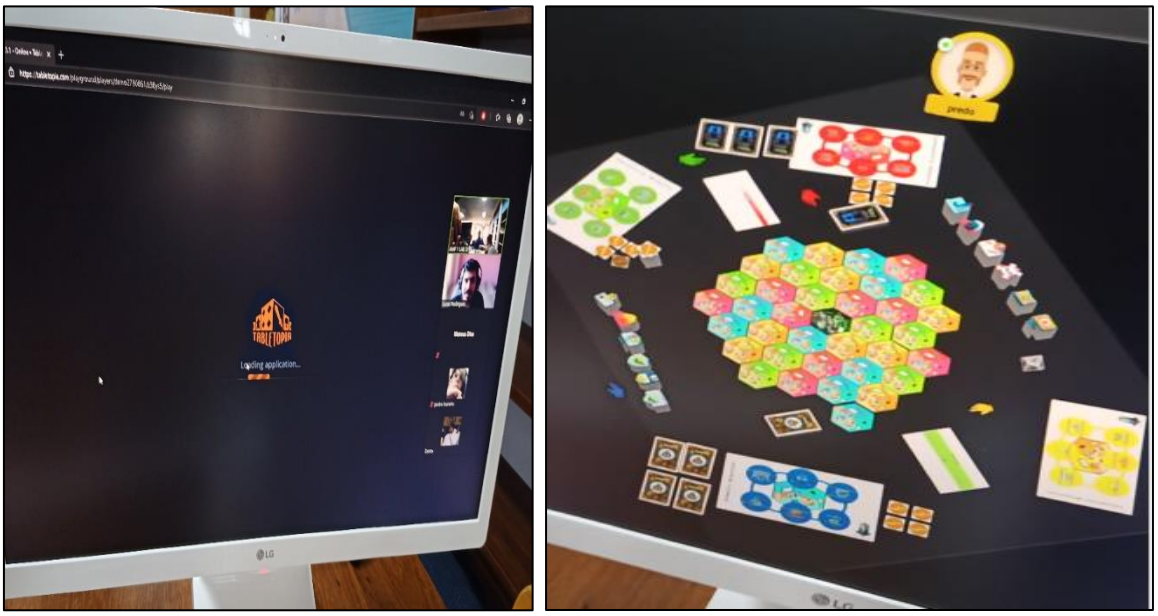
Fonte: Autoria própria.

[23] https://tabletopia.com/playground/th3-0ff1c3-bhp3jq/play-now

A turma de participantes foi de 4 pessoas na modalidade presencial em sala de aula e outras 4 pessoas na modalidade a distância, utilizando o computador pessoal para a participação na pesquisa, ou seja, a pesquisa teve 50% de participantes na modalidade presencial e outas 50% na modalidade de aulas a distância.

Todas as questões de levantamento de dados demográficos podem ser vistas no apêndice B deste trabalho.

Figura 40 - Aplicação do jogo de tabuleiro digital para a turma online



Fonte: Autoria própria.

O projeto seguiu o seguinte cronograma de aplicação:

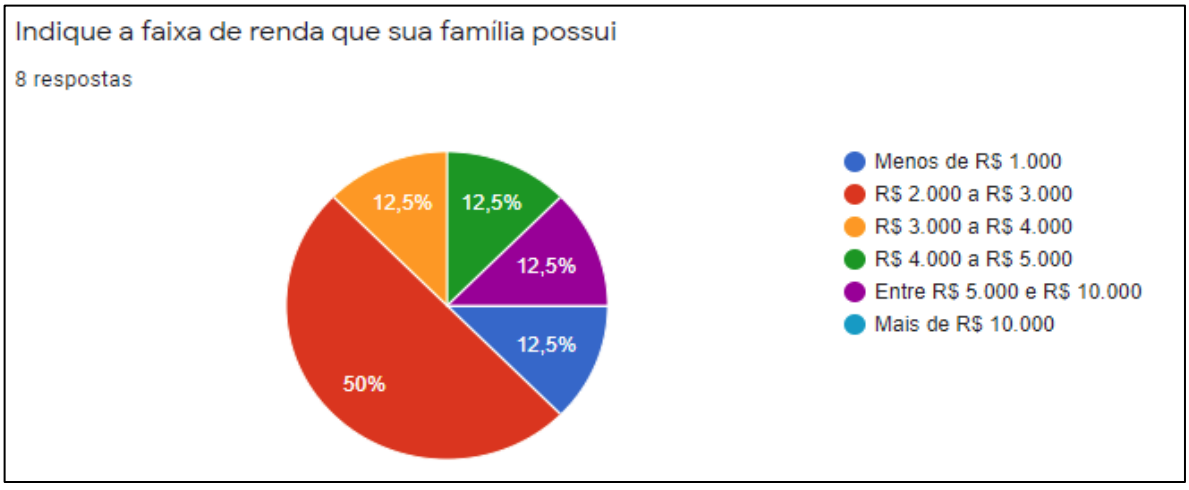
- Apresentação introdutória do Projeto e do Programa de Mestrado (PPGTER) – 15 minutos;
- Aplicação do questionário demográfico – 15 minutos;
- Aplicação do primeiro questionário de Avaliação do Conhecimento – 10 minutos;
- Apresentação dos conceitos abordados no projeto – 30 minutos;
- Demonstração de tipos de jogos de tabuleiros modernos (Eurogames e American Games) – 5 minutos;
- Explicação de regras e tira dúvidas – 15 minutos;
- Aplicação do jogo de tabuleiro no formado físico e digital – 2 horas e 15 minutos;

- Aplicação do segundo questionário de Avaliação do Conhecimento – 10 minutos;
- Aplicação do questionário para Avaliação da Qualidade de Jogos – 15 minutos;
- Conclusão da aplicação.

Segundo as respostas realizadas no questionário a faixa etária dos participantes é composta de jovens universitários dentro de um intervalo de 18 até 28 anos. Composto de participantes de ambos os sexos na aplicação da pesquisa. Compreendendo um total de 7 alunos do sexo masculino e 1 aluna do sexo feminino onde 87,5% dos participantes são do sexo masculino e outros 12,5% são do sexo feminino.

Como resultado de coleta de dados também foi avaliada a faixa de renda das famílias com os participantes da pesquisa, sendo que a maioria tem um total de renda familiar na faixa de R$ 2000,00 até R$ 3000,00. Segundo o gráfico 7 que pode ser visto abaixo.

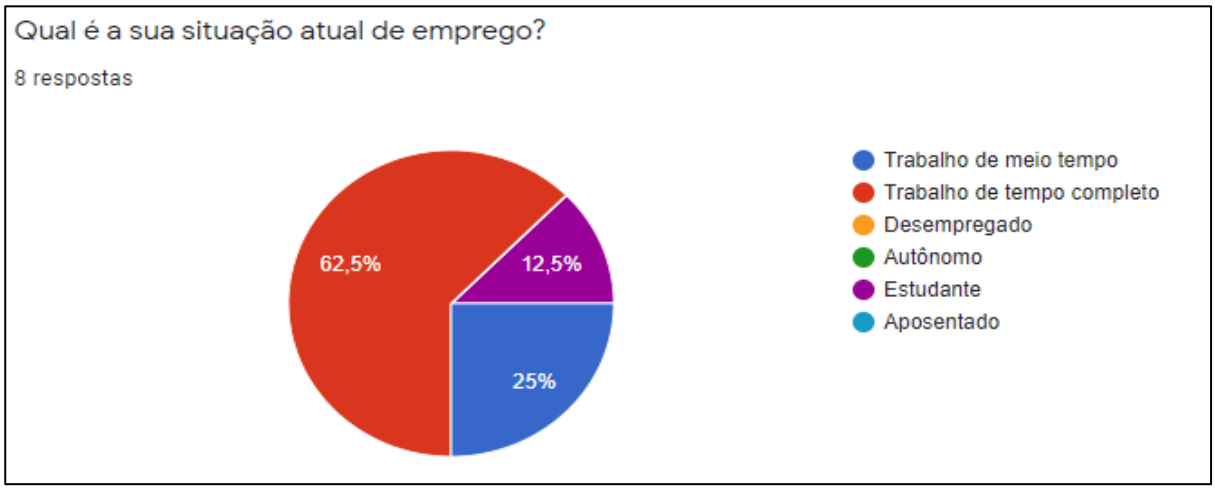
Gráfico 7 - Faixa de renda dos participantes



Fonte: Autoria própria.

Demonstrado no gráfico 8, um total de 87,5% dos participantes da aplicação da pesquisa tem alguma experiência profissional e estão colaborando no mercado de trabalho em regime de meio período ou em tempo integral. Durante a pesquisa apenas 1 participante se declarou como estudante e sem vínculo empregatício.

Gráfico 8 - Situação atual de emprego dos participantes



Fonte: Autoria própria.

Sobre as ocupações empregatícias descritas, houve estagiários em Tecnologia da Informação, desenvolvedor de softwares, desenvolvedor SAP ABAP Pleno, produtor audiovisual e UX/UI designer e analista de segurança, conforme a tabela 2. Segundo as respostas do questionamento de vínculos empregatícios, é possível utilizar o jogo de tabuleiro Th3_0ff1c3 para diversas atuações dentro da área de Tecnologia da Informação.

Tabela 2 - Situação empregatícia dos participantes

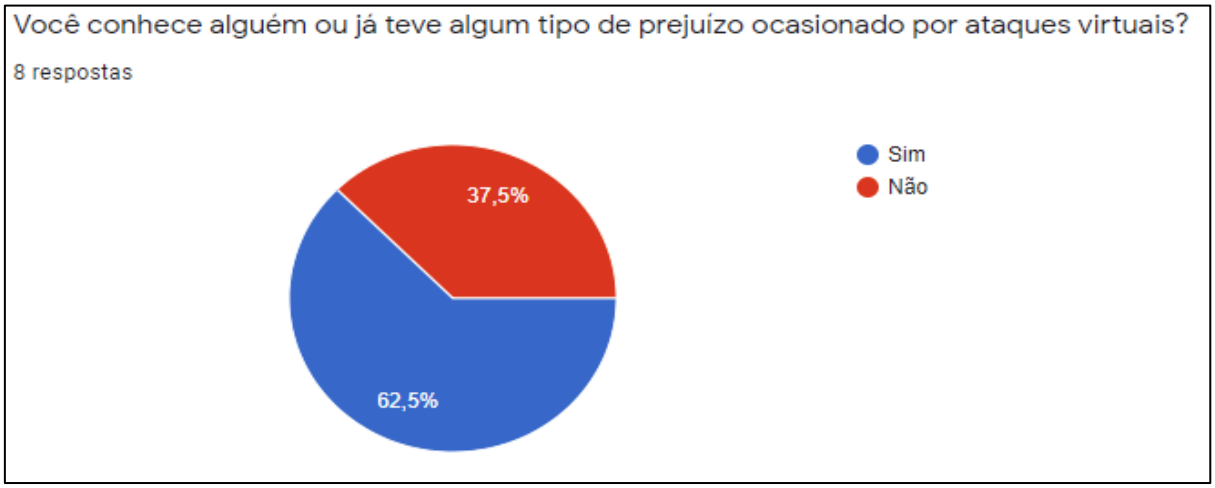
Se tiver uma ocupação além de estudante, qual sua área de atuação profissional? 7 respostas
estágio em TI
Desenvolvimento de software
Desenvolvedor SAP ABAP Pleno
Produtor audiovisual e UX/UI designer
Desenvolvedor de software
Analista de Segurança
Desenvolvedora de Software Web JavaScript

Fonte: Autoria própria.

O questionário demográfico também buscou conhecer se os ataques virtuais já atingiram os participantes de alguma forma ou se já presenciaram algum tipo de

problema com segurança da informação. Segundo o gráfico 9, tiveram ataques virtuais um total de 62,5% dos participantes contra 37,5% que não presenciaram um ataque, essa estatística reforça que há uma tendência da presença de ameaças à segurança da informação nos meios dos participantes compostas por pessoas não leigas na área da computação.

Gráfico 9 - Ataques virtuais sofridos pelos participantes



Fonte: Autoria própria.

Para um melhor entendimento foi pedido na avaliação demográfica uma descrição dos ataques sofridos e como isso afetou o participante. Segundo a tabela 3 pode ser verificada a multiplicidade de tipos e abordagens de ataques virtuais, desde ataques por *phishing* utilizando Engenharia Social, roubo de dados e sequestro de dados. Demonstrando que a maioria dos participantes já tiveram experiências variadas com problemas de ataques virtuais no meio em que vivem.

Tabela 3 - Descrição dos ataques sofridos

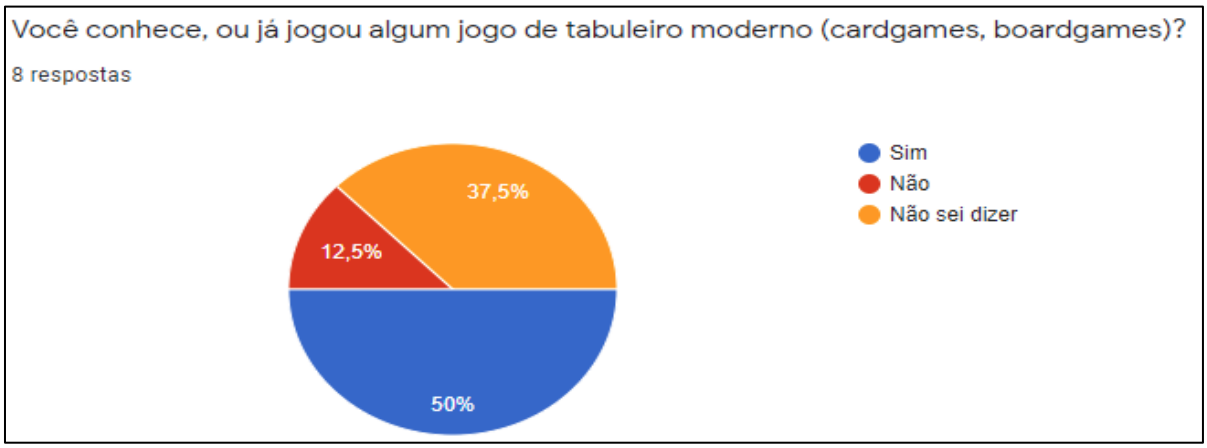
Se a resposta anterior for Sim, consegue descrever o ataque?
5 respostas
Fui roubado em um jogo online, onde as informações colocadas no site iam para uma pessoa com intensões maliciosas
Bloquearam os arquivos e pediram um valor para a recuperação
phishing, pessoas pagando para não serem expostas por "hackers"
Os dados da empresa onde eu trabalho, foram criptografados e os hackers pediam uma quantia em dinheiro para poder libera-los.
Não sei descrever exatamente, mas conheço algumas pessoas e empresas que foram infectadas com ramsonwares.

Fonte: Autoria própria.

A aplicação do questionário verificou a familiaridade com os jogos de tabuleiro entre os participantes, sendo que 50% dos participantes já tiveram alguma experiência com jogos de tabuleiros modernos e os demais com dúvidas sobre jogos de tabuleiro e que nunca jogaram, as informações podem ser vistas no gráfico 10 e com alguns descritos pelos alunos na tabela 4.

Essa menor experiência em jogos de tabuleiro trouxe uma maior dificuldade no entendimento rápido de regras e mecânicas do jogo de tabuleiro, que não são executadas na forma automatizada, como nos jogos digitais, mas sim no comum acordo de seguir regras que os jogos de tabuleiro exigem dos participantes.

Gráfico 10 - Conhecimento em jogos de tabuleiro



Fonte: Autoria própria.

Tabela 4 - Jogos de tabuleiro descritos pelos alunos

Se a resposta anterior for Sim, qual o jogo de tabuleiro jogado?
4 respostas
war, Gloomhaven
Game of thrones e outros (não lembro o nome)
Pokemon TCG, WAR, RPG mestrado
War e não lembro o nome do outro

Fonte: Autoria própria.

6.1 AVALIAÇÃO DE CONHECIMENTO

Para avaliar o conhecimento e a efetividade da aplicação do jogo de tabuleiro na turma de alunos, foi aplicada um questionário de conhecimento no início da aplicação e após a aplicação do projeto de pesquisa que pode ser vista no Apêndice C ao final deste trabalho.

O questionário foi dividido em dez 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.

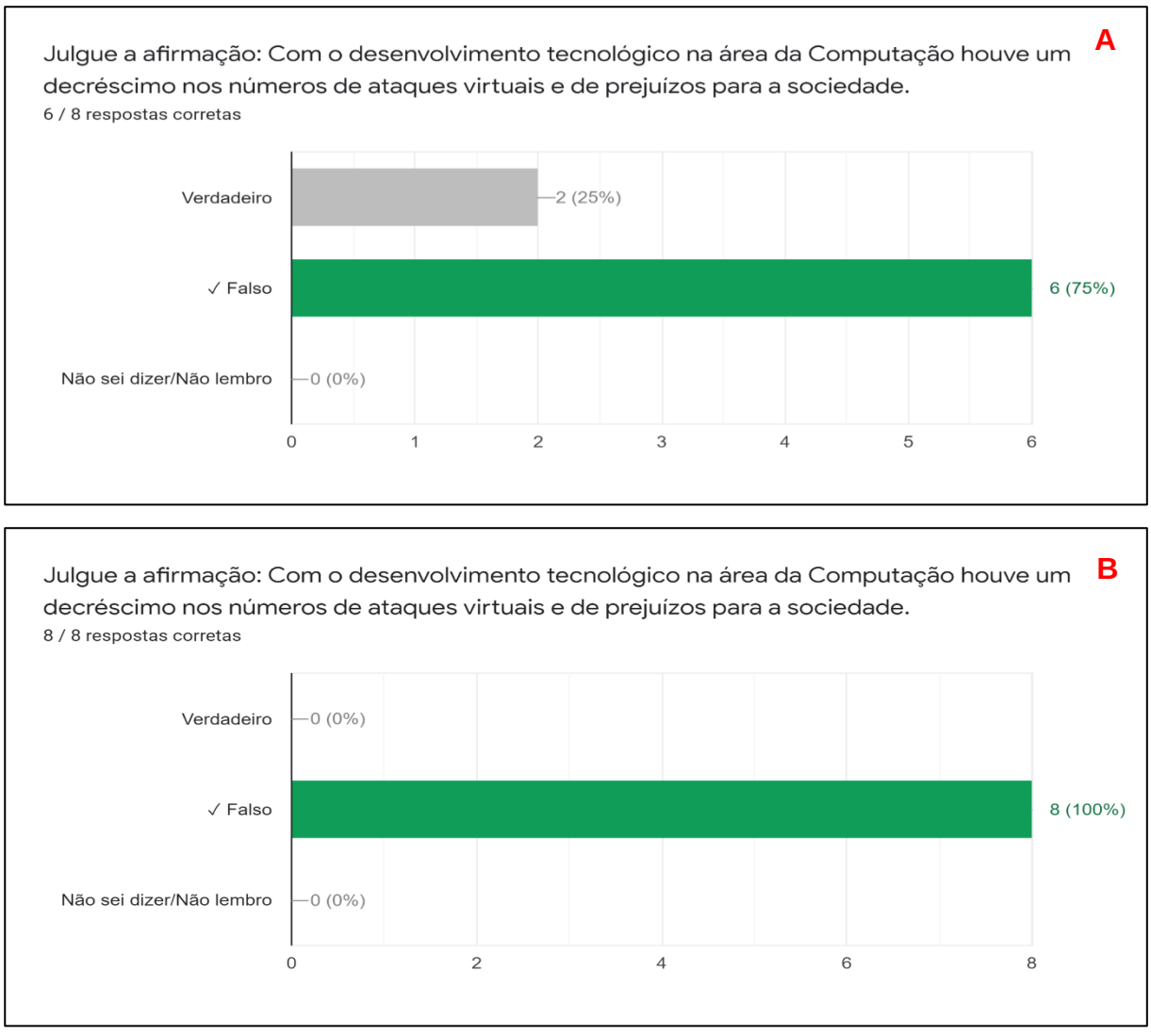
O jogo de tabuleiro Th3_0ff1c3 trabalhou todos os conceitos e efeitos dos ataques virtuais vistos nas questões propostas nas duas avaliações do conhecimento.

A primeira questão, vista no gráfico 11, tentou explorar a ideia geral de que com os avanços tecnológicos na área da computação em relação a softwares e hardwares poderia nos trazer uma maior segurança contra os ataques virtuais, mas que com os dados apresentados de estatísticas de ataques isso não é verdadeiro, pois tem elevado a quantidade de ataques virtuais. As respostas podem ser vistas nos gráficos

abaixo, o primeiro gráfico apresenta o resultado de respostas antes da aplicação do trabalho de pesquisa e o segundo gráfico mostra o resultado após a aplicação de trabalho de pesquisa. A barra de cor verde representa a alternativa correta e o total de participantes que marcaram corretamente a alternativa certa.

Após a aplicação da pesquisa, no gráfico 11B, é vista uma mudança na resposta de um participante para a alternativa correta, que aumentou para 100% das respostas corretas na primeira questão. Pode-se dizer que a aplicação do jogo de tabuleiro Th3_0ff1c3 trouxe um auxílio para o participante que corrigiu sua resposta.

Gráfico 11 - Primeira questão de avaliação antes e depois

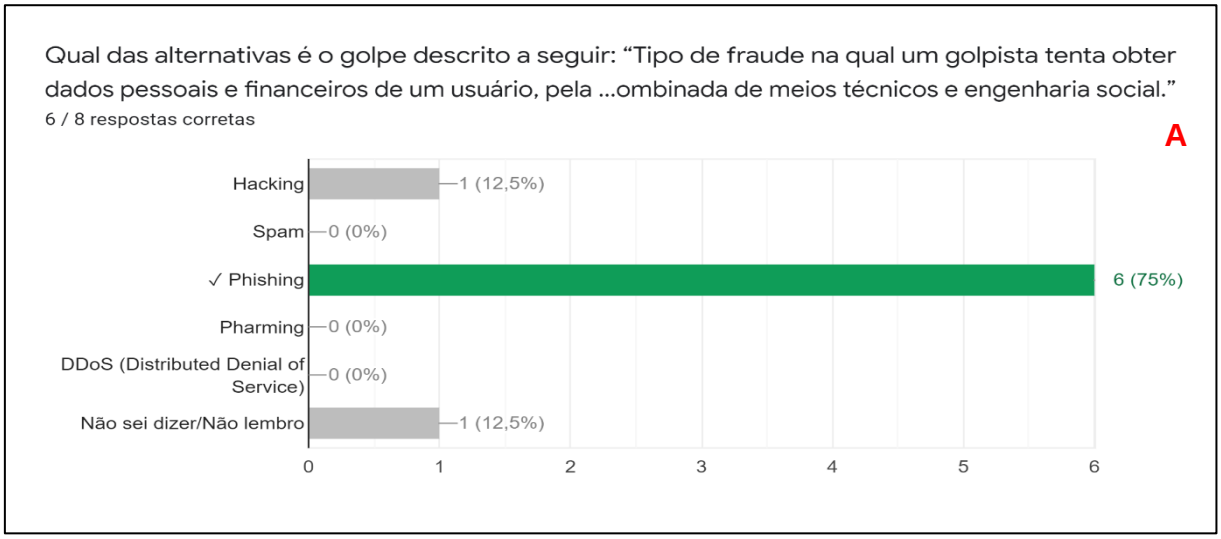


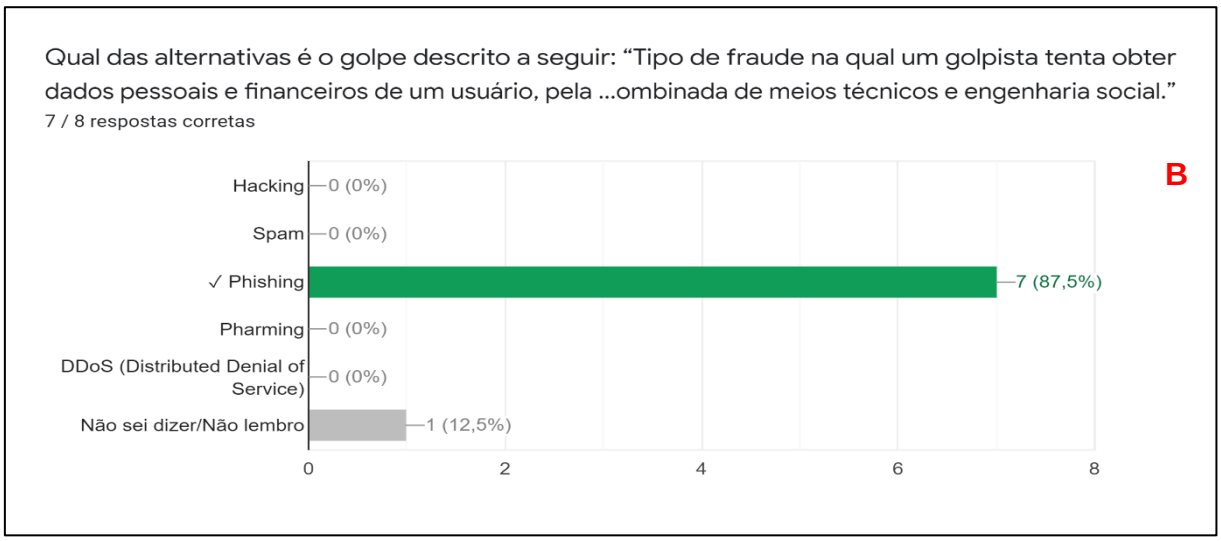
Fonte: Autoria própria.

Visto no gráfico 12, a segunda questão se refere a técnica de ataques utilizando engenharia social para enganar as pessoas e obter vantagens financeiras ou de informações chamada de *Phishing*, mostrada no gráfico abaixo.

Visto no gráfico 12B, após a aplicação deste trabalho, houve uma melhora nas respostas da questão, onde um participante corrigiu sua resposta para a alternativa correta. Já por outro lado, um participante manteve sua resposta como “Não sei dizer/Não lembro” após a aplicação do trabalho, tendo duas hipóteses, o participante realmente não entendeu o trabalho ou não houve interesse na participação.

Gráfico 12 - Segunda questão de avaliação antes e depois



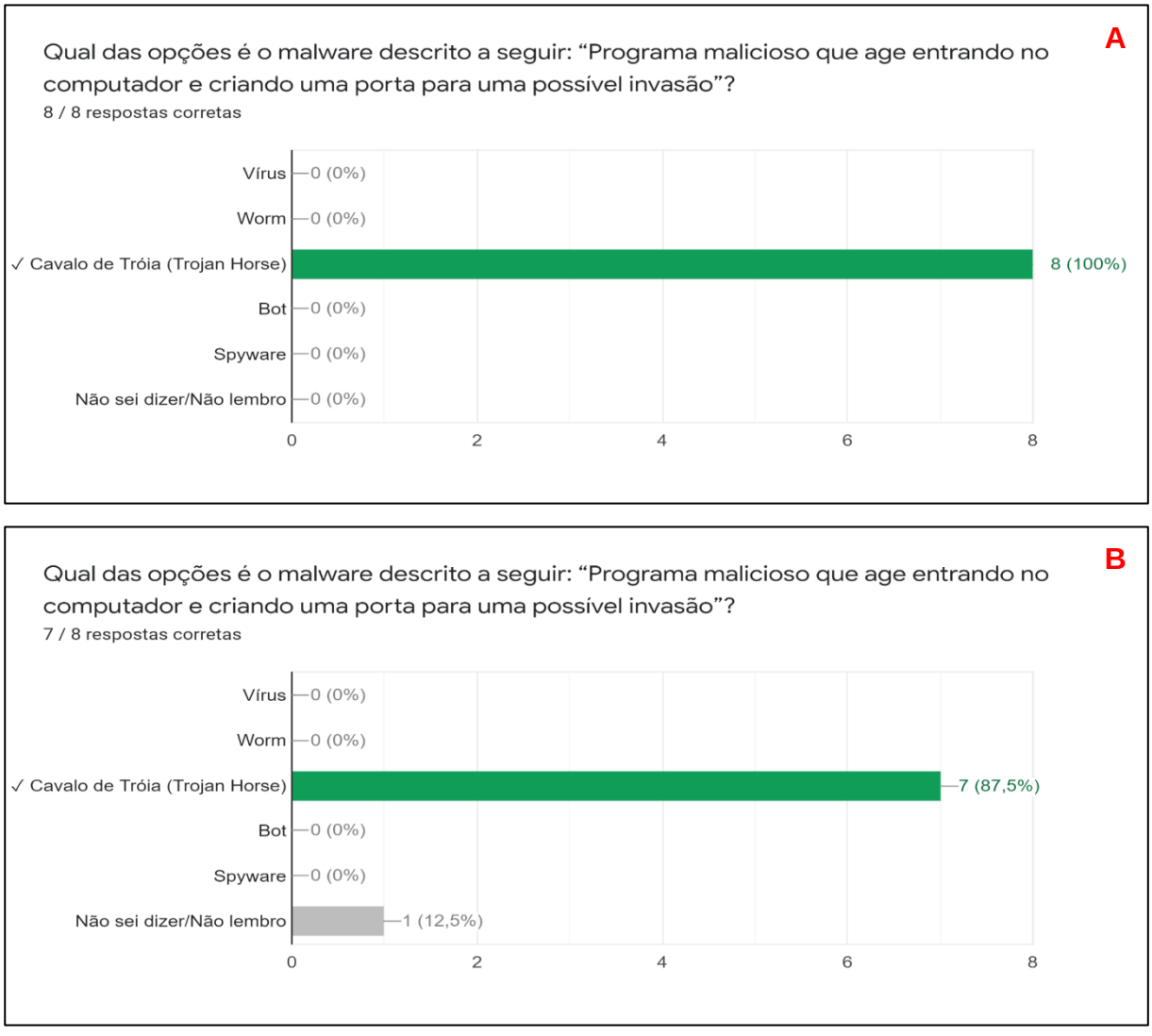


Fonte: Autoria própria.

A terceira questão do questionário avaliativo remete ao conceito do software malicioso conhecido como Cavalo de Tróia, afirmando sua principal característica de ação. A questão, vista no gráfico 13A, teve um total de acertos antes da aplicação do projeto, demonstrando que já havia conhecimento prévio do conceito apresentado.

Nesta questão houve uma resposta errada após a segunda aplicação, visto no gráfico 13B. A resposta não foi escolhida para uma alternativa de conceito incorreta, mas com uma alternativa de desconhecimento sobre o assunto afirmado. A hipótese é que houve descuido, falta de atenção ou falta de interesse na participação do projeto de pesquisa.

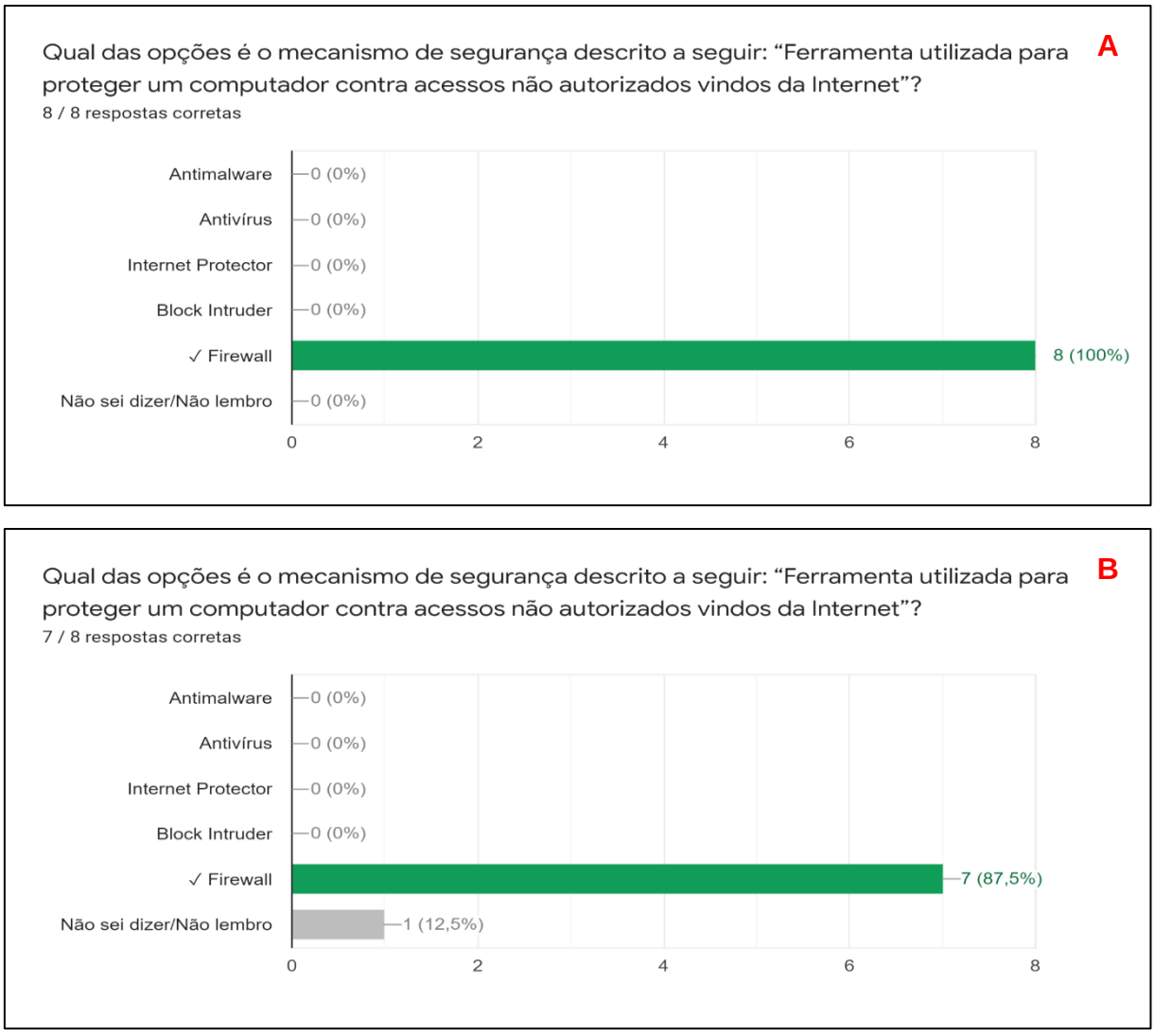
Gráfico 13 - Terceira questão de avaliação antes e depois



Fonte: Autoria própria.

A quarta questão abordou o conceito de dispositivo ou software de segurança da informação chamada de *Firewall*, na qual podemos no gráfico 14A que os participantes do projeto já tinham certo conhecimento sobre o assunto. Na primeira aplicação do gráfico 14A, houve um total de 100% de respostas corretas, já na segunda aplicação, no gráfico 14B, houve um decréscimo de respostas corretas em uma errada, novamente com a hipótese de descuido, falta de atenção ou falta de interesse durante a aplicação.

Gráfico 14 - Quarta questão de avaliação antes e depois

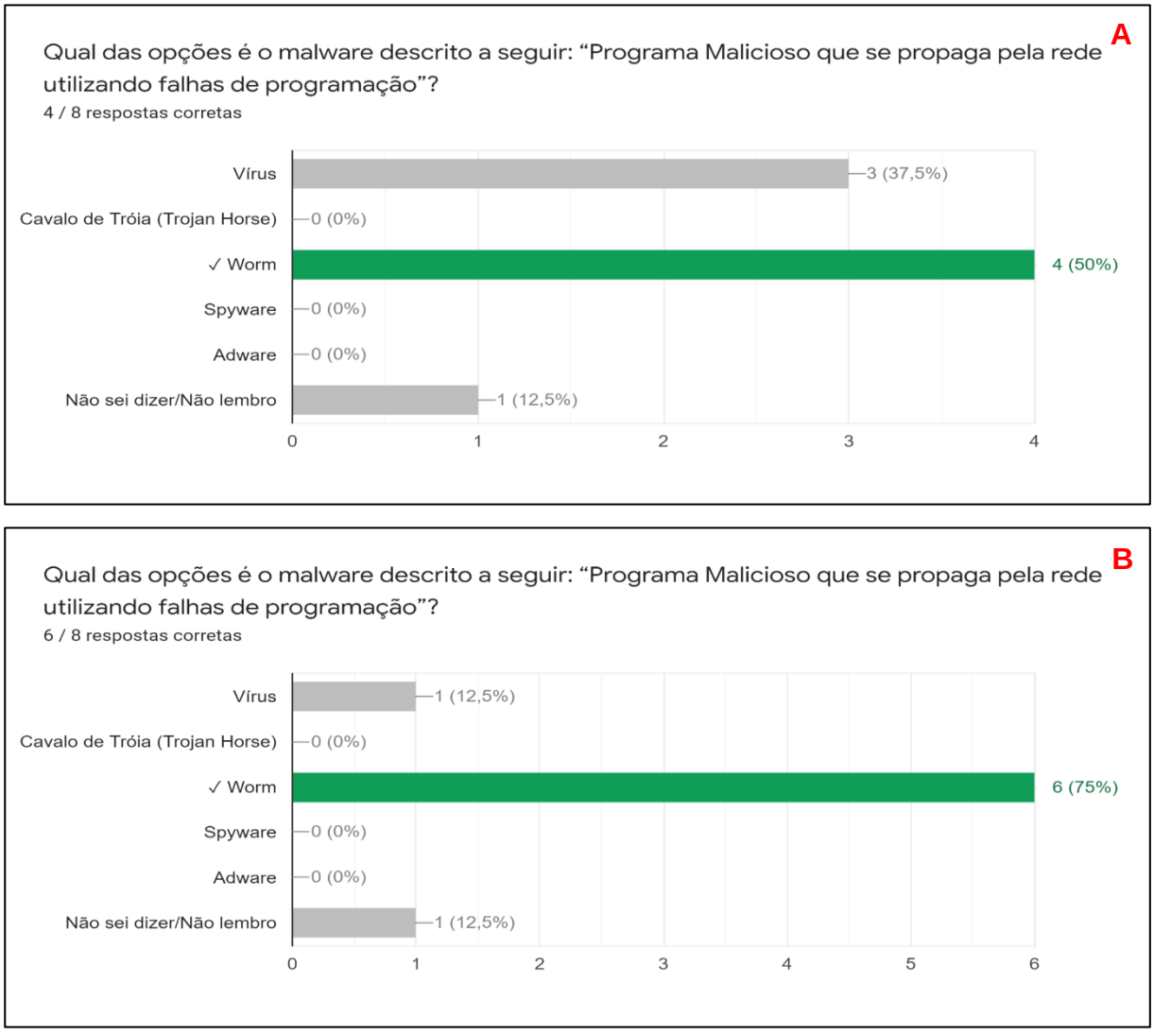


Fonte: Autoria própria.

A quinta questão abordou o conceito de *Worms*, ou Malware que explora falhas de programação ou má configuração em redes de computador, infectando os

equipamentos. Os participantes confundiram bastante o conceito da ação de um vírus de computador com a ação de um *Worm*. Visto no gráfico 15B, houve uma melhora considerável da elucidação do conceito após a aplicação do jogo de tabuleiro Th3_0ff1c3 na segunda aplicação do questionário de avaliação, por outro lado, houve um participante que manteve a resposta incorreta mesmo após a aplicação do jogo de tabuleiro, que pode não ter sido apresentado satisfatoriamente seu conceito durante a aplicação do trabalho, já um dos participantes manteve sua resposta de "Não sei dizer/Não lembro" que talvez não tenha conhecimento sobre o conceito trabalhado ou não teve interesse em responder.

Gráfico 15 - Quinta questão de avaliação antes e depois

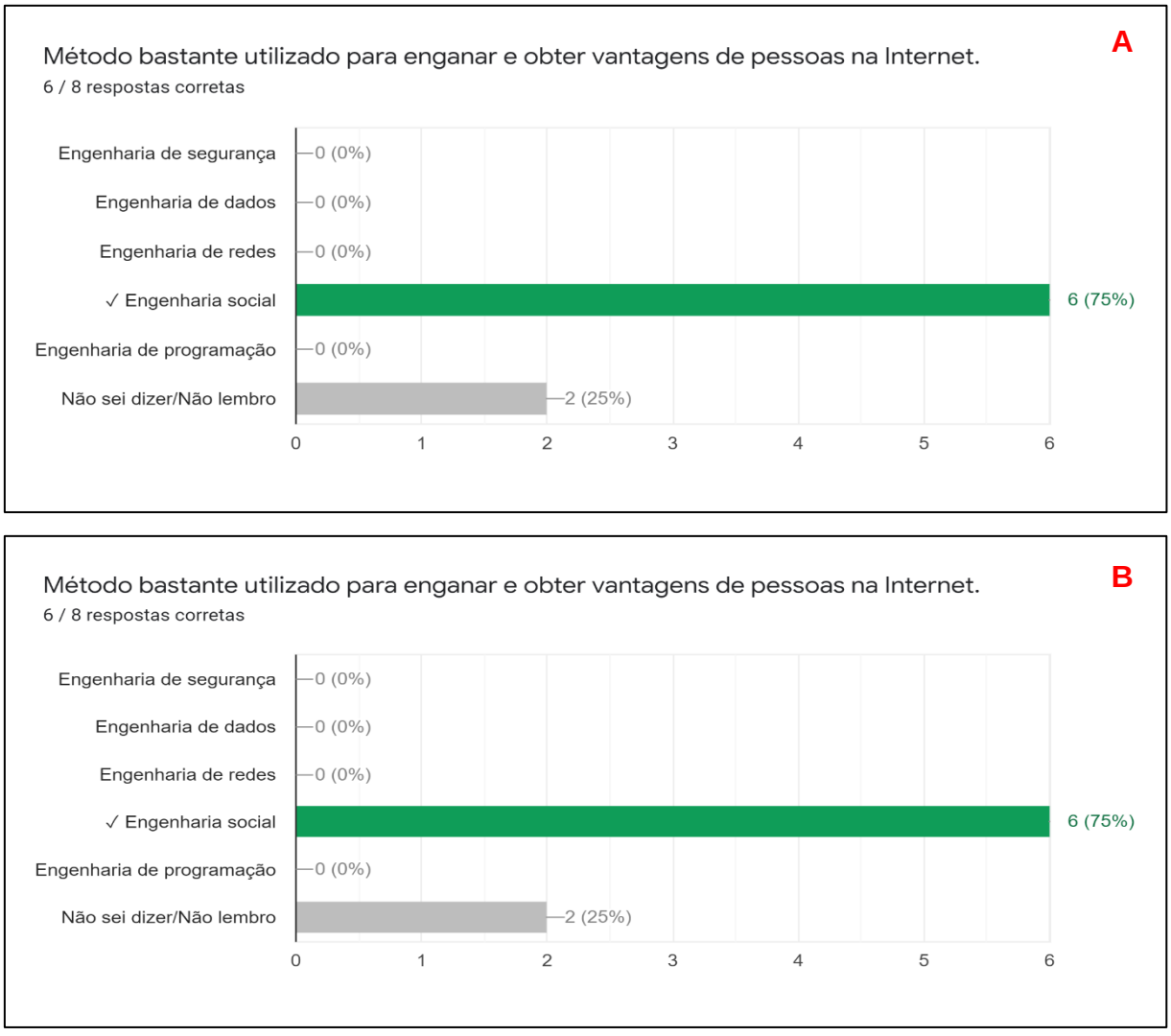


Fonte: Autoria própria.

Na sexta questão foi abordado um dos conceitos de Engenharia Social, utilizada como forma de ataque virtual e de ganho de vantagens utilizando as redes de computadores. Segundo o gráfico 16A, a maioria dos participantes já tinham visto em aula o conceito sobre a Engenharia Social. Mas como o conceito de engenharia social seja amplo e algumas vezes abstrato e não totalmente explicito dentro do jogo Th3_0ff1c3, que foi aplicado em um exemplo prático, como por exemplo o uso de técnicas de *Phishing* dentro do jogo. Isso demonstrou-se com duas respostas incorretas na primeira aplicação e a repetição na segunda aplicação, vistas no gráfico 18B.

Esse resultado afirma que é necessária uma elucidação melhor no conceito para os participantes do jogo de tabuleiro Th3_0ff1c3.

Gráfico 16 - Sexta questão de avaliação antes e depois

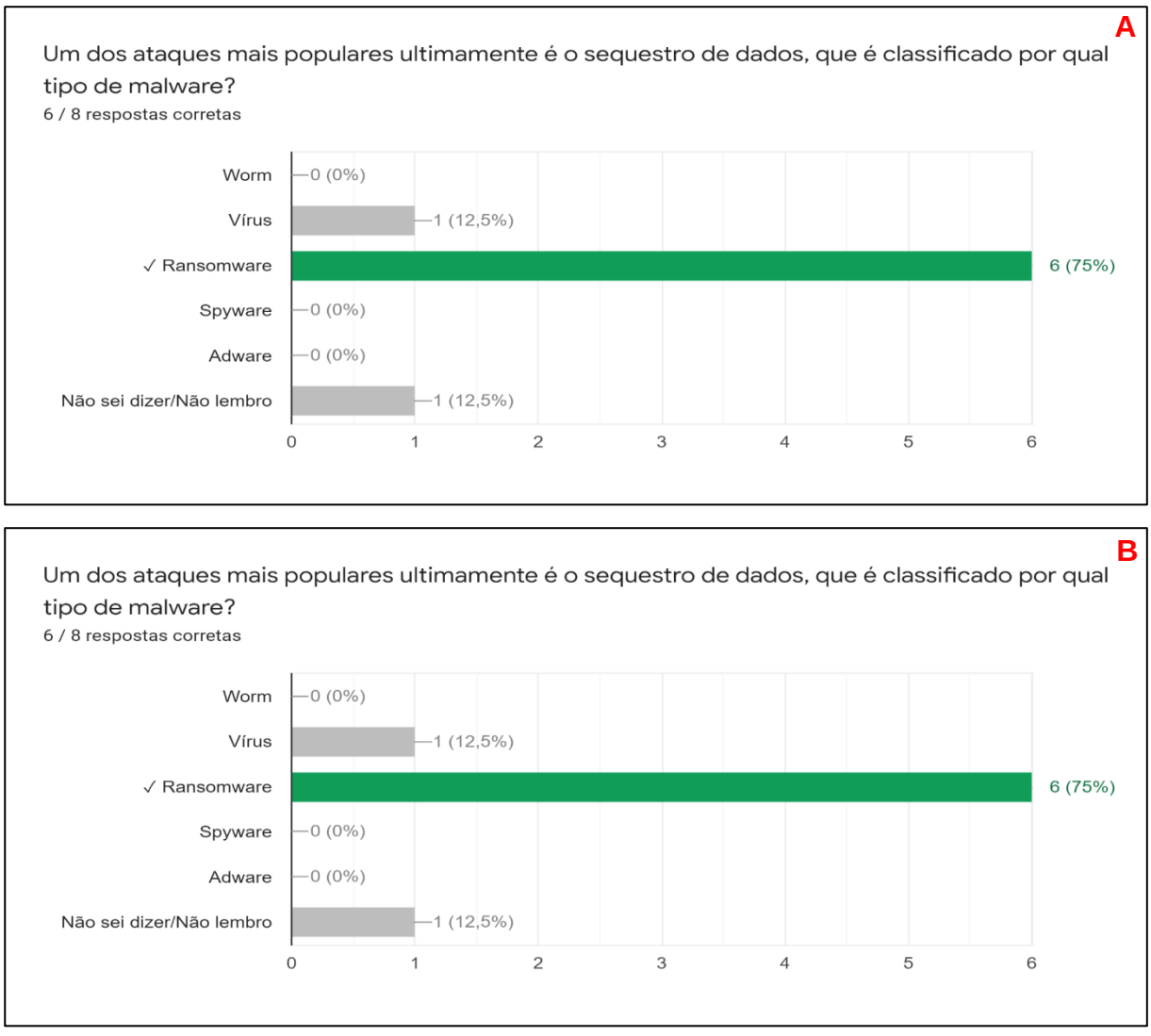


Fonte: Autoria própria.

A sétima questão abordou o conceito do ataque utilizando um programa malicioso conhecido como *Ransomware*, ou sequestro de dados, no qual é visto no gráfico 19A que mostra que a maior parte dos participantes já tinham conhecimento sobre esse tipo de ataque virtual.

Ainda assim nas aplicações não houve diferenças nos gráficos 17A e 17B, onde que um dos participantes continuou com a resposta de “vírus” e outro com a alternativa de “Não sei dizer/Não lembro”, sendo necessário reforçar o conceito no jogo de tabuleiro Th3_0ff1c3.

Gráfico 17 - Sétima questão de avaliação antes e depois

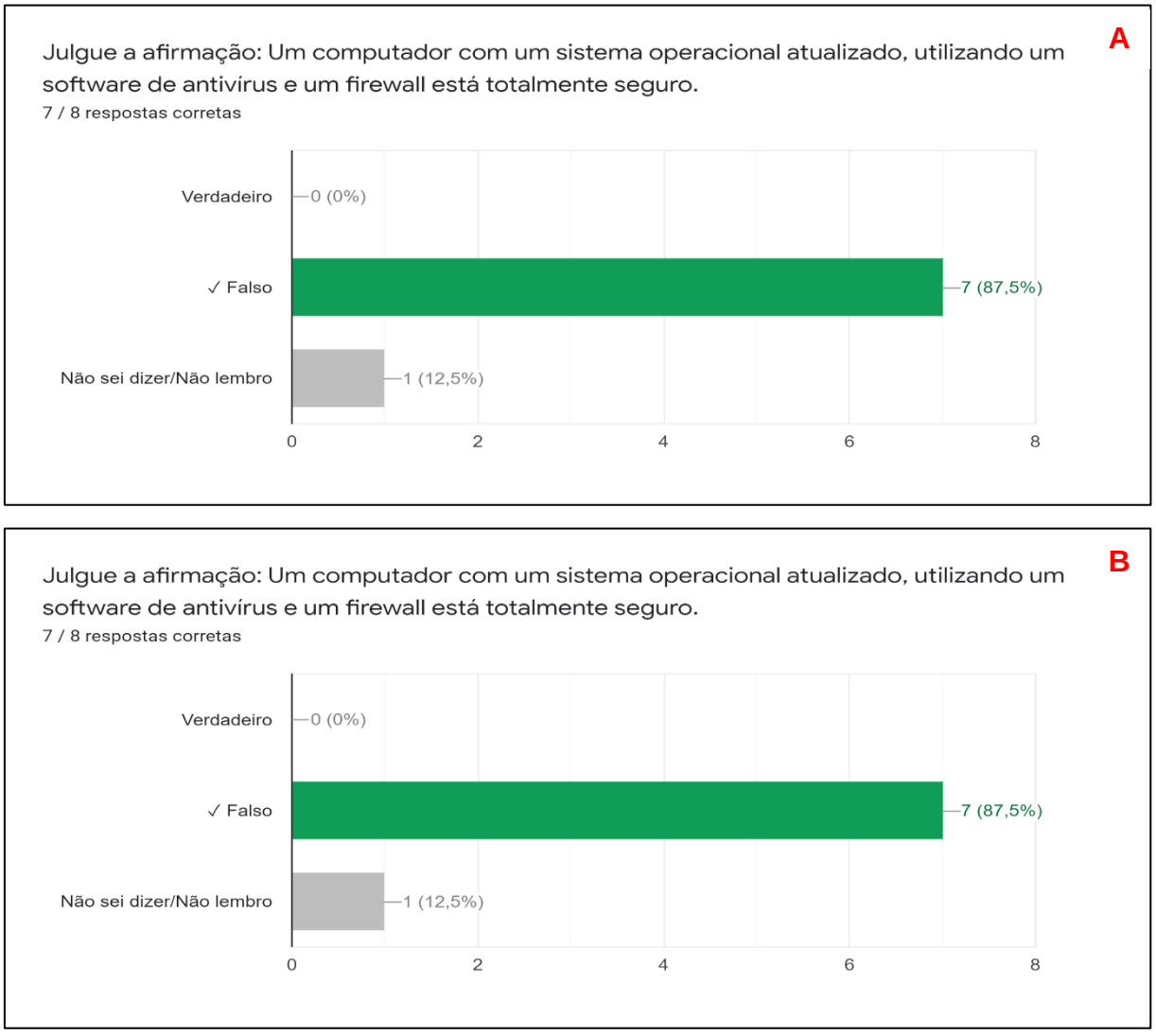


Fonte: Autoria própria.

A oitava questão apresenta uma frase afirmativa sobre a segurança da informação que engloba todos os tipos de usuários de computador, no qual confirma

que a utilização de um sistema operacional atualizado, um firewall e o software antivírus é suficiente para manter a segurança do usuário. No qual não está correta, pois as boas práticas de segurança feitas pelo usuário são importantes para manter sua segurança digital. O gráfico 18 demonstram que a grande maioria dos participantes do projeto já tinham a clareza sobre o erro da afirmação.

Gráfico 18 - Oitava questão de avaliação antes e depois



Fonte: Autoria própria.

A nona questão apresenta o conceito de um *exploit*, ou falha de programação. Bastante utilizado em ataques virtuais pela exploração de *exploits* em aplicativos e sistemas operacionais. A turma teve bastante dificuldades no conceito antes da aplicação e uma pequena melhora após a aplicação do jogo de tabuleiro Th3_0ff1c3,

a disciplina poderia reforçar o conceito em algum momento para o aprendizado dos participantes. O gráfico 19A demonstram a dificuldade em que poucos participantes acertaram a alternativa correta e houve uma melhora considerável nos acertos após a segunda aplicação da avaliação no gráfico 19B, mas também maiores dúvidas sobre o conceito gerando outras respostas incorretas.

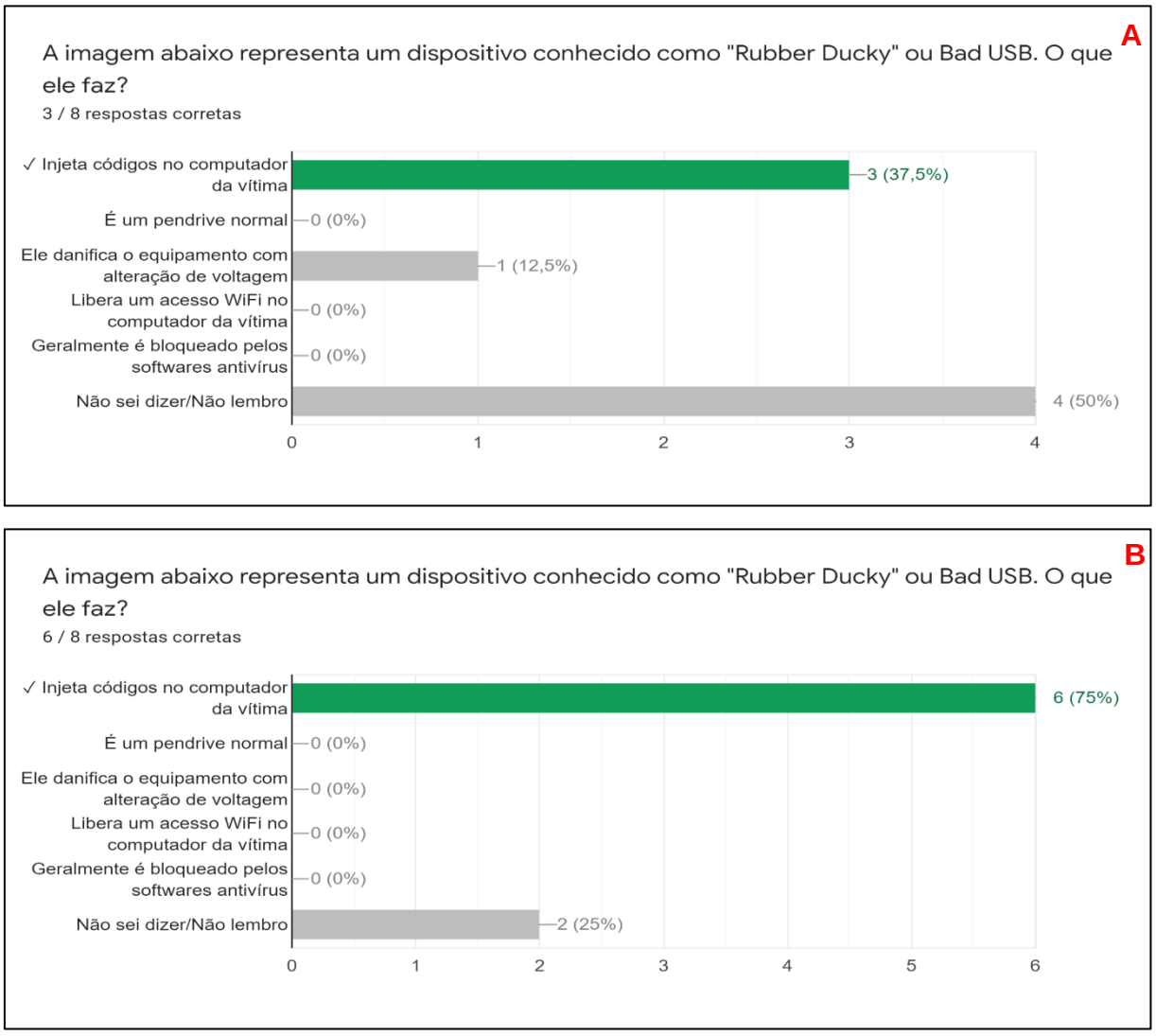
Gráfico 19 - Nona questão de avaliação antes e depois

Fonte: Autoria própria.

A última questão abordou o conceito de um dispositivo utilizado para ataques virtuais em diversos equipamentos chamado “*Bad USB”* ou “*Rubber Ducky*”, que é muito semelhante fisicamente a um dispositivo de armazenamento de memória flash popularmente chamado de Pendrive, mas que pode injetar códigos maliciosos em equipamentos no qual ele é conectado. A grande parte dos participantes relembrou

ou aprendeu o conceito após a aplicação do jogo Th3_0ff1c3, visto no gráfico 20A e 20B. Na segunda aplicação do questionário avaliativo houve um dobro de participantes que acertaram o conceito corretamente e diminuindo pela metade os participantes que responderam como “Não sei dizer/Não lembro”.

Gráfico 20 - Décima questão de avaliação antes e depois



Fonte: Autoria própria.

Na tabela 5 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 5 - 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%

Fonte: Autoria própria.

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. A aplicação do jogo de tabuleiro Th3_0ff1c3 para outros cursos de graduação ou em turmas de ensino médio que não tiveram contatos com conhecimento em segurança da informação podem trazer resultados diferentes nas aplicações de testes de avaliação do conhecimento. Fica sugerido o uso do método para outras aplicações deste projeto de pesquisa.

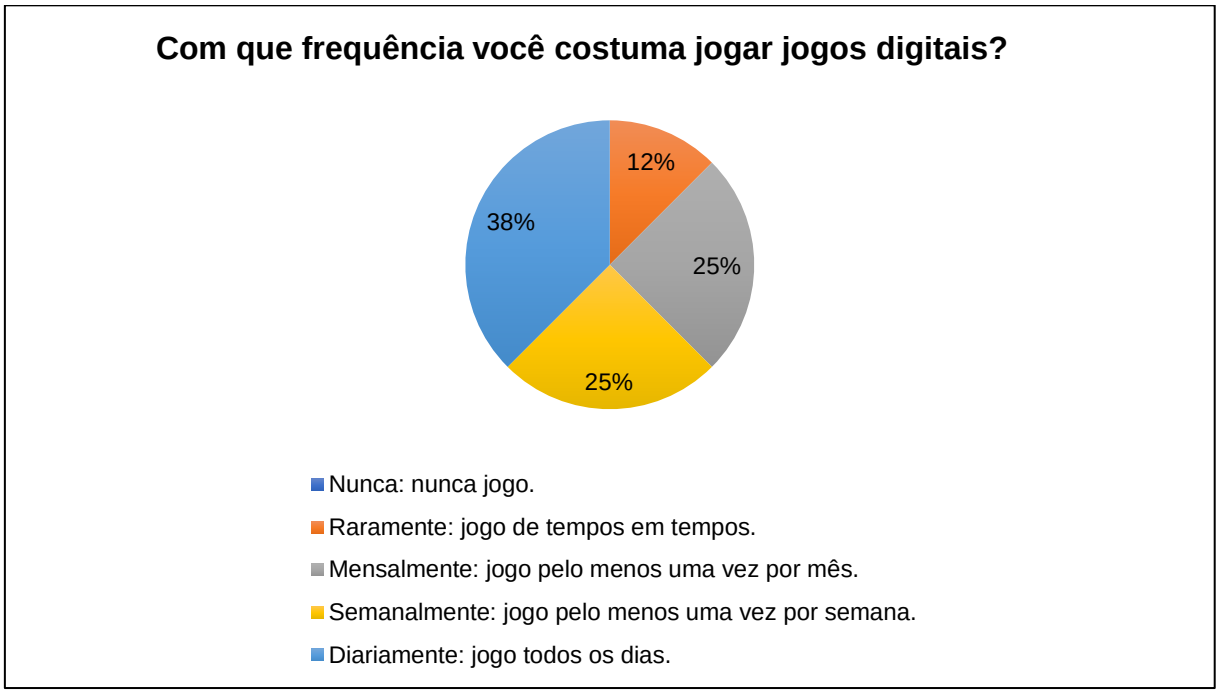
6.2 AVALIAÇÃO DE QUALIDADE DO JOGO

Segundo Petri (2018), 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.

O questionário é dividido em nove questões sobre a usabilidade do jogo de tabuleiro, a experiência do jogador e questões discursivas onde os participantes da pesquisa puderam expressas suas opiniões sobre o aprendizado após a aplicação do jogo de tabuleiro. Todas as questões podem ser vistas no apêndice D deste trabalho.

Segundo o gráfico 21 sobre a frequência que o participante costuma jogar jogos digitais compreende que 38% jogam jogos digitais todos os dias, 25% jogam semanalmente jogos digitais, 25% jogam mensalmente algum tipo de jogo digital e 12% jogam raramente um jogo digital. Ou seja, todos os participantes têm contato e experiência com jogos digitais, sendo bem ativos na utilização deles.

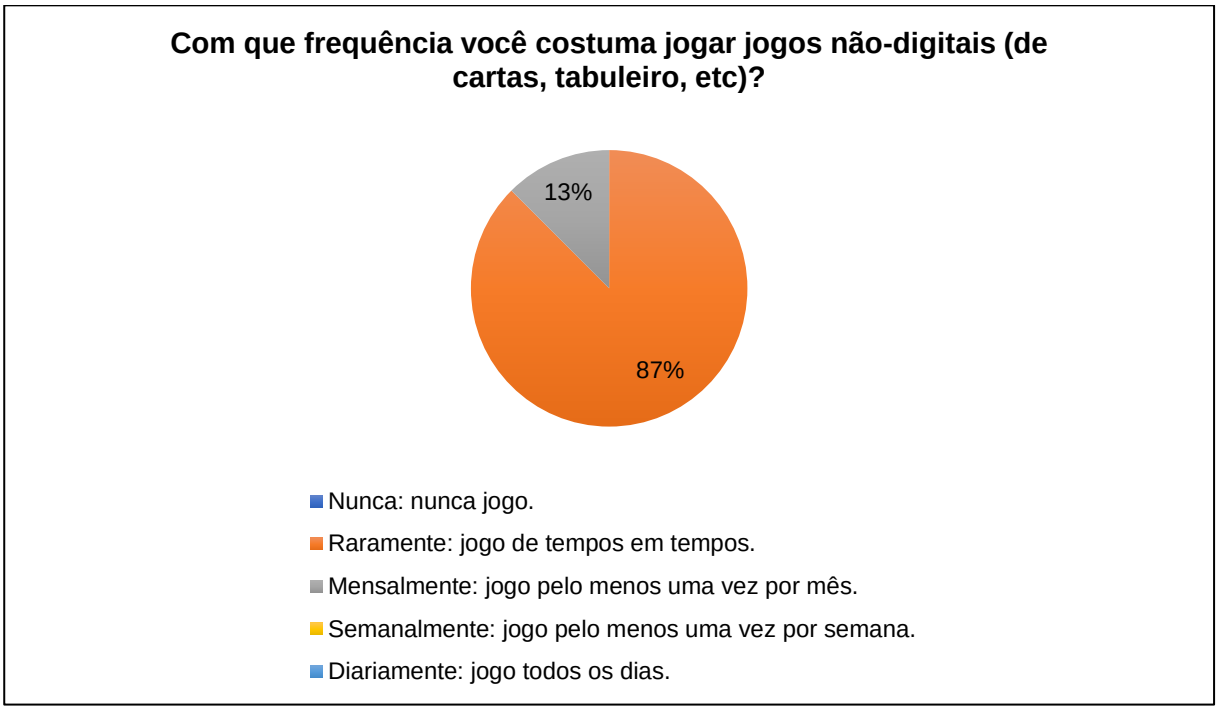
Gráfico 21 - Frequência de vezes que o participante joga jogos digitais



Fonte: Autoria própria.

Sobre a frequência de vezes que os participantes utilizam jogos não-digitais, ou jogos de tabuleiro é visto uma grande diferença no gráfico 22. Um total de 87% participantes da aplicação do trabalho raramente jogam jogos de tabuleiro, contra 13% dos participantes que jogam mensalmente algum jogo não-digital. A utilização do jogo de tabuleiro Th3_0ff1c3 foi uma nova experiência de diversão e colaboração entre os colegas, que podemos ver nas análises de resultados nos capítulos a seguir.

Gráfico 22 - Frequência de vezes que o participante joga os jogos não-digitais



Fonte: Autoria própria.

6.2.1 Análise da Usabilidade

As próximas questões avaliam o nível de satisfação dos participantes sobre a usabilidade do jogo que analisa, a estética do jogo, a aprendizibilidade, operabilidade e acessibilidade. Segundo Petri et al (2018) o método MEEGA+ caracteriza-se por:

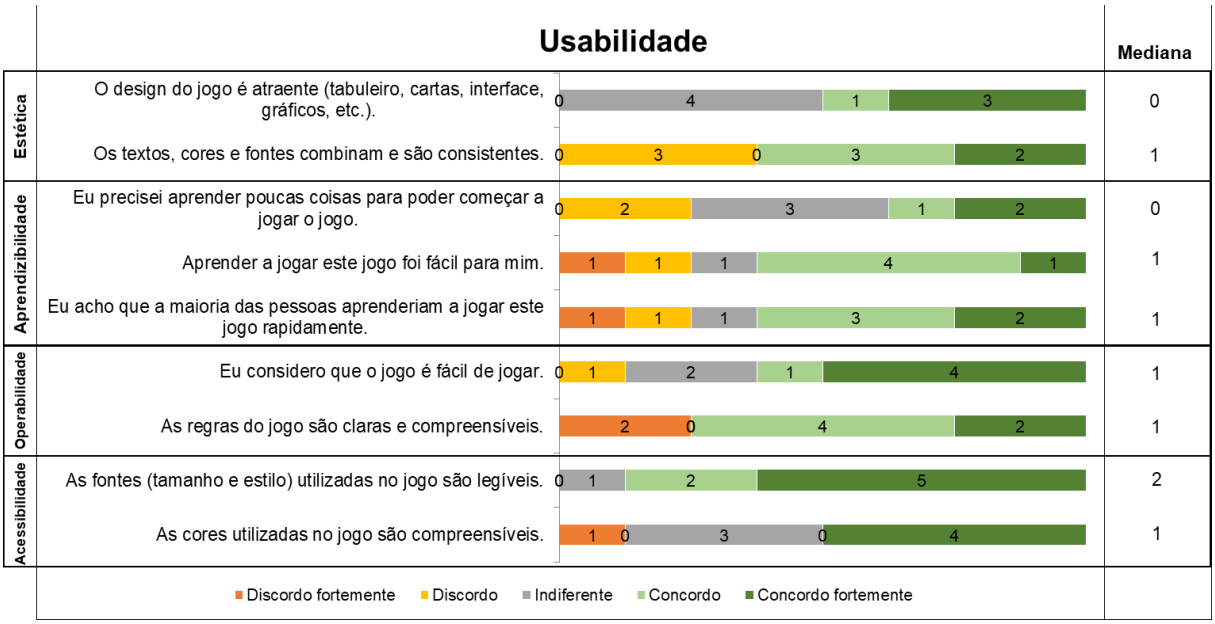
> De acordo com o modelo MEEGA+, a experiência proporcionada aos jogadores é avaliada em termos de usabilidade do jogo, confiança, desafio, satisfação, interação social, diversão, atenção focada e relevância.

As áreas analisadas compreendem o design gráfico do jogo, como imagens, cores, qualidade e clareza em entender os componentes que compõem o jogo de tabuleiro. As questões são propostas para ter opiniões de melhorias gráficas e de regras para o jogo de tabuleiro, para uma melhor qualidade e facilitação do aprendizado.

As questões foram inseridas na planilha de análise de dados do modelo de análise de jogos educacionais MEEGA+ que utiliza uma escala de satisfação do participante, a escala se difere entre as opções “Discordo fortemente”, “Discordo”, “Indiferente”, “Concordo”, e o “Concordo fortemente”.

A tabela 6 mostra o resultado da usabilidade do jogo de tabuleiro Th3_0ff1c3, onde é medido a questão do design gráfico ou estética do produto que pode ter melhorias segundo os participantes, a dificuldade ou facilidade do aprendizado do jogo de tabuleiro que pode ser afetado pela pouca experiência dos jogadores com jogos não digitais, a operabilidade que analisou o andamento das mecânicas e regras do jogo e como foi a experiência do jogador e por último a acessibilidade do jogo de tabuleiro que analisou a compreensão visual do jogo.

Tabela 6 - Usabilidade do jogo de tabuleiro Th3_0ff1c3



Fonte: Autoria própria.

6.2.1.1 Estética

A maioria dos participantes avaliaram o design do jogo de tabuleiro Th3_0ff1c3 com a resposta de “indiferente”, baseado nas respostas do gráfico 24 sobre a frequência na utilização de jogos não digitais como os de tabuleiros, a grande maioria dos participantes no total de 87% utilizam raramente jogos de tabuleiro, e em comparação com o gráfico 23 sobre jogos digitais, a grande maioria dos participantes jogam diariamente ou semanalmente jogos digitais. Os jogos digitais comerciais têm por característica as animações bem-produzidas, imagens em alta resolução, sons e músicas produzidas profissionalmente e a execução de mecânicas e regras automatizadas, trazendo uma experiência muito diferente na execução de um jogo

digital para um de tabuleiro, esse fato provavelmente influenciou a análise do desenvolvimento gráfico/estético do jogo de tabuleiro Th3_0ff1c3.

6.2.1.2 Aprendizibilidade

Um jogo de tabuleiro moderno tem por sua característica principal uma grande quantidade de regras em sua execução, por muitas vezes simular jogos digitais na forma manual e não automatizada que as máquinas podem propiciar.

O jogo de tabuleiro Th3_0ff1c3 foi desenvolvido com inspiração em regras e mecânicas de jogos de tabuleiro complexos, que tem um aprendizado um pouco mais demorado por ter muitos itens e acontecimentos que ocorrem no decorrer de cada turno de jogo.

A aplicação do trabalho de pesquisa teve um tempo curto para a execução, então os participantes tiverem pouco tempo para aprender e executar o jogo de tabuleiro, trazendo algumas dúvidas e dificuldades no aprendizado do jogo. O jogo aplicado mais vezes e com um tempo maior poderia trazer um resultado de aprendizibilidade maior e uma maior fluidez nas realizações de partidas de jogo. Isso explica o resultado indiferente sobre a necessidade de aprender coisas novas no jogo de tabuleiro Th3_0ff1c3, foi necessário aprender várias coisas em um tempo restrito.

6.2.1.3 Operabilidade

Após a leitura do manual e a explicação das regras do jogo de tabuleiro Th3_0ff1c3 durante a aplicação do projeto de pesquisa, a maioria dos participantes teve facilidade em jogar o jogo Th3_0ff1c3. O jogo foi desenvolvido utilizando conceitos e ideias de jogos de tabuleiro moderno de entrada como o Catan, que após o aprendizado das regras tem uma execução otimizada e rápida não sendo necessário consultar as regras em todo o momento.

A maioria dos participantes não estão acostumados em ler manuais extensos de regras para jogos de tabuleiro como o Th3_0ff1c3, e sentiram dificuldade em entender inicialmente as regras de jogo. Uma boa abordagem para auxiliar no aprendizado é gravar um vídeo com a explicação das regras e a execução do jogo de tabuleiro que é conhecido como *gameplay*.

6.2.1.4 Acessibilidade

A maioria dos componentes gráficos foram bem aceitas pelos participantes do jogo Th3_0ff1c3, nas artes produzidas nos hexágonos, cartas, marcadores, tamanho da fonte e estilo de letras. Em decorrência do perfil dos jogadores que tem maior proximidade com jogos digitais, o uso de cores poderia ser mais bem trabalhado no jogo Th3_0ff1c3, esse resultado pode ter ocorrido pelo tipo de papel e qualidade da impressão na gráfica.

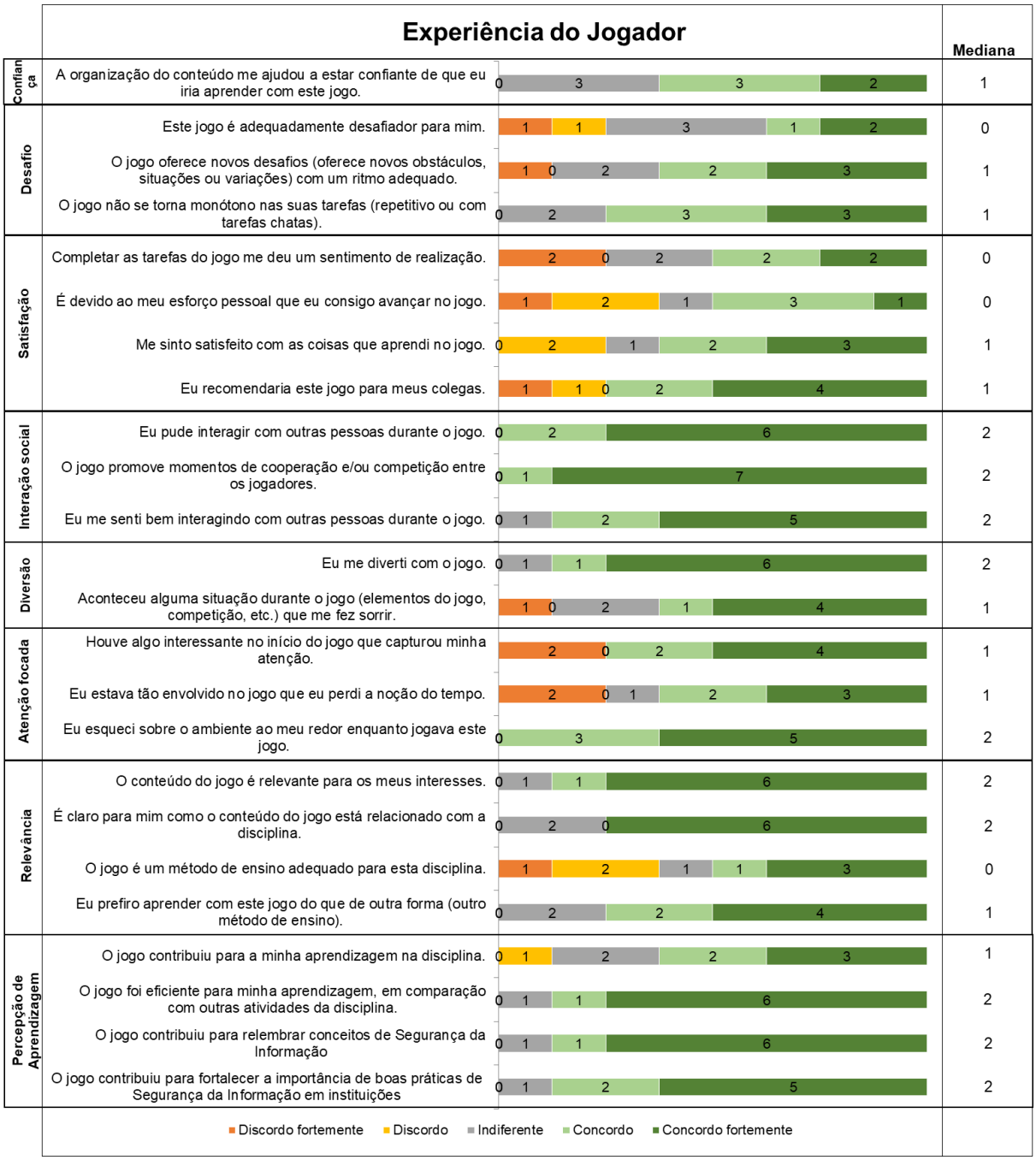
6.2.2 Análise da experiência do jogador

A análise da experiência do jogador demonstra o resultado da percepção de vários componentes sociais, de atenção, satisfação e aprendizado utilizando o jogo de tabuleiro Th3_0ff1c3. Segundo a tabela 7, percebe-se que o jogo de tabuleiro Th3_0ff1c3 não foi completamente desafiador para a maioria dos participantes pela já experiência na área da computação e seus conceitos da segurança da informação que foram vistas na disciplina. Mas ainda assim foi bastante recomendado como um auxiliador no desenvolvimento do conhecimento aplicado, trazendo uma simulação do que pode acontecer em casos de ataques virtuais.

Um dos itens bastante expressivos na tabela 7 são as análises de interação social e divertimento, houve bastante interação e colaboração entre os participantes no formato presencial e na modalidade a distância, que é uma das propostas do jogo de tabuleiro Th3_0ff1c3. O jogo de tabuleiro Th3_0ff1c3 trouxe além das explanações dos conceitos trabalhos bastante diversão entre os jogadores, tornando uma experiência leve e agradável para ser utilizada em sala de aula.

A estatísticas dos dados também apresentou que houve um grande interesse entre os participantes pela relevância do conteúdo apresentado, que trouxe uma praticidade do conteúdo visto em aula que muitas vezes se mantém apenas na teoria do conceito. A grande maioria dos conceitos apresentados no jogo Th3_0ff1c3 já tinham sido vistos durante a disciplina ou em outras disciplinas já cursadas pelos participantes da aplicação do trabalho, sendo um objeto interessante para que o aluno relembre conceitos já vistos e não para aprendizado de conceitos novos.

Tabela 7 - Experiência do jogador do jogo de tabuleiro Th3_0ff1c3



Fonte: Autoria própria.

6.2.2.1 Confiança

Em análise sobre a confiança dos participantes, houve 5 participantes que estavam plenamente confiantes de que o jogo de tabuleiro poderia trazer algo novo para o conhecimento já trabalhado na disciplina e outros 3 participantes que estavam

menos confiantes na abordagem escolhido, isso reflete a pouca experiência na utilização de jogos de tabuleiros pelos participantes.

6.2.2.2 Desafio

Já dito anteriormente, o jogo de tabuleiro Th3_0ff1c3 trouxe conceitos de SI já trabalhados pelos participantes e não houve uma grande complexidade para o aprendizado de conceitos e suas conexões com as regras e mecânicas do jogo, então o aprendizado foi relativamente rápido e não muito desafiante para estudantes da área de computação. Com isso, o jogo Th3_0ff1c3 foi uma experiência divertidas e atrativa para os participantes.

6.2.2.3 Satisfação

Pela característica do jogo Th3_0ff1c3 buscar a colaboração de todos os participantes e não ser apenas um jogo somente competitivo, pode haver a ausência da satisfação plena em vencer o jogo, além de envolver a experiência de jogar um jogo de tabuleiro na forma online pela metade da turma de participantes, onde as interações diminuem e se tornam virtuais. Por outro lado, a utilização do jogo Th3_0ff1c3 teve uma boa avaliação e seria recomendado para os outros colegas dos participantes da aplicação.

6.2.2.4 Interação Social

Neste quesito o jogo teve uma ótima avaliação pela característica de ser um jogo colaborativo e de tabuleiro, onde houve muita interação social entres os participantes no formato presencial e online.

6.2.2.5 Diversão

A utilização do jogo de tabuleiro durante a disciplina foi uma experiência divertida segundo os participantes da pesquisa, por trazer uma maior interação social somada as mecânicas de jogo. Isso se aplicou ao jogo realizado em sala de aula na modalidade presencial e a distância.

6.2.2.6 Atenção focada

Nesta análise a maioria dos participantes avaliou como positiva a capacidade do jogo Th3_0ff1c3 prender a atenção dos jogadores. E alguns participantes, por não estar presencialmente em sala de aula podem ter tido distrações na modalidade e distância, ocasionando perda de atenção e de interesse.

6.2.2.7 Relevância

Para a maioria dos participantes o conteúdo abordado no jogo de tabuleiro Th3_0ff1c3 foi bastante proveitoso para os conhecimentos abordados na disciplina. Mas por outro lado a utilização do jogo de tabuleiro Th3_0ff1c3 é recomendada como uma ferramenta de apoio para a disciplina e não um objeto central ou método para o ensino. Isso demonstrou-se pelas respostas dos participantes.

6.2.2.8 Percepção de aprendizagem

Neste item avaliativo, demonstra-se que não houve aprendizado de novos conceitos de SI após a execução do jogo, mas sim, uma boa avaliação para o fortalecimento de conhecimentos já vistos em sala de aula, pela totalidade dos participantes já com conhecimento prévio dos conceitos trabalhados durante o jogo.

6.2.2.9 Questões discursivas

No questionário do método MEEGA+ foram adicionadas cinco questões discursivas, onde os participantes puderam expressar suas opiniões sobre o jogo de tabuleiro para um adicional nos resultados. As respostas trouxeram algumas confirmações das análises estatísticas propostas pelo método MEEGA+ como a boa interação de cada participante, das análises das mecânicas do jogo de tabuleiro, sobre a necessidade de melhorias gráficas, de uma maior dificuldade para participantes com conhecimentos prévios dos conceitos abordados e comentários da boa apresentação dos conceitos sobre segurança da informação que foram aplicadas no jogo de tabuleiro Th3_0ff1c3.

Na tabela 8 foi questionado sobre o que mais chamou a atenção do participante durante o jogo, e como característica de um jogo de tabuleiro moderno, a interação

social foi bastante lembrada juntamente com o dinamismo que as regras trouxeram. Houve também uma avaliação positiva sobre como o jogo facilitou em relembrar conceitos de SI em tão pouco tempo.

Tabela 8 - O que você mais gostou no jogo?

O que você mais gostou no jogo?
Interação entre os usuários
Da dinâmica
a interação dos 4 jogadores
A dinâmica
Gostei o modo com que ele nos faz analisar o cenário e a interação com as pessoas.
Design
Gostei principalmente do estilo colaborativo do jogo, com elementos de competitividade leves e nada forçados.
O jogo permitiu aprender, relembrar e fixar conceitos de maneira muito rápida. O tempo de duração do jogo é agradável, as mecânicas são boas e confortáveis para públicos diversos. **O que mais gostei, portanto, foi o quão otimizado o tempo é neste jogo.**

Fonte: Autoria própria.

As respostas na tabela 9 são para as possíveis melhorias que podem ser feitas no jogo Th3_0ff1c3 vistas por um público acostumado a jogos digitais, na qual a maioria das sugestões pedem melhorias gráficas influenciadas pelos jogos digitais. Também é pedido revisão de regras e explicações mais simples no manual. Essa sugestão pode ser atendida com gravações de vídeos contendo explicações do jogo de tabuleiro e até futuramente um software auxiliador para o jogo, tornando o jogo de tabuleiro híbrido no quesito não digital e digital.

Tabela 9 - O que poderia ser melhorado no jogo?

O que poderia ser melhorado no jogo?
Manual, jogabilidade, explicações
As cores e os ícones mais diferentes
o sistema de defesa e ataque muito repetitivo
Acho que as cores e ícones, para diferenciar melhor
A clareza das regras e o que necessita ser feito
.
Acredito que algumas regras poderiam ser adaptadas para tornar o jogo um pouco mais desafiador.
O jogo poderia ser um pouco mais difícil. Por exemplo, o ransomware custa 2 nanocoins de resgate, mas ganhamos 3 n¢ por jogada, então sai muito barato. Ou então, para simular o

mundo real, podia ser: "pague 2 nanocoins e role um dado, se cair par, eles devolveram o arquivos, se cair impar tente novamente na próxima rodada", enquanto não se livra do ransomware pode aumentar 1 nvl de ameaça por jogada. **O cavalo de troia poderia invocar mais cartas de incidentes (não sei como implementar isso sem aumentar muito a complexidade), porque senti que no meu tempo de jogo não deu para explorar muito as cartas de incidentes, que certamente me ensinariam mais coisas.** **Algumas cartas de incidentes poderiam tentar trazer a proposta de resolver de alguma forma independente de sorte em rolagem**

Fonte: Autoria própria.

Segunda a tabela 10, o jogo de tabuleiro Th3_0ff1c3 foi um auxiliador para relembrar conceitos de SI de forma prática para os participantes com conhecimento prévio em computação.

Tabela 10 - O jogo auxiliou a relembrar algum conceito de SI?

O jogo auxiliou a relembrar algum conceito de Segurança da Informação?
Sim
Sim
sim ele lembra os tipo de ataque que ocorrer e as medidas de defesa
Sim, os conceitos dos malwares
Sim, ajudou a reforçar os conhecimentos
Sim
Sim, principalmente sobre os tipos de malware e mecanismos de defesa contra eles.
Sim, a abordagem como o jogo trouxe todos os conceitos foi muito interessante, resumida e concisa. O conceito de cavalo de troia, por exemplo. Recentemente estudamos firewall na aula, mas não havia feito a ligação com a ameaça cavalo de troia. **Fiquei bastante satisfeita com a forma como o jogo explorou os conceitos.**

Fonte: Autoria própria.

Na tabela 11 é visto a respostas da pergunta “Aprendi algo novo no jogo?”. As respostas elucidaram que todos os participantes já tinham o conhecimento prévio sobre os conceitos de SI aplicados no jogo de tabuleiro e foi uma ferramenta de retomar conhecimentos já estudados no decorrer do curso da computação.

Tabela 11 - Aprendi algo novo no jogo?

Aprendi algo novo no jogo?
Não
Não
Não
Devido ao meu conhecimento anterior não
Sim, principalmente nas cartas quando caiam no 0
Sim
Acredito que não, mas consegui revisar muitos conceitos que não exercitava há algum tempo.
Na verdade o jogo ajudou mais a organizar e formalizar conceitos, mas foi possível aprender sim. Eu apenas tinha ouvido falar sobre worms e spywares, mas com o jogo pude entender o que são, como acontecem e como prevenir ou remediar.

Fonte: Autoria própria.

A última questão aplicada no questionário solicitou aos participantes demais comentários sobre o jogo de tabuleiro Th3_0ff1c3, onde ficou destacada a diversão que o jogo trouxe e o bom resultado de ser utilizado como uma ferramenta educacional prática e eficiente em sala de aula.

Tabela 12 - Gostaria de fazer mais algum comentário?

Gostaria de fazer mais algum comentário?
Não
É divertido
deixar mais claro nas regras o sistema de moeda e defesa
Bem divertido
Adorei o modo em que foi montado
Não.
Geralmente jogos educativos pecam em não saber conciliar a mecânica com a aprendizagem, no entanto, o Th3_0ff1ce tem a dose certa de cada um. Não me senti perdendo tempo enquanto jogava, me senti verdadeiramente aprendendo e fixando conceitos. O jogo conseguiu isso sem precisar se tornar monótono. Associar conceitos a emoções é uma forma muito boa de grava-los na memória.

Fonte: Autoria própria.

7 CONSIDERAÇÕES FINAIS

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, a computação veio como uma grande auxiliadora para os desafios da sociedade, mas também trouxe alguns problemas.

O surgimento de ameaças contra a segurança digital das pessoas cresceu 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.

Os jogos digitais estão cada vez mais presentes e sendo introduzidos cada vez mais cedo dentro da sociedade, onde temos ao alcance em diversos dispositivos como computadores, *tablets*, celulares, consoles, que podem ser levados para qualquer lugar. Também temos um grande crescimento e busca de jogos não digitais, buscados pela interação social que muitos jogos digitais não apresentam, para Huizinga (2010), o jogo regula as ações e atitudes dos indivíduos nos grupos e cria diversas formas de relações sociais que acabam por se constituir em instituições. Neste trabalho foi apresentado jogos não digitais que se assemelham muito aos jogos digitais, com muitas mecânicas parecidas.

Os jogos no geral têm um papel cada vez mais importantes na formação e no manter cultural da sociedade. Segundo Huizinga (2010), 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 trabalho iniciou com a seguinte pergunta de pesquisa: “A utilização de um jogo de tabuleiro, construído com conceitos da segurança de informação e mecânicas

de jogos de tabuleiro modernos, podem ser um auxiliador/ferramentas no processo de ensino/aprendizagem sobre conceitos de Segurança da Informação?”. E foi respondida utilizando os métodos de coleta de dados por questionários e observações em uma turma de 8 alunos no curso de Sistemas de Informação na disciplina de Segurança e Auditoria de Sistemas de Informação onde houve resultados positivos na aplicação do jogo Th3_0ff1c3 como uma ferramenta de apoio a fixação de conceitos na forma prática e divertida, onde todos os participantes puderam interagir de uma forma livre e democrática.

Este trabalho teve bons resultados nas avaliações de conhecimento e uma avaliação do jogo 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.

A pesquisa aplicada apresentada teve algumas fragilidades que foram observadas como por exemplo o impacto causado pela pandemia de Covid-19 que limitou a aplicação da pesquisa de forma presencial não sendo permitido a execução em diversos ambientes físicos. A pesquisa também se limitou a ser aplicada em apenas um dia, que trouxe menos dados para coleta e tabulação de dados estatísticos. Como recomendação seria importante mais dias de aplicações com turmas de participantes mais heterogêneas, buscando assim um melhor entendimento da efetividade da utilização do jogo Th3_0ff1c3 como ferramenta educacional.

Para os trabalhos futuros utilizando o jogo de tabuleiro Th3_0ff1c3 são sugeridas as seguintes ideias para melhorias e atualizações do produto como:

- Uma maior quantidade de tipos de cartas de *malwares* e de possíveis novos tipos de ameaças virtuais;
- Uma maior quantidade de tipos de incidências de segurança que ocorrem dentro da sociedade em geral;
- Melhorias no design gráfico e de apresentação do produto;
- A possibilidade de um número maior de jogadores;
- Aplicação do jogo em mais lugares como escolas, empresas e indústrias e com públicos diversificados em faixas etárias e de áreas do conhecimento;
- Melhorar a versão digital do jogo de tabuleiro com mais configurações de início do jogo, melhores sons e mecânicas.

REFERÊNCIAS

AFRIKA TEK. Série – **A Evolução do Ransomware – Parte 1,2,3 e 4 – Como a ameaça se propaga**. 2017. Disponível em: <http://www.afrikatec.com.br/serie-evolucao-do-Ransomware-parte-4-como-ameaca-se-propaga/>. Acesso em: 15 nov. 2018.

AHO, A. V.; ULLMAN, J. D. **Foundations of computer science**. C ed ed. New York: Computer Science Press, 1995.

ALEXANDER R. **Zombicide Base Game Review**. 2016. Disponível em: <https://coopboardgames.com/cooperative-board-game-reviews/zombicide-base-game-review/>. Acesso em: 29 jan. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799:2005. **Tecnologia da Informação**. Técnicas de Segurança. Código de prática para a gestão da Segurança da Informação.

BARDIN, Laurence. **Análise de conteúdo.** São Paulo: Edições 70, 2016.
BBC LEARNING, B. **What is computational thinking?** 2015. Disponível em: <http://www.bbc.co.uk/education/guides/zp92mp3/revision>. Acesso em: 22 de dez 2019.

BARROS, A. J. S.; LEHFELD, N. A. S. Fundamentos de Metodologia Científica. 3. Edição São Paulo: Paerson Prentice Hall, 2014.

BASHAM, M. **The Script Kiddie Cookbook**. p. 131, 2005.

BURGUN, K. **What Makes a Game?** Gamasutra, mar. 2012. Disponível em: <https://www.gamasutra.com/view/feature/167418/what_makes_a_game.php> Acesso em: 22 de jan. 2020.

CAETANO, E. "**O que é hacker?"; Brasil Escola**. Disponível em: <https://brasilescola.uol.com.br/informatica/o-que-e-hacker.htm>. Acesso em 12 de janeiro de 2020.

CASTELLS, M. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Revisão: Paulo Vaz. Rio de Janeiro: Zahar, 2003.

CARMO, V. **O uso de questionários em trabalhos científicos**. 2013. Disponível em: <http://www.inf.ufsc.br/~vera.carmo/Ensino_2013_2/O_uso_de_questionarios_em_trabalhos_cient%EDficos.pdf> Acesso em: 17 de ago. 2022.

CERT.br. **Cartilha de Segurança para Internet**. Comitê Gestor da Internet no Brasil, São Paulo, 2017. Disponível em <https://cartilha.cert.br/>. Acesso em: 20 nov. 2018.

CERT.br. **Códigos maliciosos (Malware)**. Comitê Gestor da Internet no Brasil, São Paulo, 2017. Disponível em < https://cartilha.cert.br/malware/>. Acesso em: 28 fev. 2020.

CERT.br. **Golpes na Internet**. Comitê Gestor da Internet no Brasil, São Paulo, 2017. Disponível em < https://cartilha.cert.br/golpes/> Acesso em: 28 fev. 2020.

CONTROLALTHACK. **About**. 2012. Disponível em: <http://www.controlalthack.com/about.php> Acesso em: 21 de out. 2022.

CSIZMADIA, A.; CURZON, P.; DORLING, M.; et al. **Computational thinking - A guide for teachers**. 2015. Computing At School (CAS). Disponível em: <http://community.computingatschool.org.uk/files/6695/original.pdf>. Acesso em: 20 de jan. 2020

EGOV. **Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros.** Portal de e-governo, inclusão digital e sociedade do conhecimento, 2016. Disponível em: <https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros>. Acesso em: 20 nov. 2019.

ESCOLADAINTELIGENCIA. **O que é o método de ensino construtivista?** 2019. Disponível em: < https://escoladainteligencia.com.br/o-que-e-o-metodo-de-ensino-construtivista/>. Acesso em: 10 de abr. 2020.

ESET. **5 coisas que você deve saber sobre Engenharia Social**. 2016. Disponível em: <https://www.welivesecurity.com/br/2016/08/19/sobre-engenharia-social/>. Acesso em: 09 de mar. 2020.

FILHO, E. F. M., LIMA, L. K. R. S., SOUZA, N. C. **Jogo de tabuleirio nacional: lavyrinthos interrelação entre eurogame e wargame, tabuleiro mutável**. 2015. Trabalho de Conclusão de Curso (Tecnólogo em Design Gráfico) – Serviço Nacional de Aprendizagem Comercial, Goiânia, 2015.

GIL, A. **Métodos e técnicas de pesquisa social**. 5. ed. São Paulo: Atlas, 1999

GONDREE, M., PETERSON, Z. N. J. **Valuing Security by Getting [d0x3d!] Experiences with a network security board game.** 2013.

GONÇALVES, M et al. **Perícia forense computacional: metodologias, técnicas e ferramentas.** 2012. Disponível em: <http://eduvalesl.revista.inf.br/imagens_arquivos/arquivos_destaque/LXkEA5FVHGZF1FB_2015-12-19-2-33-33.pdf>. Acesso em 07 de mai. 2022.

GONZÁLEZ-TABLAS FERRERES, A. I., GONZÁLEZ VASCO, M. I. **Crypto Go: Symmetric key - English (open source) [Card game]**. 2018. Madrid: Universidad Carlos III de Madrid, Universidad Rey Juan Carlos.

GRECA, H. **O Nascimento dos Jogos de Tabuleiro Modernos: 1820-1869**. 2013. Disponível em: <https://brjoga.wordpress.com/2013/01/23/o-nascimento-dos-jogos-de-tabuleiro-modernos-1820-1869/>. Acesso em 20 de jul. 2020.

GROVER, S.; PEA, R. **Computational Thinking in K-12**: A Review of the State of the Field. Educational Researcher, v. 42, n. 1, p. 38–43, 2013.

HUIZINGA, Johan. **Homo Ludens: o jogo como elemento da cultura**. São Paulo, Perspectiva, 1990.

JACOBSON, D.; IDZIOREK, J. **Computer security literacy.** Taylor e Francis Group.

KASPERSKY. **O que é spyware? – Definição.** 2022. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/spyware>. Acesso em 20 de out. 2022.

KAYWORTH, T.; WHITTEN D. Effective Information Security Requires a Balance of Social and Technology Factors. **MIS Quarterly Executive**, v. 9, n. 3, p. 163-175, 2010.

KITCHENHAM B., PEARL BRERETON O., BUDGEN D., TURNER M., BAILEY J. and LINKMAN S.,"**Systematic literature reviews in software engineering A systematic literature review**", Information and Software Technology, vol. 51, no. 1, pp. 7-15, 2009.

KOCH, J. **Similaridade – O que é ser igual ou similar na matemática?** 2019. Disponível em: <https://www.deviante.com.br/noticias/ciencia/similaridade-o-que-e-ser-igual-ou-similar-na-matematica/> Acesso em: 08 de mar. 2020

LIUKAS, L. **Hello Ruby: adventures in coding**. Feiwel & Friends, 2015.

LIUKAS, L. **Olá Ruby**: uma aventura pela programação. 1. ed. São Paulo: Companhia das Letras, 2019.

LUBIN, R. **CIA: Collect It All**. 2016. Disponível em: <https://diegeticgames.com/cia-collect-it-all/>. Acesso em: 20 de jan. 2020

MALWAREBYTES. **Tudo Sobre ransomware**. 2016. Disponível em: <https://br.malwarebytes.com/ransomware/>. Acesso em: 06 de mar. 2020

MATOS, P.C.A. **Cibersegurança: Políticas Públicas para uma Cultura de Cibersegurança nas Empresas**. 2018. Dissertação (Mestrado em Economia e Políticas Públicas). Instituto Universitário de Lisboa, Lisboa, 2018.

MATTELART, A. História da sociedade da informação. São Paulo: Loyola, 2002.

MCMASTER, K.; RAGUE, B.; ANDERSON, N. Integrating Mathematical Thinking, Abstract Thinking, and Computational Thinking. **40th ASEE/IEEE Frontiers in Education Conference**, out. 2010. Acesso em: 21 de jan. 2020.

NIC.br. **Acesso às Tecnologias da Informação e da Comunicação (TIC).** CETIC.br, Brasil, nov. 2010. Disponível em <http://www.cetic.br/usuarios/tic/2010-total-brasil/rel-geral-04.htm>. Acesso em: 22 nov. 2018.

NUNES, D. J. **Ciência da Computação na Educação Básica**. ADUFRGS - Sindical, 6. jun. 2011. Disponível em: <https://adufrgs.org.br/artigos/ciencia-da-computacao-na-educacao-basica/> Acesso em: 23 de dez. 2019.

PAPERT, S. **Mindstorms: Children, Computers, and Powerful Ideas**. Basic Books, 1980.

PAPERT, S.; SOLOMON, C. **Twenty things to to with a Computer**. Educational Technology Magazine, 1972. Disponível em: <http://www.stager.org/articles/twentythings.pdf> Acesso em: 19 de fev. 2020.

PEREIRA, L. S. **Design de jogo de tabuleiro para aprendizado de processos políticos.** 2016. Dissertação (Trabalho de conclusão de curso em Design Visual). Universidade Federal do Rio Grande do Sul, Porto Alegre, 2016.

PETRI, G.; WANGENHEIM, C. G.; BORGATTO, A. F. **Benefícios dos Jogos Não-Digitais no Ensino de Computação.** 2018.

PETRI, G.; WANGENHEIM, C. G.; BORGATTO, A. F. **MEEGA+KIDS**: A Model for the Evaluation of Educational Games for Computing Education in Secondary School. Florianópolis: INCOD/UFSC, 2018. Disponível em: http://www.incod.ufsc.br/wp-content/uploads/2018/08/Relatorio-Tecnico-INCoD_GQS_06_2018_E-vf.pdf. Acesso em: 20 jan. 2020.

PFLEEGER, Charles P., **Security in Computing. 2a. Edition**. Editorial Precision Graphic Services Inc. NJ 07458. 1997. USA

PICCIONE, P. A. **In Search of the Meaning of Senet,** Archaeology, ago. 1980, p. 55-58. Disponível em: <http://www.gamesmuseum.uwaterloo.ca/Archives/Piccione/index.html>. Acesso em: 20 de dez. 2019.

ROCKY, R. - Entrevista com Hélio Greca para o site Raccoon. 2013. Disponível em: <http://raccoon.com.br/2013/01/17/o-nascimento-dos-jogos-de-tabuleiro-modernos> Acesso em: 15 de jan. 2020.

SAVIOLIIMA. **Algoritmos**. 2013. Disponível em: <https://programecmg.wordpress.com/2013/03/28/algoritmos/>. Acesso em: 10 de mar. 2020

SCHELL, J. **The Art of Game Design**. Burlington: Elsevier, 2008.

SHAUGHNESSY, John J.; ZECHMEISTER, Eugene B.; ZECHMEISTER, Jeanne S. **Metodologia de pesquisa em psicologia**. AMGH Editora, 2012

TOMSK. **Championship on the Tomsk game on cyber security took place in the UM.** 2018. Disponível em: <https://www.riatomsk.ru/article/20181004/championship-on-the-tomsk-game-on-cyber-security-took-place-in-the-un/>. Acesso em: 31 jan. 2020.

VAIFANUA, T. **Utah mother shares experience of son who died by suicide after 'sextortion' scam**. 2017. Disponível em: <https://fox13now.com/2017/01/13/utah-mother-shares-experience-of-son-who-committed-suicide-after-sextortion-scam/>. Acesso em: 28 jan. 2020.

SHELL, B.; MARTIN, C. **Webster's New Word – Hacker Dictionary**. p. 6, 2006.

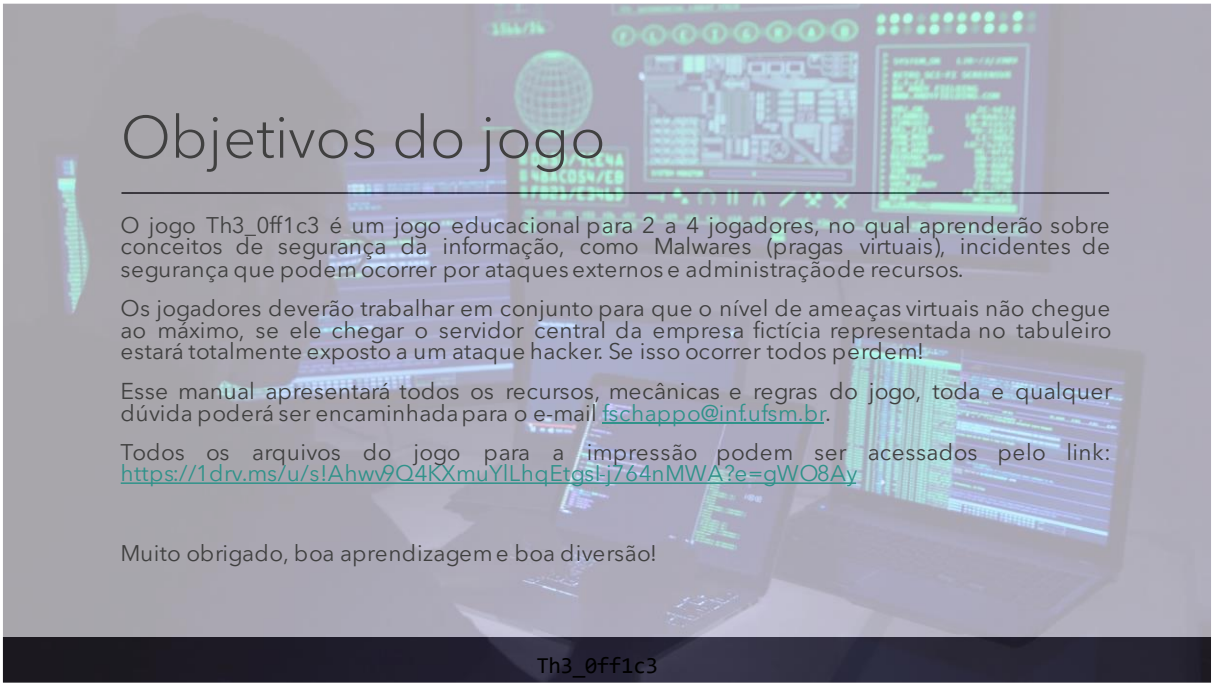
WING, J. M. Computational thinking benefits society. **Social Issues in Computing**, New York, 10 jan. 2014. Disponível em: <http://socialissues.cs.toronto.edu/index.html%3Fp=279.html>. Acesso em: 22 set. 2019.

WING, J. M. Computational thinking. **Communications of the ACM**, v. 49, n. 3, p. 33, 2006.

WOODS, S., Eurogames: **The Design, Culture and Play of Modern European Board Games.** London. McFarland. 2012.

YONEMURA, K. *et al*. **Effect of Security Education using KIPS and Gamification Theory at KOSEN**. 2018.

APENDICE A – MANUAL DO JOGO DE TABULEIRO TH3_0FF1C3



O Contrato

Parabéns! Você é a nova empresa de segurança da informação contratada pelo nosso grande escritório!

Os "hackers do mal" estão tentando roubar nossos recursos e destruir informações.

Sua missão é manter nossos serviços seguros e funcionando bem. Infelizmente estamos com poucos recursos financeiros para investir em nossa segurança digital. Por isso escolhemos você para gerenciar nossas ferramentas de defesa contra os ataques cibernéticos.

E jamais permita que nosso servidor central seja atacado e infectado, isso seria o fim de todos nós!

Vocês deverão chegar até o último turno sem deixar o nível de ameaças chegar ao máximo.

Boa sorte!

Elementos necessários –dado D10

Para inicio do jogo é necessário ter um dado do tipo D10, que pode ser adquirido via internet, lojas de elementos de jogos de RPG ou por aplicativos gratuitos.

Ex: https://dado.online/10-caras/1-dado

Obs: Alguns dados D10 tem a numeração de 0-9 e outros de 1-10. Nos dados de 0-9, o 0 indicara a compra de uma carta de incidentes de segurança, no dado de 1-10, o numero 10 indicara a compra de uma carta de incidentes de segurança.

iOS - D20 Natural Grátis

Android - RPG Simple Dice

Preparação:

2 – 4 Jogadores

Estimativa
45 Minutos

O jogo de tabuleiro "Th3_0ff1c3" pode ser jogado com 2 ou 4 jogadores. Cada jogador inicialmente deverá escolher uma cor entre a vermelha, verde, amarelo e azul. Para dois jogadores cada um deverá escolher duas cores.

Cada jogador então pegará seus 9 hexágonos correspondentes da sua cor e sua ficha da empresa de segurança

Exemplo:

Hexágono do jogador vermelho

Ficha da empresa de segurança

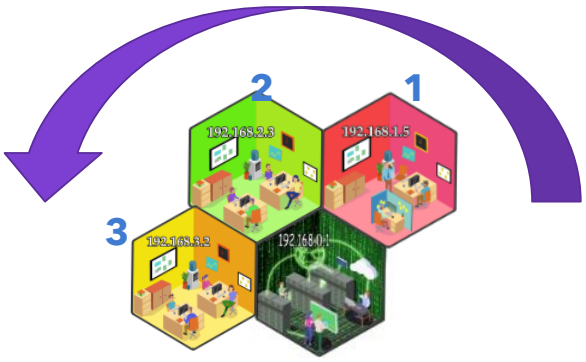
Montagem do tabuleiro

Para iniciar a montagem do tabuleiro é necessário colocar no centro da mesa o hexágono do servidor central.

Esse é o ponto mais importante do tabuleiro, todos devem defende-lo!

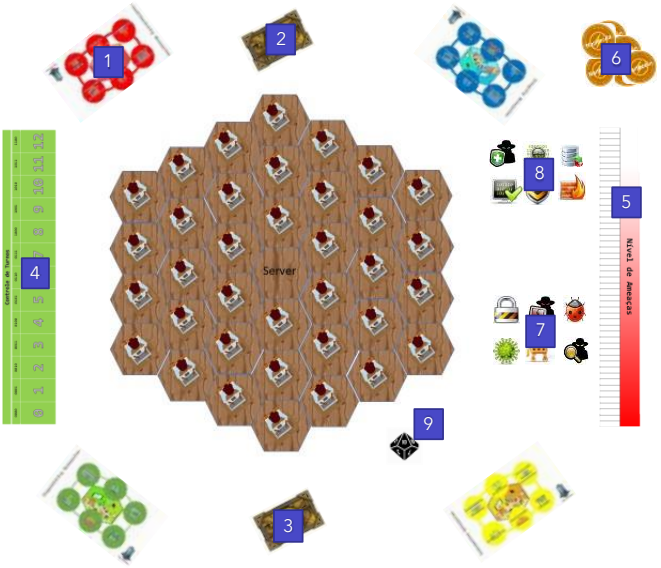
Montagem do tabuleiro

Logo após cada jogador colocará em sentido anti-horário seus hexágonos, um de cada vez, em forma espiral até que tenha terminado todos os hexágonos.



Montagem do tabuleiro

Após todos os jogadores colocarem seus hexágonos na mesa, o grande escritório estará montado. Após isso é necessário posicionar as fichas dos jogadores (1), a pilha de baralho de malwares (2), a pilha de baralho de incidentes de segurança (3), a ficha de controle de turnos (4) a ficha de controle de nível de ameaças virtuais (5), as nanocoins (6), os marcadores de tipos de malwares (7), os marcadores de recursos de segurança (8) e o dado D10 (9).

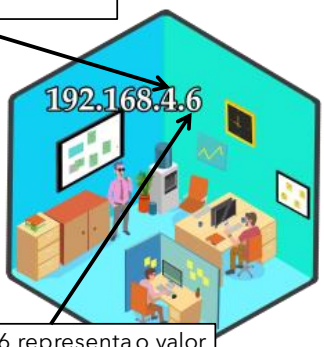


Representação do tabuleiro montado

A anatomia da estação de trabalho

As estações de trabalho são os componentes que formam o escritório, existem 4 cores diferentes para representar os 4 jogadores. Inclusive cada estação de trabalho tem um número que representa um IP do computador da estação de trabalho que tem o padrão 192.168.x.y, onde o x representa a qual jogador ela pertence e o y o valor que poderá ser sorteado pelo dado.

O número 4 indica que essa estação de trabalho está sendo protegida pelo jogador 4.



O número 6 representa o valor que poderá ser sorteado pelo dado, se o dado cair no número 6, todos as estações com o IP com final 6 será testado pelo ataque virtual.

O que é um IP?

Um Endereço de Protocolo da Internet, do inglês Internet Protocol address, é um rótulo numérico atribuído a cada dispositivo conectado a uma rede de computadores que utiliza o Protocolo de Internet para comunicação.

A anatomia de uma carta de malware

As cartas de malwares e de incidentes de segurança são as ações dos cracker, ou hackers do mal, que querem destruir o "Th3_0ff1c3".

Título da carta de Malware

Tipo de ataques

Descrição e efeito do ataque virtual

Quantos aumentos no nível de ameaças virtuais causa

O que é um Malware?

Malware é a abreviação de "software malicioso" (em inglês, malicious software) e se refere a um tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas.

Marcadores de ação contra malwares

No inicio do jogo, cada jogador receberá **3 marcadores** de cada item dos recursos de defesas de segurança, que são: O antivírus, treinamentos contra phishing, antispyware, atualização de sistemas operacionais, backup do sistema e atualização do firewall. Cada defesa bem sucedida valerá um "nanocoin" para o jogador.

Antivírus

Antispyware

Backup do sistema

Treinamentos contra phishing

Atualização de Sistemas Operacionais

Atualização do Firewall

Descrição dos marcadores de segurança

Antivírus

O marcador de antivírus imuniza a estação de trabalho do tabuleiro, se ocorrer um ataque de vírus esse marcador irá proteger o espaço, um marcador de antivírus também remove infecções por vírus de computador.

Os antivírus são programas informáticos desenvolvidos para prevenir, detectar e eliminar vírus de computador.
Wikipedia

Descrição dos marcadores de segurança

Treinamento contra phishing

O marcador de treinamento contra phishing, deixará o colaborador(a) do escritório com recursos para se defender contra um golpe do tipo phishing. Ou seja, a estação de trabalho com um treinamento contra phishing não sofrerá as penalidades de um ataque desse tipo.

Como **prevenir phishing**
Não abra anexos contidos em e-mail que não foram solicitados. Proteja suas senhas e não revele-as a ninguém. Não forneça informação confidencial a ninguém - no telefone, pessoalmente ou via e-mail. Verifique a URL do website (o endereçodo site).

Avast

Descrição dos marcadores de segurança

Antispyware

O marcador do tipo antispyware imuniza a estação de trabalho do tabuleiro, ou seja, não sofrerá as consequências de uma infecção por spyware.

Um **antispyware** é um software de segurança que tem o objetivo de detectar e remover adwares e spywares. A principal **diferença** de um **anti-spyware** de um **antivírus** é a classe de programas que eles removem. Adwares e spywares são consideradas áreas "cinza",pois nem sempre é fácil determinar o que é um adware e um spyware.

Segurança UOL

Descrição dos marcadores de segurança

Atualização de sistema operacional

O marcador do tipo de atualização de sistema operacional corrige "bugs", ou falhas de software em sistemas operacionais, os malwares do tipo "Worm" utilizam falhas em sistemas operacionais para se replicar dentro do escritório.

O Windows Update é um serviço de atualização da Microsoft para os sistemas operacionais Windows. O Windows Update é o responsável por verificar junto ao Microsoft Update as atualizações que o Windows precisa.

Wikipedia

Descrição dos marcadores de segurança

Backup do sistema

O marcador do tipo backup do sistema mantem os dados seguros contra os ataques de sequestros de dados (ransomware). Uma estação de trabalho com um backup realizado poderá se recuperar rapidamente de um sequestro de dados.

Backup é uma cópia de segurança. O termo em inglês é muito utilizado por empresas e pessoas que guardam documentos, imagens, vídeos e outros arquivos no computador ou na nuvem, hospedados em redes online como Dropbox e Google Drive.

Techtudo

Descrição dos marcadores de segurança

Atualização do firewall

O marcador do tipo atualização do firewall mantem a estação de trabalho do tabuleiro com as portas de acesso fechadas, tornando os cavalos de Tróia inacessíveis pelos hackers atacantes.

Firewall é uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

Helpdigitalti

Marcadores de ação dos malwares

Os marcadores do tipo **Malwares**, representam os tipos de ataques contra o escritório, eles são colocados para marcar os ataques bem sucedidos nas estações de trabalho sorteadas. Os tipos de malwares são: Vírus, phishing, spyware, worm, ransomware e cavalo de Tróia. Cada infecção bem sucedida eleva o **nível de ameaças virtuais**!

Vírus

Spyware

Ransomware

Phishing

Worm

Cavalo de Tróia

Descrição dos marcadores de malwares

Vírus

O marcador de vírus, infecta computadores que não estão imunizados com antivírus, os vírus só são removidos após a aplicação de um antivírus.

Em informática, um vírus de computador é um software malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática.

Wikipedia

Descrição dos marcadores de malwares

Phishing

O marcador de phishing é um ataque que rouba recursos do escritório, consequentemente do jogador que sofrer o ataque. O marcador é removido do tabuleiro após o final do turno, mas o jogador perderá um “nanocoin” por ataque bem sucedido.

Phishing é uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos.

Avast

Descrição dos marcadores de malwares

Spyware

O marcador de spyware infecta a estação de trabalho, roubando um recurso de defesa do jogador a cada inicio de turno, ele só é removido com a utilização de um antispyware.

Spyware é um tipo de malware que é difícil de se detectar. Ele coleta informações sobre seus hábitos online, histórico de navegação ou informações pessoais (como números de cartão de crédito), e geralmente usa a internet para passar estas informações a terceiros sem você saber.

Avast

Descrição dos marcadores de malwares

Worm

O marcador de worm infecta a estação de trabalho utilizando uma falha existente no sistema operacional, como a falha existe em todos os sistemas do escritório ele vai tentar em cada turno infectar a estação de trabalho a sua direita, se não houver, tentará a sua esquerda. Ele só é removido atualizando o sistema operacional.

Em informática um worm é um programa autorreplicante, diferente de um vírus, este é completo e não precisa usar outro para se propagar. Um worm pode ser projetado para tomar ações maliciosas após infestar um sistema, como por exemplo, deletar arquivos em um sistema ou enviar documentos por email.

Wikipedia

Descrição dos marcadores de malwares

Ransomware

O marcador de ransomware sequestra a estação de trabalho, tornando ela inoperante. A estação de trabalho sequestrada só poderá ser utilizada novamente pagando dois "nanocoins" ao hacker malicioso. A estação de trabalho só estará a salvo de um ataque desse tipo com um backup do sistema.

Ransomware é um tipo de software nocivo que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate em criptomoedas para que o acesso possa ser restabelecido. Caso não ocorra o mesmo, arquivos podem ser perdidos e até mesmo publicados.

Wikipedia

Descrição dos marcadores de malwares

Cavalo de Tróia

O marcador de cavalo de Tróia infecta a estação de trabalho, abrindo a porta para os hacker maliciosos atacarem. A cada rodada, se o cavalo de Tróia não for bloqueado (removido) utilizando uma atualização de firewall ele irá instalar um novo tipo de malware sorteado no próximo turno na estação de trabalho infectada.

Um **cavalo de Troia** (em inglês Trojan horse) é um **malware** (programa malicioso) que age tal como na história do **Cavalo de Troia**, entrando no computador e criando uma porta para uma possível invasão; e é fácil de ser enviado, clicando na ID do computador e enviando para qualquer outro computador.

Wikipedia

Conhecendo o jogo Th3_0ff1c3

O jogo é realizado em rodadas, ou seja, uma rodada termina quando todos os jogadores terminarem seus turnos, de forma sequencial no sentido que desejarem (horario ou anti-horário), onde todos os jogadores devem realizar tarefas sequenciais durante a partida. No inicio do jogo cada jogador receberá **4 marcadores de cada recursos de defesas de segurança** e os posicionar sobre a sua ficha da empresa de segurança que representam. Após isso cada jogador irá receber **4 fichas de nanocoins** que pode ser utilizado para comprar novos marcadores de recursos de segurança nos turnos seguintes, isso somente ocorre no inicio do jogo.

No inicio dos turnos seguintes cada jogador irá receber 3 nanocoins como o pagamento do contrato e um marcador de cada tipo de recurso de segurança pagos pelo escritório.

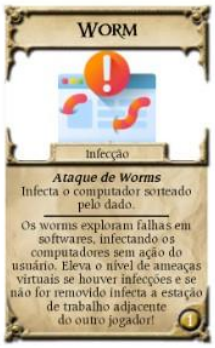
Sequencia de um turno (após o turno "0")

1) Recebimento de 3 nanocoins para cada jogador e um marcador de cada tipo de recurso de segurança;
2) Compra de recursos de segurança (1 nanocoin para cada recurso);
3) Abertura da carta do tipo de ataque por malware no turno por um jogador;
4) Aplicação dos recursos de segurança nas estações de trabalho;
5) Rolagem do dado para sorteio dos IP's atingidos pelo ataque virtual (Se cair o número 0, deverá ser comprado uma carta do baralho de incidentes de segurança e aplicado o seu efeito e novamente é rolado o dado para sortear o IP);
6) Colocação dos ataques bem sucedidos nas estações de trabalho desprotegidas e subir nível das ameaças virtuais conforme o ataque;
7) Recebimento de nanocoins por defesas bem sucedidas ou pagamento por ataques bem sucedidos;
8) Remoção das defesas que voltam ao estoque central, as infecções bem sucedidas do tipo vírus, worms, ransomwares, spyware e cavalo de Tróia ficam no tabuleiro até a sua solução!;
9) Aumento de 1 turno na ficha de controle de turnos;
10) Final de turno.

Exemplo de uma jogada

O jogador 1, pegou uma carta do tipo "worm" no tabuleiro de ameaças virtuais, o texto da carta deve ser lido para todos os jogadores saberem o efeito que ela causa no escritório.

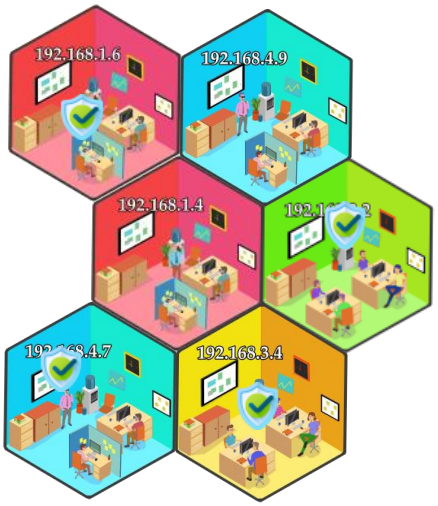
Os jogadores então saberão que devem usar o marcador de "**Atualização de sistema operacional"** para não serem infectados pelo malware.



Exemplo de uma jogada

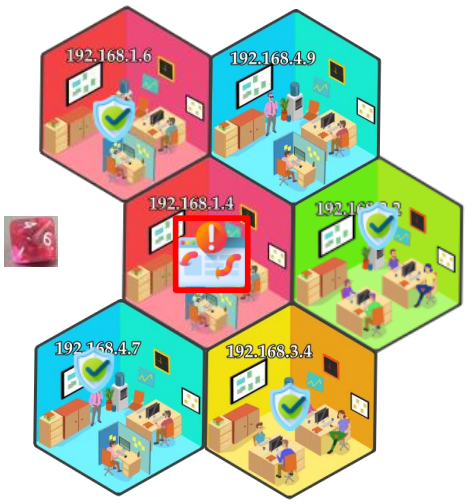
Após isso são colocado os marcadores onde cada jogador achar necessário defender nas estações de trabalho, no jogo todos sabem qual o tipo de ataque que ira ocorrer, mas não sabem onde ele vai atacar.

Quando todos colocarem seus recursos, um jogador poderá jogar o dado para sortear a estação de trabalho.



Exemplo de uma jogada

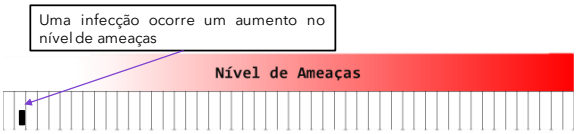
O dado deu resultado "4", todas as estações de trabalho que terminam com o IP .4 estarão suscetíveis ao ataque. Na representação do exemplo existem duas estações com o número 4, do jogador vermelho e do jogador amarelo. O jogador vermelho foi infectado, aumentando o nível de ameaças virtuais, e o amarelo defendeu-se do ataque virtual recebendo 1 nanocoin de recompensa.



Exemplo de uma jogada

Após a etapa dos ataques dos malwares, são removido todas os marcadores de recursos de segurançaque voltam ao estoque central.

As infecções por malware são persistentes e ficam até o turno seguinte, onde o jogador poderá resolver ele.



Condição de vitória

Por ser um jogo educativo colaborativo todos vencem atingindo o objetivo de chegar no ultimo turno. Pode-se ranquear os jogadores contando quantos nanocoins cada um terá no final da partida.

Versão do tabuleiro online

Você também pode jogar o jogo tabuleiro Th3_0ff1c3 no modo online e convidar os seus amigos.

O acesso é realizado pelo site "Tabletopia" e não é necessário um cadastro!

Acesse o link para jogar:
https://tabletopia.com/games/th3-0ff1c3-bhp3jq/play-now

Th3_0ff1c3

PPGTER - Pós-Graduação em Tecnologias Educacionais em Rede

Th3_0ff1c3

APENDICE B – QUESTIONÁRIO DEMOGRÁFICO

Caro aluno (a),

Este questionário foi desenvolvido apenas para fins de pesquisa do Projeto "TH3_0FF1C3: UM JOGO DE TABULEIRO EDUCACIONAL PARA O ENSINO DE CONCEITOS DA SEGURANÇA DA INFORMAÇÃO", sendo totalmente anônimo e sem fins para avaliação na disciplina.

Muito obrigado,
Mestrando: Francis Mallmann Schappo Orientadora:
Profª Drª Roseclea Duarte Medina

1. No momento você está em qual modalidade?

Marcar apenas uma oval.

- ◯ Presencial
- ◯ Online

2. Qual sua faixa etária?

Marcar apenas uma oval.

- ◯ Menos de 18 anos
- ◯ 18 a 28 anos
- ◯ 29 a 39 anos
- ◯ 40 a 50 anos
- ◯ Mais de 50 anos

3. Qual seu sexo?

Marcar apenas uma oval.

- ◯ Masculino
- ◯ Feminino
- ◯ Prefiro não dizer

4. Indique a faixa de renda que sua família possui

Marcar apenas uma oval.

- Menos de R$ 1.000
- R$ 2.000 a R$ 3.000
- R$ 3.000 a R$ 4.000
- R$ 4.000 a R$ 5.000
- Entre R$ 5.000 e R$ 10.000
- Mais de R$ 10.000

5. Qual é a sua situação atual de emprego?

Marcar apenas uma oval.

- Trabalho de meio tempo
- Trabalho de tempo completo
- Desempregado
- Autônomo
- Estudante
- Aposentado

6. Se tiver uma ocupação além de estudante, qual sua área de atuação profissional?

_____

7. Você conhece alguém ou já teve algum tipo de prejuízo ocasionado por ataques virtuais?

Marcar apenas uma oval.

- Sim
- Não

8. Se a resposta anterior for Sim, consegue descrever o ataque?

_____

9. Você conhece, ou já jogou algum jogo de tabuleiro moderno (cardgames, boardgames)?

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Não sei dizer

10. Se a resposta anterior for Sim, qual o jogo de tabuleiro jogado?

_____

APENDICE C – QUESTIONÁRIO DE CONHECIMENTO

Questionário de conhecimento

Caro aluno (a),

Este questionário foi desenvolvido apenas para fins de pesquisa do Projeto "TH3_0FF1C3: UM JOGO DE TABULEIRO EDUCACIONAL PARA O ENSINO DE CONCEITOS DA SEGURANÇA DA INFORMAÇÃO", sendo totalmente anônimo e sem fins para avaliação na disciplina. Por isso é importante não haver qualquer tipo de consulta sobre o conteúdo abordado aqui.

Muito obrigado,
Mestrando: Francis Mallmann Schappo
Orientadora: Profª Drª Roseclea Duarte Medina

*Obrigatório

1. No momento você está em qual modalidade?

Marcar apenas uma oval.

- ◯ Presencial
- ◯ Online

2. Julgue a afirmação: Com o desenvolvimento tecnológico na área da Computação houve um decréscimo nos números de ataques virtuais e de prejuízos para a sociedade. *

Marcar apenas uma oval.

- ◯ Verdadeiro
- ◯ Falso
- ◯ Não sei dizer/Não lembro

3. Qual das alternativas é o golpe descrito a seguir: “Tipo de fraude na qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.” *

Marcar apenas uma oval.

- ◯ Hacking
- ◯ Spam
- ◯ Phishing
- ◯ Pharming
- ◯ DDoS (Distributed Denial of Service)
- ◯ Não sei dizer/Não lembro

4. Qual das opções é o malware descrito a seguir: “Programa malicioso que age entrando no computador e criando uma porta para uma possível invasão”? *

Marcar apenas uma oval.

- ◯ Vírus
- ◯ Worm
- ◯ Cavalo de Tróia (Trojan Horse)
- ◯ Bot
- ◯ Spyware
- ◯ Não sei dizer/Não lembro

5. Qual das opções é o mecanismo de segurança descrito a seguir: “Ferramenta utilizada para proteger um computador contra acessos não autorizados vindos da Internet”? *

Marcar apenas uma oval.

- ◯ Antimalware
- ◯ Antivírus
- ◯ Internet Protector
- ◯ Block Intruder
- ◯ Firewall
- ◯ Não sei dizer/Não lembro

6. Qual das opções é o malware descrito a seguir: “Programa Malicioso que se propaga pela rede utilizando falhas de programação”? *

Marcar apenas uma oval.

- ◯ Vírus
- ◯ Cavalo de Tróia (Trojan Horse)
- ◯ Worm
- ◯ Spyware
- ◯ Adware
- ◯ Não sei dizer/Não lembro

7. Método bastante utilizado para enganar e obter vantagens de pessoas na Internet. *

Marcar apenas uma oval.

- ◯ Engenharia de segurança
- ◯ Engenharia de dados
- ◯ Engenharia de redes
- ◯ Engenharia social
- ◯ Engenharia de programação
- ◯ Não sei dizer/Não lembro

8. Um dos ataques mais populares ultimamente é o sequestro de dados, que é classificado por qual tipo de malware? *

Marcar apenas uma oval.

- ◯ Worm
- ◯ Vírus
- ◯ Ransomware
- ◯ Spyware
- ◯ Adware
- ◯ Não sei dizer/Não lembro

9. Julgue a afirmação: Um computador com um sistema operacional atualizado, utilizando um software de antivírus e um firewall está totalmente seguro. *

Marcar apenas uma oval.

- ◯ Verdadeiro
- ◯ Falso
- ◯ Não sei dizer/Não lembro

10. O que é um Exploit? *

Marcar apenas uma oval.

- ◯ Mutação de vírus
- ◯ Falha de código
- ◯ Defeito de hardware
- ◯ Vazamento de banco de dados
- ◯ Uma classificação de Malware
- ◯ Não sei dizer/Não lembro

11. A imagem abaixo representa um dispositivo conhecido como "Rubber Ducky" ou Bad USB. O que ele faz? *

Marcar apenas uma oval.

- [ ] Injeta códigos no computador da vítima
- [ ] É um pendrive normal
- [ ] Ele danifica o equipamento com alteração de voltagem
- [ ] Libera um acesso WiFi no computador da vítima
- [ ] Geralmente é bloqueado pelos softwares antivírus
- [ ] Não sei dizer/Não lembro

APENDICE D – QUESTIONÁRIO DE AVALIAÇÃO DA QUALIDADE DE JOGOS

Questionário para a avaliação da qualidade de jogos

Gostaríamos que você respondesse as questões abaixo sobre a sua percepção da qualidade do jogo para nos ajudar a melhorá-lo. Todos os dados são coletados anonimamente e somente serão utilizados no contexto desta pesquisa. Algumas fotografias poderão ser feitas como registro desta atividade, mas não serão publicadas em nenhum local sem autorização.

Mestrando: Francis Mallmann Schappo
Orientadora: Profª Drª Roseclea Duarte Medina

*Obrigatório

1. Você participou dessa pesquisa em qual modalidade?

Marcar apenas uma oval.

- ◯ Presencial
- ◯ Online

2. Com que frequência você costuma jogar jogos digitais? *

Marcar apenas uma oval.

- ◯ Nunca: nunca jogo.
- ◯ Raramente: jogo de tempos em tempos.
- ◯ Mensalmente: jogo pelo menos uma vez por mês.
- ◯ Semanalmente: jogo pelo menos uma vez por semana.
- ◯ Diariamente: jogo todos os dias.

3. Com que frequência você costuma jogar jogos não-digitais (de cartas, tabuleiro, etc.)? *

Marcar apenas uma oval.

- Nunca: nunca jogo.
- Raramente: jogo de tempos em tempos.
- Mensalmente: jogo pelo menos uma vez por mês.
- Semanalmente: jogo pelo menos uma vez por semana.
- Diariamente: jogo todos os dias.

Usabilidade

Por favor, marque uma opção de acordo com o quanto você concorda ou discorda de cada afirmação abaixo.

(Onde 1 - Discordo totalmente, 2 - Discordo, 3 - Nem discordo, nem concordo, 4 Concordo, 5 - Concordo totalmente).

4. O design do jogo é atraente (tabuleiro, cartas, interfaces, gráficos, etc.). *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

5. Os textos, cores e fontes combinam e são consistentes. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

6. Eu precisei aprender poucas coisas para poder começar a jogar o jogo. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

7. Aprender a jogar este jogo foi fácil para mim. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

8. Eu acho que a maioria das pessoas aprenderiam a jogar este jogo rapidamente. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

9. Eu considero que o jogo é fácil de jogar. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

10. As regras do jogo são claras e compreensíveis. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

11. As fontes (tamanho e estilo) utilizadas no jogo são legíveis. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

12. As cores utilizadas no jogo são compreensíveis. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

Experiência do Jogador

Por favor, marque uma opção de acordo com o quanto você concorda ou discorda de cada afirmação abaixo.

(Onde 1 - Discordo totalmente, 2 - Discordo, 3 - Nem discordo, nem concordo, 4 Concordo, 5 - Concordo totalmente).

13. A organização do conteúdo me ajudou a estar confiante de que eu iria aprender com este jogo. *

Marcar apenas uma oval.

Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente
	1	2	3	4	5	

14. Este jogo é adequadamente desafiador para mim. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

15. O jogo oferece novos desafios (oferece novos obstáculos, situações ou variações) com um ritmo adequado. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

16. O jogo não se torna monótono nas suas tarefas (repetitivo ou com tarefas chatas). *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

17. Completar as tarefas do jogo me deu um sentimento de realização. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

18. É devido ao meu esforço pessoal que eu consigo avançar no jogo. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

19. Me sinto satisfeito com as coisas que aprendi no jogo. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

20. Eu recomendaria este jogo para meus colegas. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

21. Eu pude interagir com outras pessoas durante o jogo. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

22. Eu me senti bem interagindo com outras pessoas durante o jogo. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

23. Eu me diverti com o jogo. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

24. Aconteceu alguma situação durante o jogo (elementos do jogo, competição, etc.) que me fez sorrir *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

25. Houve algo interessante no início do jogo que capturou minha atenção. *

Marcar apenas uma oval.

1 2 3 4 5

26. Eu estava tão envolvido no jogo que eu perdi a noção do tempo. *

Marcar apenas uma oval.

1 2 3 4 5

Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

27. Eu esqueci sobre o ambiente ao meu redor enquanto jogava este jogo. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

28. O conteúdo do jogo é relevante para os meus interesses. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

29. É claro para mim como o conteúdo do jogo está relacionado com a disciplina. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

30. O jogo é um método de ensino adequado para esta disciplina. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

31. Eu prefiro aprender com este jogo do que de outra forma (outro método de ensino). *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

32. O jogo contribuiu para a minha aprendizagem na disciplina. *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

33. O jogo foi eficiente para minha aprendizagem, em comparação com outras atividades da disciplina.
*

Marcar apenas uma oval.

	1	2	3	4	5	

34. O jogo contribuiu para relembrar conceitos de Segurança da Informação *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

35. O jogo contribuiu para fortalecer a importância de boas práticas de Segurança da Informação em instituições *

Discordo totalmente						Concordo totalmente

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente						Concordo totalmente

36. O jogo contribuiu para conscientizar sobre os danos causados pela quebra da Segurança da Informação *

Marcar apenas uma oval.

	1	2	3	4	5	
Discordo totalmente	◯	◯	◯	◯	◯	Concordo totalmente

37. O que você mais gostou no jogo? *

38. O que poderia ser melhorado no jogo? *

39. O jogo auxiliou a relembrar algum conceito de Segurança da Informação? *

40. Aprendi algo novo no jogo? *

41. Gostaria de fazer mais algum comentário? *