UNIVERSIDADE FEEVALE

LUCAS HENRIQUE DE MORAES

CTF:
UM ESTUDO TEÓRICO E PRÁTICO PARA CONSTRUÇÃO DE CONHECIMENTO NA ÁREA DE SEGURANÇA DA INFORMAÇÃO

Novo Hamburgo

2020

LUCAS HENRIQUE DE MORAES

CTF:
UM ESTUDO TEÓRICO E PRÁTICO PARA CONSTRUÇÃO DE CONHECIMENTO NA ÁREA DE SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do grau de Bacharel em Sistemas de Informação pela Universidade Feevale.

Orientadora: Prof.ª Dr.ª Adriana Neves dos Reis

Novo Hamburgo

2020

LUCAS HENRIQUE DE MORAES

Trabalho de conclusão do Curso de Sistema de Informação, com título **CTF: UM ESTUDO TEÓRICO E PRÁTICO PARA CONSTRUÇÃO DE CONHECIMENTO NA ÁREA DE SEGURANÇA DA INFORMAÇÃO**, submetido ao corpo docente da Universidade Feevale, como requisito necessário para obtenção do Grau de Bacharel em Sistemas de Informação.

Aprovado por:

_____

Prof.ª Dr.ª Adriana Neves dos Reis
Professora orientadora

_____

Prof. Dr. Ricardo Ferreira de Oliveira
Banca examinadora

_____

Prof. Dr. Vandersilvio da Silva
Banca examinadora

Novo Hamburgo, novembro de 2020.

AGRADECIMENTOS

Gostaria de agradecer a todos os que, de alguma maneira, contribuíram para a realização desse trabalho de conclusão, em especial:

À Ester, por estar comigo durante essa etapa da minha vida me incentivando e apoiando, foi uma jornada difícil com todos os problemas que esse ano trouxe, mas nunca me deixou desistir e sempre me ajudando a encarar cada obstáculo que surgiu, foram vários dias que sacrificamos para que eu pudesse realizar a pesquisa, além das conversas sobre aproveitar a jornada e o caminho para a conquista de um sonho.

À professora Drª. Adriana, que aceitou esse desafio de pegar esse projeto na metade do caminho e com excelência conduzi-lo para conclusão me orientando para a construção deste trabalho, muito obrigado por toda paciência e ensinamentos.

Ao Dr. Daniel que me orientou na primeira etapa desse trabalho de conclusão, foram muitas risadas de nervoso durante essa etapa, muitas conversas sobre futuro dessa pesquisa, ensinamentos sobre vida e cibersegurança, muito obrigado Dala.

Quero agradecer aos meus pais que sempre sonharam comigo, me apoiaram e acreditaram que era possível. A todos que, de alguma forma, contribuíram para a conclusão deste trabalho. Muito obrigado!

É necessário fazer outras perguntas, ir atrás das indagações que produzem o novo saber, observar com outros olhares através da história pessoal e coletiva, evitando a empáfia aqueles e daquelas que supõem já estar de posse do conhecimento e da certeza.

Mário Sergio Cortella

RESUMO

A popularização da internet e o advento dos *smartphones* no século XXI têm exigido uma infraestrutura cibernética com maior amplitude para atender às demandas, considerando que os criminosos e *hackers* vêm se aproveitando das falhas de segurança nos sistemas para obter vantagens. Nesse contexto, nasce a necessidade de profissionais na área de segurança da informação que tenham capacidade para lidar com os desafios que surgem diariamente, em que somente o conhecimento teórico das técnicas não se mostra suficiente. Além disso, tornam-se indispensáveis os treinamentos práticos. Diante desse cenário, apresentam-se as competições do tipo *Capture The Flag* (CTF) como ferramentas que podem auxiliar na construção de conhecimento e habilidades, tendo em vista que tais competições nesse âmbito instigam os participantes a buscarem novas técnicas, contribuindo com o crescimento da área. Para mapear o impacto que esses torneios têm na expansão dos conhecimentos dos participantes, construiu-se um referencial teórico que abordou: estilos de competição; aspectos pedagógicos; e técnicas e relatos de experiência na condução de CTF. Na segunda parte da pesquisa, as competições foram analisadas do ponto de vista teórico e do ponto de vista prático a partir da percepção de participantes de CTFs. Como principais resultados, o trabalho evidencia que CTF pode contribuir na construção de conhecimento dos seus participantes, em função do estímulo ao uso de novas ferramentas e técnicas, bem como pela motivação a continuar os estudos em cibersegurança.

Palavras-chave: CTF. Cibersegurança. Habilidades. Desenvolvimento. Competição.

ABSTRACT

The popularization of the internet and the arrival of smartphones in the 21st century are demanding a cyber infrastructure with greater breadth to meet the demands, considering that cyber criminals and hackers have been exploiting security breaches to take advantage. In this context, there is a need for information security professionals who have capacity to deal with the challenges that have increasing daily, where just theorical knowledge it's not enought. Besides that, practical knowledge becomes essencial. That said, CTF (Capture The Flag) type competitions have appeared, as a tool that can assist in building knowledge and skills, bearing in mind that the competitions encourage the participants to seek new techniques, contributing this way to the growth of the entire area. To map the impact that these competitions have on the expansion of the participants' knowledge, a theoretical framework was built with competition modalities, pedagogical aspects, techniques and experience reports in conducting the competition. In the second part of the research, the competitions are analyzed from a theoretical and practical point of view, from the CTF participants' perception. As main results, the work shows that CTF can contribute towards building knowledge of its participants, by used new tools and techniques, and also motivation them to keep studing cybersecurity.

Keywords: CTF. Cyber security. Skills. Development. Competition.

LISTA DE FIGURAS

Figura 1 – Classificação da pesquisa 14
Figura 2 – Fluxograma da pesquisa 15

LISTA DE GRÁFICOS

Gráfico 1 – Percepção dos participantes sobre palestras e cursos antes da CTF.....49
Gráfico 2 – Avaliação dos participantes sobre disposição dos desafios.....50
Gráfico 3 – Percepção dos participantes sobre divisão dos desafios por categoria.....50
Gráfico 4 – Habilidades pessoais necessárias para CTF em equipe.....52
Gráfico 5 – Competição forçou a buscar novas ferramentas ou software.....52

LISTA DE QUADROS

Quadro 1 – Quadro dos trabalhos analisados 38
Quadro 2 – Primeiras cinco questões 44
Quadro 3 – Questões sobre as palestras e/ cursos 44
Quadro 4 – Questões sobre os desafios 45
Quadro 5 – Papel dos organizadores 45
Quadro 6 – Mapeamento do humor dos participantes 46
Quadro 7 – Competições em equipe 46

LISTA DE ABREVIAÇÕES

CBL	Challenge Based Learning
CERT	Computer Emergency Report Team
CTF	Capture The Flag
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO 12
2 METODOLOGIA 14
3 REFERENCIAL TEÓRICO 16
3.1 PRINCIPAIS CONCEITOS E DEFINIÇÕES 16
3.2 ESTILOS DE CTF 19
3.2.1 *Jeopardy* 19
3.2.2 Ataque e Defesa 20
3.2.3 *King of the Hill* 22
3.2.3 *Linear* 22
3.3 ASPECTOS PEDAGÓGICOS 23
3.3.1 Trabalho em equipe 23
3.3.2 Conhecimento colaborativo 25
3.3.3 Aprendizagem baseada em desafios 26
3.4 TÉCNICAS 27
3.4.1 Criptografia 27
3.4.2 *Pentest* 28
3.4.3 Esteganografia 29
3.4.4 Engenharia reversa 29
3.4.5 Análise forense 29
3.5 TRABALHOS RELACIONADOS 30
4 ANÁLISE DE COMPETIÇÕES 33
4.1 ANÁLISE TEÓRICA 33
4.1.1 Trabalhos selecionados 33
4.1.1.1 Capture the flag: método de aprendizado para a disciplina de forense computacional em uma universidade pública 33
4.1.1.2 Using CTF tournament for reinforcing learned: skills in cybersecurity course 35
4.1.1.3 Web security training [at] uniGe: an experience 36
4.1.1.4 Maximize the learning success in it: security 37
4.1.2 Planilha 38
4.1.2.1 Planejamento 39
4.1.2.2 Execução 40

4.1.2.3 Avaliação 41
4.2 Análise prática 41
4.2.1 Participação no SBSEG 2020 42
4.2.2 Questionário 43
4.2.3 Análise dos resultados 47
4.2.3.1 Preparação para competição 47
4.2.3.2 Palestras e cursos 48
4.2.3.3 Desafios 49
4.2.3.4 Organizadores 51
4.2.3.5 Contribuição da CTF 51
5 CONSIDERAÇÕES FINAIS 54
REFERÊNCIAS 56
ANEXO A - QUESTIONÁRIO PARA COLETA DA PERCEPÇÃO DE PARTICIPANTES DE CTF 61
ANEXO B - RESPOSTAS DO QUESTIONÁRIO DE PERCEPÇÃO DE PARTICIPANTES DE CTF 73

1 INTRODUÇÃO

Diante da popularização da internet e do advento dos smartphones no século XXI, tem-se exigido uma infraestrutura cibernética mais ampla para atender às demandas. Desse modo, os criminosos e *hackers* assim têm se aproveitado de falhas de segurança nos sistemas para adquirir vantagens. Portanto, torna-se imprescindível desenvolver a segurança dos sistemas, como uma maneira de contribuir para o crescimento da área de cibersegurança: é a realização de competições de *hacker* ético, chamadas *Capture The Flag* (CTF) (RAMAN et al., 2014).

CTF é uma modalidade de competição de cibersegurança em que equipes disputam, em tempo real, por prêmios, demonstrando todas as habilidades e técnicas que possuem da área (DAVIS et al., 2014). As competições são usadas na comunidade de segurança de computadores para fins de educação e avaliação, sendo considerada uma excelente abordagem para aprender conceitos técnicos em ambientes de aprendizado (CHUNG; COHEN, 2014).

Em competições de CTF, os participantes devem dispor de um conhecimento de técnicas da área de segurança, como, por exemplo, criptografia, redes, programação, *cloud computing*, *pentest*, engenharia reversa, exploração de binários, análise forense e estenografia com o objetivo de capturar a bandeira, que pode ser um trecho de código ou até mesmo uma mensagem (GONZALEZ et al., 2019).

Essas competições ocorrem em eventos regionais, nacionais e internacionais. Quando direcionadas para profissionais. Geralmente são oferecidas recompensas na forma de significativas quantias em dinheiro. Outros eventos são voltados para estudantes da área, sendo ocasional o incentivo monetário para os competidores que se destacam durante o evento. Quando direcionadas para estudantes, é comum algumas empresas observarem os participantes durante a competição em busca da contratação de novos colaboradores (MENA, 2018).

Para Trickel et al. (2017) e Nakaya et al. (2016), existe uma demanda de profissionais na área de cibersegurança que universidade/faculdades e cursos em geral não conseguem suprir, pois:

- entende-se que o estudo teórico não seja o suficiente para preparar os profissionais para enfrentar o atual cenário;
- considera-se a prática como aspecto crucial para entender a complexidade da segurança cibernética.

Para aumentar o interesse dos alunos pela área de cibersegurança, os mesmos autores descrevem a necessidade de realizarem-se treinamentos práticos em ambientes que simulem situações reais.

Segundo Eagle e Clark (2004) e Mansurov (2016), CTF contribui de forma significativa com o desenvolvimento de habilidades dos alunos e profissionais da área de cibersegurança, as quais os currículos padrões não têm oferecido. Além disso, as competições nesse âmbito instigam os participantes a buscarem novas técnicas de conhecimento na área, uma vez que elas oferecem uma liberdade que inspira os participantes a aprimorarem suas técnicas.

Além do desenvolvimento de habilidades em cibersegurança, Mansurov (2016) apresenta o desenvolvimento dos participantes na questão pedagógica, contribuindo na construção do conhecimento dos participantes nos aspectos de trabalho em equipe, aprendizado ativo e colaborativo e aprendizagem baseada em desafios.

Assim, esta pesquisa tem como objetivo desenvolver um estudo teórico e prático de como CTF poderá contribuir para o desenvolvimento dos participantes e para área de cibersegurança. Para tanto, apresentam-se as modalidades de competições, suas formas de execução e potenciais ganhos na formação dos participantes na área de cibersegurança, analisar as principais técnicas utilizadas durantes os eventos e como cada etapa poderá contribuir para a construção de conhecimento.

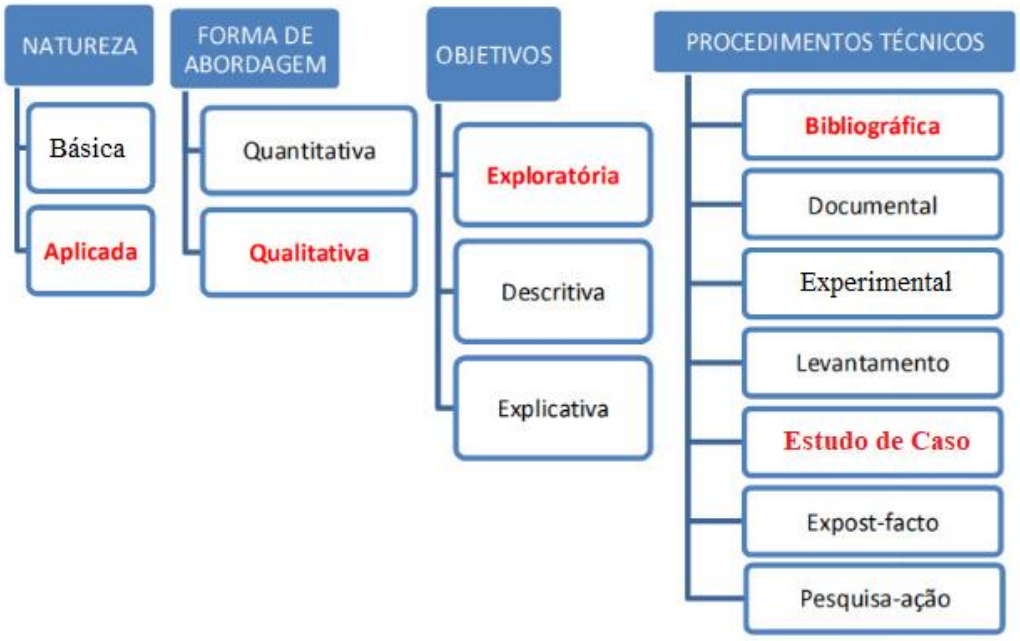
Este estudo divide-se em cinco capítulos. No primeiro capítulo, tem-se a introdução. O capítulo 2 está a metodologia utilizada para elaboração da pesquisa. No capítulo 3 contém o referencial teórico, que, por sua vez, está dividido em três seções. Na primeira seção, abordam-se os principais conceitos e definições; na segunda seção, apresenta-se o desenvolvimento dos participantes em relação aos aspectos pedagógicos. Na terceira seção, apresentam-se as principais técnicas utilizadas durante os CTFs.

O capítulo 4 está divido em duas seções, nele é realizada uma análise prática e outra teórica de competições de CTF. Na primeira seção foram selecionados trabalhos recentes para serem analisados, enquanto na segunda, foi elaborado um questionário para os participantes de Capture The Flag, encima do resultado do mesmo realizamos uma análise. No quinto e último capítulo falamos sobre os resultados, limitações e trabalhos futuros.

2 METODOLOGIA

O estudo desenvolvido neste trabalho possui características de pesquisa aplicada, pois tem o objetivo de elucidar a estruturação de CTFs e sua contribuição na geração de conhecimento, assim como no aprimoramento das habilidades de alunos e profissionais de cibersegurança. Assim, buscou-se organizar o conhecimento sobre o funcionamento e o desenvolvimento dessas competições. A seguir, Figura 1 descreve as classificações em relação aos objetivos e procedimentos metodológicos que são utilizados ao longo deste trabalho.

Figura 1 – Classificação da pesquisa



Fonte: adaptado de Bez (2011).

Em relação aos objetivos, esta pesquisa define-se como exploratória, dentro de uma abordagem qualitativa. Em sua fase inicial, investigaram-se as características da CTF e suas contribuições, delimitando assim o problema de pesquisa. Em relação aos seus objetivos previamente definidos:

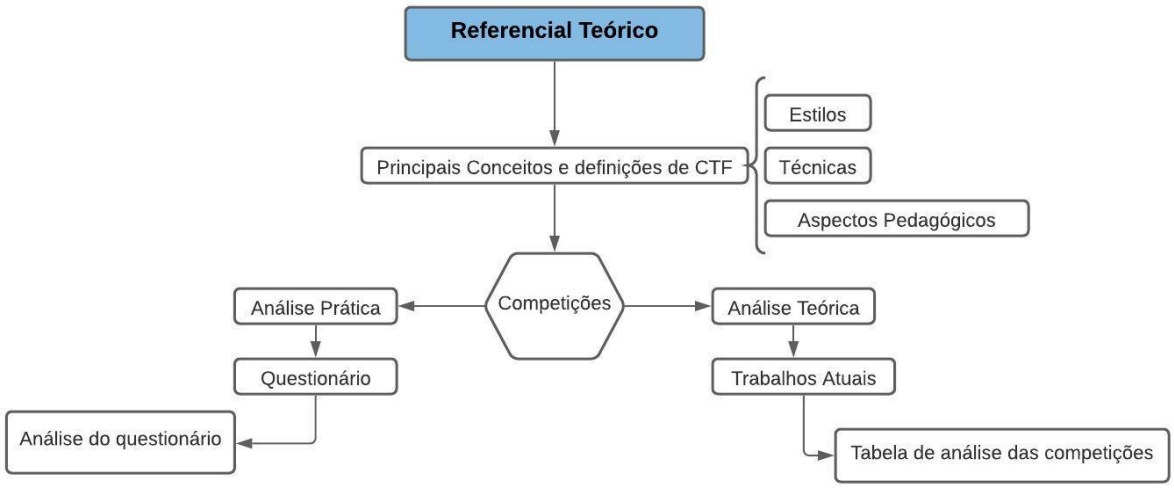
> [...] tem como finalidade proporcionar mais informações sobre o assunto que vamos investigar, possibilitando sua definição e seu delineamento, isto é, facilitar a delimitação do tema da pesquisa; orientar a fixação dos objetivos e a formulação das hipóteses ou descobrir um novo tipo de enfoque para o assunto (PRODANOV; FREITAS, 2013 p. 52).

Em relação ao levantamento bibliográfico, foram utilizadas: revisão da literatura e análise de estudos de casos em que CTF foi empregada tanto no âmbito acadêmico quanto em competições para profissionais. A revisão da literatura iniciou-se na busca de definições referentes à CTF e seus estilos de competições.

Ainda, realizou-se uma busca de que aspectos pedagógicos e em quais técnicas de segurança da informação a CTF poderia contribuir de maneira significativa. Por fim, selecionaram-se e analisaram-se pesquisas recentes que relatassem a condução de CTF, de modo a permitir a análise de sua aplicação, destacando os pontos fortes e os que requerem melhorias.

Do ponto de vista prático, realizou-se a experiência de participação em uma competição de CTF para fins de imersão em ambiente real. De modo complementar, coletou-se a percepção de participantes de CTFs, por meio de um questionário. A seguir, a Figura 2 apresenta o fluxograma da pesquisa.

Figura 2 – Fluxograma da pesquisa



Fonte: elaborada pelo autor.

Desse modo, acredita-se dar atenção aos aspectos teóricos e práticos para o uso CTF em diferentes propósitos.

3 REFERENCIAL TEÓRICO

A popularização da internet e dos *smartphones* no século XXI têm exigido cada vez mais de infraestruturas cibernéticas para atender às demandas. Dentro desse ambiente, os criminosos e *hackers* têm se aproveitando de falhas de segurança nos sistemas para adquirir vantagens, exigindo assim que os profissionais de cibersegurança estejam diariamente se atualizando sobre novas ferramentas e técnicas para defender seus servidores e informações. Portanto, existe a necessidade de desenvolver a segurança dos sistemas, logo, para contribuir para o crescimento da área de cibersegurança, são realizadas competições de *hacker* ético, chamadas *Capture The Flag* (CTF) (RAMAN et al., 2014). Nesse sentido, este capítulo apresenta o referencial teórico base para a condução deste trabalho, discutindo os principais conceitos e definições de CTF, bem como suas características e aspectos que contribuem para construção do conhecimento na área de Segurança da Informação. Além disso, o capítulo apresenta algumas técnicas envolvidas nas competições de *Capture The Flag*.

3.1 PRINCIPAIS CONCEITOS E DEFINIÇÕES

Capture The Flag é uma modalidade de competição de cibersegurança na qual equipes disputam em tempo real por prêmios, demonstrando todas suas habilidades e técnicas da área (DAVIS et al., 2014). As competições são usadas na comunidade de segurança de computadores para fins de educação e avaliação, sendo considerada uma excelente abordagem para aprender conceitos técnicos em ambiente de aprendizado (CHUNG; COHEN, 2014).

Os competidores são expostos a desafios controlados pelos organizadores, que disponibilizam um servidor configurado que possui “bandeiras” (sinalizadores) que servem como pontuação. Essas bandeiras podem ser trechos de texto ou falhas de segurança em determinados serviços, sendo necessário identificá-los nos servidores dos adversários e protegê-los no servidor de sua equipe (WI; CHOI; CHA, 2018).

As competições de CTFs são direcionadas aos profissionais da área de cibersegurança, nas quais formam-se equipes destinadas às competições realizadas em eventos regionais, nacionais e internacionais, em que geralmente são ofertadas como recompensas grandes quantias em dinheiro. Outros eventos são voltados para estudantes da área, e ocasionalmente há apoio monetário para os competidores que se destacam durante o evento. Além disso, algumas empresas observam os participantes durante as competição com o intuito de selecionar colaboradores (MENA, 2018).

Mansurov (2016) descreve CTF como uma das competições mais populares da área de cibersegurança, em que profissionais/estudantes podem demonstrar suas habilidades de cibersegurança, solucionando problemas da vida real em um ambiente controlado, sem a preocupação de sofrerem prejuízos para suas organizações ou de enfrentarem problemas judiciais.

Os participantes utilizam técnicas de invasão, que, na constituição de vários países, são condenadas em seus códigos penais. Com isso, o CTF destaca-se como uma ferramenta pedagógica que pode contribuir de forma significativa na educação dos participantes. Em relação a isso, Chung e Gohen (2014, p. 1, tradução nossa) afirmam que:

> As competições da CTF visam reunir membros da comunidade de segurança de todos os níveis de habilidade para compartilhar informações e ver quem dentre eles pode resolver os maiores desafios. A comunidade tem uma enorme admiração pelos CTF como uma plataforma de aprendizado [...].

Fonseca (2019) discorre sobre o pensamento de que CTF pode contribuir para estudantes e profissionais que tenham interesses na área de segurança da informação e não saibam por onde iniciar. Na contemporaneidade, existe uma vasta diversidade de sites e competições *online*, que permitem aos competidores adquirirem experiências e lhes proporcionam a criação de *mindset*, demonstrando que CTF vai além de um simples jogo e que se trata de uma ferramenta importante para desenvolvimento de habilidades. porque permite aos profissionais de segurança cibernética aprender e praticar a aplicação de ferramentas e técnicas de maneira prática. (CRASS, 2019, tradução nossa).

Entende-se que o CTF pode desenvolver as habilidades dos competidores na área de segurança, mas habilidades que eles já possuem e também as que podem ser adquiridas através de estudos, práticas em ambientes controlados (treinamentos) ou profissionalmente, descrevendo uma ampla gama de técnicas como criptografia, redes, programação, *cloud computing*, *pentest*, engenharia reversa, exploração de binários, análise forense e estenografia (GONZALES et al., 2019).

Raman et al. (2014) descrevem que não há necessidade de os participantes terem o conhecimento de cibersegurança devido ao fato de existirem competições que educam e treinam os alunos interessados na área, oferecendo várias sessões e testes de laboratório baseados em CTF para prepará-los, permitindo que possam realizar a prática adequadamente, tornando a experiência agradável devido à grande possibilidade de êxito das tarefas.

Boopathi et al. (2015) fazem uma reflexão de como o CTF pode contribuir na construção de conhecimento na área de cibersegurança, ao analisarem os dados de uma pesquisa do

Computer Emergency Report Team (CERT) sobre o grande número de domínios comprometidos devido à ação de *hackers* maliciosos e à capacidade dos desenvolvedores e profissionais na atualidade referente às práticas de segurança da informação. Constatou-se uma possível lacuna nas questões práticas dos currículos das graduações e de pós-graduações do local da pesquisa, sugerindo a necessidade de um treinamento prático das técnicas ensinadas durante a graduação, sendo o CTF utilizada para tal prática.

Cowan et al. (2003) descrevem que, na medida em que os alunos avançam em seu caminho de aprendizagem utilizando CTF, há um envolvimento maior deles enquanto o interesse e a retenção aumentam. A utilização do "velho modo" (utilizando-se de livros, palestras e aulas didáticas) de se ensinar segurança da informação leva os alunos a familiarizarem-se com os assuntos da área, entretanto, forma profissionais sem conhecimentos práticos, ou seja, que não conseguem aplicar suas habilidades adquiridas durante a formação. Por vezes, profissionais de cibersegurança precisam tomar decisões corretas rapidamente e terem a capacidade de trabalhar em equipe – e, principalmente, de utilizarem técnicas e habilidades de forma inovadora.

Capalbo, Reed e Arpaia (2011) fazem algumas corroborações quanto ao assunto ao relatarem que os estudantes de graduação geralmente não têm experiência em cibersegurança e que o meio acadêmico não contribui com práticas adequadas, levando os graduados a procurarem atividades extracurriculares ou estágios. Algumas graduações procuram profissionais para realizar palestras, contudo, muitas vezes isso não é o suficiente para sanar a necessidade prática da cibersegurança, indicando o CTF como ferramenta potencial de ensinar os alunos a resolverem problemas de cibersegurança com base na experiência em um ambiente de ritmo acelerado.

Eagle e Clark (2004) descrevem que o CTF pode contribuir com o desenvolvimento e a aprendizagem dos alunos, sendo que eles são conduzidos nessas competições a problemas e ambientes do mundo real, assim como a desafios em que profissionais da área de segurança da informação têm no seu cotidiano. Aos alunos que demonstram interesse em participar dessas competições, são ofertadas aulas introdutórias que visam cobrir os conhecimentos necessários para solucionar os problemas que irão enfrentar nas competições futuras.

A CTF também pode ser utilizada como uma atividade extracurricular para contribuir na construção do conhecimento dos alunos da graduação, produzindo um ambiente no qual alunos e professores podem realizar práticas dos conhecimentos previamente apresentados nas aulas, não seguindo uma grade curricular, mas realizando práticas e trocas de conhecimento entre os alunos, professores e interessados na área de cibersegurança (MANSUROV, 2016).

Segundo Cowan et al. (2013), os avanços da segurança cibernética são movidos pelo "choque" de mentes (os pesquisadores criam novas defesas e os criminosos adaptam seus ataques em resposta). Esse jogo antagônico está no centro de cada desafio de segurança cibernética, mas, infelizmente, está ausente na educação em segurança cibernética. Para Crass (2019, p. 61), "*Capture the Flag* permite aprender de uma maneira divertida e desafiadora, sendo uma prática, que nos impede de ser criminoso".

A presente pesquisa apresenta características das competições em três seções. Na primeira seção – 3.2 Estilos de CTF –, demonstram-se as modalidades que a CTF pode ser executada, descrevendo suas características e seus desafios; na seção 3.3 – Aspectos pedagógicos – abordam-se as principais contribuições da CTF como ferramenta de estudo, ressaltando sua contribuição na educação dos alunos; e na seção 3.4 – Técnicas –, realiza-se um prévio levantamento das técnicas de cibersegurança que os participantes poderão encarar em forma de desafios nas competições.

3.2 ESTILOS DE CTF

As competições podem ocorrer em três modalidades, sendo que cada uma delas pode ser realizada de duas formas: individualmente ou em equipe. Segundo Seltzer (2019) e o site CTF Zone , os estilos são *Jeopardy*, Ataque e Defesa, *King of the Hill* e Linear.

3.2.1 *Jeopardy*

O estilo *Jeopardy* é baseado em *quizzes* (questionários) referentes à área de segurança da informação, com a finalidade de testar os conhecimentos dos competidores/estudantes em determinados assuntos da cibersegurança, quais sejam: a criptografia, redes, programação, *cloud computing*, *pentest*, engenharia reversa, exploração de binários, análise forense e estenografia, em que os competidores dessa modalidade podem trabalhar sozinhos ou com uma equipe (RAJ et al., 2016).

Seltzer (2019) apresenta o estilo subdividido por assunto e nível de dificuldade, em que, a cada questão solucionada, a equipe/indivíduo pontua, sendo que, em cada nível, há uma pontuação diferente e cada acerto leva para questões mais elaboradas. Ao final de um tempo determinado, a equipe que tiver a maior pontuação vence.

> Os jogos CTF no estilo de Jeopardy colocam os organizadores executando um conjunto de desafios que cada indivíduo / equipe precisa resolver por pontos. Em geral, quanto mais complicada a tarefa, mais pontos são conquistados. Os desafios são

> geralmente independentes um do outro e, idealmente, idempotentes entre os jogadores conectados, o que leva à confiabilidade e estabilidade para grandes competições. A pontuação também é simples e agradável: some os pontos para os desafios resolvidos e use o tempo das soluções para desempatar (CAPTURE, 2019).

Os desafios *Jeopardy* são divididos em categorias, logo, cada desafio está disposto a um assunto da área da segurança de informação, como por exemplo:

- Desafio de esteganografia: o participante precisa encontrar uma determinada *flag* (bandeira) oculta em uma imagem.
- Desafio de criptografia: o participante recebe um arquivo que deverá criptografar e transmitir em segurança em uma rede, ou recebe um arquivo que deverá descriptografar e descobrir a *flag*, que normalmente é uma mensagem.
- Desafio web: o participante deve explorar um determinado site para localizar a *flag*.

O estilo *Jeopardy* é utilizado normalmente para treinamento em plataformas *online* e como um método para elencar as eliminatórias nas competições. Um exemplo disso é DefCon (sigla, em inglês, que significa Convenção de Defesa), que atualmente é a maior competição do mundo de CTF, em que milhares de pessoas participam da rodada de qualificação, disputando uma das vinte vagas disponíveis para a segunda fase, que consiste em uma disputa na modalidade Ataque e Defesa.

3.2.2 Ataque e Defesa

O estilo Ataque e Defesa exige maior conhecimento e experiência dos participantes, sendo necessário utilizar ferramentas de *hackers*, exportar e corrigir vulnerabilidades. Estabelece assim uma barreira para alunos iniciantes na área, pois os problemas simulados nesse tipo de competição equiparam-se à vida real, haja vista que exige um alto nível de conhecimento (MANSUROV, 2016).

As competições consistem na formulação de duas equipes. Cada uma das equipes possui um ambiente computacional preparado, salientando que esse tipo de competição pode ocorrer de forma *online* e/ou local. Nessa modalidade, uma equipe tenta realizar ataques ao sistema da outra e defender o seu próprio sistema. Nesse gênero específico de competição, as equipes de defesa podem preparar seus sistemas como desejarem, corrigindo todas as vulnerabilidades que forem perceptíveis e deixando somente os serviços necessários abertos no *firewall*. Em

contrapartida, os atacantes podem utilizar técnicas de intrusão para obter privilégios e informações (SELTZER, 2019).

A pontuação de uma equipe é equivalente à soma do valor das bandeiras que ela capturou, menos a soma das bandeiras que foram capturadas dessa mesma equipe, multiplicada por uma pontuação de disponibilidade determinada pela frequência com que a equipe branca conseguiu testar os serviços dessa equipe.

> Esse evento exige que os participantes protejam e operem um conjunto de serviços vulneráveis fornecidos pelos organizadores do evento, além de instâncias de ataque dos mesmos serviços operados por outras equipes. As equipes ganham pontos por capturar informações secretas (*flags*) dos hosts de outras equipes, explorando vulnerabilidades em seus serviços. Os pontos também são premiados por uma equipe por garantir que seus serviços permaneçam seguros e funcionem corretamente. O último é determinado pela consulta automatizada de serviços pela infraestrutura do jogo para verificar a disponibilidade e a funcionalidade do serviço (DAVIS et al., 2014, p. 1, tradução nossa).

Trickel (2017) relata que as competições do estilo Ataque e Defesa oferecem um ambiente para desenvolvimento de conhecimento instigante e interativo para os participantes, pois podem utilizar tanto habilidades ofensivas quanto defensivas durante um curto período de tempo. Além do conhecimento adquirido durante essas determinadas competições, esse estilo estimula a procura por um aprimoramento de seus conhecimentos no que diz respeito à cibersegurança como preparação para o dia da competição, sendo que esse estilo normalmente é realizado em grupo. Cria-se um ambiente colaborativo em que os membros dividem novos conhecimentos e técnicas.

De acordo com Trickel (2017), as competições desse modo contribuem para a comunidade de segurança da informação da seguinte maneira:

- permitindo que os alunos pratiquem toda a teoria e conceitos que adquiriram durante o curso de graduação, leitura de livros e artigos.
- estimula os participantes a aprimorarem o seu aprendizado, para que consigam lidar com os aspectos em tempo real durante o evento que ocorre em um período limitado de tempo;
- leva os participantes a um envolvimento mais profundo através da competição, fazendo com que dediquem mais tempo de aprendizado acadêmico;
- faz com que os competidores aprendam a operar em um ambiente dinâmico, tendo que tomar decisões rápidas para defender o seu ambiente de ataque, desenvolvendo

> contramedidas por meio da utilização de conhecimentos teóricos adquiridos previamente.

Davis et al. (2014) descrevem uma cena comum durante a competição nesse estilo, que são alunos buscando na web soluções que estão enfrentando em tempo real e discutindo sobre o assunto com os colegas de equipe, bem como desenvolvendo ferramentas, ou seja, estão utilizando conhecimentos que não tinham adquirido antes das competições, mas que foram alcançados durante a atividade.

3.2.3 *King of the Hill*

King of the Hill é um estilo de CTF que consiste em uma rede de computadores que contém um servidor com um serviço vulnerável, em que os competidores devem manter o controle do maior número de serviços pelo maior tempo possível para pontuar. Esse estilo é caracterizado como um *pentest*. (SELTER, 2019).

Bock, Hughey e Levin (2019) descrevem *King of the Hill* como uma competição na qual várias equipes lutam pelo controle de uma grande rede vulnerável, proporcionando para os alunos uma experiência em testes de penetração (*pentest*).

> O objetivo dos participantes do *King of the Hill* é detectar vulnerabilidades dos sistemas, explorá-las e, o mais importante de tudo, manter o controle sobre os sistemas pelo maior tempo possível. O truque está na regeneração dos conjuntos de vulnerabilidades nos sistemas. Os participantes enfrentam um dilema - tentar atacar os sistemas vizinhos ou prosseguir com a detecção de vulnerabilidades nos sistemas que já estão sob controle. Como na vida real, o maior número de pontos é dado para manter o controle sobre o *Active Directory* [...] (PHDAYS, 2012, n.p., tradução nossa).

O Facebook (2017) descreve esse estilo como sendo um sistema que deve ser comprometido pelas equipes para capturar pontos. A equipe que primeiro comprometer o servidor recebe vários pontos. Além disso, quem tiver o controle também é recompensado com base no tempo, e a cada ciclo completado, a equipe recebe uma determinada quantidade de pontos.

3.2.3 *Linear*

O estilo linear é descrito pelo site CTF Zone como uma competição utilizada para recrutamento, onde segue um uma história que vai sendo destravada a cada desafio resolvido,

até encontrar a *flag* no final e concluir a competição. Uma vez que os competidores só podem completar um desafio por vez e sugerido que ele seja realizado individualmente. Caso o competidor enfrente uma dificuldade em solucionar o desafio ficara preso naquele nível.

3.3 ASPECTOS PEDAGÓGICOS

Entende-se que CTF pode contribuir nas questões da aquisição de conhecimento. Assim, Mansurov (2016) aborda que existem três contribuições pedagógicas que a prática pode desenvolver nos participantes: o trabalho em equipe, o aprendizado ativo e colaborativo, e a aprendizagem baseada em desafios. Tais contribuições, por sua vez, serão elucidadas nas seções a seguir.

3.3.1 Trabalho em equipe

As tarefas apresentadas durante as competições de CTF têm um alto nível de complexidade, sendo crucial para os participantes o trabalho em equipe para alcançarem o sucesso nas tarefas. Dentro desse ambiente, os participantes aprimoram suas habilidades de comunicação, uma vez que a interação bem-sucedida entre os membros pode culminar na execução de um desafio (MANSUROV, 2016).

Silva (2010) faz uma reflexão que diferencia o trabalho em grupo do trabalho em equipe. Para exemplificar a diferença, ele relata uma atividade laborativa de três pessoas em fila realizando a tarefa na qual o primeiro cava o buraco, o segundo joga uma semente e o terceiro tapa o buraco. Quando estão trabalhando em grupo, cada um sabe sua função e a executa com maestria. Certo dia, um membro do grupo, que está encarregado da função de largar a semente, não comparece ao trabalho. Mesmo com um membro a menos, os trabalhadores continuam a realizar suas tarefas como faziam normalmente, abrindo buracos e tapando sem semente. Assim, evidencia-se que, mesmo em um trabalho realizado em grupo, cada indivíduo preocupa-se tão somente com a sua função, sem observar todo o contexto e o que isso representa.

Silva (2010) descreve o mesmo cenário anteriormente citado, entretanto, os colaboradores estão trabalhando em equipe. Os dois membros iriam dividir a função do colega que não havia comparecido ao labor, uma vez que entendem a importância de cada etapa do processo para alcançar o sucesso da tarefa a eles proposta. Os objetivos e metas são coletivas e não individuais, ou seja, compreendem que, para alcançar o sucesso, todas as etapas precisam

ser executadas, mesmo que falte um membro da equipe. Nesse sentido, Katzenbach e Smith (1993, n.p.) salientam:

> O desempenho de um grupo de trabalho é resultado da soma dos desempenhos individuais. O desempenho de uma equipe, além de incluir os resultados individuais, inclui o chamado resultado do trabalho coletivo. O resultado do trabalho coletivo é aquilo que dois ou mais membros precisam fazer em conjunto. E isso reflete a real contribuição dos membros de uma equipe.

Nesta senda, a importância do trabalho em equipe advém da necessidade histórica do homem em somar forças para alcançar os objetivos que, sozinhos, seriam difíceis ou impossíveis de realizarem-se , ainda mais com o desenvolvimento e a complexidade do trabalho moderno, em que existe uma dependência e/ou complementaridade de conhecimento para alcançar objetivos complexos com mais eficiência (PIANCASTELLI; FARIA; SILVEIRA, 2000).

Trabalhar em equipe, de acordo com Vergara (2002), pode ter quatro vantagens principais, sendo uma das principais a agilidade na captação das informações e o uso delas de forma mais rápida e eficiente na tomada de decisão dos problemas cotidianos, não sendo necessário envolver a alta cúpula da organização, refletindo em um processo mais demasiado.

As ideias desenvolvidas em equipe normalmente são enriquecidas, possuem maior qualidade e são mais elaboradas devido ao fato de que são discutidas e debatidas entre os membros, trazendo diversos pontos de vista do estudo do caso. E ainda, possuem uma capacidade produtiva mais lenta do que indivíduos que trabalham sozinhos, fazendo com que as vantagens sejam incomensuráveis, como já fora descrito (VERGARA, 2002).

No trabalho em equipe, os indivíduos têm a tendência de arriscar mais, pois a responsabilidade do fracasso/sucesso é compartilhada entre os membros da equipe, trazendo um conforto para cada indivíduo, no sentido de transformar ideias em ações, oportunizando a criatividade na construção de novas técnicas e métodos de realizar uma tarefa (VERGARA, 2002).

O compartilhamento das responsabilidades em equipe traz um comprometimento na realização das tarefas com foco no resultado disposto para cada equipe, sendo que o poder compartilhado entre os indivíduos desenvolve mais cumplicidade e motivação para o sucesso (VERGARA, 2002).

3.3.2 Conhecimento colaborativo

O conhecimento ativo e colaborativo dá-se em um ambiente de trabalho com as equipes de CTF, as quais precisam formar suas equipes com membros que detenham diferentes habilidades e consigam desempenhar tarefas em conjunto, utilizando-se de forma eficiente, compartilhando as informações e gerando discussões sobre o que está sendo feito durante a competição, desenvolvendo assim o conhecimento de cada um dos membros (MANSUROV, 2016 apud CONKLIN, 2006). Nesse contexto, Torres e Irala (2014, p. 1) mencionam que:

> [...] se reconhece nessas metodologias o potencial de promover uma aprendizagem mais ativa por meio do estímulo: ao pensamento crítico; ao desenvolvimento de capacidades de interação, negociação de informações e resolução de problemas; ao desenvolvimento da capacidade de autorregulação do processo de ensino-aprendizagem. Essas formas de ensinar e aprender, segundo seus defensores, tornam os alunos mais responsáveis por sua aprendizagem, levando-os a assimilar conceitos e a construir conhecimentos de uma maneira mais autônoma.

Castro e Menezes (2011) descrevem o aprendizado como uma atividade de adaptação ao meio ambiente físico e social, que está presente no cotidiano das pessoas, em que se precisa resolver problemas em conjunto tanto nas escolas quantos nas empresas. O aprendizado colaborativo ocorre durante as discussões sobre como se pode resolver determinado problema, procurando explicar as vantagens e desvantagens de uma determinada escolha, analisando, contestando, fazendo uma análise crítica e reconsiderando fatos passados para chegar a conclusões mais assertivas.

As equipes de CTFs criam um paradigma em relação ao conhecimento que somente pode ser adquirido dentro de uma sala de aula, em que o professor transfere seu conhecimento para o aluno, fazendo que ele seja um agente ativo na construção do seu conhecimento, além de contribuir com o crescimento do conhecimento de seus colegas de equipe. Trickel et al. (2017) complementam que muitos dos participantes de competições realizam postagens em *blogs*, falando sobre o que aprenderam e detalhando suas estratégias e abordagens utilizadas para conquistar pontos durante a competição.

Fagundes et al. (2006) descrevem o conhecimento como algo inacabado, que pode sempre ser construído através de debates e dúvidas referentes à “certeza” existente sobre o assunto, criando novos conceitos e conhecimentos.

> Os benefícios decorrentes das práticas pedagógicas baseadas na colaboração são inúmeros, dos quais podemos citar: a preparação para a vida em sociedade, o desenvolvimento do espírito crítico e a competência para resolver problemas de grande porte a partir das contribuições individuais. O exercício da colaboração requer sistemas apropriados para o registro das produções individuais, para a socialização

> das produções, para a coordenação das ações, para a recuperação inteligente das informações produzidas e a respectiva reflexão sobre o produto final (CASTRO; MENEZES, 2011, p. 137).

Dentro dessas circunstâncias, o trabalho colaborativo visa desenvolver a equipe em uma unidade para resolução de problemas dentro da área de segurança de informação, somando o conhecimento de todos os participantes para alcançar um único objetivo, em que cada membro é responsável por adquirir novos conhecimentos e por compartilhá-los com os seus colegas. Assim, as competições de CTF criam uma situação adequada para que os alunos busquem aprimoramento assíduo de seus conhecimentos e técnicas.

3.3.3 Aprendizagem baseada em desafios

A aprendizagem baseada em desafios é ideal para os participantes de competições de CTF, sendo que os alunos se reúnem para discutir um determinado problema apresentado à equipe, sendo necessário encontrar uma maneira de resolvê-lo rapidamente. Estimulam-se, assim, habilidades de resolução e o processo cognitivo, sendo que há uma variedade infinita de soluções para os problemas propostos, levando os estudantes a buscarem mais conhecimento referente à cibersegurança (MANSUROV, 2016).

O site *Challenge Based Learning* define esse método da seguinte maneira:

> A Aprendizagem Baseada em Desafios (CBL) fornece uma estrutura eficiente e eficaz para a aprendizagem, ao mesmo tempo em que resolve desafios do mundo real. A estrutura fomenta a colaboração para identificar grandes ideias, fazer perguntas bem pensadas e identificar, investigar e resolver desafios. A CBL ajuda os alunos a adquirir um conhecimento profundo da área e desenvolver as habilidades necessárias para prosperar em um mundo em constante mudança (CBL, 2020).

O CBL torna o aprendizado relevante, fornecendo problemas da vida real, desenvolvendo novas ideias e ferramentas para solucionar os desafios propostos, apresentando uma estrutura em que o professor apresenta o assunto e permite que o aluno mergulhe nele (JOHNSON; BROWN, 2020).

Johnson e Brown (2020) descrevem quatro pontos com os quais o CBL contribui no crescimento do conhecimento:

- A CBL desenvolve as habilidades necessárias do século XXI: relatam que 90% descrevem que os alunos tiveram melhoras significativas nas áreas-chaves de liderança, criatividade, alfabetização de mídia, solução de problemas e pensamento

crítico. Outros 70% relataram melhorias na flexibilidade e adaptabilidade dos alunos.

- Cerca de 75% dos estudantes de todas faixas etárias sentiram que aprenderam mais do que o necessário, resultado alcançado devido ao fato d os alunos estarem envolvidos na aquisição do conhecimento.
- Os professores relataram que o CBL é eficaz para envolver os alunos na sua educação e ajudá-los a dominar a matéria. 90% dos professores relataram que esse método é ótimo para otimizar o tempo limitado que possuem com os alunos, independentemente da faixa etária.
- O CBL pode ser aplicável em todas as esferas educacionais, mas se destaca em um ambiente tecnológico, podendo ser aplicado em aulas disponíveis 24 horas por dia, sete dias por semana. O estudo demonstrou que tanto alunos quanto professores possuem o conhecimento necessário para lidar com ambiente computacional e com CBL, de maneira eficaz.

3.4 TÉCNICAS

Nessa seção, descrevem-se algumas técnicas que os competidores utilizam durante as competições, anteriormente citadas por alguns autores.

3.4.1 Criptografia

A técnica de criptografia é utilizada para transformar as informações claras e objetivas em informações inelegíveis, sendo transmitidas em um canal no qual somente o emissor e o receptor tenham conhecimento da mensagem, dificultando que alguém não autorizado possa fazer sua leitura.

Durante as competições, os serviços utilizam transmissão de informações em uma rede privada ou pública, sendo necessário realizar o processo de criptografar os dados, ou seja, fazer um algoritmo que embaralha os dados a partir de uma determinada chave ou par de chaves, dependendo do sistema utilizado para realizar o procedimento.

> A palavra criptografia provém dos radicais gregos kriptos (oculto) e grapho (escrita) e é o nome dado à ciência ou arte de codificar mensagens usando uma fórmula, que também será utilizada depois para decodificar a mesma mensagem. Na criptografia moderna, esta fórmula é chamada de algoritmo. Usada há milênios pela humanidade, a criptografia se tornou essencial para garantir a privacidade das comunicações no mundo atual, principalmente em redes de computadores públicas como a internet, por

> onde circulam dados pessoais, comerciais, bancários e outros (OLIVEIRA, 2012, p. 1).

Há dois métodos de criptografia, definidos pela utilização de chaves, sendo uma como chave única e outra com de chave privada e pública. De acordo com a Cartilha do CERT.br (CARTILHA, 2012), o primeiro tipo é definido como uma criptografia que utiliza a mesma chave para codificar e decodificar. O outro método faz uso de duas chaves diferentes, uma para a codificação e a outra para a decodificação.

3.4.2 *Pentest*

Pentest é um processo que simula um ataque real ao determinado servidor a fim de avaliar os riscos associados aos pontos vulneráveis do servidor e avaliar o impacto gerado no ataque bem-sucedido (MORENO, 2019). Segundo Pava e Guardia (2015, p. 172):

> [...] consiste em simular um ataque no próprio ambiente onde se apontam vulnerabilidades. Basicamente, trata-se de um teste contra a segurança feito por uma equipe autorizada como uma forma de antecipar e prever como seria um ataque em potencial. Os experimentos realizados mostraram, por fim, as causas das falhas e as maneiras das mesmas serem identificadas com o auxílio de ferramentas disponíveis, contribuindo dessa forma para o aumento da segurança da infraestrutura[...].

Nakamura e Geus (2003) relatam que o atacante realiza uma análise do fluxo dos dados, observando quem fornece a informação, o caminho percorrido e o destino. Após essa análise, pode-se realizar o ataque em duas modalidades: oportunista ou direcionado.

O ataque oportunista é evento de menor frequência e ocorre quando uma falha é identificada e o indivíduo mal-intencionado realiza uma investida, não focando em uma rede específica, mas em um grupo de pessoas que utilizam a tecnologia com vulnerabilidade. Já o ataque direcionado acontece quando o indivíduo se dedica ao ataque a um determinado alvo. Independente de conhecer uma vulnerabilidade atual dele, realiza diversos testes à procura de acesso para obter algum tipo de vantagem.

Para a CTF, o *pentest* é de grande valia, pois conseguir identificar as vulnerabilidades é o um dos principais objetivos do jogo. Por esse motivo, é umas das técnicas que os participantes precisam aperfeiçoar, não somente para realizar os ataques nos servidores adversários, procurando um acesso ao sistema, mas também para defender seus servidores, pois não basta conhecer a vulnerabilidade dos outros, é preciso reconhecer as suas.

3.4.3 Esteganografia

Esteganografia pode ser usada para roubar dados, escondê-los em um arquivo e enviá-los por e-mail, de forma com que o meio não perceba o que está se passando, podendo também ser utilizado como comunicação secreta entre dois indivíduos (COELHO; BENTO, 2003).

> Esteganografia deriva do grego, onde estegano significa esconder, mascarar e grafia significa escrita. Logo, esteganografia é a arte da escrita encoberta. Durante toda a história, as pessoas buscam inúmeras formas de esconder informações dentro de outros meios, para, de alguma forma, obter mais privacidade para seus meios de comunicação. As abordagens mais comuns de inserção de mensagens em imagens incluem técnicas de: inserção no bit menos significativo, filtragem e mascaramento e algoritmos de transformações (JULIO, BRAZIL, ALBUQUERQUE, 2007, p. 1).

Alguns desafios de CTF *Jeopardy* disponibilizam uma *flag* dentro de uma imagem, sendo necessário decifrar e apresentar a frase, senha ou sequência de números para solucionar o problema apresentado. Às vezes, são utilizados em conjunto criptografia e esteganografia para dificultar o acesso aos dados originais.

3.4.4 Engenharia reversa

Engenharia reversa visa ao entendimento do funcionamento de um determinado programa (*software*) ou dispositivo (*hardware*) a fim de compreender ou até mesmo copiar, sendo possível identificar as vulnerabilidades do sistema para explorá-las ou utilizá-las a seu favor durante competições de CTF, sendo possível alterar suas funções para obter acesso a redes e a outros sistemas, criando neles funções que o projetista originalmente não havia criado (ULBRICH; DELLA VALE, 2004).

De acordo com o site *Hacker Security*, "engenharia reversa é a arte de fazer tudo ao contrário, muito usada por hackers especialistas em softwares para descobrir falhas, vulnerabilidades ou até mesmo desenvolver crackers" (HACKER SECURITY, 2017, n.p.).

3.4.5 Análise forense

A análise forense computacional é ciência de recuperação, aquisição e apresentação de dados que foram processados/armazenados digitalmente. Possui um conjunto de técnicas e ferramentas que são utilizadas na obtenção de evidências das alterações realizadas em mídias digitais para futuras análises, em casos de crimes relacionados a computadores a análise dos

"objetos" que podem servir como prova em julgamentos (YEAGER, 2006). Ainda, tem como um de seus objetivos identificar evidências para uma investigação em documentos e imagens, como, por exemplo, verificar se um computador sofreu uma invasão externa ou o uso não autorizado de alguma máquina local. Ela pode apontar se algum documento foi alterado e qual seu intuito. Exemplo disso é se a alteração em alguma imagem foi para melhoria da sua qualidade ou se há algum dado escondido (CARRIER, 2002).

Nas CTFs, são disponibilizados arquivos com alterações em que os competidores devem realizar uma análise para descobrir a bandeira. Podem ser disponibilizados *logs*, imagens e arquivos de áudios, e pode haver a necessidade de utilizar-se mais de uma técnica para resolver o problema.

No *HackaFlag* de Natal de 2016, foi apresentado o seguinte desafio: "Recentemente, ocorreu uma violação no sistema que controla a entrada de pessoas, dentre vários usuários precisamos saber qual o usuário conseguiu entrar. Temos o Log completo do servidor, analise o log e nos informe qual o usuário possivelmente acessou o sistema", sendo necessário que o participante soubesse realizar uma análise forense do *log* para identificar a *flag* (o desafio era estilo *Jeopardy*), que era o nome do usuário (LONGATO, 2016).

Os desafios de CTF na categoria de análise forense basicamente estão focados em analisar evidências forenses digitais, como *logs* (conforme o exemplo previamente citado), capturas de tráfego etc., extraindo as informações através dos métodos forenses para capturar a bandeira e avançar na competição/pontuar.

3.5 TRABALHOS RELACIONADOS

Na área de cibersegurança, tem crescido a necessidade de desenvolver novos profissionais para atender à demanda do mercado, em que há uma lacuna nos currículos atuais na questão da prática de segurança da informação. Dentro desse contexto, foram realizados vários trabalhos descrevendo a CTF como uma ferramenta para contribuir no desenvolvimento dos alunos e profissionais.

A pesquisa de Burns et. al. (2017) elaborou um levantamento das principais técnicas utilizadas nas competições de CTF para desenvolver um treinamento para iniciantes na área de segurança da informação com o intuito de realizar a construção de conhecimento através de desafios. Os alunos eram introduzidos aos temas na sala de aula da universidade. Inicialmente, eram submetidos somente a "temas de casa". Com o passar do tempo, iniciaram-se os desafios, utilizando a gamificação para a motivação dos envolvidos, assim como o estilo *Jeopardy* e uma

variação do estilo Ataque e Defesa. Os alunos eram expostos a desafios, subdivididos por categoria e nível de dificuldade. Eles avaliaram positivamente a experiência, considerando que foi um exercício para introduzi-los em competições de CTF.

Walter et. al. (2019) descrevem a CTF como uma ferramenta de educação na área de cibersegurança, sendo utilizada como competição, treinamento, avaliação e recrutamento, ou seja, um exercício significativo. Contudo, seu trabalho está focado em medir o fator humano de um *hacker* durante uma invasão, enquanto que as competições de CTF estão focadas em analisar o fator técnico dos participantes, desenvolvendo, assim, através do seu estudo, a compreensão do comportamento cognitivo do time vermelho (time de ataque) para que isso possa realizar uma emulação de um cenário de defesa, compreendendo a mente do atacante, gerando contribuições para o desenvolvimento das defensas dos sistemas atuais.

O trabalho de Tarakkamäki (2020) diferencia da presente pesquisa por não se aprofundar nas competições de CTF, não explorando o que cada estilo pode acrescentar para a construção de conhecimento. A pesquisa discorre sobre a classificação das ameaças cibernéticas, utilizando o modelo triângulo para avaliar o grau de risco, e utiliza somente da pesquisa de construção de conhecimento baseada em desafios, ignorando outros aspectos pedagógicos que em que CTF pode contribuir.

O trabalho desenvolvido por Bedoya (2019) discorre sobre o CTF e seus estilos, categoria de pontuação e algumas técnicas utilizadas durante as competições, além de relatar algumas das principais competições de CTF. O autor faz uma análise sobre várias plataformas para organizar uma competição em que ele realiza uma avaliação de qual poderia atender ao estudo de forma eficaz.

Goodman e Radu (2020) realizaram uma pesquisa com os participantes de CTFs e *hackathons* para analisarem os ambientes e suas contribuições na construção de conhecimento, utilizando a Aprendizagem Baseada em Desafio como fator motivador para os participantes. Os autores acreditam que ambos os eventos podem ser utilizados pelas universidades para inserirem os alunos em cibersegurança. Sugerem ainda que, no atual cenáculo crítico gerado pelo novo coronavírus (covid-19), essas ferramentas teriam um valor com maior relevância para os participantes, sendo que os eventos podem ser realizados de forma *online*.

Os autores realizaram comparações entre os eventos em relação às percepções dos participantes no que se refere ao ambiente, como, por exemplo, se haviam conhecido novas pessoas, se foram bem recebidos no evento ou se haviam adquirido aprendizado quanto a novas técnicas etc. Os autores finalizam descrevendo a estrutura dos eventos em três etapas distintas:

aprender novas técnicas, aplicá-las na solução de um problema ou na construção de um projeto, e, por fim, compartilhar experiências e conhecimento com a comunidade de cibersegurança.

4 ANÁLISE DE COMPETIÇÕES

Este capítulo está dividido em duas seções. Na primeira, realiza-se uma análise teórica sobre como estão sendo aplicadas as competições de CTF atualmente a partir dos relatos da literatura. Na segunda seção, faz-se uma análise prática de CTF, a partir do relato de experiência do acadêmico ao participar de uma competição de CTF e de um levantamento realizado por meio de questionário para coletar a percepção de participantes de diversas competições do tipo CTF.

4.1 ANÁLISE TEÓRICA

Para elucidar a aplicação de CTF como ferramenta, esta seção analisou pesquisas elaboradas no período de 2019 a 2020, trazendo, assim, dados atuais referentes a como as competições estão sendo aplicadas, bem como analisando os principais aspectos descritos no referencial teórico.

4.1.1 Trabalhos selecionados

4.1.1.1 Capture the flag: método de aprendizado para a disciplina de forense computacional em uma universidade pública

Mendes et. al (2020), durante as aulas da disciplina denominada Forense Computacional, perceberam a necessidade de analisar se os alunos estavam assimilando os conteúdos de forma correta. Dessa forma, sugeriram aplicar desafios na forma de uma competição CTF.

Em relação à preparação para a competição desenvolvida por Mendes et. al (2020), segue-se o pensamento de Eagle e Clark (2004), que, antes de apresentar os desafios, é preciso preparar os desafiantes através de aulas de cibersegurança. Porém, conforme Capalbo, Reed e Arpaia (2011), somente as aulas e palestras não são suficientes para que os alunos estejam preparados para encarar os desafios reais que estariam dispostos durante uma competição, mesmo a competição proposta sendo realizada dentro de um período mais extenso que as competições profissionais.

Os autores escolheram o estilo J*eopardy* para realizar sua análise referente os conhecimentos de cada aluno na área de análise forense. Devido ao curto prazo disponível para a realização de mais desafios, foram dispostos somente seis, tornando os dados insuficientes

para uma análise mais aprofundada dos conhecimentos dos participantes, sendo que foi disposto somente um desafio para cada técnica, não utilizando o sistema de nível de dificuldade, no qual cada desafio resolvido leva ao novo nível, em que o aluno deverá ter/desenvolver seu conhecimento referente ao assunto disposto (SELTZER, 2019).

Dentro da CTF, a rivalidade faz com que os participantes se motivem a resolver os desafios devido à "premiação", que não necessariamente precisa ser um objeto ou valor monetário, mas pode ser somente o reconhecimento que o aluno teve por sua pontuação, sendo um fator que o autor não levou em consideração durante o experimento. No decorrer da competição, utilizou-se somente o aspecto de conhecimento baseado em desafio; o restante dos aspectos pedagógicos não fora utilizado por ser uma análise individual dos conhecimentos dos participantes.

> Uma forma de estimular os alunos a aprimorarem seus conhecimentos em determinada área é o desenvolvimento de competições de conhecimento em áreas específicas. Ao ingressarem numa disputa os participantes se veem engajados na missão de provar o seu valor e o seu conhecimento. Além disso, guiados pelo instinto competitivo, não medem esforços para buscar ainda mais conhecimento e transpor qualquer barreira que surja em seu caminho (FASSBINDER, PAULA, ARAÚJO, 2012, p. 2).

Cowan et al. (2003) descrevem a CTF como um método eficaz para o ensino de cibersegurança, indicando que, quanto mais avançam no aprendizado com o esse tipo de abordagem, maior é o envolvimento, pois não se utilizam somente de palestras e aulas. Na pesquisa, o autor utilizou somente do "velho modo" de se ensinar, no qual o conhecimento está centrado na figura do professor. Os autores utilizaram os desafios como uma avaliação na disciplina denominada Forense Computacional.

Referente aos desafios da pesquisa, não seguiram a estrutura indicada por Seltzer (2019), que descreve os desafios estruturados por níveis e categoria. Havia um intervalo de um dia entre cada desafio, não gerando um espírito de rivalidade.

Trickel (2017) descreve que o curto período de tempo gera um ambiente para desenvolvimento de conhecimento instigante e interativo, porém, desconsiderou essa ideia, pois disponibilizou os desafios durante sete dias.

A pesquisa apresentou a CTF como uma atividade avaliativa para os participantes, gerando uma obrigação dos alunos a participarem. Mesmo com a obrigatoriedade, os autores conseguiram um número máximo de nove participantes nos desafios, sendo esse número cerca de 47% dos alunos "convidados". CTF é uma ferramenta para alunos interessados participarem. Apresentarem de forma obrigatória, sem nenhum tipo de gamificação, transformou-se em

somente um exercício de aula, enquanto a ideia de CTF é tirar o aluno de dentro da sala e levá-lo para um ambiente competitivo e com desafios do mundo real.

4.1.1.2 Using CTF tournament for reinforcing learned: skills in cybersecurity course

Os autores Gonzalez, Llamas e Montño (2019) desenvolveram sua pesquisa baseada em experiências com outros eventos de CTF em que estavam envolvidos, procurando encontrar uma forma de envolver os participantes e alcançar a proposta que diversos autores têm descrito, referente a sua contribuição para o desenvolvimento das habilidades em cibersegurança.

> Processo de adaptação do plano de estudos O conteúdo do nosso curso está organizado em três partes: A primeira parte é uma introdução à cibersegurança, que aborda um caminho da cibersegurança como profissional. A segunda parte é sobre sistemas de gestão de segurança da informação (SGSI) e seu impacto nas organizações. A terceira parte é sobre tópicos avançados, como hacking ético e análise forense (GONZALEZ; LLAMAS; MONTÑO, 2019, p. 2, tradução nossa).

O engajamento dos alunos deu-se durante a construção dos conteúdos abordados ao longo do curso. Além da utilização de gamificação, os autores envolveram os alunos na construção do conhecimento que desejavam, trazendo uma característica das competições de CTF, conforme Fonseca (2019) descreveu em relação à possibilidade de os alunos encontrarem conteúdos e até competições *online*, fazendo com que se preparem para uma competição futura.

Os autores escolheram o estilo *Jeopardy, que* é baseado em *quizzes* (questionários), conforme apresentado por Raj et. al (2016). Os desafios foram subdivididos em categorias e em níveis de dificuldades, seguindo o pensamento de Eagle e Clark (2004). Os alunos foram introduzidos aos assuntos de cibersegurança durante as aulas e estavam sendo levados a realizar desafios do mundo real para praticar as técnicas. Durante a competição, acrescentaram um tópico que não haviam abordado durante o curso para que os competidores desenvolvessem, durante a competição, os aspectos de trabalho em equipe e construção de conhecimento através de desafios.

> Eles passam mais de 20 horas em sala de aula trabalhando nos desafios. Consideramos que o engajamento dos alunos em atividades de cibersegurança está crescendo em nossa universidade, acreditamos que isso se deva em parte à estratégia de gamificação introduzida no curso. Alguns alunos expressaram a intenção de seguir carreiras de segurança cibernética. Os resultados gerais do torneio mostraram que todas as equipes resolveram desafios básicos no Forense, reforçando as habilidades aprendidas em aula (GONZALEZ; LLAMAS; MONTÑO, 2019, p. 5, tradução nossa).

A pesquisa coletou dados sobre a experiência dos alunos durante essa competição, conseguindo demonstrar o quanto a CTF contribuiu na construção de conhecimento e também

envolveu os alunos no assunto durante o período da competição. Os participantes sugeriram que o torneio deveria ser oferecido anualmente, sendo o *feedback* dos alunos positivo sobre o ambiente e a forma de trabalhar os desafios.

4.1.1.3 Web security training [at] uniGe: an experience

A pesquisa desenvolvida por Valenza (2019) está focada em conscientizar os desenvolvedores sobre os problemas que um sistema pode conter por não se preocupar com a segurança. Essa preocupação é compartilhada pelo trabalho desenvolvido por Boopathi et al. (2015), que realizaram a análise do grande volume de *hosts* comprometidos na sua região. Ambos os trabalhos constataram que a CTF poderia ser utilizada como uma ferramenta para a construção de conhecimento e conscientização sobre cibersegurança.

Valenza (2019) faz uma descrição de sua experiência como instrutor do curso de desenvolvimento de aplicações web que fazia parte do currículo de Bacharel em Ciência da Computação na Universidade de Gênova. Após aprender a desenvolver, os alunos considerados no estudo são apresentados aos conceitos básicos de cibersegurança da web.

Na pesquisa, o autor escolheu aplicação de CTF como uma atividade extracurricular, para que somente os alunos que tivessem interesse em cibersegurança participassem, seguindo o pensamento de Fonseca (2019), que discorre sobre como as competições podem ser um ponto de partida para os alunos desenvolverem suas habilidades e seu *mindset* e serem introduzidos às ferramentas utilizadas nessa área.

> ZenHack-Ademy começou com um piloto em junho de 2017, em seguida, teve sua primeira edição oficial no outono de 2017 e uma segunda edição no outono de 2018. As gravações de cada reunião estão disponíveis publicamente no YouTube, e também implantamos uma plataforma de desafio on-line que está disponível apenas aos alunos da nossa universidade (VALENZA, 2019, p. 4, tradução nossa).

A iniciativa desse projeto deu-se pelo fato de a universidade ter ganhado recursos para o desenvolvimento de cibersegurança pela companhia Boeing, disponibilizando para os vencedores uma bolsa para continuar sua jornada no mundo da cibersegurança.

Na preparação para as competições, os alunos eram apresentados aos assuntos através de palestras, aulas e desafios. O autor utilizou então da competição *Zenhack* para os alunos prepararem-se para a competição Boeing Hack, que estava oferecendo a bolsa de estudos através da universidade. O autor utilizou o aspecto pedagógico de aprendizagem por desafio, além de compartilhamento de conhecimento que está presente em CTF.

Valenza (2019) preocupou-se em analisar e avaliar cada passo da sua organização para encontrar os pontos necessários para analisar a experiência dos alunos no desenvolvimento dos seus conhecimentos através do curso disponibilizado e o Zenhack.

O curso havia sido subdividido em três desafios para os alunos, referentes à necessidade de os desenvolvedores preocuparem-se com a segurança de suas aplicações web, sendo que o autor disponibilizou dois desafios antes das competições, e, somente após a competição, os alunos foram apresentados ao terceiro, para que pudessem utilizá-lo como métrica da competição, tentando quantificar quanto os alunos conseguiram desenvolver-se durante a competição.

O autor desenvolveu uma pesquisa para avaliar as atividades e o crescimento dos alunos:

> [..] Nós distribuímos está pesquisa no final da atividade, para que os alunos possam comparar suas melhorias por meio de seus treinamentos em vez de seu nível de habilidade percebido atual, que iria, por sua vez, depender de seu nível atual de consciência e conhecimento do campo da cibersegurança. O histograma mostra que, após o treinamento não formal, os entrevistados se auto avaliaram melhor, testemunhando um sucesso da iniciativa (VALENZA, 2019, p. 6, tradução nossa).

O autor desenvolveu a competição com maestria e alcançou o objetivo de utilizar CTF como ferramenta de ensino, conseguindo quantificar e classificar o crescimento dos alunos antes e depois da competição.

4.1.1.4 Maximize the learning success in it: security

Os autores Fruhmann e Gebeshuber (2019) propuseram um método no qual os alunos aumentassem o sucesso do seu aprendizado, combinando o ensino universitário tradicional com a inclusão de CTF como forma de treinamento, assim como a participação em torneios regionais de cibersegurança. Dessa forma, os alunos teriam o conhecimento teórico da área e o treinamento prático das técnicas durante os desafios propostos durante as aulas práticas, e ainda, a experiência de participar de um torneio para intensificar seus conhecimentos. A motivação para a participação dos alunos foi dada através de pontos extras, além da plataforma utilizada para demonstrar a pontuação dos alunos/equipes.

Conforme Crass (2019), CTF é uma ferramenta para a busca de conhecimento e aplicação das habilidades. Tal ferramenta permite aos alunos praticarem todas as técnicas aprendidas durante seus estudos, de forma segura, sem infringir a lei. Dentro desse contexto, os pesquisadores conseguiram introduzir os alunos à cibersegurança, exercitar os conhecimentos da sala de aula e ainda fazer com que eles dessem continuidade aos estudos, para futuras

competições. Dentro do ambiente disposto, os discentes foram expostos aos aspectos pedagógicos citados por Mansurov (2016) da seguinte forma:

- Os alunos foram apresentados a desafios do mundo real durante os exercícios de laboratório, sendo que parte dos exercícios foi substituída por desafios de CTF no estilo *Jeopardy*, uttilizando CTF para fortalecer a motivação dos alunos, devido aos aspectos de gamificação.
- Os alunos foram instigados a formarem equipes para participar de torneios regionais, e, por sugestão dos professores, deveriam organizar treinamentos fora da classe para ajudar uns aos outros, criando um ambiente onde poderiam discutir sobre os assuntos da área de cibersegurança, levando ao compartilhamento de conhecimento e ao desenvolvimento do pensamento crítico.
- Para participar das competições regionais, os alunos foram "obrigados" a formar uma equipe. Com isso, conseguiram compartilhar seus conhecimentos, desenvolver a comunicação entre seus companheiros, analisar e apresentar argumentos de como solucionar o problema e analisar as vantagens e desvantagens de se utilizar determinadas técnicas.

4.1.2 Planilha

Para analisar as competições, desenvolveu-se o Quadro 1, a seguir, que consolida as características das competições identificadas nos trabalhos analisados na seção 4.1.1. e apresenta os resultados.

Quadro 1 – Quadro dos trabalhos analisados

(continua)

		Gonzalez, Llamas e Montño (2019)	**Valenza (2019)**	**Mendes et. al (2020)**	**Fruhmann e Gebeshuber (2019)**
Planejamento	Público Alvo (P ou E)	Estudante	Estudante	Estudante	Estudante
	Âmbito (R ou N ou I)	Regional	Regional	Regional	Nacional
	Foco (C ou E)		Estudos	Estudos	Competição e estudos

(conclusão)

		Gonzalez, Llamas e Montño (2019)	Valenza (2019)	Mendes et. al (2020)	Fruhmann e Gebeshuber (2019)
Planejamento	Estilo	*Jeopardy*	*Jeopardy*	*Jeopardy*	*Jeopardy*
	Aspectos Pedagógicos	Compartilhamento de conhecimento Aprendizagem baseada em desafios Trabalho em Equipe	Compartilhamento de conhecimento Aprendizagem baseada em desafios Trabalho em Equipe		Compartilhamento de conhecimento Aprendizagem baseada em desafios Trabalho em Equipe
	Técnicas			Esteganografia Decriptação Análise Forense	
Execução	Duração	Não informado	Não informado	7 dias	Não informado
	Preparação	Aulas introdutórias	Palestra Aulas introdutórias	Aulas introdutórias	Aulas introdutórias Exercícios Grupo de estudos
	Níveis de Dificuldade	Fácil Médio Avançado	Fácil Médio Avançado	Médio	
	Equipe (S ou N)	S	N	N	S
Avaliação	Certificado (S ou N)	N	S	N	N
	Prêmio		Bolsa de estudo	N	N
	Experiência		Os alunos solicitaram que a competição fossem anualmente.	Pela baixa participação dos alunos, a experiência da competição não foi satisfatória	A maioria dos alunos desejaram continuar seus estudos na área de cibersegurança

Fonte: elaborado pelo autor.

O quadro está organizado em três seções. Na primeira seção, avalia-se o planejamento das competições; na segunda seção, avaliam-se as principais características da execução, e por fim, tem-se uma seção para destacar os prêmios e as experiências relatadas pelos participantes.

4.1.2.1 Planejamento

O planejamento da CTF foi dividido em sete características para se poder mapear se o planejamento em relação à sua proposta estava norteado, por isso, foram escolhidos os aspectos de público-alvo, âmbito, desafios, foco, estilo de competição, aspectos pedagógicos e técnicas.

O público-alvo foi dividido entre as modalidades de estudante ou profissional, e, dependendo do público-alvo, poder-se-ia delimitar qual pensamento a competição estava seguindo: se o de Chung e Cohen (2014), que as competições podem ser usadas para fins de educação e avaliação, afirmando que esse tipo de competição gera um ambiente de aprendizado e avaliação, pensamento que também é seguido por Fonseca (2019), que considera que CTF é um caminho para estudantes que estão iniciando seus estudos em cibersegurança; ou o pensamento de Gonzalez et al. (2019), que acredita que os participantes necessitam de conhecimentos aprofundados para participar das competições. Em outras palavras, as competições são somente para profissionais e pesquisadores.

Em relação de âmbito, buscou-se identificar a extensão das competições. De acordo com Mena (2018), as competições podem ser realizadas em eventos regionais, nacionais e internacionais, levando em consideração que podem ser tanto voltadas para estudantes quanto para prossifionais.

Para as competições, é necessário atendar qual estilo será utilizado. Na seção 3.2 – Estilos de CTF –, estão descritos os estilos e suas respetivas execuções. Com isso, pode-se definir os desafios que a competição irá disponibilizar, com enfoque no seu objetivo.

Baseado na descrição de Mansurov (2016), avaliaram-se os aspectos pedagógicos utilizados pelos autores para desenvolver suas competições, sendo estes, além do conhecimento específico da área de cibersegurança, uma contribuição significativa para os participantes e para a forma de se ensinar, utilizando dos meios descritos na seção 4.2 – Aspectos pedagógicos.

4.1.2.2 Execução

Para essa etapa, buscou-se compreender como os autores estipularam suas competições, levando em consideração o tempo de duração destas, como realizaram a preparação dos participantes, o nivelamento dos desafios e, por fim, se a competição foi executada individualmente ou em grupo.

Referente à sua duração, o intuito era validar o pensamento de Trickel (2017), de que, no decorrer da competição, os alunos praticam toda a teoria adquirida durante seus estudos em um período determinado, estimulando os participantes a aprimorar o seu aprendizado, para conseguir lidar com desafios em tempo real, levando a um envolvimento mais profundo na competição, fazendo que se dedique mais ao seu aprendizado.

No aspecto de preparação dos participantes, buscou-se esclarecer sobre a ideia de Eagle e Clark (2004), que, em sua pesquisa, demonstraram que eram ofertadas aulas introdutórias que

visavam cobrir os conhecimentos necessários para solucionar os problemas que seriam enfrentados nas competições. Devido às aulas preparatórias, houve a preocupação de analisar os níveis de dificuldades dos desafios propostos aos alunos, uma vez que não eram profissionais de cibersegurança e que havia somente o conhecimento teórico das técnicas, para que ocorresse o envolvimento deles durante a competição, conforme a ideia de Trickel (2017).

A competição, sendo em grupo ou individual, permite-nos analisar a questão de como o CTF irá contribuir no conhecimento dos participantes. As competições em grupo podem contribuir com os aspectos citados na seção 3.3 – Aspectos pedagógicos – quando executadas individualmente. No cenário individual, seguir-se-ia o pensamento de Eagle e Clark (2004) e Mansurov (2016), de que a competição faria com que o aluno se esforçasse e se envolvesse demais com a sua educação, buscando conhecimentos fora da sala de aula.

4.1.2.3 Avaliação

Na seção de avaliação, procurou-se encontrar os resultados e premiações que cada competição ofereceu para os participantes, considerando também a experiência dos participantes.

No primeiro ponto procurou-se compreender qual a premiação que cada competição estava oferecendo para os participantes, para compreender a motivação que cada indivíduo tinha durante a competição, sendo ela pontos para determinada cadeira da faculdade, bolsa de estudo, valores monetários ou para estudo. Avaliou-se também sobre a certificação de participação.

O ponto que foi influenciado pela participação do acadêmico na competição foi a experiência dos participantes dentro da competição, durante a sua participação notou que o ambiente era tão importante quanto os desafios, algumas pesquisas buscaram compreender esse ponto.

4.2 ANÁLISE PRÁTICA

Esta seção está dividida em três partes: na primeira, faz-se um relato referente à experiência do autor com CTF; na segunda, demonstra-se o questionário que foi elaborado para construir uma competição, levando em consideração a experiência dos participantes; por fim, a terceira seção menciona os resultados do questionário e discute como o CTF pode trazer resultados.

4.2.1 Participação no SBSEG 2020

O acadêmico participou da competição SBSEG 2020 para analisar o funcionamento de uma competição e como o ambiente poderia contribuir na sua formação, sendo que o acadêmico tinha conhecimento de cibersegurança somente da parte teórica, o qual foi adquirido na cadeira de Segurança da Informação de sua universidade e durante o desenvolvimento do presente trabalho.

Analisando a descrição do evento, o acadêmico acreditou ser uma competição voltada para o estudante devido aos níveis descritos no e-mail de inscrição e por apresentar uma palestra de abertura. Os níveis estavam descritos como “Noob, Script Kiddie, CTF Player, Mr. Robot and God”, entretanto, a palestra de abertura visava somente apresentar a competição e falar previamente sobre o CTF.

A competição era voltada para pessoas que tinham um nível razoável de conhecimento de cibersegurança. Dessa forma, o acadêmico procurou os organizadores para conversar sobre CTF. Em conversa com um dos organizadores, questionando sobre o que achava referente à CTF como ferramenta de ensino para alunos, este não acredita que possa desenvolver conhecimento nos participantes, que somente serviria como ferramenta de aperfeiçoamento dos conhecimentos estudos para a competição.

A competição utilizou o estilo *Jeopardy*, no qual cada desafio estava subdividido em categorias e possuía um nível de dificuldade diferente, entretanto, todos os desafios estavam liberados para os competidores, não sendo necessário destravar novos desafios conforme iam solucionando-os, ou seja, a competição deixava os participantes livres para escolherem a área em que se sentissem mais preparados para iniciar a sua jornada. O desafio de Linux era um dos desafios em que havia uma evolução de nível, onde, a cada *flag* encontrado, destravava-se um novo desafio com maior complexidade.

A estrutura do site no qual os desafios estavam disponíveis era muito clara e objetiva, auxiliando no foco e na competição, em conjunto com a utilização do Discord – um aplicativo de voz sobre IP proprietário e gratuito – para que os participantes pudessem conversar com os organizadores e demais participantes.

> Uma forma de estimular os alunos a aprimorarem seus conhecimentos em determinada área é o desenvolvimento de competições de conhecimento em áreas específicas. Ao ingressarem numa disputa, os participantes se veem engajados na missão de provar o seu valor e o seu conhecimento. Além disso, guiados pelo instinto competitivo, não medem esforços para buscar ainda mais conhecimento e transpor qualquer barreira que surja em seu caminho (FASSBINDER; PAULA; ARAÚJO, 2012, p. 2).

Durante a competição, ficava nítida a diferença que ela pode fazer em relação ao estímulo do participante no que se refere à busca por conhecimento para solucionar os problemas, além do pensamento e da necessidade de buscar mais conhecimento sobre o assunto, uma vez que CTF não tem sido utilizada somente pela área de cibersegurança para desenvolver competições. De acordo com o organizador, ele já participou de outras competições de CTF, com enfoque em outras áreas de TI. Ainda, dentro da própria competição, o acadêmico deve retomar diversos assuntos que já haviam sido apresentados durante a faculdade a fim de solucionar os problemas. Em outros desafios, houve a necessidade de buscar e aprender novos assuntos.

Para o acadêmico, a experiência de participar de uma competição sobre o assunto que havia sido apresentado somente teoricamente durante a sua vida acadêmica despertou a curiosidade de buscar mais sobre cibersegurança. Apesar de a competição ser voltada para um público profissional, o ambiente transformou a percepção sobre a CTF, visto que seu estudo desenvolvido até o momento vinha somente da literatura.

4.2.2 Questionário

Para avaliar a experiência dos participantes de CTF, elaborou-se um questionário, tratando sobre a experiência, os desafios e a avaliação dos aspectos das competições. Solicitou-se que os participantes avaliassem também características que consideravam importantes, relacionadas às competições em equipes e também sobre a evolução de seus conhecimentos durante as competições, permitindo que se confrontasse a teoria com o mundo real, ou seja, com a percepção dos participantes.

Cada pergunta foi elaborada, pensando em obter o máximo de detalhes de como cada participante buscou conhecimento e como isso contribuiu na construção do conhecimento, além de buscar a percepção dos desafios e como seus comportamentos iam se desenvolvendo durante a competição. O questionário disponibilizado aos participantes encontra-se no Apêndice A.

Para aplicar a CTF de forma eficaz, era necessário compreender como cada participante deslumbrava os desafios e o ambiente, e compreender como cada etapa influenciava, além de analisar o quanto o participante conseguia perceber que seu conhecimento estava sendo testado durante essas competições.

As primeiras quatro questões foram elaboradas para compreender o envolvimento dos participantes com CTF, além de compreender quais meios utilizaram para adquirir conhecimento de cibersegurança. A questão cinco foi elaborada para analisar se os meios

disponíveis na questão quatro eram suficientes para formar um profissional, para avaliar se estava correta a ideia de Trickel et al. (2017) e Nakaya et al. (2016) – de que os meios citados na questão quatro não eram suficientes para a formação de um profissional de cibersegurança. O Quadro 2 apresenta tais questões.

Quadro 2 – Primeiras cinco questões

Questões	Estilo de resposta
Qual competição de CTF você participou?	Aberta
Como você conheceu a CTF?	Múltipla escolha
Como você avalia seu conhecimento antes de ter participado da competição que está em análise?	Resposta única
Antes da competição, você havia utilizado quais meios, a seguir, para aprender sobre cibersegurança?	Múltipla escolha
Referente à cibersegurança, você acredita que aulas/cursos/palestras são suficientes para formar um profissional?	Resposta única

Fonte: elaborado pelo autor.

As questões de seis a nove foram elaboradas para analisar as palestras e cursos que estão sendo oferecidos durante as competições. Quantificando a necessidade e o valor que o indivíduo dá para esse tipo de conteúdo disponível antes das competições, Raman et al. (2014) relatam que essa prática permite que os participantes possam realizar a prática adequadamente, tornando a experiência agradável devido à grande possibilidade de êxito das tarefas. O Quadro 3 apresenta as referidas questões.

Quadro 3 – Questões sobre as palestras e/ cursos

Questões	Estilo de resposta
As palestras/cursos oferecidos antes das competições forneceram uma base inicial para solucionar alguns desafios de cibersegurança?	Resposta fechada
Considerando a importância das palestras e cursos introdutórios, quanto eles contribuem para a competição?	Escala likert
Os conteúdos dispostos durante as palestras/cursos introdutórios eram atuais e bem elaborados?	Escala likert
Em geral, quanto você acha necessário que ocorra palestras/cursos introdutórios nas competições de CTF?	Escala likert

Fonte: elaborado pelo autor.

Os participantes foram questionados sobre a estrutura das competições, para analisar se estavam seguindo a ideia de Seltzer (2019), de dividir os desafios em níveis e categorias, além

de questionar o papel dos organizadores durante a competição, principalmente referente a falhas e dúvidas dos participantes. O Quadro 4 apresenta essas questões.

Quadro 4 – Questões sobre os desafios

Questões	Estilo de resposta
Considerando os desafios que foram apresentados durante a competição, eles estavam classificados por tipo e níveis de dificuldade?	Dicotômica
Os desafios estavam divididos em categorias (criptografia, esteganografia, forense e etc.)?	Dicotômica
Durante a competição, cada desafio resolvido destravava um novo desafio da categoria?	Múltipla escolha
Cada desafio apresentava um nível diferente de complexidade?	Dicotômica
Nos desafios com maior complexidade, você teve necessidade de procurar mais conteúdo para resolvê-los?	Dicotômica
Na sua opinião, os desafios estavam de acordo com o nível de complexidade descrito pelos organizadores?	Múltipla escolha
Durante a competição, você tinha acesso ao placar?	Dicotômica
Referente à estrutura da competição, como você avaliaria a disposição dos desafios?	Dicotômica

Fonte: elaborado pelo autor.

O papel dos organizadores nesse tipo de competição foi avaliado devido ao acadêmico ter participado de uma competição em que relatou que a interação com os organizadores tornou o ambiente da competição mais agradável. O Quadro 5 apresenta tais questões.

Quadro 5 – Papel dos organizadores

Questões	**Estilo de resposta**
Ao ocorrer alguma dificuldade em entender os desafios, os organizadores e/ou instrutores estavam disponíveis para esclarecimento?	Múltipla escolha
Como você avalia os auxílios dos organizadores e/ou instrutores durante a competição?	Múltipla escolha
Dentro do ambiente de competição, você acredita que os organizadores e/ou instrutores possuem papel essencial para auxiliar os participantes?	Múltipla escolha

Fonte: elaborado pelo autor.

Como a presente pesquisa estava voltada para a percepção do participante durante a competição, foram elaboradas questões para mapear o humor do participante conforme a competição ia desenvolvendo-se. Esses dados podem ser utilizados no desenvolvido de competições que consigam envolver mais o participante e auxiliar em pontos que possam ajudar na compreensão de como os indivíduos sentem-se completando os desafios ou enfrentando suas falhas. O Quadro 6 apresenta as questões.

Quadro 6 – Mapeamento do humor dos participantes

Questões	Estilo de resposta
Conforme a competição ia se desenvolvendo, sua pontuação afetava sua motivação (assinale qual opção você considera mais adequada)?	Múltipla escolha
Os desafios estarem divididos por categorias tornou-os mais atrativos, pois dessa forma poderia escolher quais desafios mais se identificavam com você?	Múltipla escolha
Durante a resolução dos desafios, quais das opções, a seguir, correspondem a como você se sentiu?	Múltipla escolha

Fonte: elaborado pelo autor.

Por fim, mapearam-se indivíduos que participaram de competições de CTF que foram necessários à formação de uma equipe. Nesse ponto, pôde-se se analisar a percepção dos participantes sobre os aspectos pedagógicos. O Quadro 7 apresenta as questões.

Quadro 7 – Competições em equipe

(continua)

Questões	Estilo de resposta
Em relação às competições em equipe, você destacaria quais habilidades pessoais como necessárias para um membro da equipe?	Múltipla escolha
Levando em consideração que para participar de uma competição de CTF em equipe, todos os membros da equipe devem manter um diálogo do que está ocorrendo com seu servidor, você acredita que a habilidade de comunicação seja aperfeiçoada durante o exercício?	Múltipla escolha
Durante a preparação para as competições, sua equipe costuma realizar reuniões para discutir novas técnicas e/ou ferramentas que podem utilizar?	Dicotômica
Sua equipe costuma realizar seus treinos utilizando situações reais (situações do trabalho)?	Dicotômica
Considerando a experiência com sua equipe, marque as opções abaixo que você considera verdadeiras:	Múltipla escolha

(conclusão)

Questões	Estilo de resposta
Para solucionar alguns desafios de CTF não basta ter o conhecimento sobre as técnicas que são necessárias. Na grande maioria das vezes é necessário utilizar uma ferramenta para criptografar um arquivo ou até mesmo para acessar um servidor remoto. Durante a competição que participou, você teve que utilizar algum software sobre o qual não tinha conhecimento?	Dicotômica
A competição forçou você a buscar novos softwares ou kit de ferramentas para solucionar os desafios?	Dicotômica
Levando em consideração sua primeira experiência com CTF, você acredita que esse tipo de competição lhe ajudou na questão de conhecimento referente aos softwares de cibersegurança?	Dicotômica
Avaliando sua experiência na CTF, você tem interesse em participar de outras?	Dicotômica
Após sua participação na CTF, marque as opções abaixo que você considera verdadeiras:	Múltipla escolha

Fonte: elaborado pelo autor.

4.2.3 Análise dos resultados

Na presente seção, dar-se-á a análise dos dados obtidos referente à pesquisa feita com os participantes de algumas competições de CTF.

Através da coleta de dados, o presente estudo obteve uma amostra com 30 respondentes no período de 20 de outubro de 2020 a 02 de novembro de 2020.

4.2.3.1 Preparação para competição

Conforme o pensamento de Eagle e Clark (2004), a CTF pode contribuir com o desenvolvimento e aprendizagem dos alunos, sendo que esses são conduzidos nessas competições à problemas e ambientes do mundo real, à desafios que profissionais da área de segurança da informação tem no seu cotidiano.

Referente à preparação, é necessário atentar-se ao nível de conhecimento dos participantes que irão escolher como foco, levando em consideração que o questionário demonstrou que 17 pessoas (56,6%) consideram que não têm nenhum ou baixo conhecimento em cibersegurança, e apenas 23,4% dos participantes consideram que seu conhecimento era bom ou profissional.

A pesquisa demonstra que a CTF não tem sido divulgada ou comentada no meio acadêmico, apesar de ser uma ferramenta com grande potencial para a construção de conhecimentos. Apenas nove pessoas relataram ter conhecido a CTF através da faculdade.

Trazer o CTF para o meio acadêmico é uma sugestão que os autores anteriormente citados acreditam ter faltado nos currículos dos cursos de cibersegurança, de forma a complementar a formação de profissionais.

Para criar o ambiente que Mansurov (2016) descreve, será necessário trilhar um caminho de construção de conhecimento, diversificando entre teorias e práticas. Questionados sobre o nível de conhecimento de cibersegurança, constatou-se que somente 33,4% (13 pessoas) dos participantes tinham o conhecimento intermediário ou superior.

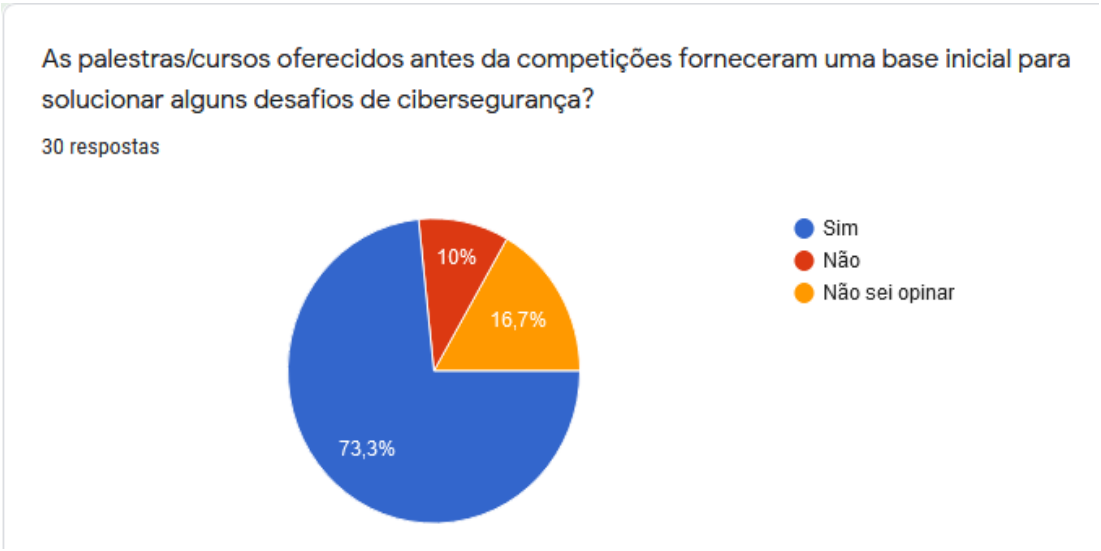
Questionados sobre por que meios buscaram conhecimento de cibersegurança, houve apenas quatro pessoas que não utilizaram meios tradicionais (cursos, aulas, palestras etc) para estudar ou praticar técnicas de cibersegurança. Os participantes tinham conhecimentos teóricos de cibersegurança e buscaram as competições para colocá-los em prática. Foram relatados somente três casos de práticas que não eram CTF.

4.2.3.2 Palestras e cursos

Foram elaboradas questões para verificar sobre as palestras e os cursos que algumas CTFs têm oferecido antes do início da competição, para que se possa analisar se a percepção dos participantes é uma prática válida.

Conforme os dados coletados, os participantes acreditam que a palestra/curso fornece uma base para os participantes resolverem os desafios de menor complexidade. Conforme mostra a Gráfico 1, vinte e duas pessoas (73,3%) acreditam nisso, sendo que, dentre os participantes, cinco deles nunca participaram de competições com esse tipo de recurso.

Gráfico 1 – Percepção dos participantes sobre palestras e cursos antes da CTF



Fonte: elaborado pelo autor.

As questões trouxeram um resultado contraditório, haja vista que, mesmo que maior parte do participantes falou que acreditavam que as palestras forneciam uma base para as competições e que 63,4% (somando todas as notas superiores seis) achavam que era necessário que ocorresse as palestras, a média referente à importância das palestras ficou abaixo do esperado, ou seja, de 5,57 numa escala de 0 a 10. Para validar os dados, tentou-se retirar da amostra os competidores que responderam à questão anterior com "não sei opinar", pois não participaram de competições com palestras ou cursos, entretanto, não se alcançou um resultado esperado, já que a média ficou em 5,77.

Apesar dos dados contraditórios nas questões anteriores, os participantes do questionário afirmaram que é importante que as palestras ou cursos ocorram antes das competições. Dezesseis pessoas deram nota superior a seis. Retirando os participantes que não participaram de competições com palestras/cursos, que deram nota zero na pesquisa, conseguiu-se uma média de aprovação de 7,11.

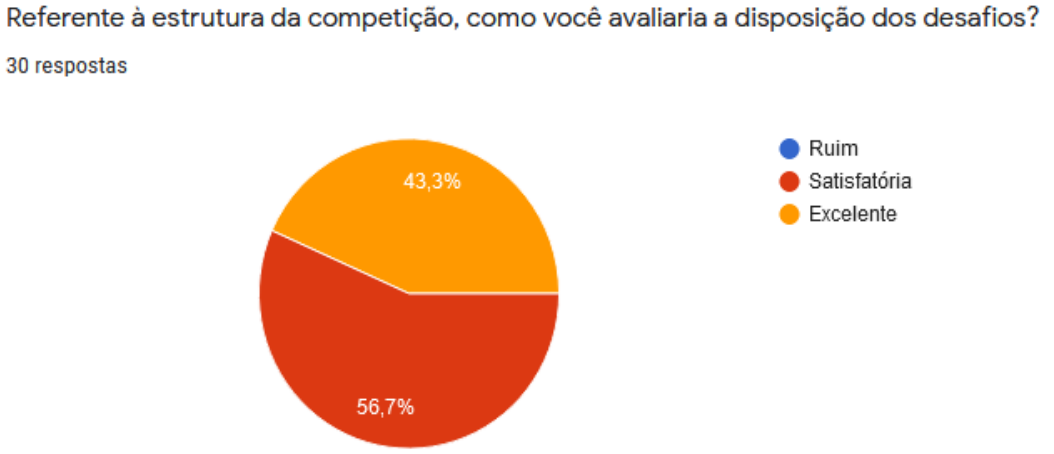
4.2.3.3 Desafios

Dentro das questões sobre os desafios, procurou-se elucidar o pensamento de Seltzer (2019) sobre o estilo de *Jeopardy*, de que grande parte das competições tem escolhido esse estilo devido à sua praticidade, não sendo necessário um grande investimento em infraestrutura.

O primeiro ponto que se buscou saber foi como as competições estavam disponibilizando os desafios para os participantes. Diante desse contexto, 96,7% das competições estavam dividindo os desafios por categoria. Esse tipo de divisão oportuniza os

participantes a buscarem quais desafios mais se identificavam, porém, somente 86,7% das competições disponibilizavam classificação por categoria e nível. Conforme a Gráfico 2, os questionados avaliaram esse tipo de estrutura de competição como satisfatória ou excelente.

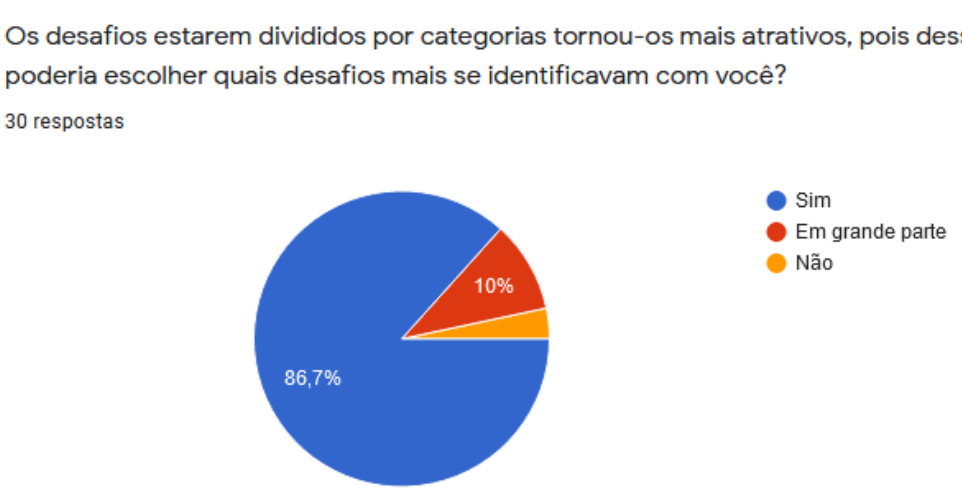
Gráfico 2 – Avaliação dos participantes sobre disposição dos desafios



Fonte: elaborado pelo autor.

Algumas competições não têm seguido a ideia de Seltzer (2019), de que cada desafio de determinada categoria liberaria um novo desafio com maior nível de complexidade. As competições disponibilizaram todos os desafios para que os usuários escolhessem qual deles desejavam escolher. Essa divisão de categoria torna as competições mais atrativas para os participantes, conforme demonstra a Gráfico 3.

Gráfico 3 – Percepção dos participantes sobre divisão dos desafios por categoria



Fonte: elaborado pelo autor.

Os participantes relatam que conforme iam solucionando os desafios, suas motivações eram maiores para seguir para o próximo desafio, também informaram que sua pontuação contribui com a sua empolgação, por isso que questionamos se as competições estavam disponibilizando o placar para os participantes.

Ainda falando sobre a percepção dos participantes conforme iam solucionando os desafios, eles relataram que se sentiam envolvidos com a competição e instigados a procurarem novos conhecimentos, além de encorajados a serem capazes de enfrentar os desafios de maior complexidade. Com isso, a ideia de Seltzer (2019) tem-se provado ideal para ser utilizada para competições no meio acadêmico, tendo em vista que essa estrutura foi aprovada pelos participantes que tiveram um nível de aceitação considerável.

4.2.3.4 Organizadores

Devido à participação do acadêmico em uma competição, considerou-se necessário analisar se os participantes tinham uma visão do papel dos organizadores para auxiliar os participantes. As respostas comprovaram que os participantes acreditam que as competições necessitam de pessoas para auxiliar em dúvidas ou erros que podem ocorrer

Ainda, relataram o auxílio dos organizadores e/ou instrutores como satisfatório e excelente, demonstrando que há necessidade da disposição pessoas para contribuir em pequenas questões e dificuldades de compreender o enunciado dos desafios.

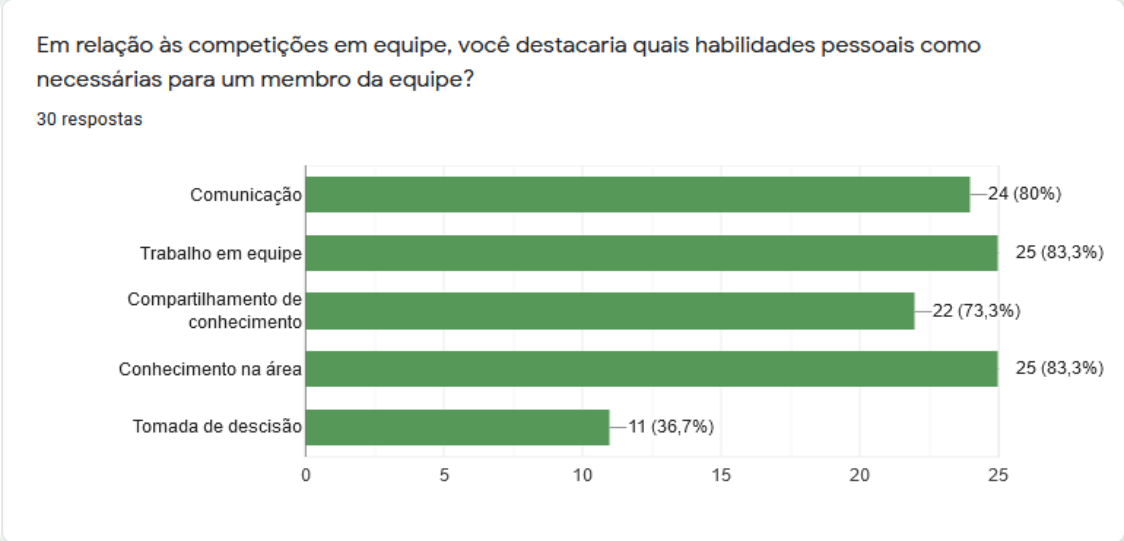
4.2.3.5 Contribuição da CTF

No capítulo 3, em que o referencial teórico é apresentado, desenvolveu-se uma seção sobre os aspectos pedagógicos com os quais a CTF pode contribuir para a construção de conhecimentos e habilidades pessoais. Nessa seção, relata-se a percepção dos participantes referente a essas possíveis contribuições da competição.

Questionados sobre como os participantes de competições em grupo devem manter um diálogo constante e claro do que está ocorrendo em seus servidores, 90% dos participantes constataram que essa habilidade é aperfeiçoada com a CTF.

Questionados sobre habilidades pessoais que cada membro de equipe necessita para melhor funcionamento da equipe, os membros destacaram as habilidades na Gráfico 4.

Gráfico 4 – Habilidades pessoais necessárias para CTF em equipe

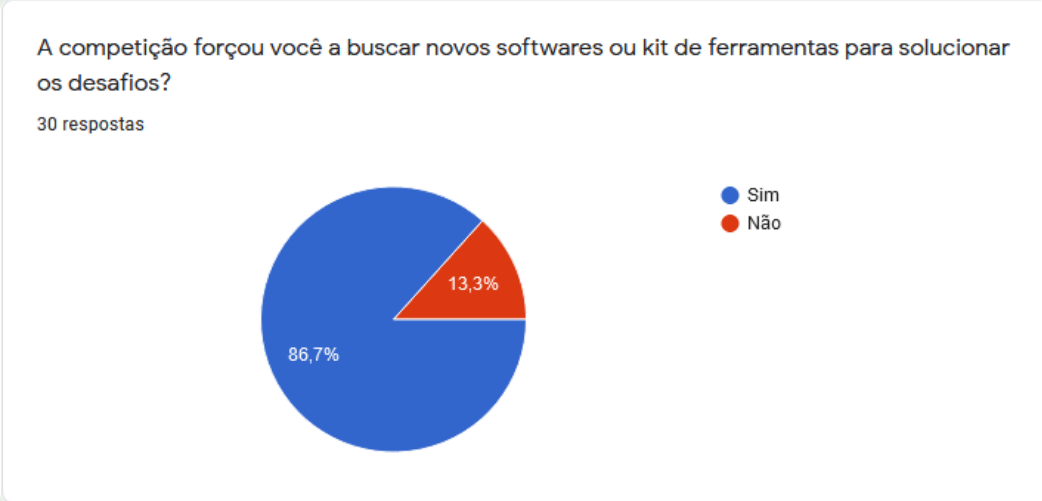


Fonte: elaborado pelo autor.

Todas essas habilidades mencionadas na questão foram direcionadas pelos aspectos pedagógicos que Mansurov (2016) descreve como as principais contribuições da CTF. Além das habilidades pessoais relatadas anteriormente, deve-se avaliar a contribuição da CTF na construção de conhecimento dos participantes na sua trajetória como profissional de cibersegurança.

Os participantes relataram que, durante as competições que participaram, tiveram que utilizar novos *softwares* ou ferramentas, sendo que 93,3% dos respondentes fizeram essa afirmativa. Relataram também que esse tipo de competições ajudou a adquirir conhecimentos *softwares* de cibersegurança.

Gráfico 5 – Competição forçou a buscar novas ferramentas ou software



Fonte: elaborado pelo autor.

Por fim, buscou-se a percepção dos participantes sobre como o ambiente de CTF foi positivo na sua vida acadêmica ou profissional. O resultado dessa questão demonstrou que a tese de alguns autores anteriormente citados também é percebida pelos participantes. Desse modo, 26 pessoas responderam que perceberam que a competição contribuiu para seu crescimento profissional, pois aprenderam muito durante ela, tanto sobre ferramentas quanto sobre técnicas, e que o ambiente os deixou entusiasmados para buscar mais conhecimentos sobre a cibersegurança, trazendo ainda mais responsabilidade para o aluno na construção do seu conhecimento e diminuindo toda a responsabilidade para os professores dentro das sala de aulas, conforme o aspecto pedagógico citado na seção 3.3.3 – Aprendizagem baseada em desafios.

5 CONSIDERAÇÕES FINAIS

Este trabalho teve o propósito de fazer uma descrição teórica e prática das competições de CTF e suas potencialidades para desenvolvimento de competências em cibersegurança. Pode-se afirmar, a partir do referencial teórico, que CTF é uma ferramenta com grande valor para formação de profissionais na área de segurança da informação, visto que pode auxiliar os estudantes da área a colocarem em prática todos conhecimentos captados durante a faculdade, cursos, palestras etc., em um ambiente controlado. Devido à construção desse ambiente, seus participantes podem empregar suas habilidades sem a preocupação de sofrerem prejuízos para suas organizações, ou problemas judiciais devido às técnicas de invasão realizadas durante a experimentação.

Além disso, os praticantes dessa atividade não conquistam somente habilidades de segurança da informação. Durante a competição, desenvolvem-se aspectos pedagógicos que são valorizados pelas organizações, como o trabalho em equipe, em razão de que os colaboradores devem trabalhar juntos para o melhor funcionamento dos setores, e contribuindo para alcançarem as metas e objetivos da organização.

O quadro de características dos torneios do tipo CTF, criado a partir da literatura, demonstra o que é necessário para a realização de uma competição bem sucedida, sem contar que a participação do acadêmico em uma CTF permitiu fazer a validação prática dos itens apontados.

Considerando o resultado do questionário disponibilizado para os estudantes e profissionais de cibersegurança que participaram de torneios de CTF, também foi possível constatar os pontos que os participantes percebem como crucial para o sucesso em busca do desenvolvimento dos conhecimentos e habilidades dos participantes. São eles: palestras e/ou cursos introdutórios; desafios divididos por categorias e níveis para estimular os participantes a seguir na competição; e participação dos organizadores para sanar as dúvidas e solucionar os problemas e erros com as ferramentas disponibilizadas.

Todas essas etapas foram realizadas para alcançar o objetivo da pesquisa que foi desenvolver um estudo teórico e prático de como CTF poderá contribuir para o desenvolvimento dos participantes e para área de cibersegurança. Buscando através dos objetivos específicos que são: apresentar as modalidades de competições, suas formas de execução e potenciais ganhos na formação dos participantes na área de cibersegurança, analisar as principais técnicas utilizadas durantes os eventos e como cada etapa poderá contribuir para a construção de conhecimento.

Quanto às limitações deste trabalho, tem-se o tamanho da amostra de respondentes do questionário. Como trabalhos futuros, percebe-se a necessidade de aplicar as percepções relatadas pelos participantes em uma competição voltada para acadêmicos, e, com isso, avaliar o sucesso da competição e sua contribuição na evolução do conhecimento dos participantes. Além de se criar um manual para iniciantes em cibersegurança encontrarem e participarem de competições de CTF, realizar um estudo de como aplicar o CTF em universidades brasileiras de forma que os alunos de cibersegurança possam conciliar os estudos teóricos e práticos, realizar um levantamento dos aspectos psicológicos dos grupos de CTF, para que possam aplicar os aspectos pedagógicos durante os treinamentos.

Por fim, o presente trabalho evidencia que esse tipo de torneio pode contribuir para a formação dos acadêmicos, além do aperfeiçoamento das equipes de segurança da informação em organizações, levando em consideração o volume expressivo de ameaças às informações e de *hosts* invadidos anualmente.

REFERÊNCIAS

ALMEIDA, Fernando José; FONSECA JÚNIOR, Fernando Moraes. **Aprendendo com projetos**: cadernos informática para a mudança em educação. Brasília: MEC/SEED/ProInfo, 1999.

BEDOYA; Daniel Ospina. **Diseño de ambiente ctf para entrenamiento en ciberseguridad**. Bogotá, Colombia: Escuela Colombiana de Ingeniería Julio Garavito, 2019. Disponível em: <https://repositorio.escuelaing.edu.co/bitstream/001/1041/4/Ospina%20Bedoya%2c%20Daniel-2019.pdf>. Acesso em: 18 jul. 2020.

BEZ, M. R. **Uso de tecnologia para apoiar a implantação de métodos ativos nos currículos de medicina**. 2011. 117 f. Proposta de Tese (Doutorado em Informática na Educação) – Programa de Pós-Graduação em Informática na Educação, Centro Interdisciplinar de Novas Tecnologias na Educação, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2011.

BOCK, Kevin; HUGHEY, George; LEVIN, Dave. King of the hill: a novel cybersecurity competition for teaching penetration testing. XVIII Workshop on Advances in Security Education, 18., 2018, Baltimore, EUA. **Anais eletrônicos** … Baltimore, EUA: USENIX, 2018. Disponível em: <https://koth.cs.umd.edu/papers/koth_ase2018.pdf>. Acesso em: 16 abr. 2020.

BOOPATHI, K.; BITHIN, S. S. A. A. Learning cyber security through gamification, **Amritapuri**, Índia, v. 8, p. 642-649, 2015.

BURNS, Taner J. et al. online ctf competitions for security education. In*:* XVII Usenix Workshop on Advances in Security Education, Vancouver, CA. **Anais eletrônicos**… Vancouver, CA: USENIX, 2017. Disponível em: <https://www.usenix.org/system/ files/conference/ase17/ ase17_paper_burns.pdf>. Acesso em: 19 maio 2020.

CAPALBO, Nicholas; REED, Theodore; ARPAIA, Michael. RTFn: Enabling cybersecurity education through a mobilecapture the flag client. In: XI The 2011 International Conference on Security and management, 2011, Las Vegas. **Anais eletrônicos**… Las Vegas: Worldcomp'11, 2011. Disponível em: <http://worldcomp-proceedings.com/proc/p2011/ SAM5058.pdf>. Acesso em: 5 maio 2020.

CARRIER, Brian. **Open source digital forensics tools**: the legal argument. 2002. Disponível em: <http://www.digital-evidence.org/papers/opensrc_legal.pdf>. Acesso em: 19 mai. 2020.

CASTRO, Alberto; MENEZES, Crediné. Aprendizagem colaborativa com suporte computacional. In: PIMENTEL, Mariano; FUKS, Hugo (orgs.). **Sistemas colaborativos**. Rio de Janeiro: Campus, 2011. p. 135-153. Disponível em: <http://sistemascolaborativos. uniriotec.br/wp-content/uploads/sites/18/2019/06/SC-cap9-aprendizagem.pdf>. Acesso em: 5 jun. 2020.

CHALENGE BASED LEARNIND (CBL). **Home**. 2020. Disponível em: <https://www.challengebasedlearning.org/pt/>. Acesso em: 20 ago. 2020.

CHUNG, Kevin; COHEN, Julian. Learning obstacles in the capture the flag model. In: XIV Usemix Summit on Gaming, Games, and Gamification in Security Education, 2014, San Diego, CA. **Anais eletrônicos**… San Diego, CA: USENIX, 2014. Disponível em: <https://www.usenix.org/conference/3gse14/summit-program/presentation/chung>. Acesso em: 1 maio 2020.

COELHO, Laura Cristina Machado; BENTO, Ricardo Jorba. **Ferramentas de esteganografia e seu uso na Infowar**. 2003. 56 f. Monografia (Especialização em Segurança de Redes) – Programa de Pós-Graduação Segurança de Redes, Universidade Católica de Brasília, Brasília, 2003.

COMPUTER EMRGENCY REPORT TEAM (CERT). **Cartilha de segurança para internet**. 2012. Disponível em: <https://cartilha.cert.br/ criptografia>. Acesso em: 7 mai. 2020.

CONKLIN, A. Cyber defense competition and information security education: an active learning solution for a capstone course. In*:* XL Annual Hawaii International Conference on System Sciences, 2006, Havaí. **Anais eletrônicos**… Havaí: IEEE, 2006.

COWAN, C. Defcon capture the flag: defending vulnerable code from intense attack. In: IV Darpa Information Survivability Conference and Exposition, 2003, Washington, USA. **Anais eletrônicos**…. Washington, USA: IEEE, 2003. Disponível em: <https://ieeexplore.ieee.org/ abstract/document/1194878>. Acesso em: 21 maio 2020.

CRASS, Torry. Evolution of the CTF: the value of training by gaming. **Pentest Magazine**, [*s. l.*], p. 60-64, dez. 2019. Disponível em: < https://pentestmag.com/product/pentest-capture-the-flag/>. Acesso em: 20 maio 2020.

CTF ZONE. 2020. Disponível em: < https://ctf.zone/ctfinfo.html>. Acesso em: 9 dez. 2020.

DAVIS, Andy et al. The fun and future of CTF. In*:* XIV Usemix Summit on Gaming. Games, and Gamification in Security Education, 2014, San Diego, CA. **Anais eletrônicos**… San Diego, CA: USENIX, 2014. Disponível em: <https://www.usenix.org/system/files/ conference/3gse14/3gse14-davis.pdf>. *Acesso em: 20 maio 2020.*

EAGLE, Chris; CLARK, John L. **Capture-the-flag**: learning computer securityunder fire. 2004. Disponível em: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a435319.pdf>. Acesso em: 10 mar. 2020.

FAGUNDES, Léa da Cruz et al. Aprendizes do futuro: as inovações começaram. In*:* FONTES, Edison L. G. (org.). **Segurança da informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

FASSBINDER, A. G. de O.; PAULA, L. C.; ARAÚJO, João Cláudio D. Experiências no estímulo à prática de programação através do desenvolvimento de atividades extracurriculares relacionadas com as competições de conhecimentos. In: XXXII Congresso da Sociedade Brsaileira de Computação (CSBC), 2012, Curitiba. **Anais**… Curitiba: Sociedade Brasileira de Computação (SBC), 2012.

FONSECA, Gabriela. **Além de um jogo [CTF], o início de uma carreira**. 5 jun. 2019. Disponível em: <https://medium.com/creditas-tech/ctf-alem-de-um-jogo-o-inicio-de-uma-carreira-d9845cdabfcf>. Acesso em: 05 out. 2020.

FRUHMANN, M.; GEBESHUBER, K. Maximize the learning success in it-security. In: XI International Conference on Education and New Learning Technologies, 2019, Palma, Spain. **Anais**… Palma, Spain: Iater, 2019.

GITHUB. FBCTF. 2017. Disponível em: <https://github.com/facebookarchive/fbctf>. Acesso em: 28 abr. 2020.

GONZALEZ, Hugo; LIAMAS, Rafael; MONTAÑO, Omar. Using CTF tournament for reinforcing learned skills in cybersecurity course. **Research in Computing Science**, San Luis Potosí, México, 133-141, 2019.

GOODMAN, Tom; RADU, Amdreea-Ina. **Learn apply reinforce/share learning**: hackathons and CTFs as general pedagogic tools in higher education,and their applicability to distance learning. 2020. Disponível em: <https://arxiv.org/pdf/2006.04226v1.pdf>. Acesso em: 01 jun. 2020.

HACKER SECURITY. **Engenharia reversa**. 2017. Disponível em: <https://hackersec.com/o-que-e-engenharia-reversa/#:~:text=Podemos%20dizer%20que%20Engenharia%20Reversa, ou%20at%C3%A9%20mesmo%20desenvolver%20crackers.>. Acesso em: 09 jul. 2020.

JOHNSON, Larry; BROWN, Samanta. Challenge based learning: the report from the implementation project. **The New Media Consortium**, Austin, 8 nov. 2020

JULIO, Eduardo Pagani; BRAZIL, Wagner Gaspar; ALBUQUERQUE, Célio Vinicius Neves. Esteganografia e suas aplicações. In: VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2007, Rio de Janeiro. **Anais**… Rio de Janeiro: FAPERJ, 2007.

KATZENBACH, Jon R.; SMITH, Douglas K. **The discipline of teams**. mar./abr. 1993. Disponível em: <https://hbr.org/1993/03/the-discipline-of-teams-2>. Acesso em: 10 maio 2020.

LONGATO, Ricardo. **Resolvendo o Hackaflag de Natal 2016**: análise de log web 1. São Paulo: Ricardo Longato, 2016, (4min21s). Disponível em: <https://www.youtube.com/watch?v=gxCh3ztqEQo&ab_channel=RicardoLongatto>. Acesso em: 09 jul. 2020.

MANSUROV, Alexander. A CTF based approach in information security education: an extracurricular activity in teaching students at Altai State University, Russia. **Modern Applied Science**, Canadá, v. 10, n. 11, ago. 2016. Disponível em: <https://pdfs.semanticscholar.org/8a56/cad25bbc560f31e595d2504c399363e18e7b.pdf>. Acesso em: 10 mar. 2020.

MENA, Isabela. **Verbete draft: o que é capture the flag (CTF)**. 7 fev. 2018. Disponível em: <https://www.projetodraft.com/verbete-draft-o-que-e-capture-the-flag-ctf/>. Acessado em: 20 de maio 2020.

MENDES, Ana Clara Nobre et al. Capture the flag: método de aprendizado para a disciplina de forense computacional em uma universidade pública. In: DALLAMUTA, João; HOLZMANN, Henrique A.; GRANZA, Marcelo H. (orgs.). **Engenharia elétrica e de computação: atividades relacionadas com o setor científico e tecnológico**. Ponta Grossa: Atena, 2020. p. 151-156.

MORENO, Daniel. **Introdução ao pentest**. São Paulo: Novatec, 2019.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. 2. ed. Birigui: Futura, 2003.

NAKAYA, Makoto. problem construction and trial practices using a contest management server for a hacking competition CTF to introduce information literacy and security. **The International Journal of E-learning and Educational Technologies in the Digital Media (IJEETDM)**, Hong Kong, v. 2, n. 4, p. 181-188, 2016. Disponível em: https://bit.ly/ 2IcWK4a. Acesso em: 4 jun. 2020.

OLIVERIA, Ronielton. Criptografia simétrica e assimétrica: os principais algoritmos de cifragem. **Revista Segurança Digital**, [*s. l.*], v. 5. p. 11-24, mar./maio 2012. Disponível em: <http://www.ronielton.eti.br/publicacoes/artigorevistaseguranca digital2012.pdf>. Acesso em: 18 maio 2020.

PAVAN, Pedro Vinicius Abreu; GUARDIA, Hélio Crestana. Pentest para auditoria de segurança de rede em ambientes corporativos. **Revista T.I.S**., São Carlos, v. 4, n. 2, p. 172-179, maio/ago. 2015. Disponível em: <http://www.revistatis.dc.ufscar.br/index.php/ revista/article/view/314/113>. Acesso em: 12 maio 2020.

PHD DAYS. **Phays CTF Over? PHDays CTF Goes On!** 20 ago. 2012. Disponível em: <https://www.phdays.com/en/press/news/phdays-ctf-over-phdays-ctf-goes-on/>. Acesso em: 18 mar. 2020.

PIANCASTELLI, Carlos Haroldo; FARIA, Horácio Pereira; SILVEIRA, Marília Rezende. O trabalho em equipe. In*:* BRASIL. Ministério da Saúde. **Organização do cuidado a partir de problemas**: uma alternativa metodológica para a atuação da equipe de saúde da família. Brasília: OPAS, 2000. Disponível em: <https://www.colegiosantanna.com.br/ formacao/downloads/O trabalho em equipe.pdf>. Acesso em: 3 jun. 2020.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013.

RAJ, Arvind S. et al. Scalable and lightweight ctf infrastructures using application containers (pre-recorded presentation). In: XXV Usenix Security Symposium, 2016, Austin, TX. **Anais eletrônicos**… Austin, TX: USENIX, 2016. Disponível em: <https://www.usenix.org/ system/files/conference/ase16/ase16-paper-raj.pdf>. Acesso em: 10 maio 2020.

RAMAN, Raghu et al. Framework for evaluating Capture The Flag (CTF) security competitions. In*:* XII International Conference for Convergence for Technology, 2014, Pune, Índia. **Anais eletrônicos**… Pune, Índia: IEEE, 2014. Disponível em: <https://ieeexplore. ieee.org/abstract/document/7092098/authors#authors>. Acesso em: 25 mai. 2020.

SECURE IOWA CONFERENCE. **Capture the flag**. 8 out. 2019. Disponível em: <https://secureiowaconference.com/index.php/sessions/capture-the-flag-ctf>. Acesso em: 22 maio 2020.

SELTZER, Larry. **Top tools and resources for running a capture the flag competition**. 19 fev. 2019. Disponível em: <https://www.csoonline.com/ article/3341318/top-tools-and-resources-for-running-a-capture-the-flag-competition.html>. Acesso em: 7 mar. 2020.

SILVA, Márcio. **A importância do trabalho em equipe**. 05 fev. 2010. Disponível em: <https://administradores.com.br/artigos/a-importancia-do-trabalho-em-equipe>. Acesso em: 1 jun. 2020.

TARAKKAMÄKI, Aleksi. **Capture the flag**: mallin soveltuminenkyberturvallisuuden opetukseen. 2020. 21 f. Tese (Bacharelado em Tecnologia da Informação) – Universidade de Jyväskylä, Jyväskylä, 2020. Disponível em: <https://jyx.jyu.fi/bitstream/handle/123456789/68964/1/URN%3ANBN%3Afi%3Ajyu-202005133171.pdf >. Acesso em: 22 jul. 2020.

TORRES, Patrícia Lupion; IRALA, Esrom Adriano F. **Aprendizagem colaborativa**: teoria e prática. 2014. Coleção Agrinho. Disponível em: <https://www.agrinho.com.br/site/wp-content/uploads/2014/09/2_03_Aprendizagem-colaborativa.pdf>. Acesso em: 28 maio 2020.

TRICKEL, E. et al. Shell we play a game? CTF as a service for security education. In: XVI Usenix Workshop on Advances in Security Education, 2017, Vancouver, CA. **Anais eletrônicos**… Vancouver, CA: USENIX, 2017. Disponível em: <https://www.usenix.org/system/files/conference/ase17/ase17_paper_trickel.pdf>. Acesso em: 10 mar. 2020.

ULBRICH, Henrique Cesar; DELLA VALLE, James. **Universidade hacker**: desvendando todos os segredos do submundo dos hackers. 4. ed. São Paulo: Digerati, 2004.

VALENZA, Andrea. Web security training [at] UniGe: an experience. In: III Conference International on Art, Science and Engineering of Programming, 2019, Gênova. **Anais**… Nova Iorque: Association for Computing Machinery, 2019.

VERGARA, S. **Gestão de pessoas**. 2. ed. São Paulo: Atlas, 2002.

WALTER, Kimberly J. Ferguson et al. Theworld of CTF is not enough data: lessons learned from a cyber deception experiment. In: V International Conference on Collaboration and Internet Computing, 2019, Los Angeles. **Anais eletrônicos**… Los Angeles: IEEE, 2019. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8998505>. Acesso em: 22 jul. 2020.

WI, SeongIl; CHOI, Jaeseung; CHA, Sang Kil. Git-based CTF: a simple and effective approach to organizingin-course attack-and-defense security competition. In: XVIII Workshop on Advances in Security Education, 2018, Baltimore, EUA. **Anais eletrônicos**… Baltimore, EUA: USENIX, 2018. Disponível em: <https://www.usenix.org/system/files/conference/ase18/ase18-paper_wi.pdf>. Acesso em: 1 maio 2020.

YEAGER, Ray. Criminal computer forensics management. In: III Annual Conference on Information Security Curriculum Development, 2006, Kennesaw, Georgia. **Anais eletrônicos**… Nova Iorque: Association for Computing Machinery, 2006. Disponível em: <https://dl.acm.org/doi/abs/10.1145/1231047.1231085>. Acesso em: 4 jun. 2020.

ANEXO A - QUESTIONÁRIO PARA COLETA DA PERCEPÇÃO DE PARTICIPANTES DE CTF

Percepção de Participantes

Este instrumento tem como objetivo coletar a percepção de participantes de competições do tipo Capture The Flag - CTF, como apoio ao trabalho de conclusão de curso "CTF: UM ESTUDO TEÓRICO E PRÁTICO PARA CONSTRUÇÃO DE CONHECIMENTO NA ÁREA DE SEGURANÇA DA INFORMAÇÃO", realizado no curso de Sistemas de Informação da Universidade Feevale.

Este questionário não exige identificação nominal, garantindo a privacidade das informações fornecidas por você.
Os dados solicitados serão utilizados unicamente para caracterizar as experiências dos participantes do estudo.
Não são conhecidos riscos aos respondentes e sua participação é totalmente voluntária.

Desde já, agradeço sua colaboração!
Autor: Lucas Henrique de Moraes (lucashdemoraes@gmail.com)

Como você conheceu a CTF? *

- [ ] Internet
- [ ] Redes sociais
- [ ] Faculdade
- [ ] Amigos
- [ ] Outros...

Antes da competição, você havia utilizado quais meios, a seguir, para aprender sobre cibersegurança? *

- [ ] Curso
- [ ] Estudos
- [ ] Aulas
- [ ] Palestras
- [ ] Outros...

Como você avalia seu conhecimento antes de ter participado da competição que está em análise? *

- ( ) Nenhum
- ( ) Baixo
- ( ) Intermediário
- ( ) Bom
- ( ) Profissional

Antes da competição, você havia utilizado quais meios, a seguir, para aprender sobre cibersegurança? *

- [ ] Curso
- [ ] Estudos
- [ ] Aulas
- [ ] Palestras
- [ ] Outros...

Referente à cibersegurança, você acredita que aulas/cursos/palestras são suficientes para formar um profissional? *

- ◯ Sim
- ◯ Talvez
- ◯ Não

As palestras/cursos oferecidos antes da competições forneceram uma base inicial para solucionar alguns desafios de cibersegurança? *

- ◯ Sim
- ◯ Não
- ◯ Não sei opinar

Referente à cibersegurança, você acredita que aulas/cursos/palestras são suficientes para formar um profissional? *

- ◯ Sim
- ◯ Talvez
- ◯ Não

As palestras/cursos oferecidos antes da competições forneceram uma base inicial para solucionar alguns desafios de cibersegurança? *

- ◯ Sim
- ◯ Não
- ◯ Não sei opinar

Os conteúdos dispostos durante as palestras/cursos introdutórios eram atuais e bem elaborados? *

- ◯ 0
- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9
- ◯ 10

Considerando a importância das palestras e cursos introdutórios, quanto eles contribuem para a competição. *

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10

Em geral, quanto você acha necessário que ocorra palestras/cursos introdutórios nas competições de CTF? *

- ◯ 0
- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5
- ◯ 6
- ◯ 7
- ◯ 8
- ◯ 9
- ◯ 10

Considerando os desafios que foram apresentados durante a competição, eles estavam classificados por tipo e níveis de dificuldade? *

- ◯ Sim
- ◯ Não

Os desafios estavam divididos em categorias (criptografia, esteganografia, forense e etc.)? *

- ◯ Sim
- ◯ Não

Durante a competição, cada desafio resolvido destravava um novo desafio da categoria? *

- Sim
- Alguns
- Não

Cada desafio apresentava um nível diferente de complexidade? *

- Sim
- Não

Nos desafios com maior complexidade, você teve necessidade de procurar mais conteúdo para resolve-los? *

- Sim
- Não

Na sua opinião, os desafios estavam de acordo com o nível de complexidade descrito pelos organizadores? *

- Sim
- Em grande parte
- Não

Durante a competição, você tinha acesso ao placar? *

- Sim
- Não

Referente à estrutura da competição, como você avaliaria a disposição dos desafios? *

- ◯ Ruim
- ◯ Satisfatória
- ◯ Excelente

Ao ocorrer alguma dificuldade em entender os desafios, os organizadores e/ou instrutores estavam disponíveis para esclarecimento? *

- ◯ Sim
- ◯ Em grande parte
- ◯ Não

Como você avalia os auxílios dos organizadores e/ou instrutores durante a competição? *

- ◯ Ruim
- ◯ Satisfatória
- ◯ Execelente

Dentro do ambiente de competição, você acredita que os organizadores e/ou instrutores possuem papel essencial para auxiliar os participantes? *

- ◯ Sim
- ◯ Não
- ◯ Não sei opinar

Conforme a competição ia se desenvolvendo, sua pontuação afetava sua motivação (assinale qual opção você considera mais adequada)? *

- ( ) Sim, quanto maior a minha pontuação mas motivado eu ficava.
- ( ) Sim, cada vez que conseguia solucionar um desafio maior era minha motivação para o próximo.
- ( ) Não, devido à complexidade dos desafios não conseguia me motivar a continuar.
- ( ) Não, como minha pontuação estava muito baixa, desisti.
- ( ) Minha motivação ia variando conforme conseguia solucionar os desafios.

Os desafios estarem divididos por categorias tornou-os mais atrativos, pois dessa forma poderia escolher quais desafios mais se identificavam com você? *

- ( ) Sim
- ( ) Em grande parte
- ( ) Não

Durante a resolução dos desafios, quais das opções, a seguir, correspondem a como você se sentiu? *

- [ ] Instigado a procurar novos conhecimentos.
- [ ] Envolvido com a competição.
- [ ] Capaz de encarar desafios maiores.
- [ ] Encorajado em resolver os desafios.
- [ ] Desanimado por ter falhado em algum desafio.

Em relação às competições em equipe, você destacaria quais habilidades pessoais como necessárias para um membro da equipe? *

- [ ] Comunicação
- [ ] Trabalho em equipe
- [ ] Compartilhamento de conhecimento
- [ ] Conhecimento na área
- [ ] Tomada de descisão

Levando em consideração que para participar de uma competição de CTF em equipe, todos os membros da equipe devem manter um diálogo do que está ocorrendo com seu servidor, você acredita que a habilidade de comunicação seja aperfeiçoada durante o exercício? *

- ( ) Sim
- ( ) Não
- ( ) Não sei opinar

Durante a preparação para as competições, sua equipe costuma realizar reuniões para discutir novas técnicas e/ou ferramentas que podem utilizar?

- ( ) Sim
- ( ) Não

Sua equipe costuma realizar seus treinos utilizando situações reais (situações do trabalho)?

- ( ) Sim
- ( ) Não

Considerando a experiência com sua equipe, marque as opções abaixo que você considera verdadeiras:

- [ ] Durante os treinamentos sempre compartilhamos conhecimentos sobre ferramentas e técnicas que apren ...
- [ ] Nossa equipe se divide por area de especialização. Durante a competição cada participante cuida de uma ...
- [ ] Utilizamos casos que nossos colegas passaram durante a semana para treinar.
- [ ] Nos reunimos para ver e solucionar ou discutir desafios de CTF de versões passadas.
- [ ] Participamos de grupo ou fórum sobre cibersegurança.

Para solucionar alguns desafios de CTF não basta ter o conhecimento sobre as técnicas que são necessárias. Na grande maioria das vezes é necessário utilizar uma ferramenta para criptografar um arquivo ou até mesmo para acessar um servidor remoto. Durante a competição que participou, você teve que utilizar algum software sobre o qual não tinha conhecimento? *

- ( ) Sim
- ( ) Não

A competição forçou você a buscar novos softwares ou kit de ferramentas para solucionar os desafios? *

- ( ) Sim
- ( ) Não

Levando em consideração sua primeira experiência com CTF, você acredita que esse tipo de competição lhe ajudou na questão de conhecimento referente aos softwares de cibersegurança? *

- ( ) Sim
- ( ) Não

Avaliando sua experiência na CTF, você tem interesse em participar de outras? *

- ○ Sim
- ○ Não

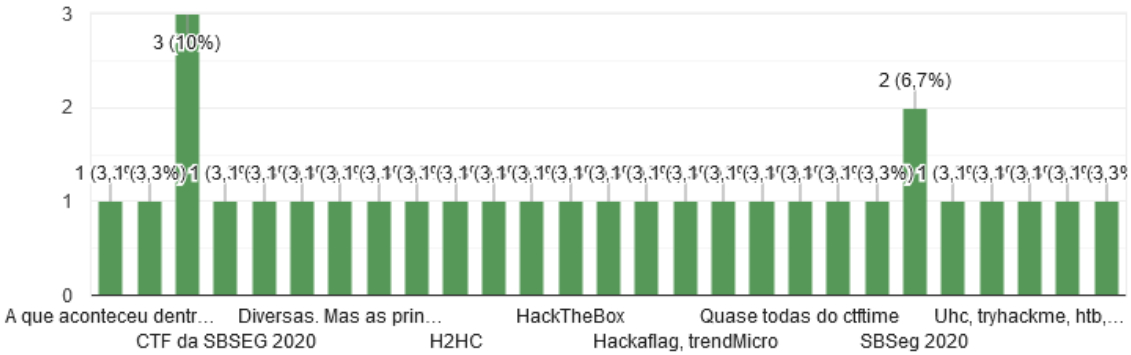
Após sua participação na CTF, marque as opções abaixo que você considera verdadeiras: *

- ☐ Percebi que competição contribuiu no meu crescimento profissional, pois aprendi muito durante a compet ...
- ☐ O ambiente de CTF conseguiu me deixar entusiasmado em seguir meus estudos e aperfeiçoamento na ár ...
- ☐ A CTF não contribuiu para minha formação.
- ☐ A CTF pode ser utilizada como ferramenta de treinamento para alunos e profissionais.
- ☐ O CTF serve somente para aprefeiçoar conhecimentos que o participante já tenha conhecimento.

ANEXO B - RESPOSTAS DO QUESTIONÁRIO DE PERCEPÇÃO DE PARTICIPANTES DE CTF

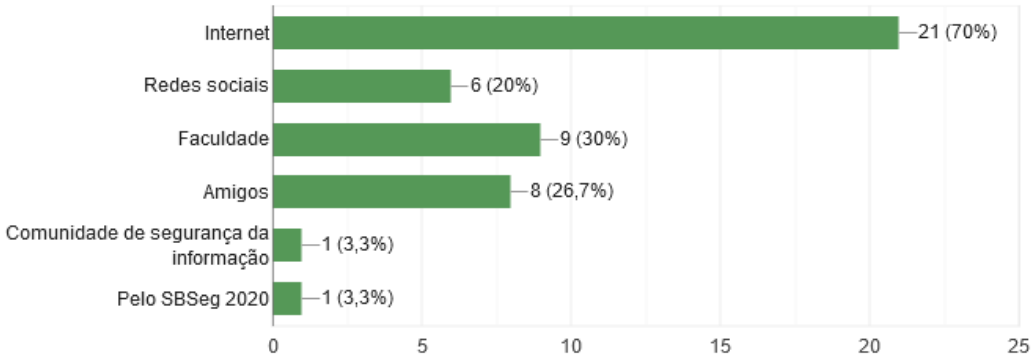
Qual competição de CTF você participou?

30 respostas



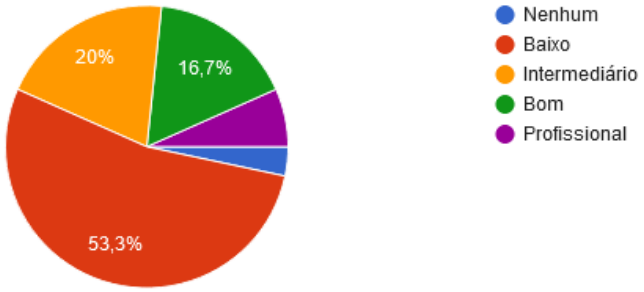
Como você conheceu a CTF?

30 respostas



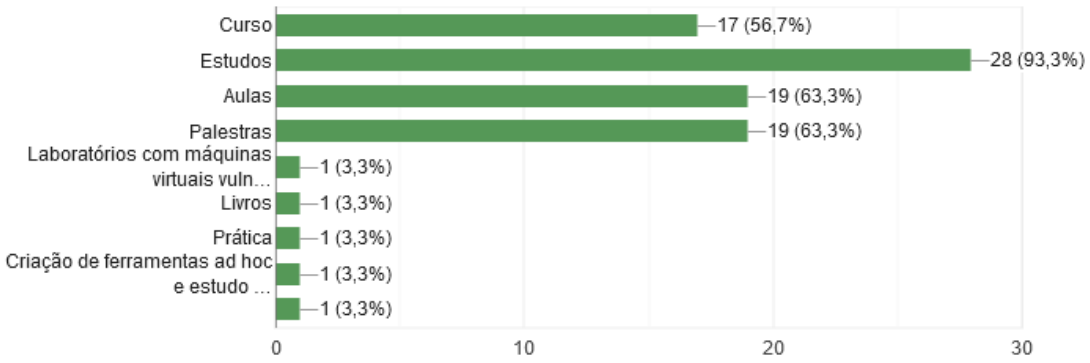
Como você avalia seu conhecimento antes de ter participado da competição que está em análise?

30 respostas



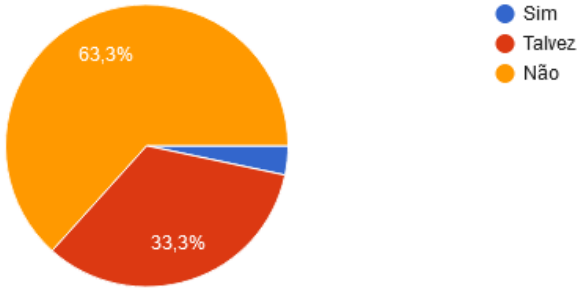
Antes da competição, você havia utilizado quais meios, a seguir, para aprender sobre cibersegurança?

30 respostas



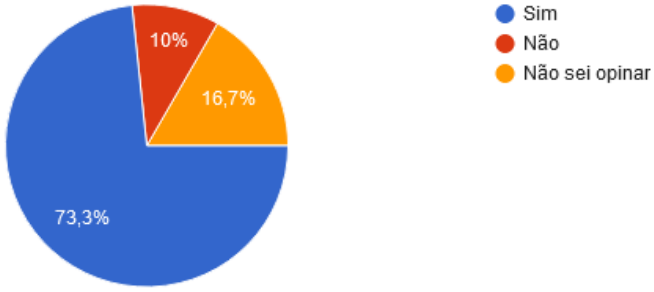
Referente à cibersegurança, você acredita que aulas/cursos/palestras são suficientes para formar um profissional?

30 respostas



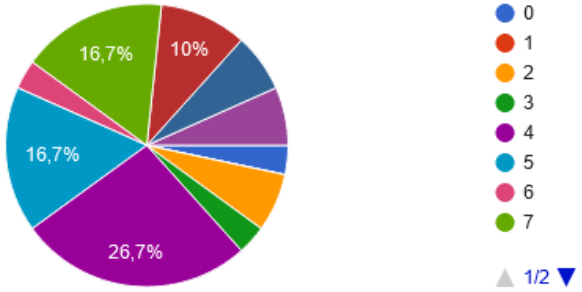
As palestras/cursos oferecidos antes da competições forneceram uma base inicial para solucionar alguns desafios de cibersegurança?

30 respostas



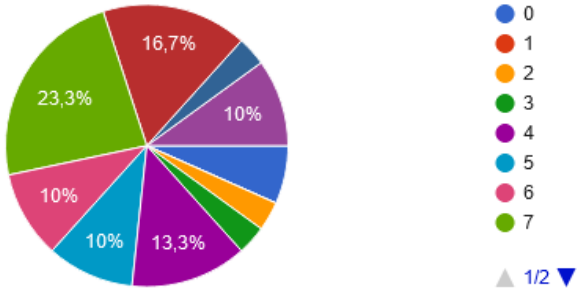
Considerando a importância das palestras e cursos introdutórios, quanto eles contribuem para a competição.

30 respostas



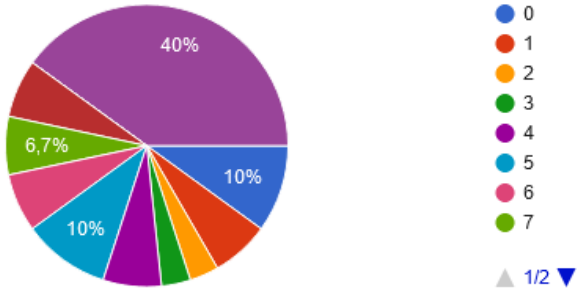
Os conteúdos dispostos durante as palestras/cursos introdutórios eram atuais e bem elaborados?

30 respostas



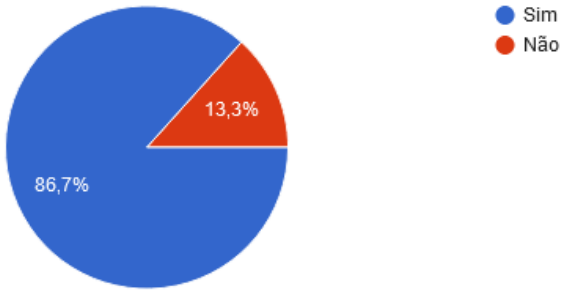
Em geral, quanto você acha necessário que ocorra palestras/cursos introdutórios nas competições de CTF?

30 respostas



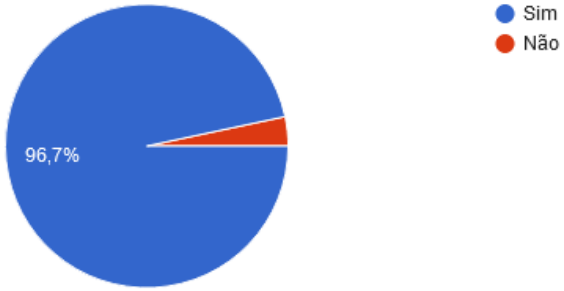
Considerando os desafios que foram apresentados durante a competição, eles estavam classificados por tipo e níveis de dificuldade?

30 respostas



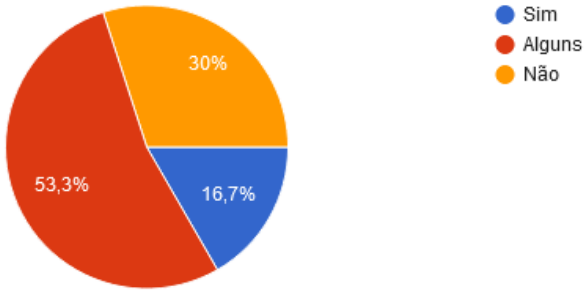
Os desafios estavam divididos em categorias (criptografia, esteganografia, forense e etc.)?

30 respostas



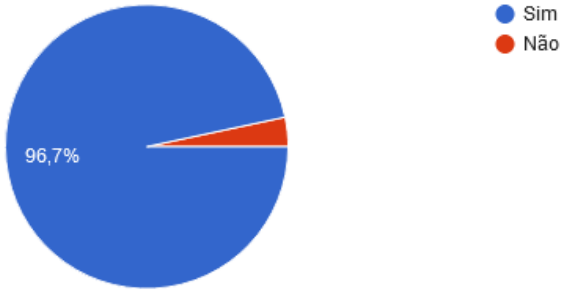
Durante a competição, cada desafio resolvido destravava um novo desafio da categoria?

30 respostas



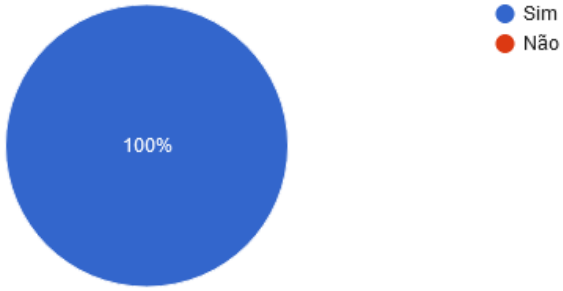
Cada desafio apresentava um nível diferente de complexidade?

30 respostas



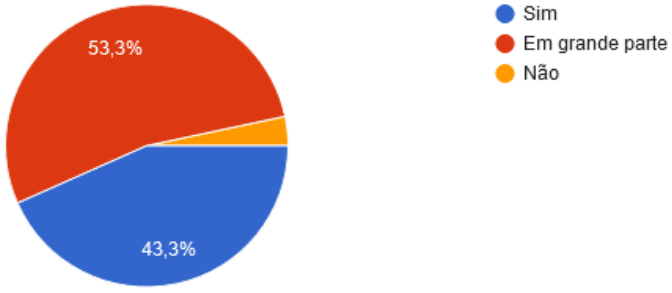
Nos desafios com maior complexidade, você teve necessidade de procurar mais conteúdo para resolve-los?

30 respostas



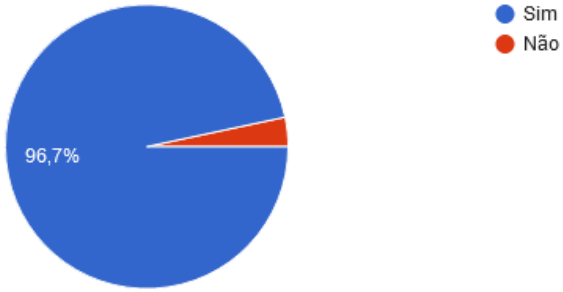
Na sua opinião, os desafios estavam de acordo com o nível de complexidade descrito pelos organizadores?

30 respostas



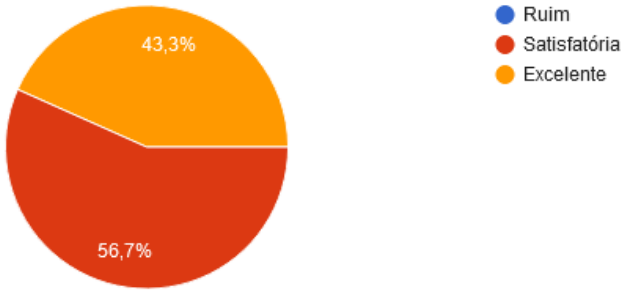
Durante a competição, você tinha acesso ao placar?

30 respostas



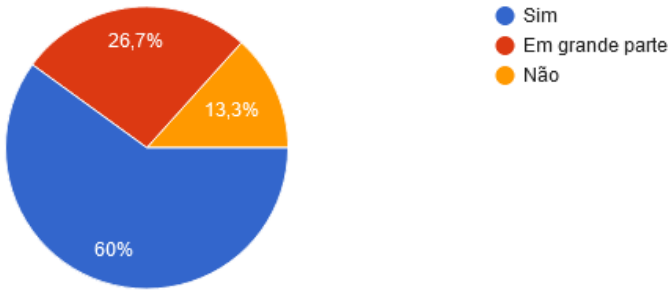
Referente à estrutura da competição, como você avaliaria a disposição dos desafios?

30 respostas



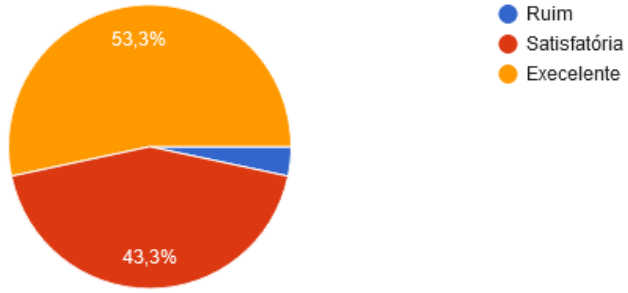
Ao ocorrer alguma dificuldade em entender os desafios, os organizadores e/ou instrutores estavam disponíveis para esclarecimento?

30 respostas



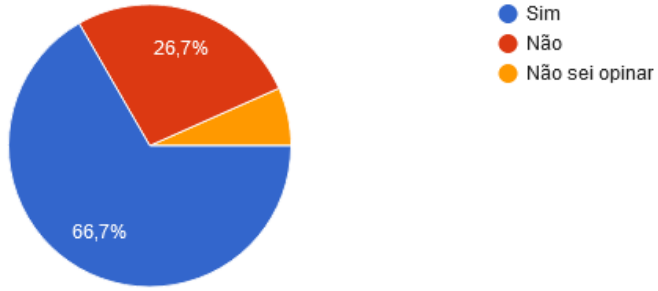
Como você avalia os auxílios dos organizadores e/ou instrutores durante a competição?

30 respostas



Dentro do ambiente de competição, você acredita que os organizadores e/ou instrutores possuem papel essencial para auxiliar os participantes?

30 respostas

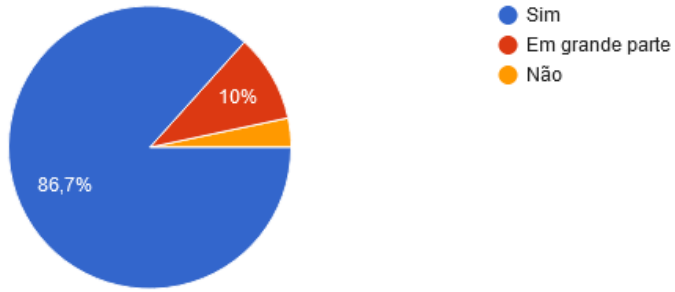


Conforme a competição ia se desenvolvendo, sua pontuação afetava sua motivação (assinale qual opção você considera mais adequada)?

30 respostas

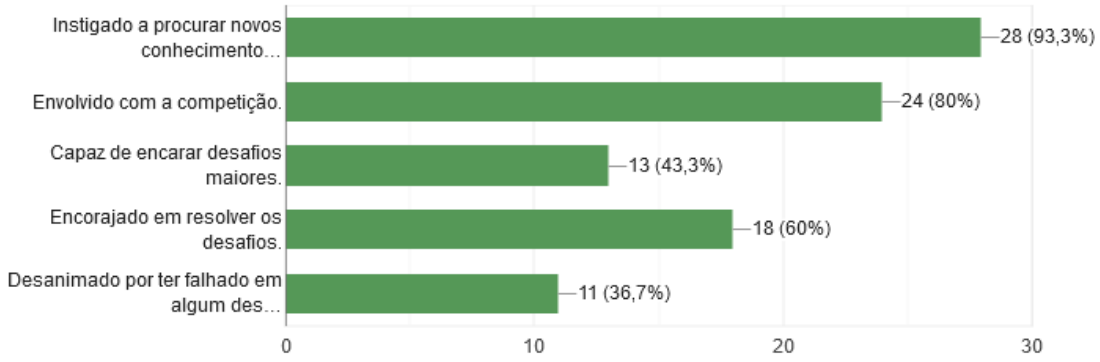
Os desafios estarem divididos por categorias tornou-os mais atrativos, pois dessa forma poderia escolher quais desafios mais se identificavam com você?

30 respostas



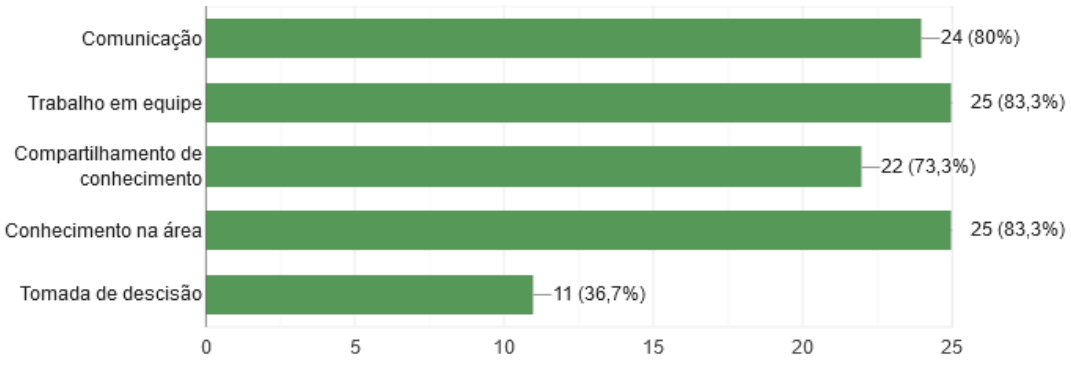
Durante a resolução dos desafios, quais das opções, a seguir, correspondem a como você se sentiu?

30 respostas



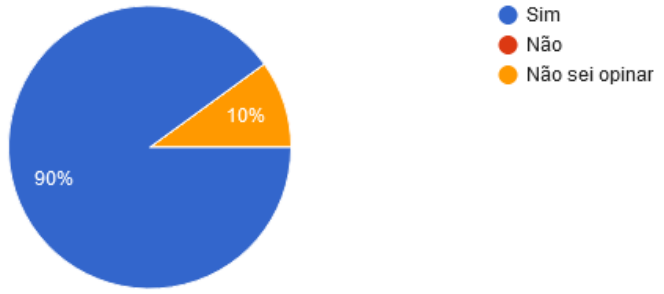
Em relação às competições em equipe, você destacaria quais habilidades pessoais como necessárias para um membro da equipe?

30 respostas



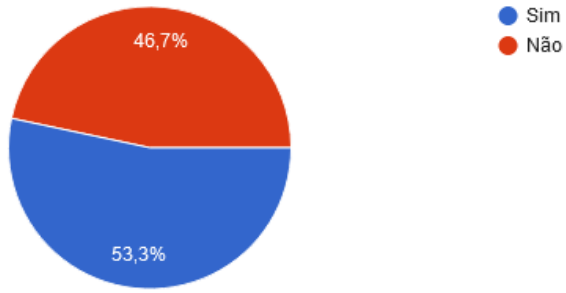
Levando em consideração que para participar de uma competição de CTF em equipe, todos os membros da equipe devem manter um diálogo do que está ocorrendo com seu servidor, você acredita que a habilidade de comunicação seja aperfeiçoada durante o exercício?

30 respostas



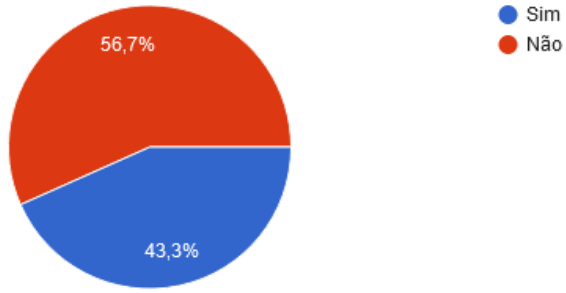
Durante a preparação para as competições, sua equipe costuma realizar reuniões para discutir novas técnicas e/ou ferramentas que podem utilizar?

30 respostas



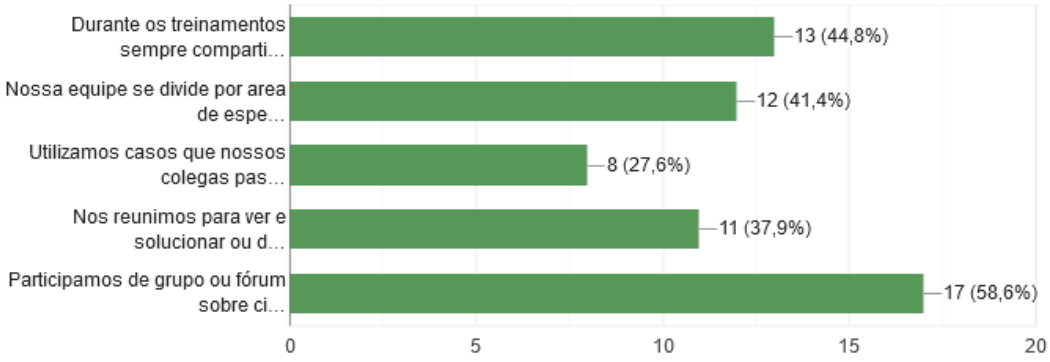
Sua equipe costuma realizar seus treinos utilizando situações reais (situações do trabalho)?

30 respostas



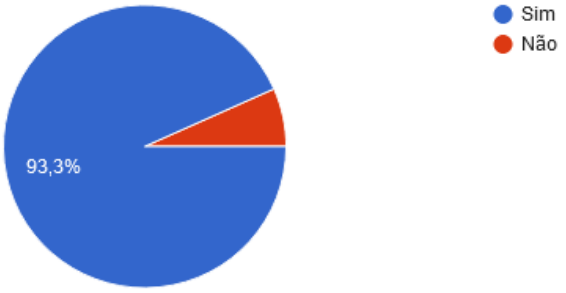
Considerando a experiência com sua equipe, marque as opções abaixo que você considera verdadeiras:

29 respostas



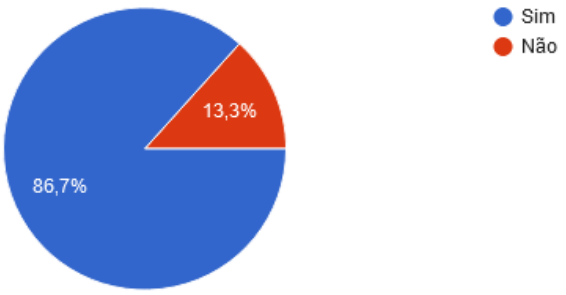
Para solucionar alguns desafios de CTF não basta ter o conhecimento sobre as técnicas que são necessárias. Na grande maioria das vezes é necessário utilizar uma ferramenta para criptografar um arquivo ou até mesmo para acessar um servidor remoto. Durante a competição que participou, você teve que utilizar algum software sobre o qual não tinha conhecimento?

30 respostas



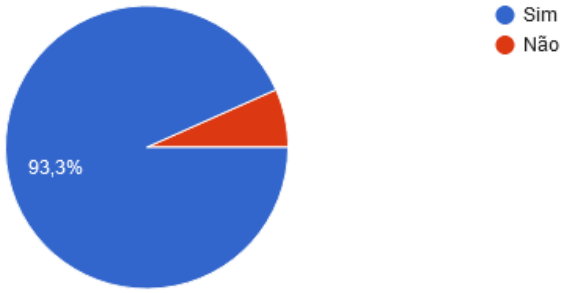
A competição forçou você a buscar novos softwares ou kit de ferramentas para solucionar os desafios?

30 respostas



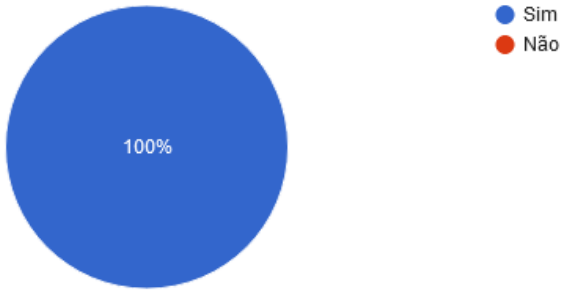
Levando em consideração sua primeira experiência com CTF, você acredita que esse tipo de competição lhe ajudou na questão de conhecimento referente aos softwares de cibersegurança?

30 respostas



Avaliando sua experiência na CTF, você tem interesse em participar de outras?

30 respostas



Após sua participação na CTF, marque as opções abaixo que você considera verdadeiras:

30 respostas