CYBERCIEGE: UMA ABORDAGEM DE JOGOS SÉRIOS NA EDUCAÇÃO DE REDES DE COMPUTADORES

Fabrício Herpich, PPGI, UFSM, fabricio.herpich@gmail.com
Rafaela Ribeiro Jardim, PPGI, UFSM, rafa.rjardim@gmail.com
Ricardo Frohlich da Silva, PPGI, UFSM, ricardosma@gmail.com
Gleizer Bierhalz Voss, PPGIE, UFRGS, gleizer.voss@gmail.com
Felipe Becker Nunes, PPGIE, UFRGS, nunesfb@gmail.com
Roseclea Duarte Medina, PPGI, UFSM, roseclea.medina@gmail.com

Resumo. Os jogos sérios vêm se destacando como ferramentas de grande potencial para a educação, pois oferecem aos estudantes a possibilidade de exercitar seus conhecimentos em cenários virtuais, permitindo maior interatividade, tentativas e erros, respeitando o tempo cognitivo do educando e enfatizando a aplicação prática de seu aprendizado. Além de serem alternativas para simulação de ambientes reais, que em sua essência são críticos ou caros. Este artigo apresenta a aplicação do jogo sério CyberCIEGE diante de uma turma de Segurança para RC. Ao mesmo tempo, discute possíveis melhorias no Design Instrucional da disciplina de acordo com os pareceres dos estudantes.

Palavras – Chave: jogos sérios, redes de computadores, CyberCIEGE.

CYBERCIEGE: AN APPROACH OF SERIOUS GAMES IN EDUCATION OF COMPUTER NETWORKS

Abstract. *Serious games have stood out as tools of great potential for education because students have the opportunity to exercise their expertise in virtual scenarios, allowing greater interactivity, trial and error, respecting the cognitive time of the student and emphasizing practical application of their learning. In addition, to being alternatives for simulating real environments, which in essence are critical or expensive. This paper presents the application of serious game CyberCIEGE front of a class Security for RC. At the same time, discusses possible improvements in instructional design of the discipline in accordance with the opinions of students.*

Keywords: *serious games, computer networks, CyberCIEGE.*

1. INTRODUÇÃO

Redes de Computadores (RC) estão cada vez mais presentes no dia-a-dia das pessoas. Com o avanço e o surgimento de novas tecnologias, essas redes passaram do simples compartilhamento de recursos para desempenhar um papel cada vez mais importante na troca dos mais diversos tipos de informações, sejam elas públicas ou pessoais. Com o aumento na utilização e do número de funcionalidades, consequentemente aumentam os riscos envolvendo RC. Neste sentido, as organizações necessitam de profissionais capacitados que, além da tarefa de realizar o projeto físico e lógico, gerenciar serviços e manter o bom desempenho, precisam garantir a segurança dessas redes com o objetivo de mantê-las em pleno funcionamento e livre de acessos não autorizados ou de eventuais ameaças.

Assim, a formação do profissional de redes não é uma tarefa trivial, pois é necessário que o mesmo aprenda uma grande quantidade de conceitos e geralmente em um curto espaço de tempo. Conceitos esses, que dado o contexto citado, muitas vezes não são bem apresentados, tornando as aulas expositivas insuficientes para a assimilação dos mesmos. Em outras palavras, a dificuldade de preparar o aluno para a prática profissional em um ambiente acadêmico é um dos maiores desafios, cabendo ao professor muitas vezes, encontrar um meio de realizar atividades práticas que despertem o interesse do aluno, possibilitando a interação do mesmo ao invés de ministrar apenas aulas teóricas expositivas.

Por sua vez, a utilização de jogos sérios pode ser uma alternativa, pois já fazem parte do cotidiano de muitas crianças, jovens e adultos. Segundo Mitamura et al. (2012), os jogos sérios têm recebido uma atenção significativa e tem havido um movimento ativo para que efetivamente enriqueçam os ambientes de aprendizagem. Geralmente, os jogos sérios podem ser definidos como uma atividade lúdica, pois é realizada em uma realidade simulada onde os participantes tentam alcançar, pelo menos, uma meta arbitrária, não trivial, agindo de acordo com as regras propostas pelo jogo (Adams, 2010).

Diante deste contexto, este artigo tem como objetivo descrever a utilização do jogo sério CyberCIEGE, o qual foi aplicado aos estudantes da turma do quinto semestre do Curso de Sistemas de Informação da Universidade Federal de Santa Maria (UFSM), possibilitando simulações da parte prática da disciplina de Redes de Computadores como forma de complementação da teoria apresentada em sala de aula, além de discutir possíveis melhorias no Design Instrucional da disciplina com base nos pareceres descritos pelos estudantes.

A ferramenta CyberCIEGE (versão 1.9v1)[1] foi selecionada para ser utilizada, pois apresenta inúmeros cenários e problemas recorrentes à Segurança de RC. Permite também o desenvolvimento de novos cenários e possui vasta documentação e materiais de apoio para alunos e professores. Além do CyberCIEGE, é possível citar como exemplos de jogos sérios: o LVRC de Ferreira et al. (2013), a proposta apresentada por Voss et al. (2013) ou ainda o LVR apresentado por Pinheiro e Filho (2012), entre outros.

2. TRABALHOS CORRELATOS

A utilização de jogos sérios permite a simulação de situações reais que em muitas vezes são críticas ou caras de serem realizadas. No caso da disciplina de Redes de Computadores, é muito custoso obter e manter um laboratório real, pois os equipamentos são de valor elevado e podem ficar obsoletos em um curto período de tempo, sendo necessário a sua substituição.

Neste sentido, Voss et al. (2013) apresentam uma proposta de desenvolvimento de um jogo sério com o objetivo de melhorar o aprendizado na área de redes de computadores. O principal objetivo do trabalho é a implementação de atividades didáticas no formato de um jogo sério desenvolvido no ambiente virtual 3D OpenSim integrado ao Moodle utilizando o Sloodle.

No trabalho de Pinheiro e Filho (2012), é apresentada uma aplicação de Realidade Virtual utilizada no treinamento continuado para profissionais na área de redes de computadores. Os resultados demonstram o potencial de aplicações RV para treinamento continuado com eficiência e custos reduzidos.

Ferreira et al. (2013) apresentam um Laboratório Virtual para o ensino de redes de computadores inserido em um ambiente virtual de aprendizagem. O Laboratório

Virtual para simulação no Moodle (LVRC) procura atender tanto alunos do ensino presencial quanto alunos de cursos à distância. Os resultados apresentados afirmam que permite o aprendizado do aluno em criação de topologias com isenção de nós e enlaces; configuração de tráfego com os protocolos TCP e UDP entre outras.

Desse modo, é importante ressaltar a relevância destas pesquisas correlacionadas, pois através delas é possível obter um estado da arte sobre o desenvolvimento desta área de estudo. Dentre os trabalhos citados, este se diferencia por permitir o desenvolvimento de topologias de redes, configurar tráfego através dos protocolos, configuração de aplicações FTP e Telnet, simulação de roteamento *unicast* e *multicast* entre outros. Além de um ambiente atrativo e com baixo custo na implantação, no qual o estudante tem a possibilidade de aprender de forma descontraída e divertida.

3. FUNDAMENTAÇÃO TEÓRICA

Nesta seção, uma revisão bibliográfica será apresentada com o objetivo de prover um embasamento teórico referente aos tópicos abordados neste trabalho. São explanados os conteúdos referentes ao ensino de Redes de Computadores, jogos sérios e CyberCIEGE, bem como, *design* instrucional.

3.1 Aplicações de jogos digitais na área de Redes de Computadores

A ausência de laboratórios físicos para a realização de atividades práticas nas instituições de ensino é um dos maiores desafios da disciplina de RC. Essa carência justifica-se devido ao alto custo de equipamentos de rede e manutenção dos mesmos. Outro fator que impede a realização de atividades práticas é o número insuficiente de equipamentos para atender a todos os alunos. Para Medina (2004), uma alternativa para solucionar esses problemas é a utilização de laboratórios virtuais, que permitem ao aluno realizar simulações/animações a partir da construção de um percurso formado por etapas, conduzindo-o ao objetivo pretendido, facilitando desta forma, a conceitualização e compreensão dos processos vivenciados e a elaboração das conclusões obtidas a partir desta experiência.

Nesse sentido, Brom et al. (2011) afirma que os jogos digitais educacionais são ferramentas que ajudam no desenvolvimento de conhecimento e habilidades cognitivas, como a resolução de problemas, o pensamento estratégico, a tomada de decisão, entre outras, propiciando uma compreensão mais profunda de certos princípios fundamentais de determinados assuntos.

O CyberCIEGE é uma ferramenta que apresenta essas características, pois disponibiliza um ambiente de simulação que permite a realização de testes em diversos equipamentos constituem uma infraestrutura de redes de computadores, podendo ser explorada para desenvolver atividades práticas e conceitos inerentes a segurança de rede.

3.1.1 CyberCIEGE

O CyberCIEGE é um jogo que disponibiliza um ambiente de simulação, onde são abordados os principais conceitos de segurança de rede. Nesse ambiente, são disponibilizados diversos cenários, cada um apresenta objetivos distintos, porém com a mesma finalidade de manter a rede segura. Essa ferramenta pode ser utilizada auxiliar no ensino de segurança de redes, no entanto é recomendado que os usuários tenham um conhecimento prévio dos conceitos de Redes de Computadores.

O objetivo principal desse jogo é disponibilizar recursos para que usuário utilize da melhor maneira para defender a rede de ataques. Para Irvine et al. (2005), os principais elementos envolvidos nesse jogo são: os mecanismos de simulação, linguagens de definição de cenário, ferramentas de desenvolvimento de cenários, registros de avaliação dos alunos e vídeos explicativos. A partir desses elementos, o CyberCIEGE fornece aos jogadores tarefas como por exemplo, configurar as estações de trabalho, servidores, sistemas operacionais, aplicativos e dispositivos de rede.

Nos seus cenários, o CyberCIEGE inclui *firewalls* configuráveis, VPNs, mecanismos de controle de acesso, entre outros. Os principais tipos de ataques encontrados são cavalo de tróia, *Denial of Service* (DoS), *exploit*, vírus, etc. Logo, é apresentada aos usuários vulnerabilidades na rede, onde é necessário realizar ações para evitar que a rede seja atacada e mantê-la segura. Os usuários devem considerar o dinheiro virtual, para escolher as estratégias para operar e defender as suas redes, evitando investimento desnecessário.

3.2 Design Instrucional

O campo de pesquisa em questão está relacionado ao processo de ensino e aprendizagem englobando diferentes contextos, em que são abordados desde os paradigmas tradicionais na educação até a utilização de novas formas de interação por meio das Tecnologias da Informação e Comunicação (TICs). O seu emprego pode ser aplicado em aulas individuais, cursos presenciais ou à distância, assim como na construção de materiais didáticos e objetos de aprendizagem.

Conforme Filatro (2004), o termo pode ser definido como a ação institucional e sistemática de ensino, que envolve o planejamento, o desenvolvimento e a utilização de métodos, técnicas, atividades, materiais, eventos e produtos educacionais em situações didáticas específicas, a fim de facilitar a aprendizagem humana a partir dos princípios de aprendizagem e instrução conhecidos. Pode também ser definido como a prática de organizar conteúdos e atividades para uma instrução eficaz (KUMAR; LEE, 2009).

Assim, uma abordagem específica para um curso educacional pode ser elaborada utilizando como base os conceitos presentes no Design Instrucional, cujo objetivo irá girar em torno de fornecer melhorias para o processo de aprendizagem dos educandos. Reiser e Dempsey (2007), reforçam estas ideias ao afirmar que o Design Instrucional (DI) é um processo sistemático que é utilizado para desenvolver cursos de educação e formação de uma forma consistente e confiável (REISER; DEMPSEY, 2007). Assim, devem ser seguidas algumas etapas para realizar o planejamento, desenvolvimento e implementação dos programas de ensino, analisando quais métodos e técnicas serão utilizados, sendo o professor o profissional responsável por este arranjo. De acordo com Filatro (2004), o Design Instrucional é desenvolvido nas seguintes fases:

- Análise: levantamento e análise de requisitos para destacar o perfil do público-alvo de seu material, assim como das necessidades e problemas na implantação de um curso ou programa; o estabelecimento de objetivos para o curso.
- Design: abrange a criação da equipe; a definição da grade curricular; a seleção de estratégias pedagógicas e tecnológicas; a fixação de cronogramas.
- Desenvolvimento: compreende a produção e adaptação de materiais impressos e digitais; a montagem de configuração de ambientes; a capacitação de professores e tutores; a definição de suporte técnico e pedagógico.
- Implementação: Constitui-se na situação didática propriamente dita, quando ocorre a aplicação da proposta de Design Instrucional.

- Avaliação: inclui a consideração sobre a eficácia do curso e a eficiência do sistema; a revisão da caracterização da audiência e a análise das estratégias pedagógicas e tecnológicas implementadas.

Com isso, a questão do Design Instrucional foi abordada neste artigo para avaliar como as respostas dos educandos podem auxiliar na montagem e formação dos cursos e disciplinas abordadas neste estudo de caso, de forma a auxiliar os professores a verificarem as dificuldades presentes e com base nisso planejar e desenvolver novas formas para a condução dos conteúdos abordados.

4. ABORDAGEM METODOLÓGICA

Este artigo apresenta uma avaliação sobre a utilização da ferramenta CyberCIEGE em disciplinas de redes de computadores como recurso de apoio e auxílio ao processo de aprendizagem dos educandos. Os conceitos referentes à teoria da aprendizagem significativa de David Ausubel são utilizados para verificar o comportamento dos estudantes ao realizar as atividades na ferramenta tendo como base os conceitos aprendidos anteriormente em sala de aula presencial. Com relação ao uso do CyberCIEGE nas atividades educacionais, objetiva-se que para cada tipo de tarefa proposta para o educando envolvendo a área de ensino de RC, a partir dos conceitos já existentes na estrutura cognitiva do mesmo, ele utilize-as como subsunçores no aprendizado destas novas informações a serem entendidas.

Como exemplo, estão os desafios propostos na ferramenta e os temas abordados em diferentes fases, como segurança da informação, *firewall*, topologia, entre outras, que envolvem novas informações que serão processadas pelo usuário utilizando-se dos conceitos já aprendidos, consequentemente buscando melhorar o processo de aprendizagem dos novos conteúdos apresentados pelo educador.

Agregado a isso, o artigo teve como objetivo também analisar com base nos dados obtidos o retorno dado pelos alunos, suas contribuições e dificuldades identificadas no uso da ferramenta CyberCIEGE e acerca dos conteúdos trabalhados. Assim é possível analisar com base no Design Instrucional, descrito anteriormente na seção 3, as melhorias e mudanças que podem ser realizadas para o planejamento da disciplina de RC.

Para a execução das abordagens descritas anteriormente, foi utilizada a ferramenta CyberCIEGE em uma turma de Graduação do curso de Sistemas de Informação, do quinto semestre, da UFSM. A seleção do jogo sério CyberCIEGE se deu visto que esta envolve problemas semelhantes aos vistos em sala de aula e se encaixa no contexto de uma abordagem colaborativa para a educação. Também proporciona um ambiente com diversos recursos, constantes atualizações e possibilita a criação de novos cenários.

Nesta primeira etapa, foram ministradas duas aulas, nas quais foram abordados diversos conteúdos relacionados à Segurança da Informação e suas ferramentas, buscando desta forma, estabelecer conceitos subsunçores, colaborando para a aprendizagem significativa e preparando os estudantes para os desafios impostos pelos jogos sérios.

A segunda etapa foi constituída de três momentos, onde realizou-se a aplicação do jogo em sala de aula, como segue:

- Primeiro Momento: caracterizou-se pela seleção de cenários, onde foram elaborados padrões de avaliação e métricas a serem utilizadas.
- Segundo Momento: para o entendimento e assimilação dos estudantes ao CyberCIEGE, foi realizada uma aula para a apresentação do jogo e cenários.

- Terceiro Momento: houve a distribuição dos cenários, portanto, foi realizado um sorteio e cada estudante recebeu uma fase para concretizar os objetivos propostos. Também foi disponibilizado um formulário com questões para serem respondidas de forma descritiva, onde o estudante esclareceu quais eram os objetivos da fase e como foram resolvidos, detalhando como sua ação determinou a solução do problema apresentado, e quais foram as dificuldades encontradas.

Por fim, a terceira etapa consistiu na análise das respostas obtidas para verificar a avaliação dos estudantes com relação ao uso da ferramenta CyberCIEGE, quais suas vantagens, desvantagens e dificuldades identificadas por eles. Desta forma, com base nestes resultados foi possível realizar uma análise com o uso da abordagem de DI para propor melhorias e soluções às dificuldades identificadas pelos estudantes, no sentido de fornecer subsídios para um melhor planejamento e desenvolvimento da disciplina de RC.

5. AVALIAÇÃO E ANÁLISE DOS RESULTADOS

Para um melhor entendimento das avaliações realizadas, a análise foi dividida em duas etapas. A primeira correspondeu à esquematização dos cenários existentes no CyberCIEGE com os tópicos correspondentes abordados na disciplina de Redes de Computadores da UFSM no curso de Sistemas de Informação, realizada por meio da análise da ementa adotada na disciplina (Tabela 1).

Na segunda etapa foram analisados os depoimentos dos estudantes, identificando as dificuldades existentes em cada tópico da disciplina abordado, de forma a avaliar se os conceitos subsunçores vistos anteriormente em sala de aula presencial foram suficientes para que os educandos pudessem resolver os problemas propostos no jogo. Por fim, a terceira fase corresponde à formulação das melhorias que podem ser efetuadas na disciplina de RC por meio da abordagem do DI, tendo como base as dificuldades identificadas anteriormente na segunda etapa.

Tabela 1 - Relação da Ementa da Disciplina com tópicos abordados no CyberCIEGE.

Ementa da Disciplina de Redes de Computadores da UFSM	Cenários do CyberCIEGE
Introdução a Redes de Computadores	Todas se aplicam.
Meios de Transmissão: guiados e não guiados	6, 7, 8 e 11.
Extensão e Segmentação da Rede	5, 6, 7, 8 e 11.
Gerência de Redes de Computadores	Todas se aplicam.
Segurança de Redes de Computadores	6, 7, 8 e 10.
✓ Conceitos Básicos	1, 2, 3, 4, 5 e 11.
✓ Ameaças	Todas se aplicam.
✓ Ataque e Defesa	1, 2, 3, 6, 9 e 11.
✓ Políticas de Segurança	Todas se aplicam.
✓ Mecanismos de Segurança	4, 5, 6, 7, 8, 9 e 10.
✓ Principais Vulnerabilidades	1, 2, 3, 4 e 5.
✓ Técnicas para Exploração de Vulnerabilidades	1, 2, 3, 4, 6 e 11.
✓ Técnicas para Obtenção de Informação	1, 2, 3 e 4.
✓ Ferramentas para Intrusão	6 e 11.

A Tabela 1 mostra que diversos tópicos da disciplina de Redes de Computadores puderam ser contemplados em diferentes fases do jogo, o que demonstra que o jogo detém de uma gama variada de áreas com diferentes problemas a serem solucionados. Realizada esta primeira etapa da pesquisa, a segunda fase foi iniciada com a aplicação

do jogo juntamente aos estudantes, que formularam um relatório descritivo sobre os conteúdos expostos nos cenários abordados, com a finalidade de obter um *feedback* dos mesmos. Na sequência disso, foram separados os relatórios por cenários, onde foram avaliadas e analisadas as informações levantadas pelos estudantes, bem como, as contribuições e dificuldades encontradas na utilização desta ferramenta.

Para a avaliação do desempenho e dificuldades encontradas pelos estudantes no decorrer da pesquisa, foram levados em consideração também alguns quesitos existentes no jogo:

- Níveis de Experiência: o CyberCIEGE possui um ranking para medir o nível de experiência do jogador, então quando os estudantes têm seu primeiro contato, ele inicia no nível "Just Starting", mas ao ir completando as Campanhas e seus respectivos Cenários, consequentemente o nível do estudante vai aumentando, podendo chegar a "Expert". Através disso é possível avaliar o desempenho do estudante na realização das campanhas e cenários, pois quanto mais alto seu nível de experiência, significa que mais fases ele completou.
- Status do Cenário: através deste status é possível saber se o estudante completou, abandonou ou realizou parte das fases propostas no cenário, permitindo inclusive o estudante continuar de onde parou. Esta informação influência diretamente no ranking do nível de experiência do estudante e através dela também pode ser avaliado o desempenho dos estudantes.
- Tempo: todos os cenários possuem um temporizador para que os objetivos sejam alcançados durante o tempo estabelecido. Portanto, é possível verificar as marcas de tempo alcançadas por cada estudante e se algum não conseguiu completar no tempo determinado, dessa forma, é possível sugerir para que o Design Instrucional seja readequado para contemplar questões que os alunos não conseguiram resolver no tempo normal.
- Dinheiro: em cada cenário o estudante possuía uma quantia de dinheiro para que fosse possível alcançar os objetivos propostos. Caso o estudante invista em equipamentos desnecessários, provavelmente não irá conseguir alcançar os objetivos determinados e por consequência disso, não conseguirá atingir bons resultados neste cenário.

Na fase "*Introduction Scenario*" são expostos conceitos sobre segurança de redes, com o intuito de apresentar definições iniciais para proteção contra ameaças e prevenção de vulnerabilidades. Nesta fase, dois estudantes haviam sido sorteados e em seus relatos, os estudantes mencionaram os assuntos vistos nos tópicos de "Exploração de Vulnerabilidades" e "Ataque e Defesa". Foi possível identificar indícios de que houve assimilação dos conteúdos teóricos vistos em aula com os abordados pelo CyberCIEGE, o que reforça que os conceitos subsunçores utilizados pelos estudantes foram captados de forma significativa e que a organização inicial da disciplina contempla as exigências necessárias.

Durante a fase "*Starting Scenarios - Patches*", os alunos deveriam manter a segurança de um servidor de aplicação *web*, para tanto foi proposta a utilização de gerenciamento de *patches*. Dois alunos relataram que obtiveram um resultado satisfatório, pois avançaram durante a fase mantendo a rede de computadores virtual ativa em quase sua totalidade.

Porém, um dos alunos não conseguiu a pontuação necessária para realizar a compra de um servidor, porque gastou seus recursos com opções desnecessárias, como treinamentos aos funcionários. Segundo consta em seu relato, os problemas foram ocasionados pela interpretação equivocada das mensagens do sistema e pelo curto espaço de tempo disponibilizado pela ferramenta para a resolução da fase.

A partir destes relatos, percebe-se que os conceitos trabalhados em aula serviram de suporte para a correta resolução dos problemas propostos e que os tópicos abordados foram suficientes. Ressalta-se que mesmo não tendo completado de forma geral os desafios, os motivos não estão ligados ao conteúdo da disciplina, mas às regras existentes no jogo.

A "*Network Traffic Analysis*" é a fase que aborda questões relacionadas ao controle de tráfego da rede, com o objeto de evitar congestionamentos. Um dos estudantes informou que foi possível assimilar os conceitos apresentados em aula com as soluções utilizadas nesta fase, o que mostra a importância dos conceitos subsunçores estarem presentes no processo cognitivo dos educandos. Porém, o outro aluno sorteado para essa mesma fase, citou que este cenário é confuso, devido às muitas opções disponíveis como soluções, dificultando a finalização da fase durante os vinte minutos propostos pela ferramenta.

Tanto a fase "*Mac Integraty*", quanto a "*Mandatory Access Controls*", apresentam um servidor multinível usado para obter um compartilhamento, porém na primeira é abordada a utilização de política de integridade de dados. Foi relatado por um dos alunos que encontrou mais dificuldades na última fase da campanha, que envolve questões de *password*, na qual foi necessário utilizar várias vezes a janela de ajuda, mas que após três tentativas foi possível concluir.

A questão da integridade de dados, conforme ementa da disciplina, envolve uma parte teórica predominante, o que pode ter ocasionado às dificuldades identificadas pelo estudante durante a realização do desafio proposto. Esta questão pode ser considerada como parte de uma possível reformulação da disciplina de acordo com os problemas identificados.

A fase "*User Identification*" explora estratégias para a identificação de usuários dos computadores apresentados nos cenários. O único estudante sorteado para a realização dessa fase expôs que não conseguiu alcançar o objetivo proposto, justificando que a fase é extensa e aborda vários tipos de permissões de usuário, o que dificultou a finalização. Os conceitos referentes a este tópico na disciplina podem não ter abordado de forma extensiva todos os aspectos relevantes envolvendo a questão de permissões de usuário, não fornecendo os subsídios necessários para a realização dos desafios, sendo uma reformulação considerada uma alternativa válida.

Já na fase "*Mandatory Access Controls - MAC Integraty*", segundo o relato de um dos estudantes, foi necessário efetuar a configuração de todos os computadores da rede para obter acesso ao servidor. Também foi necessário alterar as senhas de acesso dos usuários para garantir uma maior segurança e permissões de acesso.

A cada ação que este estudante efetuava, era apresentado um detalhamento sobre a solução e o motivo das ações tomadas, de modo que apresentou um conhecimento sobre as ações que o mesmo tomava. Isso reflete que os conceitos subsunçores trabalhados neste tópico da disciplina abrangem todas as necessidades impostas no jogo, o que acarreta a boa organização deste conteúdo na disciplina.

Na "*Physical Security*" é introduzido zonas de segurança na rede e métodos para proteção de ameaças físicas. Todos os três alunos sorteados para a realização dessa fase conseguiram alcançar os objetivos, finalizando-a com sucesso e sem dificuldades. Os conceitos utilizados como base para a resolução destes problemas foram considerados satisfatórios e suficientes, o que mostra um correto planejamento do tópico da disciplina e a forma de desenvolvimento deste pelo docente.

Com base nisso, com relação à questão envolvendo o Design Instrucional para a disciplina de RC abordada neste artigo, a partir dos testes realizados com o jogo CyeberCIEGE foi possível identificar problemas e propor possíveis melhorias na sua

estrutura geral. A seguir são descritas as alternativas possíveis de serem adotadas no planejamento e desenvolvimento da disciplina.

- Investir na questão de projetos (dinheiro e tempo): dois fatores problemáticos observados durante a execução dos testes foram os atributos de dinheiro e tempo, nos quais os estudantes demonstraram maiores dificuldades em realizar o seu gerenciamento de forma adequada. Para isso, um reforço na parte de desenvolvimento de projetos na disciplina é visto como uma alternativa válida para fornecer um maior nível de experiência dos estudantes envolvendo estes tipos de questões.
- Parte prática da disciplina: em tópicos como Integridade de Dados e Permissões dos Usuários, que envolviam a solução de problemas práticos, os alunos demonstraram maiores dificuldades em relação aos demais cenários abordados. Isso se deve ao caráter teórico predominante na disciplina, que engloba muito pouco os aspectos práticos vistos em exemplos na sala de aula. Como solução, o uso de ferramentas da área de Redes, como Cisco Packet Tracer e Network Stumbler podem ser consideradas alternativas à solução destas questões, assim como laboratórios virtuais.
- Planejamento da disciplina: foi observado que no planejamento da disciplina são considerados diversos aspectos puramente teóricos, sendo minoria os tópicos que envolvem ações práticas. Essa mescla pode ser importante para o desenvolvimento do estudante com relação aos conteúdos teóricos vistos em sala de aula, pois os problemas reais que serão solucionados por eles exigem uma aptidão prática mais completa.

Foram apresentados alguns pontos específicos dentro do planejamento e desenvolvimento da disciplina seguindo a abordagem do Design Instrucional que poderiam ser melhoradas com o objetivo de fornecer maiores subsídios para os estudantes na realização das atividades práticas. Além disso, foi observado que os conceitos subsunçores envolvendo a grande maioria dos tópicos na disciplina foram considerados suficientes para a resolução dos desafios apresentados, o que representa que a organização da disciplina está adequada, necessitando somente de algumas modificações envolvendo principalmente a parte prática dos conteúdos vistos em sala de aula.

6. CONCLUSÃO

A implantação de jogos na educação vem crescendo rapidamente devido a abordagem que é utilizada. Através do uso de jogos sérios, é possível propor aos estudantes o exercício dos seus conhecimentos em cenários virtuais, de simulação e treinamento, permitindo maior interatividade, além de possibilitar a tentativa e erro sem prejudicá-lo.

Este artigo apresentou a aplicação do jogo sério CyberCIEGE em uma disciplina de RC, proporcionando aos alunos praticarem os conhecimentos construídos em sala de aula, para que, a partir da conclusão das fases pudessem assimilar os conteúdos abordados. Para tanto, foram selecionados os cenários do jogo que abordavam assuntos contidos na ementa da disciplina que tinham relação com segurança em redes. Ao finalizar as interações com o jogo, os estudantes foram submetidos a uma avaliação, onde foram questionados aspectos tais como: os objetivos da fase e quais foram as ações tomadas para solucioná-los, bem como, quais dificuldades foram encontradas.

Ao mesmo tempo, levou-se em consideração os resultados apresentados pelo próprio jogo, onde foi possível observar o nível de experiência que o usuário alcançou, o qual está relacionado aos cenários concluídos pelo aluno. E ainda, o próprio *status* dos

cenários, o tempo de realização e o dinheiro investido em cada fase. Estas informações foram imprescindíveis, aliadas aos relatos dos estudantes, para a formulação das sugestões de melhorias no Design Instrucional da disciplina.

Como trabalho futuro, pretende-se realizar uma nova avaliação utilizando o jogo sério CyberCIEGE com outra turma e abrangendo as novas sugestões de melhorias no Design Instrucional da disciplina, conforme apontadas na Seção 5. Desta forma, será possível evidenciar se houve algum ganho ou contribuição no aprendizado destes estudantes a partir das alterações realizadas na estrutura da disciplina. Outra possibilidade que pode ser abordada nos próximos trabalhos, é a implementação de novos cenários, enfatizando novos objetivos e desafiando o estudante em outros assuntos de segurança em redes.

[1] Disponível em: <http http://cisr.nps.edu/cyberciege/downloads/setup-demo.exe>

REFERÊNCIAS BIBLIOGRÁFICAS

ADAMS. E. “Fundamentals of game design”, In: **New Riders, 2th edition**. 2010.

BROM, C., PREUSS, M. e KLEMENT, D. “Are educational computer micro-games engaging and effective for knowledge acquisition at high-schools? A quasi-experimental study”. In: **Computers & Education**, 57(3), p.1971-1988. 2011.

FERREIRA, K. H. A., LIMA, R. W., LIMA, M. V. A., CHAVES, J. O. M., ROCHA, A. "LVRC – Laboratório Virtual web para o ensino de Redes de Computadores no Moodle". In: **Nuevas Ideas En Informática Educativa TISE 2013**. v. 9, p. 539-541. 2013.

FILATRO A. “**Design Instrucional Contextualizado: Educação e Tecnologia**”. São Paulo: Editora Senac, 2004.

IRVINE, C. E., THOMPSON, M. F., ALLEN, K. “CyberCIEGE: Gaming for Information Assurance”, In: **IEEE Security and Privacy**, May/June, pp. 61-64. 2005.

KUMAR, V. e LEE, S. “Opens instructional design”. In: **International workshop on technology for education**, aug 4-5, Bangalore. Anais Bangalore: IEEE, p. 42-28, 2009.

MEDINA, R. D. "**ASTERIX: Aprendizagem significativa e tecnologias aplicadas no ensino de redes de computadores: integrando e explorando possibilidades**". In: Porto Alegre - UFRGS, 174p. Tese de Doutorado. 2004.

MITAMURA, T.; SUZUKI, Y.; OOHORI, T. “Serious games for learning programming languages”. In: **Systems, Man, and Cybernetics (SMC)**, 2012 IEEE International Conference on, pp.1812, 1817, 14-17 Oct. 2012.

PINHEIRO, C. D. B., FILHO, M.R. "LVR – Laboratório Virtual de Redes Protótipo para Auxílio ao Aprendizado em Disciplinas de Redes de Computadores". In: **XVI Simpósio Brasileiro de Informática na Educação (SBIE)**. 2005.

REISER, R. A. e DEMPSEY, J. V. “Trends and Issues in Instructional Design”. In: **Upper Saddle River, New Jersey: Pearson Education**, Inc, 2007.

VOSS, G. B., NUNES, F. B., MEDINA, R. D. “Proposta de um jogo sério para o ensino de redes de computadores no ambiente virtual 3D OpenSim”. In: **XII Simpósio Brasileiro de Games e Entretenimento (SBGames)**. 2013.