Jogo Sério na Educação: Uma Abordagem para Ensino-Aprendizagem de Redes de Computadores (Fase II)

Fabrício Herpich[1], **Rafaela R. Jardim**[1], **Ricardo F. da Silva**[1], **Gleizer B. Voss**[1], **Felipe B. Nunes**[1], **Roseclea D. Medina**[1]

[1] Universidade Federal de Santa Maria (UFSM)
Programa de Pós-Graduação em Informática (PPGI)
Santa Maria – RS – Brasil

{fabricio.herpich, rafa.rjardim, ricardosma, gleizer.voss,

nunesfb, roseclea.medina}@gmail.com

Abstract. *The serious games are simulated environments that enable test, hit and miss several times, respecting the time cognitive educating, assisting for your learning and practical application. In this context, the serious games emerge as educational technology through interactive software that aims to simulate the real environment, which in essence are critical, precise or expensive. This paper presents an analysis tool, CyberCIEGE and its application in the classroom teaching Security for Computer Networks, where it was possible to verify its contribution to the cognitive development of students through concepts subsumers and exposure to different scenarios.*

Resumo. *Os jogos sérios são ambientes simulados que possibilitam testar, acertar e errar diversas vezes, respeitando o tempo cognitivo do educando, auxiliando para o seu aprendizado e aplicação prática. Neste contexto, os jogos sérios surgem como tecnologia educacional por meio de softwares interativos que tem como objetivo simular os ambientes reais, que em sua essência são críticos, precisos ou caros. Este artigo apresenta uma análise da ferramenta CyberCIEGE e a sua aplicação em sala de aula no ensino de Segurança para Redes de Computadores, onde foi possível verificar sua contribuição para o desenvolvimento cognitivo dos estudantes, por meio de conceitos subsunçores e a exposição à diferentes cenários.*

1. Introdução

Composta por um conjunto de computadores ou outros dispositivos interligados entre si, as Redes de Computadores (RC) estão cada vez mais presentes em nosso cotidiano, seja nas empresas, residências, instituições de ensino e até mesmo na utilização de um terminal eletrônico do banco. [Tanenbaum 2003], define redes de computadores como um conjunto de computadores interconectados por uma única tecnologia.

Para administrar e manter estas redes em funcionamento, as organizações necessitam de profissionais capacitados que têm a tarefa de realizar o projeto físico e lógico, instalar *softwares*, gerenciar serviços e principalmente manter o bom desempenho, disponibilidade e segurança. No entanto, o ensino de redes de computadores não é uma

tarefa trivial, pois muitas vezes os conceitos não são bem apresentados, tornando as aulas monótonas, quando somente o professor interage na maior parte do tempo.

Desse modo, um dos desafios enfrentados pelo professor, é a dificuldade de preparar o aluno para a prática profissional em um ambiente acadêmico, para tanto, cabe ao professor encontrar um meio de realizar atividades práticas que despertem o interesse do educando, ao invés de ministrar apenas aulas teóricas. Neste contexto, [Voss et al. 2012] afirma que através da utilização de tecnologias digitais é possível facilitar o aprendizado do aluno com atividades, simulações e exercícios que complementam a fixação dos assuntos.

Neste sentido, os jogos sérios podem ser uma alternativa, pois já estão inseridos no cotidiano de muitas crianças, jovens e adultos, sendo utilizados como forma de entretenimento. Em geral, podem ser definidos como uma atividade lúdica e realizada no contexto de uma realidade simulada [Adams 2010]. Para [Mitamura et al. 2012], os chamados jogos sérios, têm recebido uma atenção significativa e tem havido um movimento ativo para que efetivamente enriqueçam os ambientes de aprendizagem.

Nesta perspectiva, a ferramenta CyberCIEGE (versão de avaliação 1.9v1)[1] foi escolhida pelo fato de apresentar inúmeros cenários e problemas recorrentes à Segurança de Redes de Computadores. Outro fator que influenciou na escolha desta ferramenta foi a possibilidade de desenvolver novos cenários e por apresentar uma documentação completar, incluindo materiais de apoio. Além desse, é possível citar como exemplos de jogos sérios o TCN5 de [Voss et al. 2013] e o JETS de [Da Silva 2012].

Diante deste contexto, este artigo tem como objetivo descrever a continuidade do trabalho realizado por [Herpich et al. 2013], demonstrando 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.

2. Trabalhos Relacionados

Com o auxílio de ambientes virtuais imersivos, de laboratórios virtuais e de jogos sérios para o ensino de Redes de Computadores, é possível expandir às possiblidades de aprendizagem dos estudantes, por meio de uma abordagem diferenciada, pois estes jogos sérios, possibilitam a simulação de situações reais nas condições e circunstâncias reais, que em muitas vezes são críticas ou caras de serem realizadas. No caso da disciplina de RC, 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.

No trabalho de [Voss et al. 2012], são apresentadas sugestões de uso de laboratórios virtuais na disciplina de RC, no qual a utilização da ferramenta deverá considerar os conteúdos a serem apresentados aos alunos. Foi efetuada uma pesquisa sobre planos de ensino e conteúdos apresentados em três universidades, onde foram apontadas diversas ferramentas para aprendizado, destacando as suas características. Além disso, foram propostas atividades de acordo com os temas da disciplina com o intuito de verificar se

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

as ferramentas estudadas atendem aos objetivos no ensino-aprendizado. Os resultados demonstraram que é possível abordar tais temas articulando-os com a utilização das ferramentas, contribuindo para uma melhor reflexão e compreensão desses.

No trabalho de [Hassan 2003], é apresentado um laboratório virtual 3D de Redes de Computadores que foi desenvolvido em Virtual Reality Modeling Language (VRML) integrada aos vários tipos de mídias disponíveis (e.g., texto, imagem, animação, áudio e vídeo). O objetivo principal deste trabalho foi fornecer um ambiente de aprendizado possibilitando a prática e desenvolvimento de habilidades em trabalhos em grupo.

Já [Gurgel et al. 2012], utilizou a ferramenta de simulação Netkit para realização de onze atividades práticas nas disciplinas: Administração e Gerenciamento de Redes do ICMC/USP. Os laboratórios virtuais de redes incluem dispositivos de *hardware* necessários para seu gerenciamento, bem como os enlaces virtuais que os interligam. Esta ferramenta proporciona a criação de laboratórios com ambientes projetados para situações específicas e também permite que o aluno configure a rede virtual desde o início, para que além de compreender conceitos, aprendam a configurar redes.

É importante ressaltar a relevância destas pesquisas, pois através delas se obtêm um panorama geral sobre o desenvolvimento desta área de estudo. Dentre os trabalhos citados, este se diferencia por permitir o desenvolvimento de novos cenários, com novos objetivos e desafios aos aprendizes. Além de proporcionar um ambiente lúdico e imersivo, no qual o estudante tem a possibilidade de aprender de forma descontraída e divertida.

3. Fundamentação Teórica

Nesta seção, é apresentada uma revisão bibliográfica, onde são explanados os conteúdos referentes ao ensino de Redes de Computadores, jogos sérios e CyberCIEGE.

3.1. Desafios no Ensino de Redes de Computadores

O ensino destes conteúdos não é uma tarefa fácil, embora seja possível ensinar por meio de livros, conceitos e teorias, a realização de atividades práticas é um fator de grande relevância no processo educacional. Segundo [Voss et al. 2013], um dos principais problemas identificados nessas atividades é a falta de utilização de ferramentas de forma pontual.

Outro desafio refere-se à ausência de um laboratório físico para a realização das atividades nas instituições de ensino, devido ao custo envolvido com aquisição e manutenção dos equipamentos, tais como *switches* e servidores, bem como a elevada taxa de obsolescência dos mesmos. A disponibilidade de equipamentos suficientes para o número de alunos também é outro fator que dificulta a realização de atividades práticas.

Para [Pinheiro et al. 2009], a utilização de ambientes simuladores podem representar situações e comportamentos difíceis de serem representados na vida real, servindo no preparo e treinamento de alunos. É o caso do jogo CyberCIEGE, que disponibiliza um ambiente onde pode-se testar diversos recursos para Segurança de Informação, proporcionando um ganho não só no que diz respeito à aprendizagem de conceitos, como também uma economia considerável em relação aos equipamentos necessários às demonstrações.

3.2. Jogos Sérios na Educação

A utilização de jogos sérios no processo de ensino-aprendizagem está em constante crescimento. Conforme Valente (2002) apud [Netto and Dos Santos 2012], isso ocorre devido a um ambiente favorável que desperta o interesse do aluno e o motiva a explorar, pesquisar e refletir.

De acordo com [Adams 2010], jogos sérios podem ser definidos como uma atividade lúdica realizada no contexto de uma realidade simulada, no qual os participantes tentam alcançar, pelo menos uma meta arbitrária, não trivial, agindo de acordo com as regras. Sendo vistos como uma ferramenta educacional de grande potencial a ser explorado quando aplicada em sala de aula. Estes jogos voltados à educação, de acordo com [Sweetser and Wyeth 2005], introduzem um modelo capaz de expor o aluno há oito diferentes tipos de experiências, que são conseguidas através da utilização e envolvimento do aluno, são eles: concentração, desafio, habilidades, habilidades de controle, objetivos claros, *feedback*, imersão e interação social.

O uso de jogos sérios permite uma experiência mais concreta, maior interação com conceitos específicos. Além disso, o formato dos jogos têm um atrativo maior, conseguindo atingir até alunos com problemas de atenção [Cone et al. 2006]. A aplicação de jogos e simulações é uma oportunidade para os alunos aplicarem conhecimentos e realizarem experimentos em um ”mundo virtual seguro”sem consequências reais [Pivec 2007]. Assim, o aprendizado baseado em jogos pode ser utilizado em conjunto com o ensino de sala de aula, adicionando novas formas de aprendizado e de aquisição de conhecimento.

3.3. Jogo Sério CyberCIEGE

É um jogo com ambiente interativo que tem como finalidade abordar aspectos de Segurança de Tecnologia da Informação (TI), através de gerenciamento de recursos e de políticas de segurança. Nele o usuário é exposto a tarefas, onde precisa ter um prévio conhecimento dos conceitos de RC para então poder solucioná-los.

Segundo [Irvine et al. 2005a], os elementos do CyberCIEGE são: mecanismo de simulação, linguagem de definição de cenário e ferramenta de desenvolvimento, registros de avaliação dos alunos e vídeos explicativos. O objetivo principal deste jogo é proporcionar medidas de segurança necessárias na tentativa de proteger a organização de TI. O CyberCIEGE possui *firewalls* configuráveis, VPNs, mecanismos de controle de acesso, entre outros. Segundo [Irvine et al. 2005b], existem diferentes tipos de ataques, tais como: Cavalo de Tróia, Denial of Service (DoS), Exploit, Vírus, entre outros ataques existentes.

O CyberCIEGE está organizado em cenários, onde são abordados tópicos referentes à Segurança de RC. Abrange uma visão geral onde o aluno precisa manter a segurança e disponibilidade da RC, por meio de configurações nos equipamentos e até mesmo o treinamento de funcionários. Em cada cenário é apresentada uma ou mais vulnerabilidades na rede, onde o aluno tem como propósito realizar ações e tomar as medidas necessárias para mantê-la segura, sendo que todas as providências tomadas estão sob avaliação e somente as medidas necessárias devem ser aplicadas, evitando gastos excessivos e desnecessários.

4. Metodologia

O desenvolvimento deste estudo surgiu através da necessidade de identificar uma ferramenta que pudesse contribuir e auxiliar o aluno em seu processo de aprendizagem na disciplina de Redes de Computadores, onde foi constatado uma dificuldade dos alunos em assimilar conceitos relacionados à Segurança da Informação, por se tratarem de assuntos demasiados teóricos, complexos e com pouco estímulo à prática.

Diante desse contexto, este estudo vislumbra identificar as principais características deste jogo (e.g., seus cenários e componentes), bem como suas vantagens e desvantagens como uma ferramenta de apoio ao processo de ensino-aprendizagem. Para apurar maiores resultados, foi aplicado em uma turma de Graduação do curso de Sistemas de Informação, do quinto semestre, da Universidade Federal de Santa Maria (UFSM). Para a realização deste trabalho, duas etapas foram previamente projetadas, como segue.

A primeira etapa caracterizou-se pelo levantamento do referencial teórico sobre o tema e os assuntos relacionados, e a seleção do jogo sério CyberCIEGE, o qual envolve problemas semelhantes aos abordados 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 implementação 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, conforme visto em [Medina 2004], 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 (Figura 1), onde foram elaborados padrões de avaliação e métricas a serem utilizadas. Para tanto, os critérios aplicados na seleção de cenários foram determinados por meio de avaliações e testes coordenados pelos autores, com a finalidade de selecionar somente aqueles condizentes com o nível abordado em cursos de graduação e que enfatizassem os recursos e ferramentas para Segurança da Informação.
- Segundo Momento: para o entendimento e assimilação dos estudantes ao jogo, foi realizada uma aula para a apresentação do jogo e cenários. Neste momento, foi solicitado que utilizassem os cenários preliminares como treinamento, com a finalidade de proporcionar um nivelamento dos estudantes perante o jogo, onde também tiveram a oportunidade de esclarecer suas dúvidas sobre a ferramenta.
- Terceiro Momento: para que houvesse uma distribuição igualitária dos cenários, foi realizado um sorteio com as fases selecionadas no Primeiro Momento. Dessa forma, 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 durante a execução.

É importante salientar que anteriormente e durante a realização destas etapas, haviam sido disponibilizados materiais de auxílio para os estudantes no Ambiente Virtual

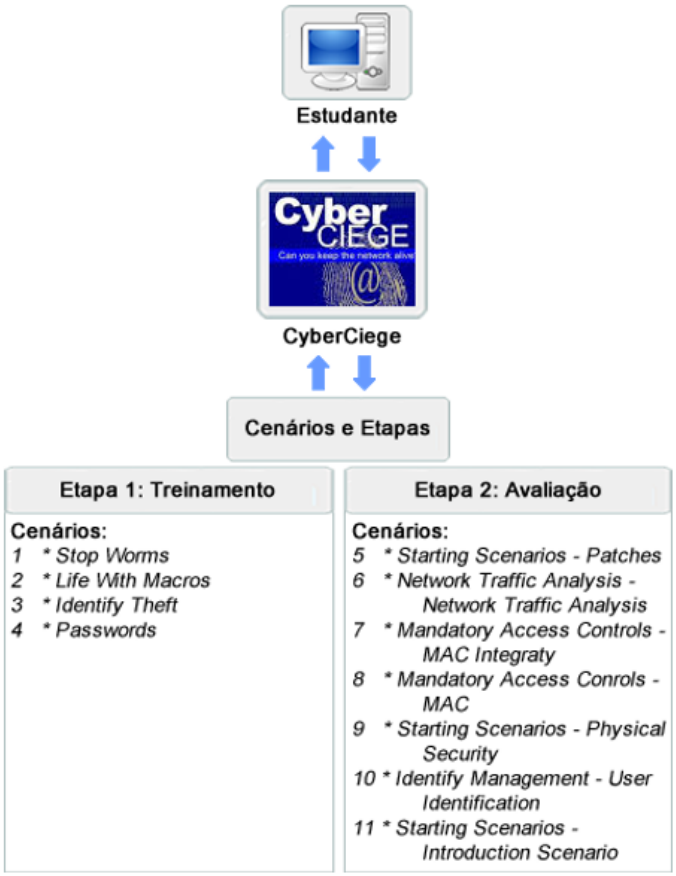


Figura 1. Cenários do CyberCIEGE selecionados.
Fonte: [Herpich et al. 2013]

de Aprendizagem (AVA) Moodle[2], o qual é utilizado amplamente pelos cursos da Universidade Federal de Santa Maria (UFSM) como ferramenta colaborativa no processo de ensino-aprendizagem.

Neste ambiente, foram incorporados vídeos do CyberCIEGE, *links*, documentação (manuais) da ferramenta, como também resumos adaptados pelos autores. Além disso, os autores envolvidos nessa pesquisa apoiaram e sanaram as dúvidas que frequentemente surgiram durante o desenvolvimento das avaliações.

5. Avaliação e Análise dos Resultados

Para um melhor entendimento das avaliações realizadas a análise foi dividida em duas etapas, onde na primeira foram selecionados os cenários que foram utilizados durante o nivelamento e treinamento dos estudantes. Na segunda etapa foram selecionados os cenários que seriam empregados durante a avaliação desta ferramenta em sala de aula.

Para a seleção destas fases, primeiramente houve uma análise da ementa adotada na disciplina de Redes de Computadores. Por meio desta, foram relacionados os tópicos condizentes com as fases propostas no CyberCIEGE (Tabela 1).

Após a aplicação do jogo aos estudantes, foi solicitado que esses formulassem um

[2]Moodle. Disponível em: http://www.moodle.org.br/

Ementa da Disciplina de Redes de Computadores ("Universidade X")	**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.

Tabela 1. Relação da Ementa da Disciplina com o CyberCIEGE.
Fonte: [Herpich et al. 2013]

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 cenário, onde foram avaliadas e analisadas as informações levantadas pelos estudantes, bem como, as contribuições e dificuldades encontradas na utilização desta ferramenta.

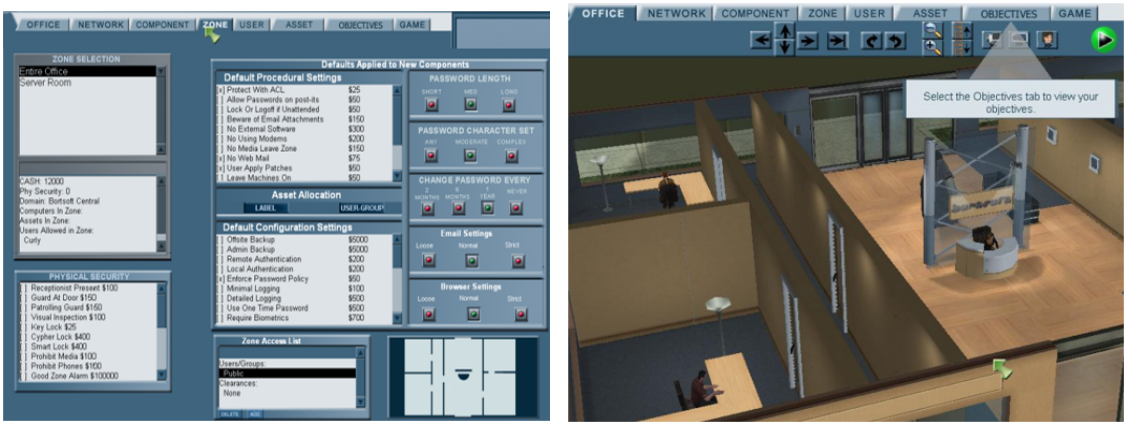
Na fase ”Introduction Scenario”são expostos conceitos sobre segurança de redes, com o intuito de apresentar definições iniciais para proteção contra ameaças e prevenção de vulnerabilidades. Nesta fase, dois estudantes haviam sido sorteados e diante de seus relatos, foi possível identificar indícios de que houve assimilação dos conteúdos teóricos vistos em aula com os abordados pelo CyberCIEGE. De forma que em ambos os relatos entregues, os estudantes mencionaram os assuntos abordados nos tópicos de ”Exploração de Vulnerabilidades”e ”Ataque e Defesa”(Tabela 1).

Durante a fase ”Starting Scenarios - Patches”, o objetivo dos estudantes era 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. Um dos alunos resolveu todos os problemas que surgiram através das dicas do ambiente, enquanto o outro não alcançou os objetivos. Conforme relato do mesmo, 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 alunos estavam envolvidos com o jogo, explorando os cenários e buscando resolver os problemas expostos.

A ”Network Traffic Analysis”é a fase que aborda questões relacionadas ao controle de tráfego da rede e tem como objeto de evitar congestionamentos. Um dos estudantes informou que foi possível assimilar os conceitos apresentados em aula com as soluções utilizadas nesta fase. Porém, o outro aluno sorteado para essa mesma fase, citou que este

cenário é confuso, devido às muitas opções disponíveis como soluções (Figura 2 - (a)), 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. Um dos dos alunos relatou que encontrou mais dificuldades na última fase da cena, que envolve questões de *password*, na qual foi necessário utilizar várias vezes a janela de ajuda, mas que após três tentativas foi possível concluir. Sendo assim, pode ser abordado como um indicativo de que este estudante não estava atento às orientações iniciais e objetivos do jogo (Figura 2 - (b)).



(a) Componentes e Ferramentas do jogo. (b) Cenário e Objetivos do jogo.

Figura 2. CyberCIEGE
Fonte: [Herpich et al. 2013]

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.

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.

Na ”Physical Security”são introduzidas as zonas de segurança na rede e métodos para proteção de ameaças físicas. Os os três alunos sorteados para a realização dessa fase conseguiram alcançar os objetivos, finalizando-a com sucesso e sem dificuldades. Cabe ressaltar que um estudante manifestou que seu interesse por segurança de RC aumentou após conhecer os inúmeros mecanismos e ferramentas que podem ser implementadas em um ambiente, de maneira semelhante às proporcionadas pelo jogo CyberCIEGE. Também foi citado por outro estudante a importância de visualizar a aplicação dos conceitos abordados em aula em um ambiente diferente do meio escolar.

6. Conclusão

A utilização de jogos sérios vem despontando como uma ferramenta de grande potencial para a educação, proporcionando ao estudante exercitar seus conhecimentos em cenários virtuais, permitindo maior interatividade. Este artigo apresentou uma análise relacionando os conteúdos abordados na ementa da disciplina de RC com os trabalhados pelo jogo sério CyberCIEGE, bem como, a aplicação deste em sala de aula.

Através dos relatos solicitados aos estudantes, foi possível identificar indícios de que esta simulação proporcionou um ambiente capaz de promover diversas experiências, diminuindo a probabilidade de erros, como na compra de equipamentos na efetiva prática profissional, já que estes processos envolvem altos valores. Nestes relatórios, os estudantes descreveram os problemas enfrentados durante a execução do jogo sério, detalhando a solução e cada ação que foi tomada, bem como, o motivo para estas ações.

Dessa forma, foram evidenciados indicativos que estes estudantes utilizaram os conceitos teóricos observados em sala de aula, de forma a solucionar as atividades propostas no jogo sério. Também é importante ressaltar que os estudantes apontaram desvantagens e dificuldades durante a execução do jogo. Foi evidenciado que máquinas sem placa de vídeo não permitem a visualização correta dos cenários, em decorrência disto evidenciou-se diversos problemas, tais como, limitação das ações dos estudantes no jogo, como também, a insatisfação e desistência destes durante as atividades propostas. Outra desvantagem apontada por estes estudantes está relacionada ao pouco tempo para resolver as fases, visto que por padrão cada cenário dispõe de vinte minutos para ser resolvido.

Como resultado geral, foi possível observar que os jogos sérios, enfatizando a utilização da ferramenta CyberCIEGE, possuem um grande potencial para colaborar no processo de ensino-aprendizagem. Dentre os quinze relatos enviados pelos estudantes, doze abordam indícios de que houve aprendizagem utilizando o *software* e que o jogo conseguiu relacionar todo o conteúdo teórico visto em sala de aula, sendo que apenas três destes relatos evidenciam que o jogo foi negativo. Porém, é importante frisar que a justificava dada por estes três contemplam: linguagem complicada (versão em inglês); muitos objetivos por fase; alguns erros e problemas na visualização dos cenários.

Como trabalhos futuros, pretende-se fomentar a disseminação de jogos sérios para a educação e contribuir através do estudo de novas ferramentas, como também, desenvolver novos cenários abordando diferentes objetivos, desafios e problematização para o CyberCIEGE. Também, se almeja em pesquisas futuras, abranger o conceito colaborativo destas tecnologias educacionais, visando proporcionar maior interação entre os participantes, sobretudo incentivando o diálogo-problematizador sobre as atividades.

Referências

Adams, E. (2010). Fundamentals of game design. *New Riders, 2th edition*.

Cone, B. D., Thompson, M. F., Irvine, C. E., and Nguyen, T. D. (2006). Cyber Security Training and Awareness Through Game Play. *IFIP International Federation for Information Processing*, 201:p. 431–436.

Da Silva, T. G. (2012). Jogos Sérios em Mundos Virtuais: uma abordagem para o ensino-aprendizagem de teste de Software. *Santa Maria: Universidade Federal de Santa Maria. Dissertação de Mestrado*, page p. 84.

Gurgel, P., Barbosa, E., and Branco, K. (2012). A ferramenta netkit e a virtualização aplicada ao ensino e aprendizagem de redes de computadores. *XXXII Congresso da Sociedade Brasileira de Computação (CSBC)*.

Hassan, E. (2003). Laboratório Virtual 3D para ensino de Redes de Computadores. *XIV Simpósio Brasileiro de Informática na Educação (SBIE)*.

Herpich, F., Jardim, R. R., Da Silva, R. F., Nunes, F. B., Voss, G. B., and Medina, R. D. (2013). Jogos Sérios na Educação: Uma Abordagem para Ensino-Aprendizagem de Redes de Computadores (Fase I). *Nuevas Ideas en Informática Educativa TISE 2013*, v. 9:p. 617–620.

Irvine, C. E., Thompson, M. F., and Allen, K. (2005a). Cyberciege: An extensible tool for information assurance education. *Proceedings of the 9th Colloquium for Information Systems Security Education*.

Irvine, C. E., Thompson, M. F., and Allen, K. (2005b). CyberCIEGE: Gaming for Information Assurance. *IEEE Security and Privacy*, pages p. 61–64.

Medina, R. D. (2004). ASTERIX: Aprendizagem significativa e tecnologias aplicadas no ensino de redes de computadores: integrando e explorando possibilidades. *Porto Alegre - Universidade Federal do Rio Grande do Sul. Tese de Doutorado*, page p. 174.

Mitamura, T., Suzuki, Y., and Oohori, T. (2012). Serious games for learning programming languages. *Systems, Man, and Cybernetics (SMC)*, pages p. 1812–1817.

Netto, D. P. D. S. and Dos Santos, M. W. A. (2012). AlfaGame: Um Jogo para auxílio no processo de alfabetização. *XXIII Simpósio Brasileiro de Informática na Educação (SBIE)*.

Pinheiro, R. P., Lins, F. A. A., and De Melo, J. C. B. (2009). A Utilização de Simulação no Ensino de Redes de Comptuadores. *IX Jornada de Ensino, Pesquisa e Extensão - JEPEX*, pages 1–3.

Pivec, M. (2007). Play and learning: potentials of game-based learning. *British Journal of Educational Technology*, v. 38.

Sweetser, P. and Wyeth, P. (2005). GameFlow: a model for evaluating player enjoyment in games. *Computers in Entertainment (CIE)*, v. 3.

Tanenbaum, A. S. (2003). Redes de computadores. trad. por vandemberg d. de souza. *Rio de Janeiro: Elsevier - 6a Reimprissão*.

Voss, G. B., Medina, R. D., Amaral, E. M. H., Araújo, F. V., Nunes, F. B., and Oliveira, T. B. (2012). Proposta de utilização de laboratórios virtuais para o ensino de redes de computadores: Articulando ferramentas, conteúdos e possibilidades. (fase i). *Revista Novas Tecnologias na Educação (RENOTE)*, v. 10(n. 2):1–10.

Voss, G. B., Nunes, F. B., Oliveira, T. B., and Medina, R. D. (2013). Tcn5 - desenvolvimento de um laboratório virtual de redes de computadores sensível ao contexto. *XXXIII Congresso da Sociedade Brasileira de Computação (CSBC)*.