UMA PROPOSTA DE FORMAÇÃO ON-LINE SOBRE SEGURANÇA DA INFORMAÇÃO: ALIANDO TEORIA E PRÁTICA

William da Silva Melo [1], Francisco Kelsen de Oliveira [2]
[1] Instituto Federal do Piauí (IFPI) 64750-000 – Paulistana – PI – Brazil.
[2] Instituto Federal do Sertão Pernambucano (IFSertão-PE) 56000-000 – Salgueiro – PE – Brazil.

williamdasilvamelo@gmail.com, francisco.oliveira@ifsertao-pe.edu.br

Abstract

Research project at master's level presented in the Post-Graduation Program in Professional and Technological Education (PROFEPT) of the Federal Institute of Education, Sciences and Technology of Sertão Pernambucano (IF Sertão-PE). This study consists of the elaboration of a proposal for online training, open and massive, focused on information security (IS). The methodology includes systematic literature review, action research and exploratory descriptive approach. Expected outcomes include promoting awareness of the safe use of the digital medium and dissemination to the academic community of key teaching / learning approaches and strategies adopted in MOOCs and IS.

Resumo

Projeto de pesquisa a nível de mestrado apresentado no programa de Pós-Graduação em Educação Profissional e Tecnológica (PROFEPT) do Instituto Federal de Educação, Ciências e Tecnologia do Sertão Pernambucano (IF Sertão-PE). Esse estudo consiste na elaboração uma proposta de formação on line, aberta e massiva, voltada para temática da segurança da informação (SI). A metodologia abarca revisão sistemática da literatura, pesquisa-ação e abordagem exploratório descritiva. Os resultados esperados incluem promover uma conscientização acerca do uso seguro do meio digital e disseminação junto à comunidade acadêmica sobre as principais abordagens e estratégias de ensino/aprendizagem adotadas nos MOOCs e na SI.

PALAVRAS-CHAVE: MOOC, Curso Online Aberto e Massivo, Ensino Profissional Tecnológico.

1) Introdução (problema de pesquisa e caracterização da contribuição)

A informação vem assumindo um caráter estratégico e tem sido considerado um ativo crítico para os mais diversos tipos de pessoas e instituições. O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação (ABNT, 2013). De acordo com Foina (2015), uma informação terá maior probabilidade de ser atacada quanto maior o valor que ela tiver.

Diante dos impactos que o vazamento de informações sigilosas pode causar e considerando as ameaças que circundam o meio digital, nota-se uma preocupação muito grande com a segurança da informação e uma necessidade de educação para que as pessoas e instituições possam se proteger desses riscos. De acordo com Lyra (2015) as pessoas devem ser treinadas e educadas sobre quais são as informações que devem ser protegidas e como devem protegê-la além disso, elas devem estar aptas a identificar situações de riscos na segurança da informação através de programas de treinamento e conscientização constantes.

O uso das ferramentas digitais e a popularização do acesso a internet trouxeram inúmeros benefícios para as pessoas, por outro lado, o espaço cibernético tem se mostrado um meio repleto de perigos, com potencial danoso muito alto, que se não usado com segurança resultam na exposição dos ativos de informação. Disseminação de vírus, acesso indevido a dados sigilosos, fraudes financeiras, cyberbullying e sequestro de dados (Ransomwere) são só alguns exemplos de ameaças que circundam o ciberespaço.

A cada ano, o World Economic Forum (WEF), fórum econômico mundial elabora um relatório evidenciando os principais riscos que podem interferir no crescimento global. Atualmente, os ataques cibernéticos ocupam a terceira posição no ranking de ameaças com maior probabilidade de ocorrerem, seguido por roubos ou fraudes de dados (4ª posição), que também têm relação direta com a segurança cibernética (WEF, 2018). Já, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), grupo responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no país afirma que os registros de ocorrências como: Fraudes digitais, Invasões, ataques de negação de serviço, dentre outros, cresceram quase 30% de

2016 para 2017 chegando a um total de oitocentos e trinta e três mil setecentos setenta e cinco (833.775) incidentes (PONTOBR, 2018).

Se observarmos os estudos relativos a segurança da informação iremos verificar uma predominância do público focado em gestores de Tecnologia da Informação (TI) e/ ou funcionários de organizações. Por outro lado, as pesquisas que tem como público dos estudantes são quase inexistentes (LYRA, 2015). Convém observarmos, que os estudantes do ensino profissional e tecnológico (EPT) que segundo o Ministério da Educação BRASIL (2018) "é uma modalidade educacional prevista na Lei de Diretrizes e Bases da Educação Nacional (LDB) com a finalidade precípua de preparar "para o exercício de profissões" têm expectativa de ingressar em breve em instituições e muito provavelmente farão uso ativo de TI. Diante da importância da educação para utilizar os meios digitais com segurança surgiu a questão norteadora: os alunos EPT da área de informática tem conhecimento necessário para utilizar o meio cibernético de forma segura?

2)Objetivos (caracterização da contribuição)

2.1 Objetivo geral

Propor um modelo de formação on-line, aberta e massiva capaz de aliar teoria e prática na temática da segurança da informação.

2.2 Objetivos específicos

Analisar a oferta de cursos (MOOCS) identificando as principais ferramentas, abordagens e metodologias empregadas;

Propor um modelo de formação on-line, aberta e massiva, capaz de aliar teoria e prática na temática da segurança da informação

Avaliar os resultados alcançados pelos discentes diante da formação proposta

3) Fundamentação teórica

3.1 Segurança da informação

A informação vem assumindo um caráter estratégico e tem sido considerado um ativo crítico para os mais diversos tipos de instituições. Lopes (2012) considera que a informação assumiu um valor fundamental para as organizações, que até pouco tempo atrás tinham o foco basicamente para os bens tangíveis e hoje em dia, enxergam a informação como principal ativo. Sendo assim, passou-se a dedicar especial atenção ao valor que a informação tem, de acordo com Sêmola (2014) fazendo bom uso da informação é possível subsidiar processos de tomada de decisão, melhorar a produtividade, otimizar tarefas, reduzir custos, obter vantagem competitiva e tratar continuidade de uma instituição.

O conceito de segurança da informação perpassa por critérios de gerenciamento que promovam confidencialidade, integridade e disponibilidade da informação. O crescente uso da tecnologia e a má utilização dela, tem gerado uma série de vulnerabilidades que podem ser exploradas, fato que coloca em risco os ativos de uma instituição. De acordo com Quintela e Branco (2013, p. 2), segurança da informação diz respeito a "proteção da informação contra ameaças que possam valer-se das vulnerabilidades dos ativos, preservando suas propriedades fundamentais: disponibilidade, integridade, confidencialidade e autenticidade".

A política de segurança da informação nos dos órgãos da Administração Pública Federal (APF) direta e indireta retrata um quadro preocupante (RIOS; TEIXEIRA FILHO; RIOS, 2017). De acordo com o Tribunal de Contas da União (TCU) apenas 64% dos órgãos pesquisados têm instituída uma Política de Segurança da Informação e Comunicação - POSIC (BRASIL, 2008). Em se tratando mais especificamente das instituições Federais de ensino superior (IFES) em 2016 foi realizada uma pesquisa com 98 IFES constatou-se que apenas 34 % possuem e utilizam de forma integral a POSIC, 51 % dos IFES sequer elaboraram uma política de segurança da informação para sua comunidade acadêmica (BRASIL, 2016).

3.2 MOOC (curso online aberto e massivo)

As possibilidades de educação a distância (EAD) estão evoluindo e se diversificando, dentre outros fatores, devido a popularização do acesso à internet e a disseminação de

ferramentas de tecnologia da informação e comunicação (TIC's) no cotidiano das pessoas. Uma inovação que tem se mostrado promissora é a do MOOC (Curso Online Aberto e Massivo) que surgiu de uma iniciativa de George Siemens quando ministrou o curso Connectivism and Connective Knowledge, na Universidade de Manitoba, no Canadá, para 25 alunos em regime presencial, também o fez para outros 2.300 alunos online (SOUZA; CYPRIANO, 2016).

Estratégias EAD visam romper as barreiras espaciais e temporais entre professor e aluno, com a influência das redes sociais e dos ambientes virtuais de aprendizagem (AVA). Com isso, o MOOC tem ganhado espaço no mundo todo e passou a ofertar ensino a distância por meio da web. Porém, com o diferencial de atender a um número exponencial de pessoas, independente de composição formal em turmas. Além disso, o MOOC possibilita acesso a mídias interativas e digitais com vídeos, animações, textos, imagens utilizando para tal, a multimídia e a internet (SILVA, 2017)

Acerca das questões didático pedagógicas envolvidas num curso MOOC, que sofre inúmeras influências diretas como: da internet, multimídia, conectivismo e da interatividade, de acordo com Riedo et al. (2014) esses, demandam uma postura pedagógica em que o aluno se torne um participante ativo ao praticar ações mais refletidas na construção do seu conhecimento. Discorrendo sobre essas questões Andrade e Silveira (2016) também reforçam que a metodologia dos MOOC's é baseada na interação, tanto entre professores e alunos quanto entre os próprios alunos. A aplicação de recursos audiovisuais e exercícios de fixação é comum, a variedade dos contextos culturais deve ser observada, além disso, O emprego de pré e pós testes, uso de ferramentas síncronas e assíncronas e utilização das redes sociais são aconselhados (BASTOS; BAGIOTTI, 2014).

4) METODOLOGIA

A metodologia definida neste trabalho irá considerar inicialmente uma Revisão Sistemática da Literatura (RSL), proposto por Kitchenham e Charters (2007) com a finalidade de investigar os estudos primários que abordam a aplicação dos MOOCS. Optou-se também, pela pesquisa ação na fase de elaboração do modelo de formação, além

de uma abordagem caráter exploratório e descritivo adotada com os sujeitos que participarem da formação produto dessa pesquisa.

A investigação das problemáticas envolvidas, a definição da abordagem usada no curso, sua elaboração, carga horária, conteúdos entre outras questões não serão definidas somente pelo pesquisador. Sendo assim, será utilizada uma abordagem de pesquisa-ação que segundo Tripp (2005) é participativa na medida em que incluem os que, de um modo ou outro, estão envolvidos nela e é colaborativa em seu modo de trabalhar. Franco (2005) Corrobora com a opinião de Tripp quando afirma que a pesquisa-ação deve ser essencialmente uma pesquisa intencionada à transformação participativa, em que sujeitos e pesquisadores interagem na produção de novos conhecimentos.

Na fase de elaboração da proposta de formação as contribuições dos envolvidos serão captadas por meio de entrevistas não estruturadas com grupo focal, serão desenvolvidos protótipos do MOOC em Segurança da informação, para serem discutidas e assim definidas nas reuniões com os participantes da pesquisa ação. Após a elaboração do modelo de formação, os alunos que aceitarem participar do curso on-line aberto e massivo inicialmente, serão submetidos a dois questionários online O primeiro questionário irá analisar o perfil dos participantes e o segundo funcionará como um pré-teste, também serão utilizadas para efeito da coleta de dados a participação do aluno no curso, os resultados dos fóruns propostos e o desempenho do estudante.

5) ESTADO ATUAL DO TRABALHO

O presente trabalho, seguindo a trilha metodológica proposta realiza uma construção inicial de protótipos e uma revisão sistemática da literatura e tem entre outros objetivos, realizar o levantamento das principais estratégias de ensino que vem sendo empregadas nos Cursos MOOC e na área da segurança da informação. Especialmente, busca identificar as estratégias de ensino que têm auferido êxito. Sendo assim, espera-se com essa RSL além de se construir uma base teórica sobre os temas, definir as melhores estratégias, recursos, técnicas e ferramentas para serem utilizadas na elaboração do MOOC proposto nesse trabalho.

6) DESENVOLVIMENTO NECESSÁRIO PARA A CONCLUSÃO

As próximas etapas do trabalho incluem a elaboração dos questionários que serão aplicados nos alunos, análise dos dados, a definição dos conteúdos, abordagens e testes que serão utilizadas. Assim, será feita qualificação do projeto, elaboração do curso, em formato online e aberto, para que então possa ser realizada a redação da dissertação.

7) AVALIAÇÃO DOS RESULTADOS

O protótipo exibido na Figura 1 propõe que cada módulo do curso MOOC contenha quatro sessões. O botão conteúdo em pdf daria ao usuário possibilidade de download do material de estudo com abordagem detalhada do assunto. O botão Navegação interativa apresentará os principais pontos do conteúdo de forma dinâmica, incluindo imagens ilustrativas, quadros comparativos, slides e banners. O conteúdo em vídeo será outra abordagem que irá compor a formação, além do estudo de caso que irá propor uma situação prática para o usuário solucionar. O tópico fórum de discussões será uma oportunidade para os alunos e o monitor trocarem experiências e opiniões sobre o conteúdo abordado.

Figura 1. Sessões de um módulo

8) REFERENCIAS BIBLIOGRÁFICAS

ABNT- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 – **Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, ABNT, 2013.

ANDRADE, M. V. M.; SILVEIRA, I. F. **Panorama da Aplicação de Massive Open Online Course (MOOC) no Ensino Superior**: Desafios e Possibilidades. EaD em FOCO, 6(3), 2016. Disponível em: <http://eademfoco.cecierj.edu.br/index.php/Revista/article/view/392>. Acesso em: 17 Ago. 2018.

BASTOS, R. C.; BIAGIOTTI, B. **MOOCs**: uma alternativa para a democratização do ensino. RENOTE. Revista Novas Tecnologias na Educação, v. 12, p. 1-9, 2014. Disponível em: <http://seer.ufrgs.br/index.php/renote/article/view/50333>. Acesso em: 17 Ago. 2018.

BRASIL. **Demanda TCU nº 265-54** [mensagem pessoal]. Mensagem recebida por no-replay@tcu.gov.br em 30 maio 2016.

BRASIL. Tribunal de Contas da União. **Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal**. Brasília: TCU, Secretaria de Fiscalização e Tecnologia da Informação. Sumario executivo, 2008. 48 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2515176.PDF>. Acesso em: 16 Ago. 2018.

BRASIL, Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. **Educação Profissional e Tecnológica (EPT)**. 2018. Disponível em: <http://portal.mec.gov.br/component/content/article?id=65251:educacao-profissional-e-tecnologica-ept>. Acesso em: 17 nov. 2018.

FOINA, Paulo Rogério. ESTRATÉGIA E SEGURANÇA DE INFORMAÇÃO. In: LYRA, Mauricio Rocha (Org.). **Governança da Segurança da Informação.** Brasília: Edição do Autor, 2015. p. 1-7. Disponível em: <http://mauriciolyra.pro.br/site/wp-content/uploads/2016/02/Livro-Completo-v4-para-impress%C3%A3o-com-ISBN.pdf>. Acesso em: 17 Ago. 2018.

FRANCO, Maria Amélia Santoro. Pedagogia da Pesquisa-Ação. **Educação e Pesquisa**, São Paulo, p.483-502, dez. 2005.

WEF - World Economic Forum. **Risks Report**. 13. ed. Genebra, 2018. Disponível em: <https://www.weforum.org/reports/the-global-risks-report-2018 > Acesso em 05 out. 2018.

KITCHENHAM, B.A.; CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. Tech. Rep. EBSE-2007-01, Keele University, 2007.

LOPES, I. M. ***Adopção de políticas de segurança de sistemas de informação na administração pública local em Portugal***. 2012. 437 f. Tese (Doutorado em Engenharia e Gestão de Sistemas de Informação) - Universidade do Minho, Portugal, 2012. Disponível em: <https://bibliotecadigital.ipb.pt/bitstream/10198/7422/3/Tese_IL.pdf>. Acesso em: 17 Ago. 2018.

LYRA, Mauricio Rocha (Org.). **Governança da Segurança da Informação.** Brasília: Edição do Autor, 2015. p. 1-7. Disponível em: <http://mauriciolyra.pro.br/site/wp-content/uploads/2016/02/Livro-Completo-v4-para-impress%C3%A3o-com-ISBN.pdf>. Acesso em: 17 Ago. 2018.

PONTOBR (Brasil). **Estatísticas dos Incidentes Reportados ao CERT.br:** Total de Incidentes Reportados por ano. 2018. Núcleo de informação e Coordenação. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 14 nov. 2018.

RIEDO, C. R. F.; PEREIRA, E. M. de A.; WASSEM, J.; GARCIA, M. F. **O desenvolvimento de um MOOC (Massive Open Online Course) de Educação Geral voltado para a formação continuada de professores:** uma breve análise de aspectos tecnológicos, econômicos, sociais e pedagógicos. In: Simpósio Internacional de Educação a Distância e Encontro de Pesquisadores em Educação a Distância, 2014, São Carlos. Qualidade na Educação: convergências de sujeitos, conhecimentos, práticas e tecnologias. São Carlos: SIED:EnPED, 2014. v. 1. p. 1-12. Disponível em: <http://www.sied-enped2016.ead.ufscar.br/ojs/index.php/2014/article/view/782>. Acesso em: 17 Ago. 2018.

RIOS, Orlivaldo Kléber Lima; TEIXEIRA FILHO, José Gilson de Almeida; RIOS, Vânia Patrícia da Silva. **Gestão de segurança da informação:** práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação. Navus - Revista de Gestão e Tecnologia, [s.l.], p.49-65, 10 abr. 2017. Disponível em: <http://navus.sc.senac.br/index.php/navus/article/view/482>. Acesso em: 17 Ago. 2018.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Elsevier, 2014.

SOUZA, Rodrigo de; CYPRIANO, Elysandra Figueredo. **MOOC:** uma alternativa contemporânea para o ensino de astronomia. Ciência & Educação (bauru)**,** [s.l.], v. 22, n. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1516-73132016000100065>. Acesso em: 17 Ago. 2018.