ISSN: 2594-4827

ABORDAGENS DE ENSINO PARA SEGURANÇA DA INFORMAÇÃO: POSSIBILIDADES NOS CURSOS ONLINE ABERTOS E MASSIVOS

William da Silva Melo[1]

Francisco Kelsen de Oliveira[2]

Recebido em: janeiro/2020
Publicado em: abril/2020

Resumo

Este estudo foi voltado para utilização de abordagens de ensino para área da segurança da informação, considerando o contexto dos cursos on-line abertos e massivos. Para isso utilizou-se a Revisão Sistemática da Literatura (RSL) que teve como objetivo identificar abordagens, ferramentas ou instrumentos aplicados no processo de ensino aprendizagem, que possam promover uma proposta de curso on-line e favoreça o elo intrínseco entre teoria e prática. A busca dos dados foi realizada no Portal Periódicos CAPES/MEC, através de combinações dos termos definidos no protocolo da revisão, para automatizar a condução da RSL a ferramenta stArt foi utilizada. As análises demonstram resultados positivos no desempenho dos aprendizes que utilizaram metodologias ativas e recursos da web se comparado com o ensino tradicional. Porém, ainda existem poucos estudos que trazem evidência para essa temática.

Palavras-chave: Curso on-line aberto e massivo; EAD; Segurança da informação.

[1] Instituto Federal Baiano. E-mail: williamdasilvamelo@gmail.com
[2] Instituto Federal SERTÃO-PE. E-mail: francisco.oliveira@ifsertao-pe.edu.br

ISSN: 2594-4827

TEACHING APPROACHES FOR INFORMATION SECURITY: POSSIBILITIES IN OPEN AND MASSIVE ONLINE COURSES

Abstract

This study focused on the use of teaching approaches for information security, considering the context of open and massive online courses. For this we used the Systematic Literature Review (RSL) that aimed to identify approaches, tools or instruments applied in the teaching-learning process, which can promote an online course proposal and favor the intrinsic link between theory and practice. The data search was performed in the CAPES / MEC Periodic Portal, through combinations of the terms defined in the review protocol, to automate the conduction of the RSL the stArt tool was used. The analyzes show positive results in the performance of learners who used active methodologies and web resources compared to traditional teaching. However, there are still few studies that bring evidence to this theme.

Keywords: Massive Open Online Course; EAD; Information security.

INTRODUÇÃO

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. 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.

Para se estabelecer um grau de importância para as informações é necessário avaliar o dano que a sua perda, ou o seu vazamento poderia provocar, não só em termos financeiros, mas também considerando a imagem, a reputação da instituição. De acordo com Foina (2015), uma informação terá maior probabilidade de ser atacada quanto maior o valor que ela tiver. Dantas (2011) acrescenta que a informação é um ativo

ISSN: 2594-4827

essencial que ocupa status de destaque logo, protegê-la tornou-se algo vital. Explica ainda que, no cenário da atualidade, a segurança da informação envolve muito mais do que ferramentas para a detecção de invasão e proteção antivírus, consiste num arcabouço de medidas voltadas para garantir a confidencialidade, disponibilidade, e integridade das informações e incluem prevenção, detecção, resposta, recuperação e continuidade de um negócio.

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 Quintella e Branco (2013, p. 2), segurança da informação diz respeito à "proteção da informação contra ameaças que possam valer-se das vulnerabilidades dos ativos, preservando suas propriedades fundamentais: disponibilidade, integridade, confidencialidade e autenticidade".

É possível observar que nos estudos relativos à 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 têm como público dos estudantes são quase inexistentes (LYRA, 2015). De acordo com Alves (2010), deve existir um plano de treinamento para alertar sobre segurança da informação que utilize estratégias como seminários e cursos de capacitação. Nesse sentido, a educação à distância (EAD) tem se destacado por oferecer flexibilidade de horários e menor custo se comparado ao ensino presencial. Segundo Nór (2018), entre 2011 a 2015 a modalidade EAD cresceu 51% nas instituições privadas, desde 1996 a lei de diretrizes bases da educação (LDB) em seu artigo 80 afirma que o poder público deve incentivar o desenvolvimento e a veiculação de programas de ensino a distância (BRASIL, 1996).

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 Tecnologias Digitais de Informação e Comunicação (TDIC's) no cotidiano das pessoas. O censo da educação superior realizada pelo

ISSN: 2594-4827

Ministério da Educação (MEC) no Brasil mostra que a educação a distância tem crescido vertiginosamente. Em 2007, a modalidade a distância representava 7,0% das matrículas de graduação já em 2017, a EaD aumentou 17,6% e já atende mais de 1,7 milhão de alunos, o que representa uma participação de 21,2% dos alunos de graduação no país. Nesse sentido, uma inovação que tem se mostrado promissora na EAD é o MOOC (Curso Online Aberto e Massivo) que surgiu de uma iniciativa de George Siemens Ministrando 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).

Características interessantes no formato dos MOOCs são: Acesso aberto a capacitação, participação assíncrona (podendo ser iniciada a qualquer momento pelo estudante), escalabilidade para quantidade de alunos e alcance abrangente de público. Ou seja, oferecem a possibilidade de atender um número exponencial de pessoas, independente de composição formal em turmas, possibilita acesso a mídias interativas e digitais com vídeos, animações, textos, imagens utilizando para tal, a multimídia e a internet (SILVA, 2017). A respeito desse formato de EAD, Forno e Knoll (2013) esclarecem que os MOOCS são diferentes dos cursos tradicionais EAD pois, eles podem ser acessados por qualquer pessoa conectada à internet, são em sua maioria gratuitos, não limitam quantidade de participantes por isso, são intitulados massivos.

PERCURSO METODOLÓGICO

Para Kitchenham e Charters (2007) a Revisão Sistemática da Literatura (RSL) adota um caminho metodológico bem definido, evidencia as contribuições relativas a um assunto ou fenômeno de forma imparcial e repetível analisando determinadas questões de pesquisa. Sendo assim, neste trabalho será elaborado um protocolo de RSL seguindo os modelos propostos por Kitchenham e Charters (2007) percorrendo as seguintes fases: planejamento, execução e resultados. Considerando as dificuldades na tabulação e sumarização dos trabalhos de forma manual foi utilizada a ferramenta StArt (State of the Art through Systematic Review) para automatizar a condução deste trabalho.

ISSN: 2594-4827

Planejamento

Nesta fase é elaborado o protocolo da RSL, onde são definidos os objetivos, as questões de pesquisa, strings de busca, critérios de inclusão e exclusão que serão utilizados. As questões de pesquisa estão definidas no quadro abaixo e seguem têm como objetivo identificar as estratégias de ensino que auferiram êxito nos cursos on-line abertos e massivos (MOOC) na área da segurança da informação. Nesse sentido, a primeira questão de pesquisa foi motivada por considerar a importância e representatividade dos MOOCs buscando-se identificar se os mesmos estão sendo utilizados na área da segurança da informação, a segunda questão de pesquisa gira em torno da efetividade dessa aplicação.

Quadro 1 – Questões de pesquisa

ID	Questões de Pesquisa
QP1	Quais são as abordagens, ferramentas ou instrumentos de ensino aprendizagem utilizadas nos MOOCS para área da segurança da informação?
QP2	Quais são as abordagens de ensino aprendizagem consideradas eficazes para os Curso on-line abertos e massivos na área da segurança da informação?

Fonte: Elaborado pelos autores.

A string utilizada na busca automatizada pelo portal de periódicos da capes foi elaborada considerando o objetivo e questões norteadoras. Os termos de busca demonstrados no quadro 2 foram combinados com os operadores *AND* e *OR* resultando na combinação de termos do quadro 3. Já o quadro 4 lista os critérios de inclusão e exclusão definidos.

Quadro 2 – Termos selecionados para busca

1ª Ordem	2º Ordem	3º Ordem
“Teaching strategy” “teaching method”	*"learning object"* *"Educational tool"* *"Case-based learning"*	*“Information security”* *“Data security”* *“Cyber security”*

ISSN: 2594-4827

	"Case-based instruction" *"case study"* *“theory and practice”*	*“Digital Security”* *“Security on the Internet”*

Fonte: Elaborado pelos autores.

Quadro 3 – Combinação dos termos de busca

("Teaching strategy" OR "teaching method") AND ("Educational tool" OR "learning object" OR “Case-based instruction" OR "case study" OR “theory and practice”) AND (“Information security” OR “Data security” OR “Cyber security” OR “Digital Security” OR “Security on the internet”)

Fonte: Elaborado pelos autores.

Quadro 4 – Critérios de Inclusão e exclusão

Critérios	ID	Descrição
Inclusão	CI1	Trabalhos que apliquem alguma estratégia ou abordagem de ensino na temática da segurança da informação utilizando MOOCs ou EAD.
	CI2	Artigos completos publicados em periódicos ou anais
	CI3	Textos escritos em Português, Espanhol ou Inglês
Exclusão	CE1	Artigos incompletos ou indisponíveis
	CE2	Trabalhos que não foram publicados em periódicos ou anais.
	CE3	Trabalhos que não apliquem alguma abordagem, estratégias ou instrumentos de ensino.
	CE4	Não aborda a área da segurança da informação, EAD ou MOOC

Fonte: Elaborado pelos autores.

ISSN: 2594-4827

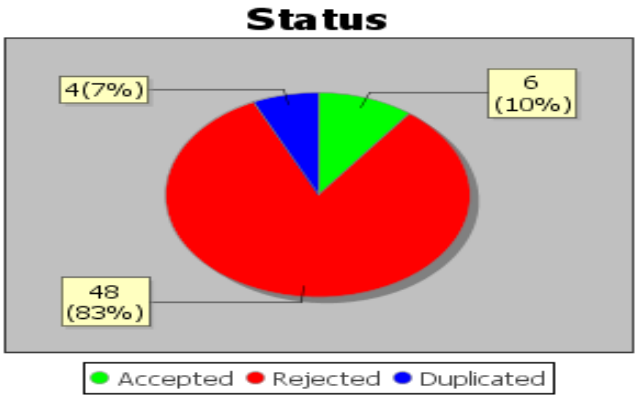
Execução

Após executar a combinação de strings de busca elaborada no protocolo da RSL e demonstrado no quadro 3, foram recuperadas 58 publicações científicas. Os dados foram exportados utilizando portal de periódicos da capes no formato BibTex e importados na ferramenta Start. Assim, foi feita a identificação dos artigos, para selecionar os mesmos foi realizada a leitura inicial do título, palavras chave e resumos de todos os artigos obtendo uma lista inicial. Posteriormente, essa lista foi refinada numa segunda leitura incluindo a introdução e conclusão dos trabalhos, na última etapa foi realizada a leitura completa dos estudos para extrair os dados que foram discutidos nos resultados.

RESULTADOS E DISCUSSÃO

Conforme podemos observar na figura 1, dos 58 artigos iniciais 4 foram identificados como registros duplicados, 48 rejeitados e 6 foram aceitos por satisfazerem os critérios de inclusão definidos no protocolo da RSL. Sendo assim, a lista inicial de trabalhos é descrita no quadro 5.

Figura 1: Resultado da seleção



Fonte: Extraída da Ferramenta StArt.

ISSN: 2594-4827

Quadro 5: Lista de artigos

ID	Título	Ano
1	*Studying and Constructing Concept Maps: a Meta-Analysis*	2018
2	*Supporting Case-based Learning in Information Security with Web-based Technology*	2013
3	*Teaching Cryptography Using Design Thinking Approach*	2016
4	*Beyond identifying privacy issues in e-learning settings -Implications for instructional designers*	2016
5	*Influences on ICT teachers knowledge and routines in a technical e-safety context*	2017
6	*A Framework for Teaching Security Design Analysis Using Case Studies and the Hybrid Flipped Classroom*	2019

Fonte: Elaborado pelos autores.

QP1

Com base na pesquisa realizada foi possível identificar a aplicação de metodologias ativas no ensino da segurança da informação tais como: Sala de aula híbrida invertida; Gamificação; Estudos de caso; Design Thinking (DT) bem como, utilização de recursos da Web (RSS, Wiki's, Tags, Nós, Tutoriais) e mapas conceituais.

As metodologias ativas encorajam o envolvimento do aluno uma vez que o desloca da posição de receptor passivo para o centro de processo de aprendizagem. Nesse sentido, o aluno não deve assumir o papel de mero receptor, não precisa ficar limitado aos recursos que são fornecidos pelo professor. Luburić et al. (2019) reconhecem a necessidade de compreensão cognitiva mais profunda dos assuntos relativos à segurança da informação tais como: Desenvolvimento de software seguro,

ISSN: 2594-4827

criptografia e infraestrutura de chave pública. Logo, eles propõem uma variante da sala de aula invertida, chamada de sala de aula híbrida invertida.

Park, Yu e Jo (2015) afirmam que o ensino híbrido combina atividades em sala de aula com atividades online, eles consideram ainda o fato de muitas instituições de ensino superior enxergarem o ensino híbrido como uma maneira de transformar a pedagogia tradicional. Com isso, na sala de aula híbrida invertida os alunos foram submetidos a materiais preparatórios contendo controles de segurança, ataques e vulnerabilidades, enquanto o exercício de laboratório é executado como uma discussão em grupo, na qual os alunos aplicam o conteúdo aprendido no curso incluindo situações onde são utilizados estudos de caso.

A aprendizagem baseada em casos para He, Yan e Yang (2013) pode ajudar os professores a trabalharem de maneira mais competente em situações relativas à segurança da informação também contribui para que os alunos aprendam de forma mais eficaz através de extensas análises, discussões e resoluções de problemas em várias situações.

A estratégia da gamificação para Luburić et al. (2019) ganhou força no ensino da segurança da informação, jogos de cartas como Shostack e Control-Alt-Hack são considerados recursos relevantes para trabalhar a conscientização sobre segurança cibernética, ameaças, ataques e contramedidas. Já o Design Thinking além de se mostrar estratégia de ensino que converte os alunos em investigadores do seu próprio mundo, pode ser considerado como um estilo de pensamento e aplicado nas mais diversas áreas.

De acordo com Alhamdani (2016) para utilizar Design Thinking no ensino de criptografia os alunos devem cumprir algumas etapas. Inicialmente, devem se envolver com a atividade para compreender o domínio do problema. Posteriormente, devem observar como as pessoas se comportam cooperam, passam por experiências como conversas com especialistas, visitas técnicas em oficinas, estúdios, podem usar diferentes fontes de informação como textos, vídeos, podcasts.

Na fase de definição do Design Thinking os alunos analisam as evidências coletadas anteriormente e se concentram em definir o problema. Com isso, passam para

ISSN: 2594-4827

fase de ideação, onde os alunos descobrem soluções para os problemas, criam um esboço ou modelo na fase de prototipação a fim de explicar melhor o produto até chegarem na momento do teste, que consiste num processo interativo de aprender o que funciona o que não funciona e depois adaptar seu protótipo com base no feedback (ALHAMDANI, 2016)

Os recursos da Web são utilizados no ensino no sentido de permitir ao aluno participação e colaboração, para Luburić et al. (2019) a web 2.0 tem um impacto positivo pois com ela, os instrutores e alunos compartilham suas próprias opiniões e experiências de aprendizado usando as mais diversas ferramentas como blogs, redes sociais, wiki's, tags, RSS. Outro instrumento identificado no ensino das mais diversas áreas do conhecimento, inclusive na área da segurança foram os mapas conceituais que consistem em diagramas de nó-link no qual cada nó representa um conceito e cada link identifica o relacionamento entre os dois conceitos que ele conecta (SCHROEDER et al., 2017).

Um modelo de aprendizagem que estimula somente memorização textual por exemplo, não tem o poder de relacionar os conhecimentos e conectá-los para compreender seus significados como os mapas conceituais propõem. De acordo com os estudos de Schroeder et al. (2017) Aprender com mapas conceituais foi considerado mais eficaz do que aprender através de palestras ou discussões, ou construindo ou estudando textos especialmente se os alunos elaboram o mapa conceitual. Afinal, para criar um mapa conceitual o aluno precisa conhecer os principais conceitos do assunto, além de utilizar sua capacidade de sintetizar, sumarizar e relacionar as ideias através de uma representação visual.

QP2

Interessante observar que várias das abordagens citadas comprovaram eficácia no processo de ensino aprendizagem na área da segurança da informação. O trabalho de Luburić et al. (2019), que utiliza sala de aula híbrida invertida e estudos de caso, comparou os resultados de duas turmas no curso de desenvolvimento de software seguro uma com a abordagem citada (turma 2) e outra utilizando abordagem tradicional (turma 1). Os resultados do comparativo entre as turmas mostram que a turma 2 obteve

ISSN: 2594-4827

uma melhoria significativa no que diz respeito a compreensão mais detalhada sobre as funcionalidades necessárias a um software seguro.

A comprovação da efetividade na aplicação dos mapas conceituais segundo Schroeder et al. (2017) ficou evidenciada diante do melhor desempenho obtido pelos alunos quando eles estudaram ou elaboraram mapas conceituais em detrimento dos resultados alcançados usando outras estratégias tais como: Discussões, palestras, esboços e textos. Para eles, quando um aluno elabora um mapa conceitual esse resultado ainda é melhor considerando o desempenho de um aluno que apenas estuda com esse mapa.

O trabalho de He, Yan e Yang (2013) que aplica biblioteca de estudos de caso e ferramentas da Web 2.0 como RSS, wiki's, tags, nós e tutoriais valida seus resultados por meio de entrevistas com os alunos. Já a utilização do Design Thinking demonstra que os alunos que usam DT conseguem resolver questões mais complexas do que os alunos que aprendem da forma tradicional (ALHAMDANI, 2016).

CONSIDERAÇÕES FINAIS

Diante do estudo realizado pode-se perceber que existem poucos artigos que trazem evidência para a temática: Segurança da informação no contexto da EAD, nenhum deles relatou experiências em cursos on-line abertos e massivos. Os resultados encontrados indicam que a metodologia tradicional de ensino não foi utilizada possivelmente, por não promover uma aprendizagem prática. Afinal, essa área do conhecimento demanda que os alunos dominem os conceitos e suas aplicações logo, a maioria dos estudos utilizaram em sua abordagem metodologias ativas de ensino aprendizagem, com práticas em laboratórios, estudos de casos, elaboração de mapas conceituais, gamificação, Design Thinking ou recursos da web que promovam uma maior autonomia e proficiência no estudante. Nesse sentido, diante dos resultados positivos evidenciados na pesquisa compreendemos que as metodologias ativas e os recursos da web são possibilidades muito efetivas para aplicação nos cursos online abertos e massivos. Por outro lado, ficou evidenciado que nenhum trabalho apresentou

ISSN: 2594-4827

relação com a Educação Profissional e Tecnológica (EPT) tão pouco abordou a formação que aliasse teoria e prática nos cursos on-line abertos e massivos.

REFERÊNCIAS

ALHAMDANI, Wasim A.. Teaching Cryptography Using Design Thinking Approach. **Journal Of Applied Security Research**, [s.l.], v. 11, n. 1, p.78-89, 2 jan. 2016. Informa UK Limited. Disponível em: <http://dx.doi.org/10.1080/19361610.2015.1069646> Acesso em: 21 Ago. 2019.

ALVES, Cássio B. **Segurança da Informação vs. Engenharia Social:** Como se proteger para não ser mais uma vítima, 2010. Disponível em: < https://s3.us-east-2.amazonaws.com/administradores-website/_assets/modules/academicos/academico_3641.pdf > Acesso em: 21 Ago. 2019.

BRASIL. Ministério de Educação. **LDB - Lei nº 9394/96**, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da Educação Nacional. Brasília: MEC, 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9394.htm> Acesso em: 24 Ago. 2019.

DANTAS, Marcus Leal. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

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: 21 Ago. 2019.

FORNO, J. P.; KNOLL, G. F. **Os MOOCS no mundo**: um levantamento de cursos online abertos massivos. Nuances: estudos sobre Educação, Presidente Prudente,SP, v. 24, n. 3, p. 178-194, set./dez., 2013. Disponível em: <http://reaparana.com.br/portal/wp-content/uploads/2014/10/Os-MOOCs-no-mundo-2013.pdf >. Acesso em: 21 Ago. 2019.

HE, Wu; YUAN, Xiaohong; YANG, Li. **Supporting Case-based Learning in Information Security with Web-based Technology**. [s.l.]. 2013. Disponível em: <https://pdfs.semanticscholar.org/f8ab/e022d666a7289e139fe5c2585f6697ba275f.pdf > Acesso em: 21 Ago. 2019.

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.

ISSN: 2594-4827

Disponível em: <https://bibliotecadigital.ipb.pt/bitstream/10198/7422/3/Tese_IL.pdf>. Acesso em: 21 Ago. 2019.

LUBURIć, Nikola et al. A Framework for Teaching Security Design Analysis Using Case Studies and the Hybrid Flipped Classroom. **Acm Transactions On Computing Education**, [s.l.], v. 19, n. 3, p.1-19, 16 jan. 2019. Association for Computing Machinery (ACM). Disponível em: <http://dx.doi.org/10.1145/3289238> Acesso em: 21 Ago. 2019.

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

NÓR, Bárbara. **Cursos EAD estão crescendo no Brasil**. Revista Exame. Sl. 01 fev. 2018. Disponível em: <https://exame.abril.com.br/carreira/cursos-ead-estao-crescendo-no-brasil/>. Acesso em: 05 Ago. 2019.

PARK, Y.; YU, J. H.; JO, I. Clustering blended learning courses by online behavior data: A case study in a Korean higher education institute. **The Internet And Higher Education**, [s.l.], v. 29, p.1-11, abr. 2016. Elsevier BV. Disponível em:< http://dx.doi.org/10.1016/j.iheduc.2015.11.001>. Acesso em: 21 Ago. 2019.

QUINTELLA, Heitor Luiz Murat de Meirelles; BRANCO, Marcelo Pereira de Oliveira. **Fatores Criticos de Sucesso em Seguranca da Informacao em Um Orgao da Administracao Publica Federal.** In: SIMPOSIO NACIONAL DE INOVACAO E SUSTENTABILIDADE (SINGEP), 2., 2013, São Paulo. Anais do II SINGEP e I S2IS. Sao Paulo: Uninove, 2013. p. 1-16. Disponível em:<http://repositorio.uninove.br/xmlui/handle/123456789/494>. Acesso em: 21 Ago. 2019.

SILVA, Henrique Salustiano. **Revisão sistemática sobre uso de moocs no brasil.** 2017. 19 f. Tese (Doutorado) - Curso de Ti, Ufsm, Constantina, 2017. Disponível em: <https://repositorio.ufsm.br/handle/1/12046>. Acesso em: 17 Ago. 2018.

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: 21 Ago. 2019.

SCHROEDER, Noah L. et al. Studying and Constructing Concept Maps: a Meta-Analysis. **Educational Psychology Review**, [s.l.], v. 30, n. 2, p.431-455, 21 mar. 2017. Springer Nature. Disponível em: <http://dx.doi.org/10.1007/s10648-017-9403-9>. Acesso em: 21 Ago. 2019.

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